Some Analogue of Cramer-Shoup

[1]Mohamad Rushdan Md. Said & [2]Norliana Muslim

[1, 2] Laboratory of Theoretical Studies
Institute for Mathematical Research
Universiti Putra Malaysia

[1] mrushdan@fsas.upm.edu.my

Abstract

LUCELG and Cramer-Shoup are examples of public key cryptosystem. LUCELG uses a special group based on the Lucas function, also known as second order linear recurrence relation but the first practical Lucas function in a cryptosystem is LUC. 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, analogous systems based on Lucas function and its extension are proposed and analyzed.

Introduction

In ElGamal cryptosystem [3] proposed by Taher Elgamal, the security relies on the difficulty of computing discrete logarithms. Based on the same difficult mathematical functions as ElGamal, LUCELG uses the calculation of Lucas functions instead of discrete logarithms. The extended Lucas function is used to construct a cubic analogue of the RSA [8].

In 1998, Ronald Cramer and Victor Shoup extended ElGamal scheme and developed Cramer-Shoup cryptosystem [1]. In Cramer-Shoup, they introduced a random element into the encryption process, such that a given plaintext will produce a different ciphertext on subsequent runs on the system. The consequence is that, unlike ElGamal, Cramer-Shoup is not susceptible to adaptive chosen ciphertext attack.

We extend the Cramer-Shoup cryptosystem to the second and the third order analogues by showing the key generation, encryption and decryption processes. We will see how the extended Lucas function and its extension perform in Cramer-Shoup and show sub exponentiation instead of exponentiation.

LUCELG Cryptosystem

In 1994 [9], the following cryptographic application of Lucas function an analogue to ElGamal cryptosystem was proposed.

The receiver chooses a prime p and the initial values P, and $Q=1$ which are publicized, chosen such that $P^2-4Q \mod p$ is a quadratic non-residue, and such that $V_{(p+1)/t}(P,Q) \not\equiv 2 \bmod p$, for all $t>1$ dividing $(p+1)$. Let us say Alice sends a message to Bob, so Bob (receiver) must choose the private key x, and publish the public key $y \equiv V_x(P,Q) \bmod p$.

A message m is an integer satisfying $1 \le m \le p-1$. To encrypt a message, Alice needs to choose a secret number k, which is an integer satisfying $1 \le k \le p-1$, calculates

$$G \equiv V_k(y,Q) \bmod p,\ e_1 \equiv V_k(P,Q) \bmod p$$

and $e_2 \equiv Gm \bmod p$. The encrypted message is the pair (e_1, e_2).

To decrypt the message, Bob needs to compute $V_x(e_1,Q) \equiv V_x(V_k(P,Q),Q^k) \equiv V_{kx}(P,Q) \equiv G \bmod p$ and the inverse of G. Then Bob can find the message m, because $m \equiv e_2 G^{-1} \bmod p$.

It is very important that Q is chosen so that $Q \equiv 1 \bmod p$; the recipient needs to know $Q^k \bmod p$ for the secret value k in order to compute $V_{kx}(P,Q)$ from $V_k(P,Q)$ using

$V_{ks}(P,Q) \equiv V_k(V_s(P,Q),Q^k)$. This problem can be solved by taking $Q \equiv 1 \bmod p$.

Let $\alpha = \frac{1}{2}\left(P + \sqrt{P^2 - 4Q}\right)$, and $\Delta = P^2 - 4Q$. Choose Legendre symbol $(\Delta / p) = -1$, then $O_{\Delta/P} \in F_{p^2}$, the finite field of p^2 element, via an isomorphism that we denote by φ_p. The condition $(\Delta / p) = -1$ is to make sure that one is working in the finite field $\mathbf{F}_p^2$ rather than $\mathbf{F}_p$.

Cramer-Shoup Cryptosystem

According to [1], we assume that we have a group G of prime order q, the plaintext are elements of G and use a universal one-way family of hash functions that map long bit strings to elements of Z_q.

The receiver, Bob picks $g_1, g_2 \in G$, $x_1, x_2, y_1, y_2, z \in Z_q$ and computes $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, $h = g_1^z$. Next, a hash function H is chosen from the family of universal one-way hash functions. The public key is (g_1, g_2, c, d, h, H) and the private key is (x_1, x_2, y_1, y_2, z).

Alice as the sender, chooses $k \in Z_q$ and calculates $u_1 = g_1^k, u_2 = g_2^k$, $e = h^k m$, $\alpha = H(u_1, u_2, e)$ and $v = c^k d^{k\alpha}$. The ciphertext is (u_1, u_2, e, v).

Before recovering the message, Bob computes $\alpha = H(u_1, u_2, e)$, and tests if $u_1^{x_1 + y_1\alpha} u_2^{x_2 + y_2\alpha} = v$. If this condition does not hold, the decryption output is 'reject'; otherwise, its output is $m = \frac{e}{u_1^z}$.

