Abstract

Since the introduction of public-key cryptography by Diffie and Hellman in 1976, the potential for the use of the discrete logarithm problem in public-key cryptosystems has been recognized. Although the discrete logarithm problem as first employed by Diffie and Hellman was defined explicitly as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers module a prime, this idea can be extended to arbitrary groups and in particular, to elliptic curve groups. The resulting public – key systems provide relatively small block size, high speed, and high security. This paper identified an efficient performance of concurrent algorithm using complementary recoding over

References


**Index Terms**

Computer Science

Applied Mathematics

**Keywords**

Secret sharing, Elliptic Curve Cryptography (ECC),