2025 International Conference on Computational, Communication and Information Technology (ICCCIT) | 979-8-3315-1296-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICCCIT62592.2025.10927856

Comprehensive Survey of Post-Quantum Secure Lattice-Based Authentication Schemes for VANETs

Dheerendra Mishra,Γ *Senior Member, IEEE*
Department of Mathematics,
Bioinformatics and Computer Applications
Maulana Azad National Institute of Technology,
Bhopal 462003, India
dheerendra@manit.ac.in

Manish Nagar Γ
Department of Mathematics,
Bioinformatics and Computer Applications
Maulana Azad National Institute of Technology
Bhopal 462003, India
2330401002@stu.manit.ac.in

***Abstract*—Intelligent Transportation Systems (ITS) rely heavily on Vehicular Ad Hoc Networks (VANETs) to enable secure and reliable communication between vehicles and roadside infrastructure. However, Shor's algorithm poses a significant threat to conventional cryptographic systems. To counteract this threat, post-quantum cryptography offers quantum-resistant solutions capable of providing secure authentication in the face of quantum adversaries. This paper presents a comprehensive survey of recently proposed six post-quantum state-of-the-art authentication protocols designed to meet the security and performance demands of VANETs. The survey identifies key strengths and limitations in existing approaches, providing valuable insights to guide future research in designing robust, efficient, and quantum-resistant authentication mechanisms for next-generation vehicular networks.**

***Index Terms*—Vehicular ad hoc Network; Autonomous Vehicle; Secure communication; Quantum-Resistant Schemes; Lattice-based cryptography.**

I. Introduction

Transportation systems are a cornerstone of modern society, directly influencing economic growth, urban development, and individuals' quality of life. The rapid expansion of the automobile industry, as evidenced by the millions of vehicles added to roads annually, has brought significant benefits and raised critical challenges, particularly in road safety and traffic management. Vehicular Ad Hoc Networks (VANETs) have emerged as a promising framework to address these challenges, enabling intelligent transportation systems that enhance safety, streamline traffic management, and facilitate autonomous driving. VANETs leverage real-time communication between vehicles and infrastructure to share vital information, such as traffic conditions, road hazards, and vehicle positions. Functionally, VANETs are a specialized form of mobile ad hoc networks (MANETs) characterized by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. These networks consist of vehicles equipped with onboard units (OBUs), roadside units (RSUs) deployed along roadways, and a Trusted Authority (TA) responsible for centralized oversight.

The VANET system operates over a wireless medium, relying on an open network where nodes communicate through shared channels. While this connectivity is essential for enabling seamless communication between vehicles and infrastructure, it also makes the system inherently vulnerable to security threats. A determined adversary could exploit these open channels to infiltrate the network, communicate with legitimate parties, and potentially compromise the entire system. This susceptibility exposes VANETs to various attacks, potentially leading to malicious incidents with far-reaching consequences.

Robust mechanisms for ensuring authentication and data integrity are imperative to address these risks. Authentication is essential to verify that information exchanged between parties originates from authorized entities. Without this safeguard, adversaries could impersonate legitimate users, manipulate data, or inject false information into the system. Equally critical is the need to protect user privacy. In a VANET environment, vehicles frequently broadcast their identities and locations to facilitate communication with other vehicles and RSUs. However, if this information is not adequately encrypted or anonymized, it becomes susceptible to interception and misuse. Two primary challenges arise from these vulnerabilities. First, malicious actors could track a vehicle's movements, analyzing its daily routine to breach the driver's privacy. Second, such unauthorized access to vehicle data could enable illegal activities, such as stalking, theft, or orchestrating traffic disruptions. Addressing these concerns necessitates designing a security framework that ensures both the authenticity of transmitted information and the confidentiality of sensitive user data. By balancing these priorities, VANETs can mitigate threats and foster trust in intelligent transportation systems.

