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

Marius Iulian Mihailescu[1]

1 Spiru Haret University

Potential competing interests: No potential competing interests to declare.

The author(s) provides with some general information on symmetric key generation and different constructions in cryptography, and how these concepts might potentially relate to Pythagorean Triples.

Symmetric Key Generation: The authors demonstrates that symmetric key generation is a crucial component of symmetric-key cryptography. In symmetric-key cryptography, the same key is used for both encryption and decryption. The process of generating symmetric keys typically involves using a secure random number generator to create a key of a certain length (e.g., 128 bits, 256 bits). These keys should be truly random and secret to ensure the security of the encryption scheme.

The authors demonstrates that Pythagorean Triples are sets of three positive integers (a, b, c) that satisfy the Pythagorean theorem (a^2 + b^2 = c^2). While these triples have interesting mathematical properties, they are not commonly used for symmetric key generation due to their deterministic nature. Secure key generation relies on true randomness to ensure unpredictability.

Tree Construction: Another important aspect, the author can relate and develop further the idea using tree structures that are commonly used in cryptography for various purposes, including key management, authentication, and hierarchical encryption. One well-known tree structure is the Merkle tree, which is used in various cryptographic protocols, such as blockchain technology.

Merkle trees are binary trees where each leaf node contains a cryptographic hash of a data block, and each non-leaf node contains the hash of its child nodes. This structure allows for efficient verification of data integrity and provides a way to construct a chain of trust.

The author(s) explored the idea of using Pythagorean or Reciprocal Pythagorean Triples in cryptography, with a carefully analyze of their properties and determine how they could be applied to key generation or tree construction while ensuring security and unpredictability.

Another important aspect are the implementations provided in different programming languages, such as C# and C++. An interesting approach especially for undergraduate and graduate students when they are trying to understand the mathematical background and how the algorithms can be put in practice.