We first verify that this is an encryption scheme, in the sense that the decryption of an encryption of a message yields the message. Since $u_1 = g_1^k$ and $u_2 = g_2^k$, we have $u_1^{x_1} u_2^{x_2} = g_1^{kx_1} g_2^{kx_2} = c^k$. Likewise, $u_1^{y_1} u_2^{y_2} = d^k$ and $u_1^z = h^k$. Therefore, the test performed by the decryption algorithm will pass, and the output will be $\frac{e}{u_1^z} = m$.

Second Order Analogue of Cramer-Shoup

Analogous to Cramer-Shoup, we introduce a cryptosystem that uses the Lucas functions [6]. The receiver chooses a prime p, the initial alues P_1, P_2 and $Q = 1$. Let us say Alice is the sender and Bob is the receiver, so Bob must choose the private key $(x_1, x_2, y_1, y_2, z) \in F_{p^2}^*$ and compute

$$c \equiv V_{x_1}(P_1,1) \cdot V_{x_2}(P_2,1) \bmod p,$$
$$d \equiv V_{y_1}(P_1,1) \cdot V_{y_2}(P_2,1) \bmod p$$

and $h \equiv V_z(P_1,1) \bmod p$.

Here, Bob's public key is $(P_1, P_2, c, d, h, F_{p^2}^*)$ and his secret key is (x_1, x_2, y_1, y_2, z).

To encrypt a message, Alice must represent her message m as an integer such that $1 \le m \le p-1$, choose a secret k such that $1 \le k \le p-1$ and calculates

$$u_1 \equiv V_k(P_1,1) \bmod p,\ u_2 \equiv V_k(P_2,1) \bmod p,$$
$$G \equiv V_k(h,1) \bmod p \equiv V_k(V_z(P_1,1),1) \bmod p,$$
$$e \equiv Gm \bmod p,$$
$$\alpha \equiv H(u_1, u_2, e),\ v \equiv V_k(c,1) \cdot V_{k\alpha}(d,1) \bmod p$$

then, Alice sends the ciphertext (u_1, u_2, e, v) to Bob.

To decrypt the message, Bob use his private key to compute

$$m \equiv \frac{e}{V_z(u_1,1)} \bmod p \equiv \frac{Gm}{V_z(u_1,1)} \bmod p$$
$$\equiv \frac{V_k(V_z(P_1,1),1)}{V_z(V_k(P_1,1),1)} \cdot m \bmod p$$

Note:

Before recovering the message, Bob must use his private key (x_1, x_2, y_1, y_2) and the ciphertext (u_1, u_2) to formulate an equation that is equal to v. If this equation is not equal to v, the output is 'reject', otherwise we continue by calculating m. This method is similar to Cramer-Shoup cryptosystem.

Cubic Analogue of the Lucas Sequence

By analogy with the Lucas sequence, we consider the cubic equation

$$x^3 - Px^2 + Qx - R = 0$$

with roots α , β, γ and integer coefficients P,Q,R and define the following sequences of numbers:

$$V_n(P,Q,R) = \alpha^n + \beta^n + \gamma^n$$
$$U_n(P,Q,R) = \alpha^n + \omega\beta^n + \omega^2\gamma^n$$
$$W_n(P,Q,R) = \alpha^n + \omega^2\beta^n + \omega\gamma^n$$

where $\omega = \frac{1}{2}(-1+\sqrt{-3})$ is a cube root of unity. Then the sequences $(V)_n, (U)_n$ and $(W)_n$ all satisfy the linear recurrence with characteristic equation $X_{n+3} = PX_{n+2} - QX_{n+1} + RX_n$. All the V_n must be integers, as the first three of the numbers are integers, that is

$$V_0(P,Q,R)=3, V_1(P,Q,R)=P \text{ and } V_2(P,Q,R)=P^2-2Q.$$

We state some properties of the sequence $(V)_n$ which are straightforward consequences of the definition. **Proposition 2** is the rule for the composition of powers for the third order function. We omit the proofs.

Proposition 1 If α, β and γ are the roots of the equation $x^3 - Px^2 + Qx - R = 0$, then $V_k(Q,PR,R^2) = (\alpha\beta)^2 + (\alpha\gamma)^2 + (\beta\gamma)^2$

Proposition 2 If α, β and γ are the roots of the equation $x^3 - Px^2 + Qx - R = 0$, then

$$V_{nk}(P,Q,R) = V_n(V_k(P,Q,R), V_k(Q,PR,R^2), R^k)$$

Proposition 3 If α, β and γ are the roots of the equation $x^3 - Px^2 + Qx - R = 0$, then $V_k(Q,P,1) = V_{-k}(P,Q,1)$.

