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

Siddaramanna Sheela[1]

1 Jawaharlal Nehru National College of Engineering

Potential competing interests: No potential competing interests to declare.

This paper mainly discusses about the generation of Pythagorean and Reciprocal Pythagorean triplets with lot of illustrations. The explanation flow of the paper is good. But it would be better if the following modifications are incorporated.

1. Minor grammatical mistakes like repetition of words, joining of two words.
2. Section number is not given to any of the sections. It will be difficult to understand for the reader to know which is main section and which is subsection.
3. In page 6, 7 and 19, word Chapter is used. But in any technical paper Chapter word is not considered. So, please address this issue.
4. Since many methods are explained, author must mention which method belongs to which reference paper, means provide citation for each case referred.
5. Some of the Case headings are not proper. For example, instead of writing, “Case 1.3: Another Method to Generate Pythagorean Primitive Triple”, author can write it as, Case 1.3: Generate Pythagorean Primitive Triple according to [mention the reference in which this method is given]
6. Case 2 is defined in page 7 and directly Case 2.6.1 is defined in page 11, then what about Case 2.1 to Case 2.5? they are not declared.
7. In page 10, Case 2.2 is referred, but it is not declared in the paper.
8. In page 1 and 19, The KDC authenticates authenticate and secures ……. is mentioned. I think sentence correction is required. Similarly the sentence, Key generation and secure are critical to the …….. also need correction.
9. Implementation programs for the generation of Pythagorean and Reciprocal Pythagorean triplets are not required. It can be implemented in any language. Only equations are enough else algorithm is more than sufficient rather than complete program. Because, compared to understanding of programs, understanding of algorithms are more effective.
10. Some programs are in smaller font size and some are in normal font size. Maintain uniformity or replace by algorithms.
11. Table captions are not proper. In table caption only the words below table are mentioned. It doesn’t look good. For example, author can write table caption as “Table 1: Sample results of Case 1.1”
12. The main objective of this paper is to generate secrete information required for key generation. But the explanation is more on Triplet generation rather than cryptosystem. In the generated X, Y and Z values, it is not mentioned that how

KDC will authenticate user A or B. It is mentioned in page 19 that KDC authenticates the initiator, but what procedure it is following to authenticate is not discussed.

13. From the entire paper one can understand how Pythagorean and Reciprocal Pythagorean triplets can be generated but no one can understand how actually authentication can be done.
14. How robust the system is? This point is not addressed. No evaluation tests are conducted that to accept that this system is secure.
15. If the author mentions how this approach will increase security compared to existing methods, then it will add weightage to the work carried out.
16. Based on the paper description, I recommend the author to modify the title.