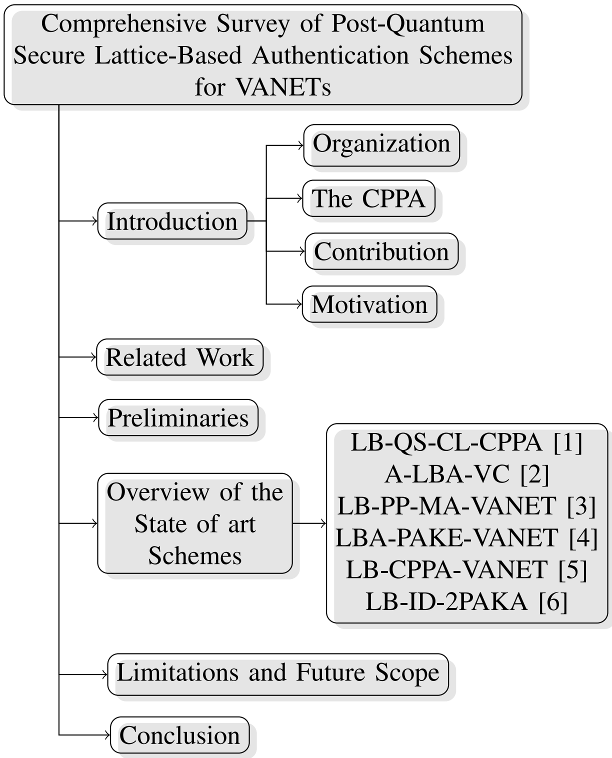
A distinguishing feature of VANETs is their dynamic topology, which is driven by the constant mobility of vehicles. This characteristic introduces significant challenges in maintaining secure communication and ensuring user privacy. Among the core security requirements, authentication stands out as a fundamental pillar. It ensures that only legitimate entities participate in the network, safeguarding against impersonation attacks and unauthorized communications. With its post-quantum security guarantees, Lattice-based cryptography has recently garnered attention as a viable solution for VANET authentication schemes. Its resistance to attacks by quantum computers makes it a compelling candidate for future-proofing

979-8-3315-1296-5/25/$31.00 ©2025 IEEE
DOI 10.1109/ICCCIT.2025.130

VANET security systems.

VANETs require Conditional Privacy-Preserving Authentication (CPPA) schemes to address security and privacy challenges effectively. These methods ensure that a vehicle's true identity remains hidden from unauthorized entities, maintaining user anonymity. However, in situations requiring accountability, the Trusted Authority (TA) can reveal the vehicle's identity when necessary. CPPA achieves a critical balance between safeguarding user privacy and ensuring network security by enabling anonymous authentication. It verifies message senders' legitimacy without disclosing their identities, thereby protecting sensitive information while preventing unauthorized access or malicious activity. This dual functionality strengthens trust within the VANET environment, ensuring the network operates securely while respecting the privacy of its users.

A. Organization



B. The CPPA

The CPPA schemes have the following characteristics:
Privacy-preserving authentication Each vehicle user and RSU in the VANET system possesses a unique identity. Verifying the sender's legitimacy is essential when transmitting messages to other users or RSUs. The user's identity must remain confidential and accessible only to the Trusted Authority (TA), which has exclusive rights to reveal the user's identity if necessary.
Integrity of the message Ensuring message integrity during transmission is crucial to prevent unauthorized modifications. The recipient must verify the message's integrity by checking its computational authenticity to detect any alterations from the original content sent by the originating party.
Unlinkability When user A sends two messages in the VANET system at different times, an adversary cannot identify both the messages sent by user A and cannot link the message.
Traceability The trusted authority can trace the identity of the user in the VANET system, if needed, from the user pseudo-identity.

In the context of the authentication and the privacy of the vehicle user, several CPPA systems have been proposed over the years. The hardness assumption of the existing CPPA system is based on the conventional non-quantum safe conventional mathematical hard problem, viz., the Diffe-Hellman and Elliptic Curve Diffie Hellman (ECDH) problems. The main concern with these schemes is that they are unsafe on quantum computers. To counter the threats accruing from quantum computing on the VANET system, various authentication schemes have been proposed recently based on the lattice hard problems. Despite these initiatives, current schemes continue to suffer vulnerabilities to numerous types of attacks, including replay, impersonation, and man-in-the-middle attacks, which threaten the network's security and reliability. In addition, many of these schemes have efficiency issues, especially in contexts with limited resources where latency and processing overhead are important considerations. To overcome these problems, a balance between strong security protocols and performance enhancements must be made, opening up opportunities for further research into more effective, safe, and quantum-resistant authentication schemes.

