ISSN: 0128-7680
Pertanika J. Sci. & Technol. 13(1): 61 - 74 (2005)

A Cryptosystem Analogous to LUCELG and a Digital Signature Scheme

[1]Choo Mun Yoong & [2]Mohamad Rushdan Md Said
[1]Inti College Malaysia,
Jalan BBN12/1, Bandar Baru Nilai
71800 Nilai, Negeri Sembilan, Malaysia
[2]Institute for Mathematical Research and Department of Mathematics
Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
E-mail: cmyoong@yahoo.com, mrushdan@fsas.upm.edu.my

Received: 9 June 2003

ABSTRAK

ElGamal dan LUC adalah dua contoh sistem kripto awam. Berdasarkan kepada dua sistem ini, LUCELG dibangunkan dengan mengambil kira kekuatan kedua-dua sistem tersebut. Gabungan ElGamal dan sistem kripto beranalog kubik kepada RSA (LUC3) menghasilkan satu sistem kripto yang baru. Mengikut kaedah (Smith94), satu skema tandatangan digital dicadangkan. Aspek keselamatan sistem dikaji dan walaupun sistem-sistem ini bergantung pada kesukaran pemfaktoran atau masalah logaritma diskrit, namun sistem-sistem ini tidak boleh dibanding secara terus.

ABSTRACT

ElGamal and LUC are examples of a public-key cryptosystem. Based on these two systems, LUCELG that depends on the strength of the two systems was constructed. The combination of ElGamal and the cubic analogue of the LUC cryptosystem (LUC_3) produces a new public-key cryptosystem. Following (Smith94), a new digital signature scheme is proposed. The security aspects of the system are also looked into and although all these systems appear to depend on the intractability of factorization or of the discrete logarithm problem, the systems do not seem to be readily comparable.

Keywords: Public-key cryptosystem, lucas functions, encryption, decryption

PUBLIC-KEY CRYPTOSYSTEMS

Public-key cryptosystem is a concept invented by Diffie and Hellman (1976). They presented the concept but not the practical implementation of a system. Since 1976, numerous public-key systems have been proposed but many of these are insecure and impractical such as Knapsack public-key encryption and Merkle-Hellman knapsack encryption (Men). Only a few are secure and practical. One such example presented by Rivest *et al.* (1978) as a practical way to implement a public-key cryptosystem is the well-known RSA cryptosystem (RSA). Smith & Lennon (1993), following cryptographic application of Lucas function (Lucas), proposed an analogue to RSA, known as the LUC cryptosystem (Smith 93).

Let α, β be the roots of the quadratic equation

$$x^2 - Px + Q = 0.$$

Two particular solutions of the general second-order linear recurrence relation denoted by U_n and V_n, are defined by

$$V_n = \alpha^n + \beta^n$$

and

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

These are sequences of integers since we have:

$$U_0 = O, U_1 = 1, V_0 = 2, \text{ and } V_1 = P.$$

These sequences depend only on the integers P and Q, and the terms are called the Lucas functions of P and Q. They are sometimes written as $U_n(P,Q)$ and $V_n(P,Q)$, in order to show their dependence on P and Q. They were first discussed by Lucas (1878) and satisfy the second-order linear recurrence relations

$$V_n(P,Q) = PV_{n-1} - QV_{n-2} : U_n(P,Q) = PU_{n-1} - QU_{n-2}.$$

If N is any positive integer, then

$$V_n(P \bmod N, Q \bmod N) = V_n(P,Q) \bmod N$$
$$U_n(P \bmod N, Q \bmod N) = U_n(P,Q) \bmod N,$$

because this result is certainly true when n is 0 or 1, and for every n which is 2 or greater, we have

$$V_n(P \bmod N, Q \bmod N) = P \bmod N(V_{n-1}(P,Q) \bmod N) - Q \bmod N(V_{n-2}(P,Q) \bmod N).$$

Similarly

$$U_n(P \bmod N, Q \bmod N) = P \bmod N(U_{n-1}(P,Q) \bmod N) - Q \bmod N(U_{n-2}(P,Q) \bmod N).$$

If we take $Q = 1$, we then get the simple relationship

$$V_{nk}(P,1) = V_n(V_k(P,1),1).$$

This composition result is important as it is a clear generalization of the rule for composition of power, with the subscript of a Lucas function playing the role of a power, thus enabling Smith to construct an analogous system to RSA. He then went on to introduce an analogue to the ElGamal cryptosystem (Elg), naming it LUCELG (Smith94) and a digital signature system, LUCELG DS.

