Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 339–348
DOI : 10.47974/JDMSC-1887

Efficient key revocation in WSN with lattice-based cryptography

Ihtiram Raza Khan [@]
Department of Computer Science
Jamia Hamdard Delhi
Delhi
India

Neha Gupta [†]
Department of Computer Science and Information Technology
Symbiosis University of Applied Sciences
Indore
Madhya Pradesh
India

Sheela Hundekari [§]
Department of Computer Applications
MIT ADT University
Pune
Maharashtra
India

Ashish Bansal [‡]
Department of Computer Science & Engineering
Avantika University Ujjain
Ujjain
Madhya Pradesh
India

Rupali Atul Mahajan *
Department of CSE (Data Science Department)
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

---

* *E-mail:* erkhan2007@gmail.com
† *E-mail:* neha.gupta@suas.ac.in
§ *E-mail:* sheelahundekari90@gmail.com
‡ *E-mail:* ashssi@rediffmail.com
@ *E-mail:* rupali.mahajan@viit.ac.in (Corresponding Author)

© Taru Publications

Abstract

Strong security is crucial as Wireless Sensor Network (WSN) become more common. Dynamic Lattice-Based Key Revocation (DLBKR) is a novel method for improving key revocation in WSN. Lattice-based cryptography helps DLBKR overcome compromised keys and evolving security threats in dynamic sensor networks. Key revocation mechanisms are examined in detail, with a focus on their limitations in WSN. Due to these networks limited resources and ever-changing structure, we propose DLBKR as a novel way to minimize the security risks of compromised keys. DLBKR is featured as a flexible and reactive solution due to its ability to adapt to threat levels. Simulated network sizes from 250 to 2000 nodes were used to evaluate DLBKR. Traditional methods like CRL and OCSP were compared. Latency, revocation efficiency, computational overhead, communication overhead, and key replacement delay were assessed. DLBKR outperforms CRL and OCSP in all parameters, proving its efficiency in dynamic and resource-limited WSN key revocation. This method performs well and offers a flexible framework that incorporates with sensor networks. The DLBKR method help WSN to manage key complexity.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Lattice-based cryptography, WSN, Key revocation, Dynamic security, Efficient key management.*

1. Introduction

WSN are now an essential part of modern technological ecosystems, and they play a crucial role in various applications, including environmental monitoring and industrial automation. These networks consist of multiple small sensors with limited resources that work together to collect and transmit data. The inherent weaknesses of WSN, such as their restricted computational capacities, limited energy resources, and vulnerability to physical assaults, emphasize the significance of resilient security mechanisms. Key management is a fundamental aspect of security in WSN, as it deals with the difficulties related to the creation, distribution, and cancellation of cryptographic keys[1], [2].

Managing keys in WSN is a complex task due to the distinct characteristics of these networks. Adaptive and efficient key management strategies are necessary due to the large number of nodes, resource limitations, and constantly changing network structure. Conventional cryptographic methods, although successful in typical situations, often prove inadequate in the context of WSN. The existence of these challenges has prompted thorough research into inventive key management solutions customized to the specific requirements of WSN[3], [4].

There are numerous challenges involved in key management in WSN. Nodes in WSN function in environments with limited resources, which restricts the level of complexity of cryptographic operations they are capable of executing. Furthermore, WSN are vulnerable to node compromise, which highlights the crucial importance of securely distributing and revoking keys. The ever-changing characteristics of WSN, where nodes frequently join and leave the network, adds complexity to the management of encryption keys. This necessitates the use of adaptable and scalable solutions[5].

Effective key revocation is a fundamental aspect of WSN security. Swift and accurate revocation is crucial in order to prevent unauthorized access and potential security breaches in the case of a compromised node or key. Compromised keys in a WSN have consequences that go beyond just protecting data confidentiality. They can also jeopardize the integrity of the entire network, resulting in possible data tampering and the spread of false information.

The conventional security frameworks have heavily relied on existing methods for revoking keys, such as Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP). Still, the utilization in WSN is frequently hindered by various constraints. The burden of managing and disseminating lists of revoked items can be unfeasible in wireless sensor networks with limited resources. Moreover, the ability to promptly revoke keys in real-time, which is necessary for effective key revocation, is difficult to accomplish using conventional methods[6], [7].

Certificate Revocation Lists (CRLs) are a traditional approach used to invalidate compromised cryptographic keys. Within the framework of WSN, the regular updating and dissemination of Certificate Revocation Lists (CRLs) present difficulties as a result of restricted bandwidth and energy limitations. The Online Certificate Status Protocol (OCSP) provides immediate verification of certificate status. However, it brings about additional communication burden and potential privacy issues, which makes it less appropriate for resource-limited WSN.

