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

Steven D. Galbraith[1]

1 University of Auckland

Potential competing interests: No potential competing interests to declare.

The paper is about Pythagorean triples, and "reciprocal" triples, and a possible application to cryptography. Unfortunately I do not consider the paper suitable for publication at the moment.

The first part of paper is about methods to construct Pythagorean triples, and to obtain "reciprocal" triples (and 4-tuples, 5-tuples) from original ones. Some examples and program code are given. There are references to previous work. It seems ok, but I personally did not find anything very interesting or original here.

The second part of the paper is called "Main Work" and states that it describes a key exchange process. But this part of the paper is very vague and sketchy. I am an expert in cryptography, but I cannot understand exactly what is the proposed system.

I recomment to the author to very clearly write down the protocol. I would expect something of the form "A computes ... and sends ... to B, then B computes ...". Normally in cryptography papers there is a clear description of the protocol, even with pseudocode sometimes. It is also necessary to give a proof of correctness, which explains that A and B compute the same key.

Also there is something very important missing that is needed for every paper in cryptography: there is no discussion of security. What is the key size or security parameter? What is the best attack on the scheme? What evidence do you have that the protocol is secure?

Qeios ID: QZ4IIP · https://doi.org/10.32388/QZ4IIP