Analysis of Multidimensional Periodic Arrays

Rafael Arce, Francis Castro, José Ortiz, Ivelisse Rubio*, Ivelisse Rubio, University of Puerto Rico, Río Piedras

In order to use arrays in digital watermarking and cryptography, the arrays need to be robust to attacks and there is a need to measure the complexity of the arrays. For periodic sequences (one-dimensional arrays), the linear complexity is defined as the degree of the minimal polynomial that generates the sequence. We present a generalization of the definition of linear complexity to determine linear complexity of multidimensional arrays and present tight bounds on the linear complexity of arrays generated by the Moreno-Tirkel construction.

Keywords: periodic arrays, digital watermarking, complexity, cryptography

1