Abstract

In this paper, we introduce a new notion called the *dual function* for studying Boolean functions. First, we discuss general properties of the dual function that are related to resiliency and additive autocorrelation. Second, we look at preferred functions which are Boolean functions with the lowest 3-valued spectrum. We prove that if a balanced preferred function has a dual function which is also preferred, then it is resilient, has high nonlinearity and optimal additive autocorrelation. We demonstrate four such constrctions of optimal Boolean functions using the Kasami, Dillon-Dobbertin, Segre hyperoval and Welch-Gong Transformation functions. Third, we compute the additive autocorrelation of some known resilient preferred functions in the literature by using the dual function. We conclude that our construction yields highly nonlinear resilient functions with better additive autocorrelation than the Maiorana-McFarland functions. We also analysed the saturated functions, which are resilient functions with optimized algebraic degree and nonlinearity. We show that their additive autocorrelation have high peak values, and they become linear when we fix very few bits. These potential weaknesses have to be taken into consideration before we deploy them in applications.