|  |
| --- |
|  |
| 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.** | **--** |  |
| **Is the title of the article suitable?****(If not please suggest an alternative title)** | **Yes** |  |
| 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. | **No** |  |
| **Are subsections and structure of the manuscript appropriate?** | **No** |  |
| **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.** |  **Abstract Clarity:** Add an abstract summarizing the paper's purpose, key methods, and major findings to provide readers with an overview. **Code Formatting:** Improve the formatting of Python code snippets for readability. Use consistent indentation and standard Python conventions. **Algorithm Explanations:** Provide a detailed explanation of each algorithm presented, including the rationale behind each step and its significance in the context of elliptic curves. **Mathematical Notation:** Ensure consistent and accurate use of mathematical notation throughout the manuscript. For example, clarify the representation of FpF\_pFp​ and related field elements. **Section Organization:** Structure sections logically. Start with basic concepts, progress to implementation details, and conclude with applications and findings. **Error Handling:** Elaborate on the error handling in Python code, especially when points at infinity or non-invertible moduli are encountered. **Figures and Diagrams:** Include diagrams or plots for concepts like point addition on elliptic curves, Cayley’s table, and the finite field representation to aid understanding. **Consistency in Terminology:** Maintain uniform terminology for key concepts, such as "finite fields," "elliptic curve groups," and "point addition." **Context for Applications:** Discuss practical applications of elliptic curve algorithms, such as cryptography or error correction, to demonstrate relevance. **Scatter Plot Results:** Expand on the scatter plot section to describe the insights gained from plotting the points of the elliptic curve. **Error in Point Addition Example:** Verify and correct the example showing nGnGnG calculations where modulus operation is applied. Ensure output matches expected values. **Modular Arithmetic Explanation:** Clarify the modular arithmetic operations used in the elliptic curve algorithms, especially in the context of point addition and multiplication. **Schoof’s Algorithm Details:** Provide a comprehensive explanation of Schoof's algorithm, including its computational complexity and importance in elliptic curve applications. **Citations for Cryptographic Use:** Include references and explanations of the cryptographic use of elliptic curves, especially in Diffie-Hellman key exchange. **Elliptic Curve Parameters:** Clearly define elliptic curve parameters used in examples, such as a,b,G,p,a, b, G, p,a,b,G,p, and nnn, to avoid confusion. **Typos and Grammar:** Correct typographical errors, such as "finite finite field" in multiple locations, to improve professionalism. **Code Comments:** Add descriptive comments to Python code snippets to make them self-explanatory and easier to follow. **Point at Infinity Explanation:** Elaborate on the concept of the point at infinity in elliptic curves and its role in group operations. **Conclusion and Future Work:** Include a conclusion summarizing the manuscript's contributions and propose potential future work or research directions. **Reference Formatting:** Standardize reference formatting according to a recognized citation style and ensure all cited works are relevant to the manuscript. |  |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.****-** | **No****Cite this paper: https://www.researchgate.net/profile/Chaitanya-Mahamuni/publication/344295537\_A\_Multivariate\_Public\_Key\_Cryptosystem\_MPKC\_for\_Digital\_Image\_and\_Video\_Encryption\_based\_on\_Multiple\_Permutation\_Polynomials\_over\_Finite\_Fields\_with\_a\_Novel\_Approach\_for\_Secure\_Key\_Transmission/links/5f64449ba6fdcc00862974a5/A-Multivariate-Public-Key-Cryptosystem-MPKC-for-Digital-Image-and-Video-Encryption-based-on-Multiple-Permutation-Polynomials-over-Finite-Fields-with-a-Novel-Approach-for-Secure-Key-Transmission.pdf** |  |
| Minor REVISION commentsIs the language/English quality of the article suitable for scholarly communications? | No |  |
| Optional/General comments | Included above |  |

|  |
| --- |
| **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 |  |