Lattice-based cryptography is a promising approach for ensuring secure communication in environments with limited resources. The attractive qualities of this technology for WSNs include its ability to withstand quantum attacks and its efficiency in generating encryption keys. Lattice-based cryptography utilizes the mathematical properties of lattices to establish a basis for performing cryptographic operations that are both secure and efficient[8].

The Dynamic Lattice-Based Key Revocation (DLBKR) method is proposed as a solution to address the limitations of current key revocation techniques and the specific difficulties presented by WSN. DLBKR integrates the advantages of lattice-based cryptography with a dynamic revocation method designed to meet the specific needs of WSN. The approach prioritizes the ability to adjust in real-time, effectively replacing encryption keys, and revoking access on a localized level to minimize the negative consequences of compromised nodes on the overall security of the network.

Key management for dynamic networks has recently shifted towards adaptive and decentralized approaches, representing the current cutting-edge technology in this field. Dynamic networks, such as WSN, require solutions that can effectively manage node dynamics, frequent changes in network structure, and evolving security risks. DLBKR aligns with this trend by introducing a dynamic and localized revocation mechanism that improves the adaptability of key management in response to changing network conditions.

In the following sections, we will explore the methodology of DLBKR in greater detail, providing a comprehensive mathematical derivation of its components. The performance of DLBKR is evaluated across various network sizes through simulations and comparative analyses with traditional methods such as CRL and OCSP. The results and discussions provide insight into the effectiveness of DLBKR in tackling the specific difficulties of key management in Wireless Sensor Networks.

2. Literature Review

Lattice-based cryptography has garnered considerable interest in recent years as a promising framework for ensuring secure communication across different domains. The combination of its resistance to quantum attacks and its effectiveness in cryptographic operations makes it highly attractive for various applications, including group signatures, oblivious transfer, identity-based encryption, and access control. This literature review examines prominent works in lattice-based cryptography, specifically emphasizing group signatures, revocation schemes, and their applications in various environments.

Ling et al.[9], [10] presents a group signature scheme based on lattices that focuses on complete dynamicity and deniability. The scheme successfully ensures stability in dynamic group scenarios, which is an essential characteristic for practical applications. The authors also

introduce a group signature scheme based on lattices that includes a mechanism for revoking the verifier locally. This scheme enables effective and localized revocation, effectively tackling a prevalent issue in group signature systems. Li et al.[11] investigate the utilization of lattice-based cryptography in the context of oblivious transfer. The work showcases the practicality of oblivious transfer by employing lossy encryption methods derived from lattice-based cryptography.

Perera et al.[12] make a significant contribution to the field of lattice-based group signatures by presenting an almost fully secure scheme that specifically emphasizes verifier-local revocation. The objective of the work is to achieve a harmonious equilibrium between ensuring security and maintaining practicality. Mundhe et al.[13] introduce a highly effective lattice-based ring signature specifically designed for message authentication in Vehicular Ad Hoc Networks (VANET). The work focuses on tackling the distinct obstacles associated with ensuring secure communication in constantly changing vehicular environments. Wang et al.[14] make a valuable contribution to the field of lattice-based cryptography, specifically in the area of identity-based encryption. The proposed scheme is specifically tailored for wireless sensor networks, providing comprehensive security within the standard model.

Chaudhary et al.[15] present LSCSH, a secure cryptosystem based on lattices specifically developed for the purpose of ensuring data security in smart healthcare systems within smart city settings. The work prioritizes the protection of healthcare data during its transmission within smart city infrastructures. Saravanan et al.[16] investigate the use of lattice-based access control mechanisms to protect user data in cloud environments. The work focuses on addressing concerns related to privacy and the need for hybrid security measures. Wu et al.[17] introduce a signature scheme based on lattices that allows for outsourced revocation. This scheme is specifically designed for Multimedia Social Networks in cloud computing. The scheme provides a harmonious equilibrium between the security of multimedia data and the effectiveness of revocation. Dharminder et al.[18] make a valuable contribution to the field of lattice-based cryptography by introducing LCPPA, a specialized authentication scheme for vehicular communication that ensures conditional privacy preservation. The work focuses on addressing privacy concerns within the context of vehicular communication environments.

