

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

Michał Wroński¹

¹ NASK National Research Institute

Potential competing interests: No potential competing interests to declare.

The article discusses an algorithm for establishing a session key based on Pythagorean and Reciprocal Pythagorean triples. One positive aspect of the reviewed article is its novel approach to establishing a shared key. Unfortunately, I think it is difficult to consider the article as meeting the standards required for scientific papers. I believe the article's structure should be revised—different methods of generating Pythagorean triples, in my opinion, should be included as an appendix at the end of the article. My main criticism, however, concerns the brevity of the description of the cryptosystem itself, which is based on Pythagorean triples. It is not entirely clear what the algorithm is really about, what level of security it offers for given parameters, or whether there are any known attacks or vulnerabilities for the proposed cryptosystem.