Key exchange for new cryptosystem analogous to LUCELG and Cramer-Shoup

ABSTRACT

Key exchange or key establishment is any process in cryptography by which users are able to share or exchange a secret key. The problem on the key exchange is how to exchange any keys or information so that no third party can obtain a copy. This paper will discuss the Diffie-Hellman key exchange and the key exchange for new cryptosystem analogous to LUCELG and Cramer-Shoup that have been proposed by the same author in 2009. In the analog cryptosystem, the encryption and decryption algorithm are based on the defined Lucas function and its security have been proved that is polynomial time equivalent to the generalized discrete logarithm problems. Hence, one protocol will be proposed to provide the key establishment. Basically the protocol uses the second order linear recurrence relation and the multiplicative group of integers modulo p. In the protocol, the third party will not be able to alter the contents of communication between three parties.

Keyword: Key exchange; Diffie-Hellman key exchange; Key establishment; Protocol; Analogous LUCELG and Cramer-Shoup.