

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 (<i>Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here</i>)
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 manuscript proposes new post-quantum signature scheme that combines lattice-based cryptography with matrix groups,	
Is the title of the article suitable? (If not please suggest an alternative title)	I suggest to make the title a bit simpler Such as Enhanced Post-Quantum Security: A Matrix Group Approach to Lattice-Based Signature Schemes Or Efficient Lattice-Based Signatures using Matrix Group Transformations	
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.	Easy to follow	
Are subsections and structure of the manuscript appropriate?	It's well organized	
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, with a solid theoretical foundation in hard lattice and matrix problems, and a technically sound approach as supported by practical simulation results. The use of hard mathematical problems such as SVP and MGCP reinforces security of the scheme. It also includes numerical simulations to validate the computational efficiency of the proposed scheme.	
Are the references sufficient and	Yes	

recent? If you have suggestions of additional references, please mention them in the review form. -		
<u>Minor</u> REVISION comments Is the language/English quality of the article suitable for scholarly communications?	Yes	
<u>Optional/General</u> comments	<ol style="list-style-type: none"> 1) I wonder the detailed environment where you simulated the scheme. Could you provide the specifications or settings for the simulation? 2) Also, are there any specific hardware requirements or constraints for the practical implementation? Are there any restriction for simulation, especially regarding the key size. 3) I suggest more detailed comparison with other signature schemes. 4) It would be helpful to add how the scheme scales with significantly larger matrix sizes or complex configurations. 5) There are several lattice-based hard problems beyond SVP and LWE. Based on the content of the paper, the explanation of that the proposed scheme specifically relies on SVP and LWE appears somewhat unclear. 	

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?	<i>(If yes, Kindly please write down the ethical issues here in details)</i>	

Reviewer Details:

Name:	YeonJun Kim
Department, University & Country	Republic of Korea