Ciphers and Ordinary Difference Equations

Roberto La Scala

University of Bari, Bari, Italy

robertlascala@gmail.com

Many stream or block ciphers of application interest such as Trivium, Bluetooth's E0, Keeloq, etc can be modeled as systems of explicit ordinary difference equations over finite fields. Such systems indeed determine the evolution over discrete time of the internal state of these ciphers which is simply a vector with entries in a finite field. The use of the formal theory of algebraic difference equations, so-called Difference Algebra, allows the study of some fundamental properties of difference ciphers, such as their invertibility and periodicity. This study implies the precise definition of algebraic attacks for the purpose of assessing cipher's security. Such modeling and the corresponding cryptanalysis allows hence the development of new cryptosystems.