International Journal of Cryptology Research 4(1): 68 - 72 (2013)

Key Exchange for New Cryptosystem Analogous to LUCELG and Cramer-Shoup

[1*] Norliana Muslim and [2]Mohamad Rushdan Md. Said

[1]Faculty of Engineering, Universiti Selangor,
Jalan Timur Tambahan, 45600 Bestari Jaya,
Selangor, Malaysia

[2]Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia,

E-mail: norliana_muslim@unisel.edu.my and
mrushdan@putra.upm.edu.my

*Corresponding author

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.

Keywords: Key exchange, Diffie-Hellman key exchange, key establishment, protocol, analogous LUCELG and Cramer-Shoup.

1. INTRODUCTION

The Diffie-Hellman key exchange (Diffie and Hellman, 1976) is one of the practical examples of the cryptography key exchange. In their discrete logarithm based scheme, two parties that have no prior knowledge to each other will establish a shared secret key and the key can then be used to encrypt subsequent communications using a symmetric cipher key.

The summarized Diffie-Hellman key exchange between Ali and Borhan with Eka as an eavesdropper is described in Figure 1. The first is for Ali and Borhan to agree on a prime p and a nonzero integer g modulo p such that its order in F_p^* is a large prime.

Ali	**Eka**	**Borhan**
Ali and Borhan agree to exchange keys:	Eka can sees: A, B, g and prime number P	Borhan and Ali agree to exchange keys:
Ali chooses a secret nonzero integer a, and then calculate $A \equiv g^a \bmod p$		Borhan chooses a secret nonzero integer b, and then calculate $B \equiv g^b \bmod p$
Ali and Borhan exchange keys		
Ali receives B	Eka can see the value of $A$and B	Borhan receives A
Ali determined common shared key, B^a		Borhan determined common shared key, A^b

Figure 1: Diffie-Hellman Key Exchange

The following is the example of Diffie-Hellman key exchange:

1. Ali and Borhan agree to use the prime p = 941 and the primitive root g = 627.
2. Ali chooses a secret key $a = 347$ and calculates $A = 390 = 627^{347} \bmod 941$.
3. Similarly, Bob chooses a secret key $b = 781$ and calculates $B = 691 \equiv 627^{781} \bmod 941$.
4. Ali and Borhan exchange each other the number 390 and 691. The numbers a = 347 and b = 781 are not transmitted and remain secret.
5. Then Ali and Borhan are both able to compute $470 \equiv 627^{347\times781} \bmod 941 \equiv A^b \equiv B^a \bmod p$. So, the number 470 is Ali and Borhan shared secret.

Note that it should be difficult for Ali to solve for Borhan's private key or for Borhan to solve Ali's private key. If it is not difficult, Ekaas an eavesdropper may simply replace her own private or public key, access to Borhan's public key into her private key, then produce a fake shared secret key and solve for Borhan's private key.

Now, the new variant cryptosystem of LUCELG (ElGamal (1985)) and Cramer-Shoup (Cramer and Shoup (1998)) was proposed by utilize the second order linear recurrence relation as cryptographic keys (Lucas (1878)). In both encryption and decryption process, the Lucas cipher was derived as $V_n(P,Q) \bmod p$ (Muslim and Md. Said (2009)).

In this present paper, we propose a cryptographic protocol for the variant cryptosystem by showing the corresponding process between Ali, Borhan and Eka. The idea for the key agreement protocol for cryptosystem analogous to LUCELG and Cramer-Shoup is derived from the following key exchange figure:

Ali	**Eka**	**Borhan**
Ali and Borhan agree to exchange keys:	Eka can sees: P_1, P_2, prime number p, Q =1	Borhan and Ali agree to exchange keys:
Ali generates one secret key, k and α then calculate u_1, u_2, e and v		Borhan generates five secret keys (x_1, x_2, y_1, y_2, z) then calculate c, d and h
Ali and Borhan exchange keys		
Ali receives c, d and h	Eka can see the value of c, d, h, u_1, u_2, e and v	Borhan receives u_1, u_2, e and v
Ali determined common shared key, s		Borhan determined common shared key, s

Figure 2: Key Exchange for Variant Cryptosystem

2. KEY AGREEMENT PROTOCOL FOR VARIANT CRYPTOSYSTEM

Definition 1 (Menezes *et al*. (1996))

A cryptographic protocol is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

Now, let say the guys Ali and Borhan have chosen the variant encryption scheme to use in communicating over an unsecured channel. To encrypt messages, they require a key and the communication protocol is proposed as the following:

1. Ali and Borhan agree to use prime number $p = 7, P_1 = 2, P_2 = 3$ and Q = 1.

2. Borhan chooses secret key $(2,3,3,2,3) \in F_{7^2}^*$, then sends his public keys *c*, *d* and *h* to Ali such that
$$c \equiv V_{x_1}(P_1,1) \cdot V_{x_2}(P_2,1) \bmod p \equiv V_2(2,1) \cdot V_3(3,1) \bmod 7 \equiv 2 \cdot 4 \bmod 7 \equiv 1 \bmod 7$$
$$d \equiv V_{y_1}(P_1,1) \cdot V_{y_2}(P_2,1) \equiv V_3(2,1) \cdot V_2(3,1) \bmod 7 \equiv 2 \cdot 7 \bmod 7 \equiv 0 \bmod 7$$
$$h \equiv V_z(P_1,1) \bmod p \equiv V_3(2,1) \bmod 7 \equiv 2 \bmod 7$$

3. Ali generates a key for the variant encryption scheme by chooses a secret key *k* = 2.

4. Ali encrypts the key u_1, u_2, e and *v* using Borhan's public key and sends the encrypted key to Borhan. The encrypted process are:

$$u_1 \equiv V_k(P_1,1) \bmod p \equiv V_2(2,1) \bmod 7 \equiv 2 \bmod 7$$
$$u_2 \equiv V_k(P_2,1) \bmod p \equiv V_2(3,1) \bmod 7 \equiv 0 \bmod 7$$
$$G \equiv V_k(h,1) \bmod p \equiv V_2(2,1) \bmod 7 \equiv 2 \bmod 7$$
$$e \equiv G \cdot m \bmod p \equiv 2 \cdot 5 \bmod 7 \equiv 3 \bmod 7$$
$$\alpha = H(u_1, u_2, e) = 2$$
$$v \equiv V_k(c,1) \cdot V_{k\alpha}(d,1) \bmod p \equiv V_2(1,1) \cdot V_4(0,1) \bmod 7 \equiv 6 \cdot 2 \bmod 7 \equiv 5 \bmod 7$$

5. Borhan decrypts using his private key and recovers the secret key by calculating
$$s \equiv e \cdot V_z(u_1,1)^{-1} \bmod p \equiv 3 \cdot V_3(2,1)^{-1} \bmod 7 \equiv 3 \cdot 2^{-1} \bmod 7 \equiv 5 \bmod 7$$

6. Ali and Borhan begin communicating with privacy and now share a common secret key *s*.

Both Ali and Borhan have reached at the same value because $V_k(c,1) \cdot V_{k\alpha}(d,1) \bmod p$ and $e \cdot V_z(u_1,1)^{-1} \bmod p$ are equal. In the protocol, only $(2,3,3,2,3) \in F_{7^2}^*$ and *k* =2 are kept secret. All other values such as $P_1 = 2, P_2 = 3, c = 1, d = 0, h = 2,$ and $F_{7^2}^*$ can be clearly seen by the eavesdropper, Eka. Unfortunately, she is not able to construct any combination to alter the communications.

The shared secret key now can be used as an encryption key by Ali and Borhan in order to send messages across the same open communications

channel. To enhance the security, large numbers of (x_1, x_2, y_1, y_2, z) in the multiplicative group, k and prime number p are needed.

3. CONCLUSION

The Diffie-Hellman key exchange and the key agreement protocol for new cryptosystem analogous to LUCELG and Cramer-Shoup have been defined. Further research can be continued by discussing the current protocol to other scenarios in key agreement such as password-authenticated or secure remote password protocol.

REFERENCES

Cramer, R. and Shoup, V. 1998. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *CRYPTO'98, LNCS*. **1462**:13-25.

Diffie, W. and Hellman, M. E. 1976. New Directions in Cryptography. *IEEE Transaction on Information Theory*. **22**(1976): 644-654.

ElGamal, T. 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*. **31**(1985): 469-472.

Lucas, F. E. A. 1878. Theories des functions numeriques simplement periodiques. *American Jnl. Math*. **1**: 184-240, 289-321.

Menezes, P., Oorschot, P. and Vanstone, S. 1996. *Handbook of Applied Cryptography*. CRC Press. 33-35.

Muslim, N. and Md. Said, M. R. 2009. A new cryptosystem analogous to Lucelg and Cramer-Shoup. *International Journal of Cryptology Research*. **1**(2): 191-204.