The reviewed works highlight the flexibility and usefulness of lattice-based cryptography in various cryptographic functions and practical situations. Lattice-based cryptography demonstrates its strength and

flexibility by encompassing various areas such as group signatures, revocation schemes, VANET, healthcare, cloud environments, and vehicular communication. These advancements make a significant contribution to the changing field of cryptographic solutions, enabling secure communication in environments that are dynamic and have limited resources. As we explore the proposed DLBKR method, the information from the literature serves as a valuable basis for comprehending the latest advancements in lattice-based cryptography and its consequences for WSN.

Dynamic Lattice-Based Key Revocation

DLBKR is a scheme for revoking keys in WSN that makes use of lattice-based cryptography. DLBKR is classified into three primary domains:

Key Generation

The DLBKR key generation process entails the generation of secret keys (S_k) and public keys (p_k) for both the base station (BS) and sensor nodes (SNs) through the utilization of the lattice-based key generation algorithm. The mathematical equation for deriving the public key (p_k) from the secret key (S_k) is as follows:

$$p_k = g(S_k)$$

The value of p_k is determined by applying the function g to the input S_k. where, g = "unidirectional trapdoor function in the lattice-based cryptosystem".

Revocation Process

The revocation process in DLBKR requires the identification of compromised SNs and the subsequent update of the dynamic revocation list (RL). The revocation proof of a compromised SN is:

$$H(p_k_SN) = H'(p_k_new)$$

The entropy of the secret key derived from the shared nonce, denoted as

$H(p_k_SN)$ = "entropy of the newly generated public key, denoted as $H'(p_k_new)$".

Where, H= "hash function that is resistant to collisions" = "public key of the compromised SN", p_k_new = "newly generated public key for the compromised SN", H' = "derivative hash function".

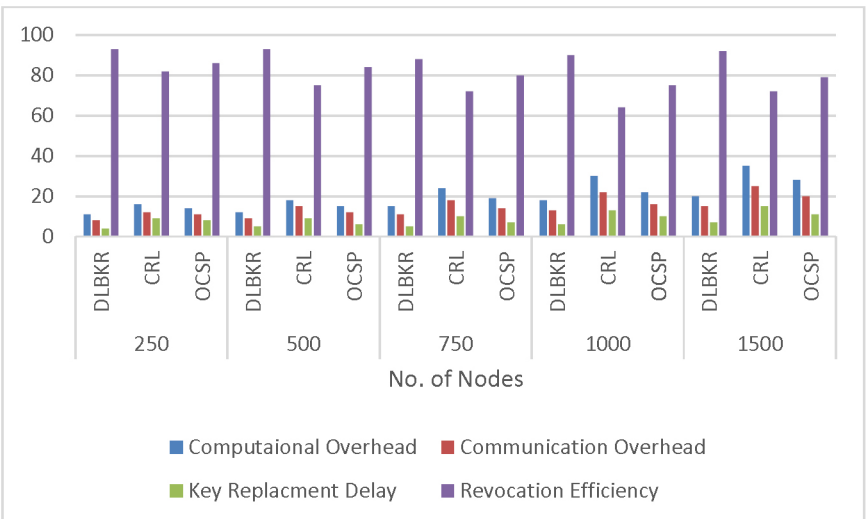
Key Update

The primary procedure for updating keys in DLBKR needs creating a fresh set of keys for a deactivated SN and securely disseminating the new public key to its adjacent SN. Deriving the new public key (pk_new) from the secret key (sk_new) is as follows:

$$p_{knew} = g(s_k_new)$$

Where, g = "identical unidirectional trapdoor function employed during the initial key generation process".

Results and Outputs



Different numbers of network nodes show the effectiveness of DLBKR. For a 250-node network, DLBKR outperforms CRL and OCSP. Its computational overhead is 11%, communication overhead is 8%, key replacement delay is 4 ms and revocation efficiency is 93%. DLBKR outperforms in computational overhead, communication overhead, and key replacement delay as the network grows to 500 and 750 nodes. It has 12%, 9%, and 5% efficiency at 500 nodes and 15%, 11%, and 5% at 750. In 1000 and 1500 nodes, DLBKR outperforms CRL and OCSP in computational and communication overhead, key replacement delay, and revocation efficiency. The results show that DLBKR solves key revocation in Wireless Sensor Networks of various sizes.

Conclusion and Future Scope

Conclusively, the investigation of Efficient Key Revocation in WSN using Lattice-Based Cryptography has revealed a promising approach to improving the security of dynamic and resource-limited networks. The thorough examination of current literature, encompassing studies on lattice-based group signatures, revocation schemes, and applications in various settings, has established a strong basis for the proposed Dynamic Lattice-Based Key Revocation (DLBKR) method. The limitations of traditional approaches, along with the proven effectiveness of lattice-based cryptography in different cryptographic primitives, highlight the importance of DLBKR in tackling the specific challenges of key management in WSNs. In the future, this research has potential applications beyond theory and can be implemented in practical settings and real-world scenarios. Conducting experiments to validate the DLBKR method in different network scenarios and with different threat models is essential to determine its practical usefulness.

