|  |  |
| --- | --- |
| Book Name: | **Finite Abelian Groups, Elliptic Curves, Blockchain with Hashing and Graphs** |
| Manuscript Number: | **Ms\_BPR\_3842.7** |
| Title of the Manuscript: | **A Python Programming Initiative for Elliptic Curves over Finite Fields** |
| Type of the Article | **Book chapter** |

General guidelines for the Peer Review process:

This Book’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/book-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 manuscript introduces a Python-based approach to studying elliptic curves over finite fields, an essential area of research with applications in cryptography and computational number theory. Its step-by-step methodology and practical examples make it accessible for both beginners and experienced researchers. The inclusion of Scatter plot, Cayley’s table, Diffie-Hellman, Schoof’s algorithm and its implementation further adds value by addressing a significant problem in counting points on elliptic curves efficiently. Basic Theoretical aspects are missing in every concept used in the manuscript. |  |
| **Is the title of the article suitable?****(If not please suggest an alternative title)** | The current title is appropriate as it reflects the core content. But to have more clarity, the title could be considered to be as "Implementing Elliptic Curves over Finite Fields with Python: Algorithms and Applications" |  |

|  |  |  |
| --- | --- | --- |
| **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 not provided in this document. Including a brief summary of the manuscript's objectives, methods, and key contributions is essential.Suggestions:* Clearly state the problem being addressed (e.g., the importance of elliptic curves in cryptography).
 |  |
| **Are subsections and structure of the manuscript appropriate?** | With logical divisions covering significant topics like polynomial irreducibility, point addition, and particular algorithms, the manuscript is well-structured.* Include an introduction outlining the significance of elliptic curves in mathematics and cryptography in order to improve readability even more.
* Make sure that a brief explanation of the significance of each subsection comes first.

However, adding a conclusion summarizing the key contributions and potential future directions could improve the flow and completeness. |  |
| **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.** | By proposing precise algorithms with Python code to verify important ideas in elliptic curve theory, the manuscript showcases scientific robustness. The provided examples guarantee reproducibility and confirm that implementations are valid. Schoof's algorithm is used to illustrate its technical depth and demonstrate sophisticated elliptic curve point counting techniques. |  |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.****-** | The references are adequate and provide the subject's technical and chronological context. However, the list could still be improved by incorporating more recent research on elliptic curve applications or cryptographic implementations published since 2020. Papers on post-quantum cryptography orelliptic curve optimizations in blockchain systems are possible suggestions |  |
| Minor REVISION comments**Is the language/English quality of the article suitable for scholarly communications?** | There are some typographical errors (such as "finite finite field," "po in t s," and "curren t\_point"), however the paper exhibits sufficient scientific language. To correct these minor mistakes in syntax, grammar, and formatting, a comprehensive proofread is advised. |  |
| **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: |  |
| Department, University & Country |  |