CORR 2001-35

The GH Public-key Cryptosystem

Guang Gong*, Lein Harn*, & Huapeng Wu

Abstract This paper will propose an efficient algorithm that utilizes the signed-digit representation to compute the kth term of a characteristic sequence generated by a linear feedback shift register of order 3 over $GF(q)$. We will also propose an efficient algorithm to compute the $(h-dk)$th term of the characteristic sequence based on the knowledge of the kth term where k is unknown. Incorporating these results, we construct the ElGamal-like digital signature algorithm for the public-key cryptography based on the 3rd-order characteristic sequences which was proposed by Gong and Harn in 1999.

Key Words Public-key cryptosystem, digital signature, third-order linear feedback shift register sequences over finite fields.