LUCELG PUBLIC-KEY SYSTEM

In LUCELG, the receiver chooses a prime p and the initial values P, and $Q = 1$ which are publicized such that $P^2 - 4Q \bmod p$ is a quadratic non-residue, and

$$V_{\frac{(p+1)}{t}}(P,Q) \not\equiv 2 \bmod p,$$

for all $t > 1$ dividing $(P + 1)$. Let us say Alice wants to send 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 m $p-1$. To encrypt a message, Alice needs to choose a secret number k, which is an integer satisfying 1 k p – 1, calculates $G \equiv Vk(y,Q) \bmod p$, $e_1 \equiv Vk(P,Q) \bmod p$ and $e_2 \equiv Gm \bmod p$. The encrypted message is the pair .

To decrypt the message, Bob needs to compute

$$Vx(e1,Q) \equiv Vx(Vk(P,Q),Qk) \equiv Vkx(P,Q) \equiv G \bmod p$$

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

$$V_{kx}(P,Q) = V_k(V_x(P,Q),Q^k)$$

This problem can be solved by taking $Q \equiv 1 \bmod p$.

Let $a = \frac{1}{2}\left[P + \sqrt{P^2 - 4Q}\right]$, and $\Delta = P^2 - 4Q$; 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 (Δ/p) is to make sure that one is working in the finite field $\mathbf{F}_{p^2}$ rather than $\mathbf{F}_p$. The condition that Vc(P,Q) $\neq 2 \bmod p$ for proper divisors c of $p + 1$ is to ensure that the multiplicative order of the image $\varphi_p(\alpha) \in F_{p^2}$ is equal to $p + 1$. If $\varphi_p(\alpha^n) = 1$ then $V_n(\alpha) \equiv 2 \bmod p$ and $U_n(\alpha)$, which does not happen for any proper divisor of $p + 1$ by this condition.

THE EXTENDED LUCAS FUNCTIONS

In [SL], Said and Loxton (2003) obtained two results, using the extended theory of the Lucas function by Lehmer (1930) [Leh], which were used to develop a public-key cryptosystem analagous to LUC. These are the higher order analogues of the two equations that were used in the LUC system: the extension of the rule for the composition of powers and the extension of Euler totient function for the elements of the sequence of the third order linear recurrence relation.

Let a, β, γ be the roots of the polynomial equation $x^3 - Px^2 + Qx - R = 0$. By analogy with the Lucas sequence and referring to the cubic equation above, the extended Lucas sequence of numbers are defined as

$$V_n(P,Q,R) = \alpha^n + \beta^n + \gamma^n,$$
$$U_n(P,Q,R) = \alpha^n + \omega\beta^n + w2\gamma^n$$
$$W_n(P,Q,R) = \alpha^n + \omega^2\beta^n + w\gamma^n,$$

where $\omega = \frac{1}{2}\left(-1+\sqrt{-3}\right)$ 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

$$V0(P,Q,R) = 3$$
$$V1(P,Q,R) = P$$

and

$$V_2(P,Q,R) = P^2 - 2Q.$$

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

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

Let N be a product of two distinct odd primes p and q. If we pick a number e such that $(e, \Phi(N)) = 1$, then we can solve

$$ed \equiv 1 \bmod \Phi(N)$$

for d where d is the inverse of e modulo $\Phi(N) = \overline{p}\ \overline{q}$ the function defined in [SL]. Therefore

$$\begin{aligned} V_d(V_e(P,Q,1),V_e(Q,P,1),1) &= V_{ed}(P,Q,1) \\ &= V_{k\Phi(N)+1}(P,Q,1) \text{ for some integer } k \\ &= P \bmod N \end{aligned}$$

and in a similar manner, we have

$$V_d(V_e(Q,P,1),V_e(P,Q,1),1) \equiv Q \bmod N.$$

A NEW PUBLIC-KEY CRYPTOSYSTEM

In this system, a prime p and the initial values of P, Q and R are publicized. Each user chooses a private key x, and publishes the public keys

$$\begin{aligned} y &\equiv V_x(P,Q,1) \bmod p \\ y' &\equiv V_x(P,Q,1) \bmod p \end{aligned}$$

