CORR 99-29

Decomposition and Classification of Cascaded GMW Functions

Zong Duo Dai*, Guang Gong, Ding Feng Ye*

Abstract A cascaded GMW function, which defines a cascaded GMW sequence, is a composition of a finite number of trace functions and exponential functions over finite fields, and is determined by a parameter system. Two such functions are said to be cyclically equivalent if the sequences defined by them are cyclically equivalent. In this paper, the problem how to decompose any given cascaded GMW function by trace functions is studied, then the problem how to classify the cascaded GMW functions according to the defining parameters and the cyclically equivalence relation is solved, based on a solution of the former problem.

Keywords: cascaded GMW functions, cascaded GMW sequences, finite field chains.