ALEXANDER BORS, Carleton University

Wreath products and cascaded feedback shift registers

In cryptography, cascade connections are a means of combining multiple feedback shift registers (FSRs) into hopefully more secure stream ciphers. In this talk, we present recent results, obtained in joint work with Maghsoudi and Wang, on the periods of bit sequences produced by cascade connections of two FSRs. We observe that those periods may be viewed as cycle lengths of a certain permutation on vectors that is an element of a so-called imprimitive permutational wreath product (a certain kind of permutation group). This allows us to study periods of cascade connections with algebraic methods, obtaining both an upper bound on the maximum period of a cascade connection and a complete understanding of the periods in the important case of the cascade connection of an n-dimensional De Bruijn sequence into an m-dimensional linear FSR.