A message m is an integer satisfying 1 m $p-1$. To encrypt the message for user, the sender needs to choose a secret k, such that 1 k $p-1$, and compute

$$\begin{aligned} G &\equiv V_k(y,y',1) \bmod p, \\ d_1 &\equiv V_k(P,Q,1) \bmod p, \\ d_2 &\equiv V_k(Q,P,1) \bmod p, \\ d_3 &\equiv Gm \bmod p. \end{aligned} \tag{1}$$

The encrypted message consists of (d_1,d_2,d_3). To decrypt the message, the user computes

$$\begin{aligned} V_x(d_1,d_2,1) &\equiv V_x(V_k(P,Q,1),V_k(Q,P,1),1) \bmod p \\ &\equiv V_{xk}(P,Q,1) \bmod p, \\ &\equiv G \end{aligned}$$

and then calculates G^{-1}. The extended Euclidean algorithm can be applied to calculate G^{-1}. He then inverts the result modulo p and recovers $m \equiv d_3 G^{-1} \bmod p$.

Example 1:
Let us choose a prime p = 101 and we will use small parameters for P, Q as an example. Suppose we take the initial values $P = 6$, $Q = 9$, $R = 1$; the equation of a cubic is $f(x) \equiv x^3 - 6x^2 + 9x - 1 \bmod 101$. Bob chooses a secret key, $x = 2$, and computes the values $V_2(6,9,1) = 18$ and $V_2(9,6,1) = 69$, and these values are the public keys. If Alice wants to send a message, she needs to choose a secret random key, $k = 3$. She then computes

$$\begin{aligned} G &\equiv V_k(V_x(P,Q,1),V_x(Q,P,1),1) \bmod 101 \\ &\equiv V_3(V_2(6,9,1)\,V_2(9,6,1),1) \bmod 101 \end{aligned}$$

$$\equiv V_3(18,69,1) \bmod 101$$
$$\equiv 2109 \bmod 101$$
$$\equiv 89$$

and

$$d_3 \equiv mV_3(18,69,1) \bmod 101$$
$$\equiv 100x(89) \bmod 101$$
$$\equiv 12$$

The encryption messages are $(V_3(6,9,1), V_3(9,6,1), d_3) = (57,570,12)$. If Bob wants to decrypt the encrypted message, he needs to compute

$$G \equiv V_2(V3(6,9,1)\, V_3(9,6,1),1) \bmod 101$$
$$\equiv V2(57,570,1) \bmod 101$$
$$\equiv 2109 \bmod 101$$
$$\equiv 89$$

and calculate for G^{-1}: Using the extended Euclidean algorithm, we get

$$89y \equiv 1 \bmod 101$$
$$101 = 89(1) + 12$$
$$89 = 12(7) + 5$$
$$12 = 5(2) + 2$$
$$5 = 2(2) + 1$$

Working from the bottom to the top

$$1 = 5 - (2)$$
$$= 5 - [12 - 5(2)](2)$$
$$= (5)5 - 12(2)$$
$$= (5)[89 - 12(7)] - - 12(2)$$
$$= (5)89 - 12(37)$$
$$= (5)89 - (37)[101 - 89(1)]$$
$$= (42)89 - (37)101,$$

and thus $G^{-1} = 42$. From equation (1),

$$d_3 \equiv Gm \bmod 101$$
$$m \equiv G^{-1}d_3 \bmod 101$$
$$\equiv 504 \bmod 101$$
$$\equiv 100$$

In conclusion, Bob can decrypt the message, $m = 100$ from Alice.

