CORR 2000-30

On Welch-Gong Transformation Sequence Generators

G. Gong & A.M. Youssef

Abstract Welch-Gong (WG) transformation sequences are binary sequences of period $2^n - 1$ with 2-level auto correlation. These sequences were discovered by Golomb, Gong and Gaal in 1998 and verified for $5 \leq n \leq 20$. Later on, No, Chung and Yun found another way to construct the WG sequences and verified their result for $5 \leq n \leq 23$. Dillon first proved this result for odd n in 1998, and finally, Dobbertin and Dillon proved it for even n in 1999. In this paper, we investigate a two-faced property of the WG transformation sequences for application in stream ciphers and pseudo-random number generators. One is to present randomness or unpredictability of the WG transformation sequences. The other is to exhibit the security property of the WG transformations regarded as Boolean functions. It is shown that the WG transformation sequences, in addition to the known 2-level auto correlation, have three-level cross correlation with m-sequences, large linear span increasing exponentially with n and efficient implementation. Thus this is the first type of pseudo-random sequences with good correlation and statistic properties, large linear span and efficient implementation. When the WG transformation are regarded as Boolean functions, it is proved that they have high nonlinearity. A criterion for whether the WG transformation regarded as Boolean functions are r-resilient is derived.

Keywords Stream cipher, pseudo-random sequence (number) generator, auto/cross correlation, linear span, Boolean function, non-linearity, r-resilient property.