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

Suleyman Aydinyuz[1]

[1] Pamukkale University

Potential competing interests: No potential competing interests to declare.

Peer Review Report - Key Generation Based on Pythagorean and Reciprocal Pythagorean Triples

General Evaluation: The paper underscores the significance of key generation and exchange for the security of cryptosystems. The proposed approach centers on symmetric key generation based on Pythagorean and Reciprocal Pythagorean triples. Such a method hints at potential innovation in the field of cryptography.

Strengths:

1. The paper introduces an innovative approach by employing Pythagorean and Reciprocal Pythagorean triples for key generation.
2. The integration of the KDC for user authentication and key exchange could facilitate secure key distribution.
3. The inclusion of encrypted timestamps might establish a synchronized secure link between the two parties.

Areas for Improvement:

1. A more detailed analysis of the advantages and potential vulnerabilities of using Pythagorean and Reciprocal Pythagorean triples for key generation is required.
2. Further technical details on the security aspects of the KDC should be addressed. Specifically, the potential of the KDC becoming a target and its protective measures against such threats.
3. It would be beneficial to provide experimental results on the performance of the proposed system in real-world applications.

Conclusion: The paper proposes a method that might introduce a new dimension to the cryptography domain. However, it seems to lack technical depth and practical implications of the proposed approach. It is recommended for the authors to address the highlighted concerns, enriching the paper with comprehensive information and insights.

Recommendation

Certainly! Incorporating references can lend more credibility to the review.

- **M. Asci,** S. Aydinyuz “k-order Fibonacci Polynomials on AES-Like Cryptology”***Computer Modelling in Engineering***

and Sciences (2022), Vol. 131, No. 1, 277-293.

- S. Aydinyuz, **M. Asci** "Error detection and correction for coding theory on k- order Gaussian Fibonacci matrices" ***Mathematical Biosciences and Engineering***(2023), Vol. 20, No. 2, 1993-2010.