LUCELG DS DIGITAL SIGNATURE SCHEME

A signature scheme is a method of signing a message stored in electronic form. It consists of two components: a signing algorithm and a verification algorithm. Let us say Alice sends a message to Bob, after Bob has signed the message; he sends back the message to Alice to verify it. So, Alice then knows that Bob has received the message.

Now, let us see how Bob computes the signed message. Bob computes his 'signature' S for the M message using D_B:

$$S = D_B(M)$$

Then Bob encrypts S using E_A and sends $E_A(S)$ to Alice. He does not need to send M, because it can be computed from S. After getting the $E_A(S)$, Alice decrypts the ciphertext with D_A to get S. She knows who the sender of the signature is (in this case Bob). Later, Alice can obtain the message M with the encryption procedure of the sender, $M = EB(S)$, where $E_B(S)$ is available on the public file.

She can possess a message-signature pair which is similar to a signed paper document. Bob cannot deny sending this message to Alice, because no one else could create $S = D_B(M)$. To create $S = D_B(M)$, we need the secret key which is kept by Bob. Finally, Alice can confirm that Bob signed the document. And Alice cannot modify M, since she needs to create the corresponding signature $S = D_B(M')$ as well.

To sign a message, we need to satisfy some requirements. Let B be the recipient of a message M signed by A. Then A's signature must satisfy the following requirements:

- B must be able to validate A's signature.
- It must be impossible for anyone, including B, to forge A's signature.
- If A denies signing message M, it must be possible for a third party to resolve a dispute arising between A and B.

LUCELG DS

In this digital signature scheme [Smith94], two public key values are needed. They are

$$y \equiv V_x(P,1) \bmod p$$

and

$$y' \equiv U_x(P,1) \bmod p$$

Similarly, two values for the part of the signature are needed. A secret key k, must be chosen for each message, m.

$$r \equiv V_k(P,1) \bmod p$$

and

$$r' \equiv U_k(P,1) \bmod p.$$

The s component of the signature is calculated similar to ElGamal [Elg], except that the equation is solved modulo $(p+1)$ rather than modulo $(p-1)$. Using the extended Euclidean algorithm we can solve for s by using

$$s \equiv k^{-1}(m - xr) \bmod (p + 1) \tag{2}$$

To verify a LUCELG DS signature, we need to check

$$V_m \equiv Vs_{k+xr} \bmod p$$

that is the right hand side (RHS) must be the same with the left hand side(LHS). The left hand side

$$\text{LHS} \equiv Vm(P,1) \bmod p$$

The right hand side (RHS) equation is more complicated than in ElGamal. From the equation above we know that

$$2V_{sk+xr} \equiv V_{sk}V_{xr} + DU_{sk}U_{xr} \bmod p$$

$$RHS \equiv \frac{1}{2}\{V_r(y,1)\,V_s(r,1) + Dy'U_r(y,1)\,r'U_s(r,1)\} \bmod p \tag{3}$$

where

$$D \equiv P^2 - 4 \bmod p.$$

If RHS = LHS then the quadruple (m,r,r',s) is an authentic LUCELG DS signature.

A NEW DIGITAL SIGNATURE SCHEME

The main idea of the protocol described below is to generate a new digital signature scheme. In this scheme, two public-keys are necessary. The public-keys are set up as follow:

(i) Choose a large prime p of at least 512-bit length.
(ii) Choose a random number k in the range $1 \le k \le p$. A random key should be chosen for each message (or message block),
(iii) Choose as a document to be signed, where $0 \le m \le p$.

The public keys are

$$y \equiv V_x(P,Q,1) \bmod p, \text{ and } y' \equiv V_x(Q,P,1) \bmod p.$$

The Signing Procedure

The signing procedure of a message say, consists of the following steps:
Σ Alice computes a signing using a secret value key, x. Say Alice publishes the value $y \equiv V_x(P,Q,1) \bmod p$ and $y' \equiv V_x(Q,P,1) \bmod p$.
Σ User Alice chooses a random k with $\gcd(k, p+1)=1$, is a secret value. If k is chosen such that $\gcd(k, p+1)$, then the equation (2) has a solution for s. By the equation above, we have