C. Contribution

The contribution of the paper is as follows:

1) This paper presents a comprehensive survey of recently proposed post-quantum secure lattice-based authentication schemes for VANETs, emphasizing the underlying lattice hardness assumptions, such as the Short Integer Solution (SIS), Learning with Errors (LWE), and Ring Learning with Errors (RLWE) problems.
2) The paper critically analyzes the advantages and limitations of these lattice-based authentication schemes, focusing on their effectiveness in preserving privacy and ensuring security within the complex and dynamic VANET environment.
3) Additionally, the paper outlines future research directions, suggesting improvements in efficiency and security by transitioning from the RLWE hardness assumption to the Module Learning with Errors (MLWE) problem, which offers enhanced scalability and performance.

D. Motivation

Quantum computing can perform complex computations at unprecedented speeds, posing a significant threat to traditional cryptographic systems. Algorithms such as Shor's algorithm [7] can efficiently solve mathematical problems, such as integer factorization and discrete logarithms, which underpin the security of widely used cryptosystems like RSA and ECC. As quantum computers advance, these cryptosystems become increasingly vulnerable, necessitating the adoption of quantum-resistant solutions.

One promising approach is lattice-based cryptography, which relies on lattice computationally hard problems, such as the Short Integer Solution (SIS), Learning with Errors (LWE), and their variants. These problems are believed to resist quantum attacks, making lattice-based cryptosystems a robust alternative for securing digital communications. This quantum threat extends to VANETs, where secure communication is vital for operating autonomous vehicles. Lattice-based cryptography has the potential to address these challenges, providing a quantum-safe foundation for VANET authentication schemes. This realization motivates us to explore and analyze the latest advancements in lattice-based authentication schemes tailored for VANETs.

II. Related Work

In recent years, various surveys have reviewed advancements in VANET security, particularly with a focus on post-quantum cryptographic techniques. To highlight the landscape of lattice-based schemes for VANET, we analyze relevant surveys published recently, addressing significant advancements and continuing challenges. Here, we summarize each of these works, which are referenced as [8]–[12].

Table I provides a detailed analysis of the previously published survey on VANET authentication schemes. The survey [8]–[12] covered almost all schemes published up to 2023. In Table I, we discuss the focus area of the survey papers, the key contribution of the survey, the challenges identified by the authors in their survey paper, and the proposed future direction based on the identified problems.

III. Preliminaries

A. *Hardness Assumptions*

SIS [13]: Let a uniformly random matrix $A \in \mathbb{Z}_y^{s\times r}$, the SIS problem is to find a nonzero vector $w \in \mathbb{Z}^r$, such that $Aw = 0 \mod q$ and $\|w\|_2 \leq \delta$, where $\delta \in \mathbb{R}$

Example: Suppose the parameters for SIS problem are: $y = 7$ (modulus), $r = 3$ (dimension of the vector), $s = 2$ (dimension of the matrix), $\delta = 2$ (norm).

Let a generated matrix $A = \begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 5 \end{pmatrix}$. Now we have to find a non-zero vector $z = (z_1, z_2, z_3)$ such that: $Aw \equiv 0 \mod 7$ and $\|w\|_2 \leq 2$.

We have to calculate Az by these two equations: $2w_1 + 4w_2 + 1w_3 \equiv 0 \mod 7$ and $w_1 + 3w_2 + 5w_3 \equiv 0 \mod 7$. We can test wether w_1, w_2, w_3 satisfy the condition $\|w\|_2 \leq 2$ is a solution. Let's consider

$w = (0, 1, 1)$, the norm of the solution is $\|w\|_2 = \sqrt{0^2 + 1^2 + 1^2} = \sqrt{3} \leq 2$ (satisfy).

