A new cryptosystem analogous to LUCELG and Cramer-Shoup

ABSTRACT

A special group based on a linear recurrence equation plays an important role in modern cryptography. Its relation appeared differently in various cryptosystem. Some cryptosystems that use this linear recurrence property are LUC, LUCDIF, and LUCELG but the first practical Lucas function in a cryptosystem is LUC, presented by Peter Smith and Michael Lennon in 1993. Cramer-Shoup is a practical public key cryptosystem provably secure against adaptive chosen ciphertext attack that requires a universal one-way hash function. Based on LUCELG and Cramer-Shoup cryptosystems, a new public key cryptosystem is developed by generating the key generation, encryption and decryption algorithm. There are two types of security for the new cryptosystem that we are concerned which are the security of Lucas function and its security against an adaptive chosen ciphertext attack. Since the encryption and decryption algorithm of a new cryptosystem is based on the defined Lucas function, it is believed that the security of Lucas function is polynomial-time equivalent to the generalized discrete logarithm problems. Moreover, the new cryptosystem is secure against adaptive chosen ciphertext attack by assuming that the hash function is chosen from a universal one-way family and the Diffie-Hellm an decision problem is hard in the finite field.

Keyword: Lucas function; Public key cryptosystem; Discrete log problem; Adaptive chosen ciphertext attack; Hash function