$$r \equiv Vk(P,Q,1) \bmod p, \text{ and } r' \equiv Vk(Q,P,1) \bmod p$$

- Using the extended Euclidean algorithm, s can be solved by using

$$s \equiv k^{-1}(m - xr) \bmod (p+1). \tag{4}$$

- User Alice calculates the left hand side

$$Vm \equiv V_{xr+sk} \bmod p.$$

From the properties of the extended Lucas functions [SL], we have

$$3Vn+m \equiv V_n V_m + W_n U_m + W_m U_n \bmod p$$

thus

$$V_{xr+sk} \equiv \frac{1}{3}\{y,y',1)\, Vs(r,r',1)\, Wr(y,y',1)\, Us(r,r',1) + Ws(r,r',1)\, Ur(y,y',1)\, Ur(y,y',1)\} \bmod p \tag{5}$$

where

$$U_{sk} = U_s(V_k(P,Q,R),V_k(Q,P,1),1) = U_s(r,r',1)$$
$$W_{sk} = W_s(V_k(P,Q,R),V_k(Q,P,1),1) = W_s(r,r',1)$$
$$V_{sk} = V_s(V_k(P,Q,R),V_k(Q,P,1),1) = V_s(r,r',1)$$

This is the same as

$$U_{rx} = U_r(y,y',1)$$
$$W_{rx} = W_r(y,y',1)$$
$$V_{rx} = V_r(y,y',1)$$

Verification Procedure

To verify a signature (m,r,r',s), we examine whether

$$Vm \equiv V_{xr+sk} \bmod p$$

because $m \equiv xr + sk \bmod (p + 1)$. The right hand side (RHS) is more complicated than the LUCELG DS. If RHS = LHS, then the signature is valid.

Example 2:
Suppose Bob wants to sign the message $m = 5$, and he chooses the random value and the secret key $x = 2$, (note that gcd (3,8) = 1). The value for $P = 6$, $Q = 9$ and the function f is given by

$$f(x) = x^3 - 6x^2 + 9x - 1.$$

Let p be a prime, p = 7, and α, β, γ are roots of $f(x)$. By using the Cardan's formulae [Tig], we can calculate

$$\alpha = 2 + u + v$$
$$\beta = 2 + \omega u + \omega^2 v$$
$$\gamma = 2 + \omega^2 u + \omega v$$

where $u^3 = \frac{1}{2}(-1 + \sqrt{-3})$ and $v^3(-1 + \sqrt{-3})$. The public keys are

$$y \equiv V^2(6,9,1) \bmod 7$$
$$\equiv 18 \bmod 7$$
$$\equiv 4 \bmod 7$$

$$y \equiv V^2(9,6,1) \bmod 7$$
$$\equiv 69$$

Bob chooses the random value $k = 3$, and computes

$$r \equiv V3(6,9,1) \bmod 7$$
$$\equiv 57 \bmod 7$$
$$\equiv 1 \bmod.$$

$$r' \equiv V_3(9,6,1) \bmod 7$$
$$\equiv 570 \bmod 7$$
$$\equiv 3 \bmod 7.$$

and from equation (4), we know

$$s \equiv k^{-1}(m - xr) \bmod (p + 1)$$
$$\equiv 3^{-1}(5 - 2) \bmod 8$$
$$\equiv 3(3) \bmod 8$$
$$\equiv 1$$

