On Ideal t-Tuple Distribution of Orthogonal Functions in Filtering de Bruijn Generators

Guang Gong

Uniformity of binary tuples of various lengths in a pseudorandom sequence is an important randomness property for cryptographic applications. We consider the problem how to convert a uniformly distributed binary tuples of length n in a pseudorandom sequence into another a pseudorandom sequence with uniformly distributed binary tuples through filtering models.

In general, not any filtering function can be used to achieve uniformity in binary tuples. We restrict ourselves to the family of orthogonal functions, i.e., those correspond to binary sequences with ideal 2-level autocorrelation, which are also a rich source for known APN functions and almost bent functions. It is known that if we apply the so-called WG transform to the known orthogonal functions, then there is only one class whose orthogonality remains, called WG-sequences. This result is first conjectured in 1997, proved by Dillon for odd n and Dillon and Dobbertin in 2004 for even n. WG transformation and WG sequences have been used in WG stream cipher, which is to filter over an linear feedback shift register sequence. After the twenty years of discovering WG transformations, there is no much more significant results on randomness on WG transformation sequences reported. In this talk, I will present our new results on uniformity of WG transformation as filtering functions on de Bruijn sequences. Surprisingly, we have found that there are only two classes of orthogonal functions whose WG transformations will reserve some uniformity of the output sequences, where one is obtained by decimation from the original WG transformation and the other class is obtained by decimation from WG transformation over 3-term sequences, the later does not have 2-level autocorrelation.

This is a joint work with Kalikinkar Mandal.