Lattice Based Authentication of Mobile Agent

Pradeep Kumar [1], Kakoli Banerjee [2], Sakshi Verma [3], Sushant Singh [4], Shivansh Singh [5], Aryan kumar[6]
JSS Academy of Technical Education, Noida

***Abstract*—Lattice-based cryptography forms a strong founda- tion for secure authentication, especially in the case of mobile agents. Building on the hardness of lattice problems, these schemes provide security against quantum attacks, which is important for long-term security. Lattice-based authentication schemes, such as those based on NTRU, allow for secure and anonymous communication between mobile users, foreign agents, and home agents in roaming environments. Furthermore, lattice- based VSS schemes enhance the security and efficiency of secret sharing processes, and hence suitable for authentication systems. Using matrix vector operations with a good complexity, these lattice-based VSS schemes provide practical quantum-resistant schemes for secure authentication in the public cloud computing context. Generally, latticebased cryptography gives promise to meeting the increasingly changing nature of the threats in the mobile and cloud computing, by safeguarding information and secure communication against future quantum threats.**

***Index Terms*—Lattice, Cryptography, Authentication, Quantum Computing**

I. INTRODUCTION

As technology evolves, the need for secure, efficient, and future-proof authentication systems has never been more pressing. The rise of interconnected devices, online services, and mobile applications has created vast networks that are increasingly exposed to sophisticated security threats. From online shopping to mobile payments, users rely on these systems daily, yet they remain vulnerable to risks such as data breaches, identity theft, and malicious attacks. Traditionally, cryptography has been centered around the backbone of two methods: RSA and ECC, but these methods are challenged as quantum computing threatens to shake them, rendering them unable to be secure against an attack using a quantum method.

Lattice-based cryptography is emerging as the newest breakthrough to address these concerns. Lattice-based cryptography relies on the mathematical problems SVP and LWE, which have proven to be resistant to quantum attacks. This makes it a promising alternative for building secure systems that can withstand the computational power of quantum computers. In addition, the efficiency it can achieve in resource-poor environments like those in mobile agents and IoT devices has made it significant for current cryptographic applications. This paper proposes a new scheme known as Modified and Enhanced Lattice-Based Cryptography, where lattice-based principles of cryptography are combined with MAC for data integrity and secure key exchange with improved performance. The framework is designed for such ubiquitous networks, taking into consideration the low computational overhead of the protocol, the protocol's scalability, and adapting to dynamic environments. Based on advanced encryption techniques along with matrix-vector operations, MAC not only adds another layer of security but, at the same time, ensures practical implementation in reality.

In this introduction, it reviews the limitations of traditional cryptographic methods and shows that lattice-based techniques can bypass the existing bottlenecks. Its robust security against impersonation, replay attacks, and man-in-the-middle attacks makes the technique a strong candidate for applications in e-commerce, healthcare, and cloud computing.

The growth of complexities in cyber threats, combined with the swift evolution of quantum computing, presents an op- timistic solution with lattice-based authentication for secure sensitive data and communication channels. This theory is founded on rigor at the conceptual level with efficiency at the practical level.

II. LITERATURE SURVEY

Rachid El Bansarkhani [2012] presented a new construction of a lattice-based verifiable secret sharing scheme. Lattice- based secret sharing schemes are gaining more attention due to the strong security guarantees they have in the post-quantum era. This work introduced an innovative scheme based on a lattice-based hash function to secure secrets, so that the linearity of the hash function allows the verification of shares by individual participants, further building up trust in the scheme. The security analysis shows that the breaking of this scheme is actually equivalent to solving the approximate Shortest Vector Problem, which is a computationally hard problem. It shows that in the (n, n)-scheme, all participants must reconstruct the secret; otherwise, less than all participants cannot obtain the basis matrix or the secret because it is computationally infeasible. This approach clearly indicates an excellent advancement in the sector of secure and verifiable secret sharing, particularly lattice-based cryptographic primitives' applicability for enhancing robustness.