Corollary 1 If α, β and γ are the roots of the equation $x^3 - Px^2 + Qx - R = 0$, then $V_{nk}(P,Q,1) = V_n(V_k(P,Q,1), V_{-k}(P,Q,1), 1)$.

Corollary 2 $V_k^2 = 2V_{-k}(P,Q,1) + V_{2k}(P,Q,1)$.

From **Proposition 2**, the term $V_{ed}(P,Q,R)$ can be written as the d-*th* term of another sequence of functions defined by integers $V_e(P,Q,R)$, $V_e(Q,PR,R^2)$, and R^k that is

$$V_{ed}(P,Q,R) = V_d(V_e(P,Q,R), V_e(Q,PR,R^2), R^k).$$

If we let $R=1$ the expression can be simplified to

$$V_{ed}(P,Q,1) = V_d(V_e(P,Q,1), V_e(Q,P,1), 1)$$
$$= V_d(V_e(P,Q,1), V_{-e}(P,Q,1), 1).$$

Third Order Analog of Cramer-Shoup

The receiver chooses a prime p, the initial values P_1, P_2, Q_1, Q_2 and $R=1$. Let us say Alice is the sender and Bob is the receiver, so Bob must choose the private key $(x_1, x_2, y_1, y_2, z) \in F_{p^2}^*$ and compute

$$c \equiv V_{x_1}(P_1,Q_1,1) \cdot V_{x_2}(P_2,Q_2,1) \bmod p,$$
$$d \equiv V_{y_1}(P_1,Q_1,1) \cdot V_{y_2}(P_2,Q_2,1) \bmod p$$

and

$$h_1 \equiv V_z(P_1,Q_1,1) \bmod p$$
$$h_2 \equiv V_z(Q_1,P_1,1) \bmod p.$$

Here, Bob's public key is $(P_1,P_2,Q_1,Q_2,c,d,h,F_{p^2}^*)$ and his secret key is (x_1, x_2, y_1, y_2, z).

To encrypt a message, Alice must represent her message m as an integer such that

$1 \le m \le p-1$, choose a secret k such that $1 \le k \le p-1$ and calculates

$$u_1 \equiv V_k(P_1,Q_1,1) \bmod p, u_2 \equiv V_k(Q_1,P_1,1) \bmod p,$$
$$G \equiv V_k(h_1,h_2,1) \bmod p = V_k(V_z(P_1,Q_1,1),V_z(Q_1,P_1,1),1) \bmod p,$$
$$e \equiv Gm \bmod p,$$
$$\alpha \equiv H(u_1,u_2,e),\ v \equiv V_k(c,1) \cdot V_{k\alpha}(d,1) \bmod p.$$

Then, Alice sends the ciphertext (u_1,u_2,e,v) to Bob. To decrypt the message, Bob use his private key to compute

$$m \equiv \frac{e}{V_z(u_1,u_2,1)} \bmod p \equiv \frac{Gm}{V_z(u_1,u_2,1)} \bmod p$$
$$\equiv \frac{V_k(V_z(P_1,Q_1,1),V_z(Q_1,P_1,1),1)}{V_z(V_k(P_1,Q_1,1),V_k(Q_1,P_1,1)1)} \cdot m \bmod p\ .$$

Before recovering the message, Bob must use his private key (x_1,x_2,y_1,y_2) and the ciphertext (u_1,u_2) to formulate an equation that is equal to v. If this equation is not equal to v, the output is 'reject', otherwise we continue by calculating m. This method is similar to Cramer-Shoup cryptosystem.

Conclusion

The proposed cryptosystems use the second and third order linear recurrence relations in Cramer-Shoup cryptosystem, which is similar to the method to develop LUCELG. Our further research will examine the security and the efficiency of the proposed cryptosystems.

References

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

[2] Diffie, W. and Hellman, M.E. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, Vol. **22**, No 6, 644-654.

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

[4] Smith, P. and Lennon, M. 1993. LUC: A new public key system. *Proceedings, Ninth International Conference on Information Security ,IFIP/Sec.*

[5] Lucas, F.E.A. 1878. Theorie des functions numeriques simplement periodiques, *American Jnl Math.*, 1, 184-240,289-321.

[6] Muslim, N. and Said, M.R.M. 2006. A Cryptosystem Analogous to LUCELG, *Proceeding of the National Conference on Cryptology 2006, NCC06.*

[7] Rivest, L., Shamir, A. and Adleman, L. 1978. A method for obtain digital signatures and public key cryptosystem, *Communications of the ACM*, Vol. **21**, No 2, 120-126.

[8] Said, M.R.M. and John, L. 2003. 'A cubic analogue of the RSA cryptosystem', *Bulletin of the Australia Mathematical Society* **68**, 21-38.

[9] Smith, P. and Skinner, C. 1994. A public-key cryptosystem and a digital signature systems based on the Lucas function analogue to discrete logarithms. *Pre-proceedings Asia Crypt'94*, 298-306.