Abstract

We construct two classes of balanced S-boxes with high nonlinearity $2^{n-1} - 2^{(n-1)/2}$ for n odd. Our S-boxes also have low maximum correlation, which reduces the bound of Zhang and Chan [23] by a factor of $\sqrt{2}$. The first class of S-boxes have low maximum differential while the second class corresponds to GMW sequences, whose algebraic structure allows us to construct a larger family of highly nonlinear S-boxes with reduced maximum correlation. Moreover, both classes of S-boxes can achieve high algebraic degree.