

Abstract We explore three applications of geometric sequences in constructing cryptographic Boolean functions. First, we construct 1-resilient functions of n Boolean variables with nonlinearity $2^{n-1} - 2^{(n-1)/2}$, n odd. The Hadamard transform of these functions is 3-valued, which limits the efficiency of certain stream cipher attacks. From the case for n odd, we construct highly nonlinear 1-resilient functions which disprove a conjecture of Pasalic and Johansson for n even. Our constructions do not have a potential weakness shared by resilient functions which are formed from concatenation of linear functions. Second, we give a new construction for balanced Boolean functions with high nonlinearity, exceeding $2^{n-1} - 2^{(n-1)/2}$, which is not based on the direct sum construction. Moreover, these functions have high algebraic degree and large linear span. Third, we construct balanced vectorial Boolean functions with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and low maximum correlation. They can be used as nonlinear combiners for stream cipher systems with high throughput.