Ruhui Ma [2015] give an overview of Lattice-based Access Authentication Scheme for IoT in Space Information Networks. Lattice-based cryptography is increasingly recognized in terms of its potential to offer security for modern communication systems against quantum threats. Here, the authors introduce the novel lattice-based access authentication (LAA) scheme that caters to varied Internet of Things Devices and mobile entities. The proposed protocols,
based on lattice cryptography, achieve comprehensive security properties, including mutual authentication, conditional anonymity, unlinkability, data confidentiality and integrity, unforgeability, undeniability, key establishment, and perfect forward and backward secrecy (PFS/PBS). In addition, the scheme resists both traditional protocol attacks and quantum- based threats. Comparative security and performance analyses show that this approach presents better efficiency and security than those currently available authentication schemes, highlighting its feasibility and robustness for modern and future networks.

Dilli prasad sharma [2015] presented an in-depth review of mobile agent-based authentication: a model for user authentication in a distributed system.The model uses mobile agents to accomplish user authentication in a two-phase process in which an access request is made and an access decision is found. It proposes a mobile agent (AMA) that migrates among different machines in the network to provide authentication services. The system provides high-level security for dynamic application because of using mobile code verification signatures and password-based encryption. Another example of the mobile agent-based system that is widely used in large-scale systems is the mobile agent-based security model that can provide agent-based security without the need of a single centralized server.

Berguig et al. [2019] Mutual Authentication- and ECC- Based Security for Mobile Agent. This paper is studying the mobile agents' security problem along with migration in distributed networks and proposing a solution which is based on ECC to authenticate each other. Such highly autonomous mobile agents migrating from one platform to another do make it vulnerable to many types of attacks such as replay, man-in-the-middle type of attacks, unauthorized accesses. Since ECC provides higher security with shorter key sizes than other cryptographic systems, it can reduce the computational requirement and effectively protect the data from attacks. Also, mobile agents are made portable and flexible by using binary serialization.

Yousheng Zhou [2020] proposed Lattice-Based Authentication scheme where, Lattice-based cryptography is a key focus in post-quantum cryptographic research due to its high resistance to quantum attacks. NTRU encryption algorithm was known to be efficient, however, has the decryption error which restricts it from larger-scale applications. Optimizing its parameters has enhanced its security and therefore it can be safely incorporated in roaming authentication protocols. It has mutual authentication and conditional anonymity, and resilience against attacks such as replay and quantum attacks. Its adaptation into new technologies like 5G and edge computing will still remain a challenge, requiring more research.

Naveed Khan [2022] provide insight into Lattice-Based Authentication Scheme to Prevent Quantum Attack. The advent of quantum computing poses significant vulnerabilities to traditional cryptographic algorithms, as Shor's algorithm can break such schemes efficiently. To counter this, lattice- based cryptography has emerged as a strong alternative, especially for public cloud computing environments. This work proposes a lattice-based authentication mechanism that ensures secure peer interactions. It has been verified with the ROR model, and the performance analysis reflects that the scheme is strong, lightweight, and also communication- and computation-cost-effective. Although the scheme is feasible and implementable, further works will focus on the cost optimization of this approach, and extending this approach to IoT-enabled devices in the public cloud will also be considered in future works to depict its suitability in new emerging technologies.

Pradeep Kumar [2022]. provided a detailed review of, secure mobile agent mobility in health care systems employing polynomial-primed threshold secret sharing plan with Blowfish algorithms are provided by Al-Emran. The challenge of this research is to increase the security of mobile agent migration in health care systems and overcome problems such as integrity, confidentiality and authentication of sensitive data exchanged between medical personnel. The authors propose a secure method by implementing this polynomial based threshold secret sharing with Blowfish encryption that protects against unauthorized access and denial-of-service attacks. The method will not only securely transmit medical information but also strives to keep computational overhead low, which means it will be fast enough for real-world health care uses such as telemedicine and patient data management.

Jingyu Chen [2024] provided a detailed review of Lattice- based threshold secret sharing (TSS) schemes which have gained attention as a secure foundation for applications like threshold cryptography, blockchain, and federated learning. This manuscript provides the first comprehensive review of such schemes, classifying them by function and analyzing their features and limitations. While lattice-based TSS offers strong security against quantum attacks, it remains in the developmental stage, with challenges such as optimizing performance, reducing storage overhead, and improving adaptability. Current research highlights the potential of lattice-based TSS in advanced systems, but further exploration is needed to refine these solutions and broaden their practical applications.