Check the equations:

$$\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0+4+1 \\ 1+3+5 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$

$(5 \mod 7 = 5$ and $9 \mod 7 = 2)$
Therefore $w = (0, 1, 1)$ is not a solution.

LWE [14]: We define a system of equations as $Ax = B$, where A is the coefficient matrix of order $s \times r$ whose entries belong to $\mathbb{Z}_y$, i.e., $A \in \mathbb{Z}_y^{s\times r}$, x is the column matrix of order $r \times 1$, and $x \in \mathbb{Z}_y^s$, and $b \in \mathbb{Z}_y^s$. Then we can find x by the Gaussian Elimination method, but if we add an error vector $e \in \mathbb{Z}_y^s$ in the given system, then the system looks like as $A \cdot x + e = b$. The LWE problem is to find the value of s without knowing the error vector.

R-LWE [15]: Ring Learning with Error defines over Ideal Lattice. The algebraic structure $\frac{\mathbb{Z}_y[x]}{(x^n+1)}$ (where y is an integer and n is a power of two) contains all integer irreducible polynomials modulo $x^n + 1$ over $\mathbb{Z}_y[x]$ of degree less than or equal to $n - 1$, is a polynomial ring. Chosen $A \in \frac{\mathbb{Z}_y[x]}{(x^n+1)}$ uniformly random and $s \in \frac{\mathbb{Z}_y[x]}{(x^n+1)}$, $e \in \frac{\mathbb{Z}_y[x]}{(x^n+1)}$ from error distribution. Calculating the value of b from $As + e = b$, then from (A, b) to find the value of s is the Ring Learning with Error problem.

IV. Overview of the State of Art Schemes

Several lattice-based authentication protocols have been presented over the years, each addressing a distinct aspect of vehicular ad hoc network (VANET) security. In this paper, we explore some of the most recent advancements in lattice-based authentication protocols developed specifically for VANET applications. By leveraging lattice-based cryptography resistance to quantum attacks, these schemes aim to improve security, which is crucial for future-proofing VANET communications. In this section, we discuss the recently proposed six [1]–[6] lattice-based authentication schemes for VANET that are not covered by the existing survey papers with their security aspect, limitations, and future direction. Table II mentions the hard problems of the respective schemes, and Table III provides the gap analysis of the proposed schemes in terms of different security aspects. The indication of the right tick in Comparison Table III mentions that the particular schemes resist the security attributes, and the cross icon indicates that the specific scheme is vulnerable to the security attributes. The dash icon indicates gaps in the particular schemes; the author does not provide complete proof of the schemes to resist the security attributes.

A. *LB-QS-CL-CPPA [1]*

The LB-QS-CL-CPPA stand for Quantum Secure Certificate Less Conditional Privacy-preserving authentication for VANET was proposed by Verma et al. to address the master secret key and key-escrow problem. The scheme is based on the SIS lattice hard problem. The authors claim that their scheme is secure against (Modification attack, Impersonation attack, and replay attack) but there is no proof for Man-in-the-middle attack, Perfect Forward Secrecy which claims that the scheme is secure against these attacks. The scheme follows the security aspect, such as (Anonymity-Integrity-Authentication-Traceability), but does not follow the mutual authentication. The author compares their scheme with the previous proposed

