Journal Name:	**Asian Journal of Mathematics and Computer Research**
Manuscript Number:	**Ms_AJOMCOR_12529**
Title of the Manuscript:	**MATRIX GROUPS AND EFFICIENT LATTICE-BASED SIGNATURE SCHEMES: A THEORETICAL AND PRACTICAL APPROACH TO POST-QUANTUM SECURITY**
Type of the Article	

General guidelines for the Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty'**, provided the manuscript is scientifically robust and technically sound.
To know the complete guidelines for the Peer Review process, reviewers are requested to visit this link:

https://r1.reviewerhub.org/general-editorial-policy/

Important Policies Regarding Peer Review

Peer review Comments Approval Policy: https://r1.reviewerhub.org/peer-review-comments-approval-policy/
Benefits for Reviewers: https://r1.reviewerhub.org/benefits-for-reviewers

PART 1: Review Comments

Compulsory REVISION comments	**Reviewer's comment**	**Author's Feedback** *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Please write a few sentences regarding the importance of this manuscript for the scientific community. Why do you like (or dislike) this manuscript? A minimum of 3-4 sentences may be required for this part.	1. This manuscript presents a novel approach to enhancing post-quantum security through lattice-based cryptography and matrix group theory, which is highly relevant to the growing need for quantum-resistant cryptographic solutions. 2. The combination of lattice problems (SVP and LWE) with the Matrix Group Conjugacy Problem (MGCP) is an innovative angle, potentially strengthening cryptographic primitives in a post-quantum world. 3. The manuscript makes an important contribution to the field by demonstrating both theoretical foundations and practical implementation of a digital signature scheme. 4. Given the increasing interest in post- quantum cryptography, the research is timely and could provide a valuable alternative to classical cryptographic systems.	-

Is the title of the article suitable? (If not please suggest an alternative title)	The title of the manuscript is suitable, as it clearly indicates the core concepts (matrix groups, lattice-based cryptography, and post- quantum security). However, it could be made slightly more concise. A possible alternative could be: ***"Matrix Group-Based Lattice Signature Schemes for Post- Quantum Security."***	
Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.	The abstract is well-composed, capturing the key points: the proposal of a lattice-based digital signature scheme, the focus on post- quantum security, and the theoretical and practical analyses involved. However, Instead of simply stating that computational efficiency is explored through simulations, specify the type of results or findings these simulations demonstrate (e.g., the scheme's performance metrics, practicality, or comparative efficiency).	
Are subsections and structure of the manuscript appropriate?	The structure of the manuscript is clear, well- organized, and follows a logical progression from introduction to theoretical foundations, algorithm description, security analysis, numerical simulations, and performance analysis. The inclusion of practical simulations and performance analysis adds an empirical dimension to the theoretical claims, further strengthening the manuscript.	
Please write a few sentences regarding the scientific correctness of this manuscript. Why do you think that this manuscript is scientifically robust and technically sound? A minimum of 3-4 sentences may be required for this part.	The manuscript is scientifically robust and technically sound. The core concept of using matrix groups in conjunction with lattice- based problems is well-justified, and the security relies on well-established hardness assumptions (SVP, LWE, and MGCP), which have been extensively studied in the cryptographic literature. The proof of security and theorems presented in the manuscript are logically structured, with clear reasoning and mathematical rigor. Additionally, the implementation of numerical simulations to validate the signing and verification process demonstrates practical feasibility, supporting the theoretical claims made in the paper.	
Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form. **-**	The references included in the paper are solid foundational resources for both lattice-based cryptography and matrix group theory, covering seminal works by Ajtai on lattice problems, Shor on quantum algorithms, and Lyubashevsky on lattice signatures. Additionally, key recent works by John, Udoaka, and Musa provide a relevant context for the application of matrix groups in cryptography.	
Minor REVISION comments **Is the language/English quality of the article suitable for scholarly communications?**	The language quality of the article is generally suitable for scholarly communication. The writing is formal and precise, with clear terminology that is appropriate for an audience familiar with cryptography and theoretical computer science.	
Optional/General comments		

PART 2:

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Are there ethical issues in this manuscript?	*(If yes, Kindly please write down the ethical issues here in details)*	

Reviewer Details:

Name:	**Vijay Kumar Tadakamalla**
Department, University & Country	**CVR College of Engineering, India**