Review of: "Symmetric Key generation And Tree Construction in Cryptosystem based on Pythagorean and Reciprocal Pythagorean Triples"

Joe Louis Paul Ignatius[1]

1 Sri Sivasubramaniya Nadar College of Engineering

Potential competing interests: No potential competing interests to declare.

Review Comments

The paper titled "**Symmetric Key Generation and Tree Construction in Cryptosystem based on Pythagorean and Reciprocal Pythagorean Triples**" is interesting and offers a fresh perspective on symmetric key generation within a cryptosystem. The utilization of Pythagorean and reciprocal Pythagorean triples to enhance cryptographic security is good. The article demonstrates a solid foundation in mathematical concepts, which is commendable. However, there are certain aspects that need further clarification and improvement.

General Findings:

1. Rephrase the sentence "The KDC authenticates authenticate and secures the exchange of secret information to generate keys." - -used "authenticate" twice
2. Introduction needs to be revised. It starts straightway with the "Diophantine equation". It should be rewritten from the layman's point of view. Introduction may start with "Key generation and key exchange". There is no continuity between the abstract and the Introduction.
3. Pythagorean Triples may be discussed as the separate section. Is it the new approach to generate all Pythagorean triples or reusing the approach which was already proposed in the literature? Justify it!
4. Equation numbers are found to be missing for all equations.
5. It is not necessary to present the code to generate Pythagorean Triples for x is an odd integer or even integer respectively. Maybe thought as presenting it as the algorithm. So that, any researcher can implement the same in their own choice of the programming language.
6. A separate section number can be given for "Application of Pythagorean Triple in Cryptosystem".
7. The Figure shown in Page no. 20 is not clear.
8. No references are cited for "Application of Pythagorean Triple in Cryptosystem" in the article.
9. There are many related works related to the proposed work. What is the significance of the proposed work, limitations and assumptions with respect to the related works?
10. Analysis of the results and its inference are very important!
11. Figure's and Table's numbers must be cited in the running text.

Major Findings:

1. While the article introduces the concept of the proposed cryptosystem, it lacks a comprehensive explanation of how the Pythagorean and reciprocal Pythagorean triples are integrated into the symmetric key generation process. Providing a step-by-step breakdown of the algorithm, along with pseudocode or diagrams, would greatly enhance the reader's understanding.
2. It would be valuable to include a comparative analysis of the proposed cryptosystem against existing symmetric key generation methods. This could help highlight the strengths and weaknesses of the approach and demonstrate its effectiveness in terms of security and efficiency.
3. Since security is a critical aspect of any cryptographic system, the article should address potential vulnerabilities and attacks that the proposed cryptosystem might face. It's important to discuss how the Pythagorean triples' complexity contributes to resistance against attacks.
4. How does the proposed cryptosystem address the issue of key distribution, especially in scenarios where secure key exchange between parties is required?
5. Are there any limitations or scenarios in which the proposed cryptosystem might not be as effective or suitable as other symmetric key generation methods?
6. While the theoretical foundation is well-covered, the article could benefit from discussing practical implementation considerations. This could include factors such as computational complexity, scalability, and real-world feasibility.
7. Can you elaborate on the computational overhead introduced by the use of Pythagorean and reciprocal Pythagorean triples? How does this impact the efficiency of the cryptosystem in practical applications?
8. Have you considered the potential impact of quantum computing advancements on the security of the proposed cryptosystem, given that Pythagorean triples are based on classical mathematical principles?
9. Ensure that all claims, statements, and mathematical derivations are properly cited from reputable sources. Additionally, consider including references to prior work in cryptography that the proposed approach builds upon or diverges from.