CORR 2002-18

Charles C.Y. Lam & Guang Gong*

Randomness of Elliptic Curve Sequences

Abstract In this paper, we introduce linear feedback register sequences (LFSR) over the group of the elliptic curve points, and a way of generating binary sequences from these LFSR sequences. The former is called *LFSR-EC sequences*. Properties on representation, period, and linear span of these two types of sequences are discussed. A special case of this generation is then discussed in detail.