III. PROBLEM SOLUTION

In our context, mobile agents' software systems that are designed to travel across heterogeneous systems to accomplish specific tasks face several security threats. The focus is on validating these and the environments they interact with, especially when under attack. Impending security demands are not met by traditional patents (RSA and ECC). They risk being violent by powerful quantum computers that can compromise the cryptographic promote that written techniques rely on.

The Problem with Traditional Authentication Methods RSA and ECC have long been two of the most widely used algo- rithms for secure communication. However, their underlying bases are mathematical problems which could be solved by quantum computers. This is a serious matter, as with advances in quantum computing, not too long from now breaking into such systems would become feasible, thereby compromising vulnerable mobile agents that are vulnerable to attacks like: Impersonation Attacks: An attacker assuming the identity of the agent or platform Man-in-the-middle attacks: Eavesdrop- ping and then modifying conversations between the agent and the platform. Replaying valid messages (to deceive the system). This is where the power of lattice-based cryptography comes in. Why Lattice-Based Authentication Is the Optimal Solution Lattice-based cryptography is a new, yet much more secure, mode of authentication in the resistance to quantum attacks. So, here's how it compares to RSA and ECC:

Resistance to Quantum Attacks. Lattice-based cryptography was designed to resist attacks of quantum computers. On the other hand, lattice-based systems are based on problems with which quantum algorithms don't have a good approach unlike RSA and ECC.

Efficient for Mobile Agents: Mobile agents often working in resource-bounded environment. They do not have the processing power of larger servers, Lattice based authentication offers a better solution when it comes to efficiency and less resource consumption than RSA and ECC. Scalable and Adaptive: E-commerce, healthcare, and financial applications, to name a few, make use of mobile agents and thus call for a scalable and adaptive authentication scheme. Lattice-based systems can better scale and adapt to new situations than current systems do. Thus, it would enable it to co-evolve with changing system requirements, and so it seemed possible for it to suit the need to protect mobile agents in the future. Lattice-Based Authentication to Address Such Issues

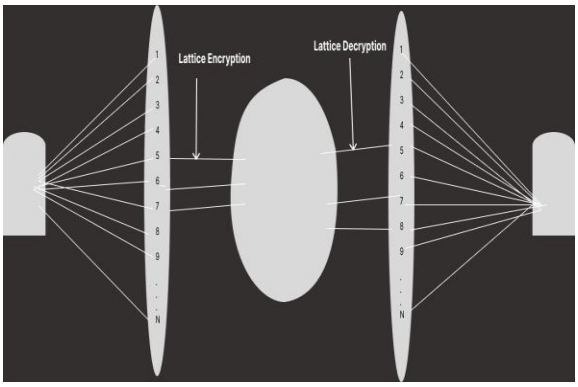
Here's how such a lattice-based authentication system completes the loopholes: Mutual authentication: The first step toward securing mobile agents is mutual authentication between the agent and the platform that it is communicating with. Traditional systems like RSA are open to interception and manipulation. Lattice-based authentication solves this by allowing a secure, verifiable protocol in which both ends authenticate each other before passing along sensitive information. Which reduces the possibility of impersonation or unauthorized access.

Secure key exchange: After the identities are mutually authenticated, the mobile agent and the platform should be able to exchange keys with each other needed for encrypting any ongoing communication. For instance, the RSA key exchange applied by traditional systems is a quantum-vulnerable process. Lattice-based systems make use of a post-quantum key exchange scheme. Therefore, even in case an adversary has a quantum computer, the base exchanging keys will be irrecoverable.

Intrusion Detection and Anomaly Monitoring: Lattice-based authentication not only protects key exchanges but also includes continuous monitoring for abnormal behavior that might indicate a breach. For instance, if an agent suddenly starts sending out messages that are not in line with its norm, the system can flag this as a potential threat. This proactive monitoring allows for the detection and prevention of malicious entities before they can do damage.

Lattice-based authentication solves important problems Defenses Against Quantum Attacks: Traditional kinds of authentication systems like RSA and ECC are susceptible to attacks from quantum computers while the lattice-based cryptography has defenses that can withstand quantum algorithms. Improved Security of Mobile Agents: Mobile agents operate in dynamic environments and are thus vulnerable to multiple varieties of attacks. General Purpose
— Impersonation Resourcefulness and Minimalism: Mobile agents are typically running on low-computation power machines. Lattice-based authentication provides a lightweight solution without sacrificing security properties, which is desirable for resource-constrained devices. Lattice-Based Schemes: Robustness against Advances in Technology Quantum computing is nearing, and with it, the end of classical cryptography. Though RSA and ECC might be replaced by quantum advances, lattice-based systems will not need a change to be used securely for authentication.

