Abstract

Boolean functions with good autocorrelation properties play an important role in the design of block ciphers and stream ciphers. Rotation symmetric Boolean functions (RSBFs), also called idempotent, which are invariant under the action of cyclic group, have recently proven to be very useful in several areas of cryptography. In this paper we present a theoretical construction of balanced odd-variable RSBFs satisfying the strict avalanche criterion (SAC) for the first time. Compared with the known balanced Boolean functions with SAC property, the constructed functions have higher algebraic degree and the best global avalanche characteristic property. In addition, the count of balanced RSBFs satisfying SAC is also studied.