Abstract

Stream cipher systems are considered desirable and secure if composed of Boolean functions (B.Fs) that are characterized by high resiliency. Resiliency is one of the main cryptographic security criteria for a given Boolean function. One of the classes of functions satisfying high resiliency with desirable cryptographic properties include the Plateaued functions whose design construction is of significant interest. The main known methods for these functions' construction are based on the Walsh spectrum or the related truth table concatenations if not algebraic methods. This paper examines the Haar spectral transform as an alternative method for the design of such functions. As its contribution, the paper presents different methods utilizing the Haar spectral coefficients' distribution for the design of highly resilient functions including Plateaued functions. The paper presents two methods of approaches namely; design of resilient BFs within the current variable domain without considering lower variable domains and using the lower variable domains to construct resilient functions within the higher variable domain. In the process, a Haar based construction method of
References


Index Terms

Computer Science               Applied Mathematics

Keywords