IV. FRAMEWORK



V. CASE STUDY

A case study on a lattice-based authentication system for mobile agents demonstrates its efficiency in securing communication in dynamic and distributed environments. Mobile agents, which are running autonomously across different platforms, demand strong authentication mechanisms to ward off unauthorized access and secure interactions. The

authentication system, based on lattice cryptography, offers resistance against quantum attacks and preserves key security properties such as mutual authentication, anonymity, data integrity, and unforgeability. The realization includes lattice-based key exchange protocols and signature schemes that are computationally efficient and lightweight, making them suitable for mobile agents with inadequate resources. Performance analysis reveals that the system effectively balances security with low communication and computation overhead, addressing the unique challenges of mobile agent environments. This case study demonstrates the potential of lattice-based solutions to secure mobile agents against advanced threats, paving the way for their application in critical fields like e-commerce, healthcare, and smart environments.

A lattice-based authentication framework was proposed to overcome those issues. This method uses advanced mathemat- ical structures called lattices to create cryptographic protocols that can withstand potential future quantum computational ad- vancements. This technique, unlike regular techniques, ensures that necessary processes, such as the identification of individu- als (mutual authentication), protecting the properties of agents (anonymity), ensuring that the information is unchanged (data integrity), and preventing counterfeit use (unforgeability) are achieved.
What's special about this system is that it's efficient. Such a compact data is purpose-built to be light in weight; therefore, it will ensure smooth running within devices where resource availability is very limited, like mobile phones or small IoT devices. It also achieves a trade-off between good security and resource usage at the same time, so it's perfectly suited for real-time distributed environments.

VI. CONCLUSION

Lattice-based cryptography provides a strong and secure method for authentication systems, with quantum computing being a threat in real terms against traditional approaches such as RSA and ECC. It is the use of mathematical challenges re- lated to problems in lattices that provide long-term protection against attacks, thus it serves as a tool for security systems to future-proof their systems.

This paper has pointed out how newer lattice-based methods, in the form of enhanced authentication frameworks and secret- sharing techniques, that have been designed to get rid of the older systems' vulnerabilities. Such methods are much more secure and efficient with the use of limited-resource devices, such as mobile agents, which prevent common threats, like impersonation and data tampering, and respond to special demands of modern applications from areas like e-commerce and healthcare.
Such potential looks ahead for making those systems even better by increasing the performance and adapting with in respect of new technologies such as IoT and 5G. Lattice- based cryptography can play a significant role in keeping sensitive information secret and ensuring secure communication, especially in today's changing digital world. In summary, lattice-based cryptography is a practical and forward-thinking solution addressing the increasing challenges in security. It can withstand quantum attacks and has flexibility for many applications, making it a very critical foundation for the future of secure authentication.

REFERENCES

[1] Zhou, Y., Wang, L. (2020). A Lattice-Based Authentication Scheme for Roaming Service in Ubiquitous Networks with Anonymity. Security and Communication Networks, 2020(1), 2637916.
[2] Chen, J., Deng, H., Su, H., Yuan, M., Ren, Y. (2024). Lattice-Based Threshold Secret Sharing Scheme and Its Applications: A Survey. Electronics, 13(2), 287.
[3] El Bansarkhani, R., Meziani, M. (2012). An efficient lattice-based secret sharing construction. In Information Security Theory and Practice. Se- curity, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems: 6th IFIP WG 11.2 International Workshop, WISTP 2012, Egham, UK, June 20-22, 2012. Proceedings 6 (pp. 160-168). Springer Berlin Heidelberg.
[4] Khan, Z. J. N., Ullah, I., Pathan, M. S., Lim, H. (2023). Lattice- based authentication scheme to prevent quantum attack in public cloud environment. Comput Mater Continua, 75(1), 35-49.

[5] Ma, R., Cao, J., Feng, D., Li, H. (2019). LAA: lattice-based access authentication scheme for IoT in space information networks. IEEE Internet of Things Journal, 7(4), 2791-2805.