TABLE I: Comparison of Survey Papers on Lattice-Based Authentication for VANET

Survey Paper	Number of Schemes Discussed	Year	Focus Area	Key Contributions	Challenges Identified	Future Directions Suggested
[8]	19 authentication schemes	2021	Relevant authentication schemes for VANET structure	How to construct authentication schemes with affordable expenses, low communication overhead, and restricted computing overhead through the use of modern technologies like 5G, 5G-SDN, and Blockchain.	privacy of vehicle on charging station, Management issue for TA	focus to use hybrid schemes such as SDN-Blockchain, along with traditional cryptography scheme
[9]	Covered relevant schemes and dividend into four parts	2021	privacy-preserving authentication schemes	categorized authentication and privacy schemes into four main types, each having its security criteria, security mechanisms, strengths, weaknesses, defences against attacks, and performance indicators	key management and distributing issues, security issues	focus on key management distribution, constructing lightweight authentication schemes
[10]	Covered relevant authentication schemes	2021	privacy-preserving authentication schemes	present a thorough analysis of authentication schemes, including their classifications, advantages, and limitations.	The main limitations of current cryptographic mechanisms are a lot of memory demands for revocation lists and certificates	Focus on constructing lightweight and efficient privacy-preserving authentication schemes
[11]	Covered relevant schemes published between 2013-21	2022	VANET communication techniques and their improvements	complete taxonomy of VANET techniques, classification of VANET services, detailed discussion, provide challenges related to VANET	Classified challenges as VANET Applications Challenges, Data Networking Challenge and Resource Management Challenge	More research is required to determine how vehicle movement affects edge computing node performance.
[12]	five types Classifications of different schemes	2023	Certificate-Less authentication schemes	Complete classification and comparison of all schemes with different attributes	Need to reduce the computation and the communication overhead	Recommended designing lightweight certificate-less authentication or aggregation schemes in the future

state-of-the-art scheme and claims that it is more computationally efficient than the previous proposed schemes. The scheme has some serious problems, such as the scheme required to establish secure channels to transmit the information between the nodes in the system, and the scheme is also under the area of threat generated by quantum computing. Another aspect that can be improved is the efficiency of any scheme. The same problem may happen with this scheme. We can reduce the computational cost of this scheme by switching the hardness problem to the MLWE problem. Since there is no security compromise to using the MLWE problem instead of the initial lattice hard problems $\{$LWE, SIS, RLWE$\}$. Therefore by using the MLWE problem, one can construct an efficient and secure authentication scheme for the VANET system.

B. A-LBA-VC [2]

The A-LBA-VC scheme stands for Anonymous lattice-based authentication protocol for vehicular communications. The mathematical foundation of this scheme is based on the lattice hard problem SIS. In this scheme, the authors used the Canetti and Krawczyk (CK) adversary model to assess the security of the authentication protocol. This scheme provides enhanced safety features, including anonymity and unlinkability. The scheme increases security, tampering resistance, and key revocation efficiency over large networks by keeping public keys on a distributed ledger. In addition, it offers improved safety and flexibility by providing a multi-domain authentication system for vehicular communication. Both official and unofficial approaches assess the protocol's security, showing its resistance to frequent attacks. Additionally, a performance study shows that the proposed protocol performs better than the present ones, making it a good fit for vehicular communication applications.

C. LB-PP-MA-VANET [3]

The LB-PP-MA-VANET stands for Lattice-based Privacy-preserving mutual authentication scheme for VANET proposed by Nath et al. The scheme proposed an encryption algorithm based on the traditional LWE lattice problem. The scheme consists of four parts: System Initialization, Authentication, Message Exchange (in both V2V and V2I contexts), and Batch Authentication. In the system initialization phase. This scheme makes effective vehicle communication possible, eliminating the need for continuous TA interaction during message transfers. Unlike many other authentication schemes, this approach does not require vehicles to produce parameters for secure message exchange. This facilitates fast message exchanges between vehicles in VANET. Tables II and III give the scheme's hardness, security attributes, and characteristics.