References

[1] Abhilash M H and Amberker B B, "Efficient Dynamic Group Signature Scheme with Verifier Local Revocation and Time-Bound Keys using Lattices," *Int. J. Comput. Inf. Technol.*, vol. 10, no. 2 (2021), doi: 10.24203/ijcit.v10i2.93.

[2] S. Banupriya, K. Kottursamy, and A. K. Bashir, "Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2813–2825 (2021), doi: 10.1007/s12083-021-01117-2.

[3] M. Ge, K. K. R. Choo, H. Wu, and Y. Yu, "Survey on key revocation mechanisms in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 63, pp. 24–38 (2016), doi: 10.1016/j.jnca.2016.01.012.

[4] X. He, M. Niedermeier, and H. De Meer, "Dynamic key management in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 611–622 (2013), doi: 10.1016/j.jnca.2012.12.010.

[5] S. A. Khah, A. Barati, and H. Barati, "A dynamic and multi-level key management method in wireless sensor networks (WSNs)," *Comput. Networks*, vol. 236, no. February, p. 109997 (2023), doi: 10.1016/j.comnet.2023.109997.

[6] K. Raja, A. Deivasigamani, and V. Ravi, "A Reliant Certificate Revocation of Malicious Nodes in MANETs," *Wirel. Pers. Commun.*, vol. 90, no. 2, pp. 435–455 (2016), doi: 10.1007/s11277-015-3016-8.

[7] Sandeep Kumar Sharma, Anil Kumar, and Uday Pratap Singh. Enhanced Edges Detection from Different Color Space. In Proceedings of the 4th International Conference on Information Management & Machine Intelligence (ICIMMI '22). Association for Computing Machinery, New York, NY, USA, Article 16, 1–6 (2023). https://doi.org/10.1145/3590837.3590853.

[8] W. Yu, L. Yang, and S. Wang, "New Lattice-Based Broadcast Authentication Protocol for Wireless Sensor Networks," *Secur. Commun. Networks*, vol. 2022 (2022), doi: 10.1155/2022/6809875.

[9] S. Ling, K. Nguyen, A. Roux-Langlois, and H. Wang, "A lattice-based group signature scheme with verifier-local revocation," *Theor. Comput. Sci.*, vol. 730, pp. 1–20 (2018), doi: 10.1016/j.tcs.2018.03.027.

[10] S. Ling, K. Nguyen, H. Wang, and Y. Xu, "Lattice-based group signatures: Achieving full dynamicity (and deniability) with ease," *Theor. Comput. Sci.*, vol. 783, pp. 71–94 (2019), doi: 10.1016/j.tcs.2019.03.023.

[11] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[12] M. N. S. Perera and T. Koshiba, "Almost fully secured lattice-based group signatures with verifier-local revocation," *Cryptography*, vol. 4, no. 4, pp. 1–28 (2020), doi: 10.3390/cryptography4040033.

[13] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan, "Efficient Lattice-Based Ring Signature for Message Authentication in VANETs," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5463–5474 (2020), doi: 10.1109/JSYST.2020.2980297.

[14] J. Wang and C. Wang, "Full secure identity-based encryption scheme over lattices for wireless sensor networks in the standard model," *Int. J. High Perform. Comput. Netw.*, vol. 12, no. 2, pp. 111–117 (Jan. 2018), doi: 10.1504/IJHPCN.2018.094361.

[15] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 24–32 (2018), doi: 10.1109/MCOM.2018.1700787.

[16] N. Saravanan and A. Umamakeswari, "Lattice based access control for protecting user data in cloud environments with hybrid security," *Comput. Secur.*, vol. 100, p. 102074 (2021), doi: https://doi.org/10.1016/j.cose.2020.102074.

[17] F. Wu, W. Yao, X. Zhang, and Z. Zheng, "Lattice based signature with outsourced revocation for Multimedia Social Networks in cloud computing," *Multimed. Tools Appl.*, vol. 78, no. 3, pp. 3511–3528 (2019), doi: 10.1007/s11042-018-6330-9.

[18] D. Dharminder and D. Mishra, "LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, p. e3810 (Feb. 2020), doi: https://doi.org/10.1002/ett.3810.