Soto-Quirós, Juan Pablo; Rodríguez, Domingo
A new approach to mathematical cryptography using the discrete ambiguity function. (Spanish. English summary) Zbl 1458.94280

Summary: Through cryptography, be modified and hide certain information, so that only a certain group of people can interpret it through a key. When trying to use various fields of mathematics for this process, the concept of mathematical cryptography is developed.

Most mathematical cryptographic methods focus on number theory. Also, there are other cryptographic methods in the area of quantum physics and algebraic geometry, particularly hyperelliptical curves defined over finite bodies and finite fields. This paper introduces a new method of mathematical cryptography with signal processing techniques, through of a dimensional harmonic representations such as the discrete ambiguity function. This paper uses two equivalent definitions in module discrete ambiguity function.

This new cryptographic method uses the concept of symmetric key to making the process of encrypting and decrypting the message.

MSC:
94A60 Cryptography
94A12 Signal theory (characterization, reconstruction, filtering, etc.)
42A38 Fourier and Fourier-Stieltjes transforms and other transforms of Fourier type

Keywords:
discrete ambiguity function; cryptography; symmetric keys; discrete Fourier transform

Full Text: DOI