D. LBA-PAKE-VANET [4]

The LBA-PAKE-VANET stands for Lattice-based anonymous password-based authentication key exchange scheme for VANET is proposed by Ahmad and Jagatheswari which based on the RLWE problem. It is based on the Ding error reconciliation method [16], which includes the mod_2 and characteristic functions. The scheme used the QROM model as the formal security proof. Their security analysis claims that the scheme is secure against attacking methods, including {Authentication, Man-in-the-middle attacks, Perfect Forward Secrecy(PFS), user anonymity, and quantum attacks}. They compare their schemes with five different schemes on the mentioned attacking methods and claim that the scheme is secure on these attacking methods. They also claim by the computational analysis that their scheme is more computationally efficient. However, the computational cost on the user side of the scheme is greater than the compared schemes due to the sampling operations and hash functions. We can reduce the computational cost in the future after managing the tradeoff between security and efficiency by using less number of sampling and hash functions. To check the authenticity and timeline of the message during the key exchange communication between vehicles and other VANET Components such as {RSU, Vehicle}, the freshness check concept plays an important role. Freshness is guaranteed by {timestamps, nonces (unique random values for each session), or sequence numbers}. The concept of freshness check avoids replay attacks. The scheme claims that it is secure against replay attacks; however, there is no mechanism for freshness checks in the scheme. Therefore, there are various loopholes related to efficiency and security in the scheme. So, there is a scope to construct secure and efficient authentication schemes relying on the hardness of RLWE and more efficient MLWE problems.

E. LB-CPPA-VANET [5]

The LB-CPPA-VANET stands for the Lattice-Based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network proposed by Li et al. It is based on the SIS problem's hardness assumption, and the scheme's security is tested by the Random Oracle Model(ROM). In this scheme, the authors compare the scheme with previously proposed schemes and claim that their scheme is more efficient than previously proposed authentication schemes for the VANET system.

The author claims that the scheme is secure against {Man-in-the-middle attack, Impersonation attack, Replay attack, Modification attack, Stolen verifier table attack, Quantum attacks}. Does the scheme follow mutual authentication? There is no proof related to mutual authentication in the scheme. The efficiency of the scheme can be reduced by changing the dimensions of the scheme. Since the scheme is based on SIS problems, there is a change to construct the same structural-based authentication scheme relying on the hardness of MLWE.

F. LB-ID-2PAKA [6]

The LB-ID-2PAKA stands for Lattice and Identity-based two-party authenticated key exchange scheme for Vehicular communication. This scheme is based on the variants of the SIS lattice hard problems. The security aspect of the scheme is tested by the ROM by proofing its semantic security. The authors claim that their scheme is computationally efficient because they use only the addition and multiplication operation of matrices and vectors in the entire communication process. They also claim that their scheme is secure against {Man-in-the-Middle attack, Unknown key-share attack, Known-key security attack, Perfect Forward Secrecy, No key control (NKC)}. The scheme does not provide proof of a Replay attack or Denial of Service, Impersonation, or Modification attacks.

TABLE II: Lattice-based Schemes for VANET

Year	Authors	Hardness
2024	Verma et al. [1]	SIS/ISIS
	Shahidinejad et al [2]	SIS
	Nath et al. [3]	LWE
2023	LBA-PAKE [4]	RLWE
2022	Li et al. [5]	SIS
	Gupta et al. [6]	SIS

TABLE III: Gap Analysis of the Schemes

Security Atributes	**[1]**	**[2]**	**[4]**	**[5]**	**[3]**	**[6]**
Man-in-the-middle attack	–	–	✓	✓	✓	✓
Impersonation attack	✓	–	–	✓	–	–
Replay Attack	✓	✓	✗	✓	–	–
Modification attack	✓	✓	–	✓	–	–
Stolen verifier table attack	–		–	✓	–	–
Perfect Forward Secrecy(PFS)	–	✓	✓	–	–	✓
Mutual Authentication	–	–	✗	–	–	–
Quantum attack	✗	✗	✗	✗	✗	–

V. LIMITATIONS AND FUTURE SCOPE

1) The existing Post Quantum Lattice-based secure schemes for the VANET structure face limitations from both efficiency and security points. These methods could compromise the security of vehicle communications since they frequently have high computational costs or are vulnerable to sophisticated attacks. To address these issues,

there is a lot of scope in designing a secure, lattice-based authentication key exchange protocol for the VANET environment. To enhance the efficiency in the future, we could shift the hardness assumption from {LWE, SIS, RLWE, BiSIS} to {MLWE [17], MSIS [17]} and can construct an efficient and secure authentication scheme for VANET based on these hard problems.

