| | |
|---|---|
| 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.** | This work introduces matrix groups to lattice-based digital signatures, which is important for post-quantum cryptography research. This paper uses the Matrix Group Conjugacy Problem (MGCP), which has been understudied in cryptographic protocols, to improve security against quantum attacks as quantum computing advances. The suggested scheme's effectiveness and efficiency are supported by mathematical rigor and practical simulations, making it a valuable contribution to theoretical and applied cryptography. This publication solves a major security issue and introduces lattice-based cryptography and matrix group theory, expanding post-quantum cryptographic research. The reliance on various problems (SVP, LWE, and MGCP) for hardness could be a negative due to the complexity of establishing hardness in varied circumstances. However, its prospective applications and solid theoretical foundation make this work significant. | |
| **Is the title of the article suitable? (If not please suggest an alternative title)** | he article—**"Matrix Groups and Efficient Lattice-Based Signature Schemes: A Practical Approach to Post-Quantum Security"**—is suitable, as it clearly reflects the ntribution of the paper. | |
| **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 article abstract usually summarizes the research's main ideas, methodologies, and objectives. It describes the unique lattice-based digital signature technique, the cryptographic hardness assumptions (SVP, LWE, and MGCP), and the theoretical and practical aspects. Some recommendations to increase clarity and completeness:<br>(i) Highlight the Motivation or Problem Clearly<br>(ii) Mention Computational Efficiency More Explicitly | |
| **Are subsections and structure of the manuscript appropriate?** | Yes, the subsections and structure of the manuscript are generally appropriate for the content and purpose of the paper. | |
| **Please write a few sentences** | This manuscript is theoretically and technically sound due to its rigorous mathematical | |

| | | |
|---|---|---|
| **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.** | foundations and well-structured lattice-based cryptography technique. The proposed signature system uses the Shortest Vector Problem (SVP) and Learning With Errors (LWE), which are known to be secure against quantum assaults. The Matrix Group Conjugacy Problem (MGCP) as a security assumption increases complexity by using an advanced group theory notion that has not been widely studied in cryptographic methods. The work offers comprehensive theoretical proofs, such as Theorems 3.1 and 3.2, that verify key creation, signature, and verification. Furthermore, the numerical simulations demonstrate the scheme's viability and computing efficiency, proving the manuscript's scientific validity. Its theoretical rigor and practical validity make the manuscript a significant post-quantum cryptography contribution. | |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.** **-** | This manuscript's references provide enough theoretical background and support for the proposed signature technique. The references include founding works on lattice-based cryptography (e.g., Micciancio and Regev, Ajtai's work on hard instances of lattice problems, and Peikert's work) and more recent studies on related topics like the Matrix Group Conjugacy Problem and lattice-based cryptographic constructions. | |
| Minor REVISION comments<br><br>**Is the language/English quality of the article suitable for scholarly communications?** | The **language** and **English quality** of the article are generally **suitable for scholarly communication**, but there are a few areas where slight improvements could be made to enhance clarity and readability. The manuscript is technically sound, and the content is presented in a clear and structured manner. However, some sentences could benefit from refinement in terms of style, grammar, and conciseness to ensure the paper is as accessible as possible to a broad academic audience. | |

**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: | **Anand Kumar Rai** |
| Department, University & Country | **Lucknow Public College of Professional Studies, India** |