CORR 2001-48

Linear Recursive Sequences over Elliptic Curves

Guang Gong*, Charles C.Y. Lam

Abstract In this paper, we introduce linear feedback shift register sequences (LFSR) over the group of the lliptic curve points, and a construction of binary sequences obtained 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. Also, the even case for the elliptic curve sequence proposed in [5] is analysed.