To verify the signature $(m,r,r',s) = (5,1,3,1)$, we check whether

$$V_m \equiv V_{xr+sk} \bmod p.$$

To check the right hand side, from equation (5) we have

$$
\begin{aligned}
V_{xr+sk} &\equiv \frac{1}{3}\{V_r(y,y',1)\,V_s(r,r',1)\,W_r(y,y',1)\,U_s(r,r',1) \\
&\quad + \mathrm{Ws(r,r',1)Ur(y,y',1)} \bmod p \\
&\equiv \frac{1}{3}\{V_1(4,6,1)\,Vl(1,3,1)+W_1(4,6,1)\,U_1(1,3,1)\,W_1(1,3,1)\,U_1(4,6,1)\}\bmod 7 \\
&\equiv \frac{1}{3}\{V_1(18,69,1)\,V_1(57,570,1)+W_1(18,69,1)\,U_1(57,570,1) \\
&\quad + W_1(57,570,1)\,U_1(18,69,1)\} \bmod 7 \\
&\equiv \frac{1}{3}\{V_2(6,9,1)\,V_3(6,9,1)+W_2(6,9,1)\,U_3(6,9,1)+W_3(6,9,1)\,U_2(6,9,1)\}\bmod 7 \\
&\equiv \frac{1}{3}\{(\alpha^2+\beta^2+\gamma^2)(\alpha^3+\beta^3+\gamma^3)+(\alpha^2+\omega^2\beta^2+\omega\gamma^2)(\alpha^3+\omega\beta^3+\omega^2\gamma^3) \\
&\quad + (\alpha^3+\omega^2\beta^3+\omega\gamma^3)(\alpha^2+\omega\beta^2+\omega^2\gamma^2)\} \bmod 7 \\
&\equiv \{\alpha^5+\beta^5+\gamma^5+\alpha^2\beta^3+\alpha^2\gamma^3+\beta^2\alpha^3+\beta^2\gamma^3+\gamma^2\alpha^3+\gamma^2\beta^3\} \\
&\quad + \{\alpha^5+\beta^5+\gamma^5+\omega^2\alpha^2\beta^3+\omega\alpha^2\gamma^3+\omega\beta^2\alpha^3+\omega^2\beta^2\gamma^3+\omega^2\gamma^2\alpha^3+\omega\gamma^2\beta^3\} \\
&\quad + \{\alpha^5+\beta^5+\gamma^5+\omega\alpha^2\beta^3+\omega^2\alpha^2\gamma^3+\omega^2\beta^2\alpha^3+\omega\beta^2\gamma^3+\omega\gamma^2\alpha^3+\omega^2\gamma^2\beta^3\}\bmod 7 \\
&\equiv \alpha^5+\beta^5+\gamma^5 \bmod 7 \\
&\equiv 5.
\end{aligned}
$$

To check the left hand side, we calculate $V_m = V_5$. We know that $V_0 = 3$, $V_1 = 6$, $V_2 = 18$, and

$$
\begin{aligned}
V_3 &\equiv 6V_2 - 9V_1 + V_0 \bmod 7 \\
&\equiv 6(18) - 9(6) + 3 \bmod 7 \\
&\equiv 108 - 54 + 3 \bmod 7 \\
&\equiv 1 \bmod 7
\end{aligned}
$$

By using the same method, $V_4 \bmod 7 \equiv 4$, and

$$
\begin{aligned}
V_5 &\equiv PV_4 - QV_3 + V_2 \bmod 7 \\
&\equiv 6(4) - 9(1) + 18 \bmod 7 \\
&\equiv 5 \bmod 7
\end{aligned}
$$

Since $V_5 \equiv V_{xr+sk} \bmod 4$, so the quadruple (5,1,3,1) of Bob signature is an authentic signature.

CRYPTOGRAPHIC STRENGTH

There are two ways to discuss the security of a cryptosystem. These are computational security and unconditional security. We call a cryptosystem 'computationally secure' if the best-known method of breaking the cryptosystem needs a large amount of computer time, such as Shift Cipher and Substitution

Cipher. Another approach is to give some evidence of computational security by reducing the security of the cryptosystem to some difficult problems. We know that RSA and its variants depend on the intractability of factorization but this only provides a proof of security relative to some other problems, not an absolute proof of security. The same is true for LUCELG and the proposed system which depend on the intractability of the discrete logarithm problem. A cryptosystem is defined to be 'unconditionally secure' if it cannot be broken, even with infinite computational resources.

Randomized Encryption

The proposed cryptosystem is a randomized encryption. The randomized encryption techniques increases the cryptographic security of an encryption process through the following methods [Men]:

- Increasing the effective size of the plaintext message space.
- Decreasing the effectiveness of chosen plaintext attacks by virtue of a one to many mappings of plaintext to ciphertext.
- Decreasing the effectiveness of statistical attack by leveling the *a priori* probability distribution of inputs.