2) **Establishing an equilibrium between Security and Efficiency Options:** One of the main directions for the near future is to find the perfect equilibrium between efficiency and security. This includes determining the trade-offs when choosing parameter sets that ensure specified security levels and improving lattice-based protocols' response time and resource consumption. A proper equilibrium may be achieved by designing schemes with particular use cases in consideration, such as high-assurance protocols for cloud computing or lightweight cryptography for embedded systems.
3) **Improving Efficiency for Realistic Implementation:** Although lattice-based systems provide promising security promises, their efficacy is still a matter of concern for real-world implementation, particularly in limited contexts like Internet of Things devices or real-time applications. It is imperative to find ways to minimize computational overhead, optimize key creation and exchange procedures, and shrink the number of lattice parameters. The performance of these schemes can be greatly improved by investigating combinations that combine lattice-based techniques with other cryptographic methods, hardware acceleration, and algorithmic advances such as efficient lattice reduction methods.
4) The decision-making approach to communicating with the entire system of the vehicle directly depends on Artificial intelligence (Al) and Machine Learning(ML). There is an opportunity to integrate VANET authentication schemes into these smart systems. The integration of these systems could enhance security. For example, ML algorithms could improve the resilience of VANET connections by more accurately predicting and handling potential security risks in real-time.
5) Integration of (FL+VLC+6G): The integration of Federal Learning(FL), Visible Light Communication (VLC), and 6G supports the Vehicle-to-Everything(V2X) service. It can enhance the efficiency and security of the autonomous vehicular system.

VI. Conclusion

This paper provides a comprehensive review of recently proposed post-quantum secure authentication schemes for VANETs, focusing on their cryptographic hardness assumptions, advantages, and limitations. We evaluated six lattice-based schemes based on SIS, ISIS, BiSIS, and RLWE problems. Our analysis highlights several areas that require further exploration, particularly in enhancing both security and efficiency. To advance the field, we recommend developing more lightweight cryptographic solutions optimized for resource-constrained environments in VANETs. Additionally, transitioning to more robust lattice assumptions, such as the Module Learning with Errors (M-LWE) problem, could provide a better balance between security and efficiency, offering quantum resistance without sacrificing system performance.

References

[1] G. K. Verma, N. M. Wani, and P. Gope, "Quantum-secure certificate-less conditional privacy-preserving authentication for vanet," *arXiv preprint arXiv:2403.13743*, 2024.

[2] A. Shahidinejad, J. Abawajy, and S. Huda, "Anonymous lattice-based authentication protocol for vehicular communications," *Vehicular Communications*, p. 100803, 2024.

[3] H. J. Nath and H. Choudhury, "Lbpv: Lattice-based privacy-preserving mutual authentication scheme for vanet," *Computers and Electrical Engineering*, vol. 120, p. 109765, 2024.

[4] A. Ahmad and S. Jagatheswari, "Lba-pake: Lattice-based anonymous password based authentication key exchange scheme for vanet," in *2023 12th International Conference on Advanced Computing (ICoAC)*, pp. 1–8, IEEE, 2023.

[5] Q. Li, D. He, Z. Yang, Q. Xie, and K.-K. R. Choo, "Lattice-based conditional privacy-preserving authentication protocol for the vehicular ad hoc network," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4336–4347, 2022.

[6] D. S. Gupta, S. Ray, T. Singh, and 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.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[8] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE access*, vol. 9, pp. 31309–31321, 2021.

[9] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in vanets: Attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021.

[10] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in vanets," *Computer Science Review*, vol. 41, p. 100411, 2021.

[11] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," *IEEE Access*, vol. 10, pp. 86127–86180, 2022.

[12] S. K. Sripathi Venkata Naga, R. Yesuraj, S. Munuswamy, and K. Arputharaj, "A comprehensive survey on certificate-less authentication schemes for vehicular ad hoc networks in intelligent transportation systems," *Sensors*, vol. 23, no. 5, p. 2682, 2023.

[13] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 99–108, 1996.

[14] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.

[15] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pp. 1–23, Springer, 2010.

[16] J. Ding, X. Xie, and X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem," *Cryptology ePrint Archive*, 2012.

[17] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.