CORR 2000-20

On the Quadratic Span of Binary Sequences

A.M. Youssef & G. Gong

Abstract The length of the shortest FSR that generates a sequence is called the span of the sequence. If the feedback function is linear, then the Berlekamp-Massey algorithm can be used to efficiently determine the length of the shortest linear FSR that generate the sequence and its associated linear feedback function. However, for a general nonlinear feedback function, determining the span and an associated feedback function efficiently is difficult because of the nonlinearities involved. Because of its tractability, most of the current research ahs focused on studying the linear span of a sequence. However, a sequence with a large linear span may be generated by a much shorter feedback shift register with nonlinear feedback function. In this paper we study the quadratic span of binary sequences. We prove that (i) If the quadratic span of the sequence $s_0, s_1, \ldots, s_{n-1}$ is $> n/2$, then the quadratic span of the sequence $s_0, s_1, \ldots, s_n$ remains unchanged. BAsed on our experimental results, we conjecture the following: (ii) Let $N_n(q)$ be the number of binary sequences of length n and quadratic span $q > n/2$. Then $N_n(q)$ is a function of the difference $(n-q)$ only, i.e., $N_n(q) = N_{n+i}(q+i)$. (iii) For moderately large n, the expected value of the quadratic span of a randomly selected sequence of length n is given by $E(q_n) \approx \sqrt{2n}$.

Keywords stream ciphers, shift registers, quadratic span, quadratic span profile