[6] Sharma, D. P. (2015). Mobile Agent-Based Authentication: A Model for User Authentication in a Distributed System. International Journal of Computer Applications, 112(13).

[7] Roy, K. S., Deb, S., Kalita, H. K. (2022). A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks. Digital Communications and Networks.

[8] Berguig, Y., Laassiri, J., Hanaoui, S., Krit, S. D. (2019). Mobile agent security based on mutual authentication and elliptic curve cryptography. Int J Innov Technol Explor Eng,

[9] Tate, S. R., Xu, K. (2003). Mobile Agent Security Through Multi- Agent Cryptographic Protocols. In International Conference on Internet Computing (pp. 462-470).

[10] Berkovits, S., Guttman, J. D., Swarup, V. (1998). Authentication for mobile agents. Mobile agents and security, 114-136.

[11] Mundhe, P., Yadav, V. K., Verma, S., Venkatesan, S. (2020). Efficient lattice-based ring signature for message authentication in VANETs. IEEE Systems Journal, 14(4), 5463-5474.

[12] Boorghany, A., Sarmadi, S. B., Jalili, R. (2015). On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards. ACM Transactions on Embedded Computing Systems (TECS), 14(3), 1-25.

[13] Zhou, Y., Wang, L. (2020). A Lattice-Based Authentication Scheme for Roaming Service in Ubiquitous Networks with Anonymity. Security and Communication Networks, 2020(1), 2637916.

[14] Patsakis, C., van Rest, J., Choras´, M., Bouroche, M. (2016). Privacy- preserving biometric authentication and matching via lattice-based en- cryption. In Data Privacy Management, and Security Assurance: 10th International Workshop, DPM 2015, and 4th International Workshop, QASA 2015, Vienna, Austria, September 21–22, 2015. Revised Selected Papers 10 (pp. 169-182). Springer International Publishing.

[15] Xie, R., He, C., Xu, C., Gao, C. (2019). Lattice-based dynamic group signature for anonymous authentication in IoT. Annals of Telecommunications, 74, 531-542.

[16] Dabra, V., Bala, A., Kumari, S. (2020). LBA-PAKE: lattice-based anonymous password authenticated key exchange for mobile devices. IEEE Systems Journal, 15(4), 5067-5077.

[17] Tian, Y., Li, Y., Deng, R. H., Sengupta, B., Yang, G. (2021). Lattice- based remote user authentication from reusable fuzzy signature. Journal of computer security, 29(3), 273-298.

[18] Liu, J., Yu, Y., Jia, J., Wang, S., Fan, P., Wang, H., Zhang, H. (2019). Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks. Tsinghua Science and Technology, 24(5), 575-584.

[19] Chaudhary, R., Aujla, G. S., Kumar, N., Zeadally, S. (2018). Lattice- based public key cryptosystem for internet of things environment: Challenges and solutions. IEEE Internet of Things Journal, 6(3), 4897- 4909.

[20] Zhang, X., Xu, C., Zhang, Y. (2017). Fuzzy identity-based signature scheme from lattice and its application in biometric authentication. KSII Transactions on Internet and Information Systems (TIIS), 11(5), 2762- 2777.

[21] Alkhulaifi, A., El-Alfy, E. S. M. (2020, May). Exploring lattice-based post-quantum signature for JWT authentication: review and case study. In 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring) (pp. 1-5). IEEE.

[22] Lyubashevsky, V. (2008, March). Lattice-based identification schemes secure under active attacks. In International workshop on public key cryptography (pp. 162-179). Berlin, Heidelberg: Springer Berlin Hei- delberg.

[23] Dharminder, D., Mishra, D. (2020). LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication. Transac- tions on Emerging Telecommunications Technologies, 31(2), e3810.

[24] Huang, J. J., Tseng, Y. F., Yang, Q. L., Fan, C. I. (2018). A lattice-based group authentication scheme. Applied Sciences, 8(6), 987.

[25] Chaudhary, R., Jindal, A., Aujla, G. S., Kumar,

N., Das, A. K., Saxena, N. (2018). LSCSH: Lattice-based secure cryptosystem for smart health- care in smart cities environment. IEEE Communications Magazine, 56(4), 24-32.