Discrete Logarithm Problem

The discrete logarithm problem (DLP) is the following [Men]: given a prime p, a generator α of Z_p^* and an element $\beta \in Z_p^*$, find the integer x, $0 \quad x \quad p-2$, such that $ax \equiv \beta \bmod p$.

The best algorithm for solving the Discrete Logarithm (DLP) problem relies on combining congruences multiplicatively [Smith94]. This cannot be done with extended Lucas functions because extended Lucas functions are not closed under multiplication. Hence these subexponential algorithms cannot be applied to our proposed system. Breaking the system is equivalent to solving for x in equation $V_x(P,Q,1)$, where P, C and p are known. To find Vx(P,Q,1) we need to compute $(\alpha^2+\beta^2+\gamma^2)$, $(\alpha^3+\beta^3+\gamma^3)$,... and therefore inefficient if x is large.

The most powerful method for computing discrete logarithms is the index-calculus algorithm. This algorithm cannot be applied to the proposed encryption algorithm. But let us see how the index-calculus method works to ElGamal cryptosystem [Stin]. The method uses a factor base, which is a set B of 'small' prime. Suppose B = $\{p1,p2,...,p_B\}$. The first step is to find the logarithms of the B primes in factor base. The second step is to compute a discrete log of element β. We construct $C = B + 10 \bmod p$,

$$\alpha^{Xj} \equiv P_1^{A1j} P_2^{A2j} \ldots P_B^{ABj} \bmod p$$

with $1 \quad j \quad C$, and

$$X_j \equiv A_{1j} log_\alpha P_1 + A_{2j} log_\alpha P_2 + \ldots + A_{Bj} log\alpha P_B \bmod p - 1.$$

Then we take the random value x, compute $\alpha^x \bmod p$, and then determine if

$\alpha^s \bmod p$ has all its factors in B. If we have successfully carried out the precomputation step, we choose a random integer, s where $(1 \leq s \leq p-2)$ and compute

$$y \equiv m\alpha^s \bmod p$$

Factor y over the factor base B. If this can be done, we obtain a congruence of the form

$$m\alpha^s \equiv P_1^{A1j} P_2^{A2j} \ldots P_B^{ABj} \bmod p$$

This can be written equivalently as

$$(log_\alpha m) + s \equiv A_{1j} log_\alpha P_1 + A_{2j} log_\alpha P_2 + \ldots + A_{Bj} log\ \alpha P_B \bmod p - 1.$$

since everything is known, except $log_\alpha m$. But this cannot apply to the proposed system because we have $(\alpha^s + \beta^s + \gamma^s)$

CONCLUSIONS

The proposed system is a combination of ElGamal and the cubic analogue of the RSA cryptosystem. The security of this cryptosystem, as does LUCELG, depends on the intractability of the discrete logarithm problem. Further research can be continued to discuss the complexity of the algorithms and the efficiency of the proposed cryptosystem. Other aspects of security could also be investigated.

REFERENCES

DIFFIE, W. and M.E. HELLMAN. 1976. New directions in cryptography. *IEEE Transactions on Information Theory* **IT-22(6):** 644-654.

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

LEHMER, D.H. 1930. An extended theory of Lucas functions. *Annals of Math:* 419-448.

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

MENEZES, A., P.V OORSCHOT and S. VANSTORE. *HandBook of Applied Cryptography.* Boca, Raton, London: Tokyo CRC Press.

RIVEST, L., A. SHAMIR and L. ADLEMAN. 1978. A method for obtain digital signatures and public key cryptosystem. *Communications of the ACM* **21(2):** 120-126.

SAID, M.R.M. and J. LOXTON. 2003. A cubic analogue of the RSA cryptosystem. *Bulletin of The Australian Mathematical Society* **68:** 21-38.

SMITH, P. and M. LENNON. 1993. LUC: A new public key system. In *Ninth IFIP Symposium on Computer Security* ed. E. G. Douglas, pp. 103-117. Elsevier Science Publishers.

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

STINSON, R.D. 1990. *Cryptography: Theory and Practice.* Boca Raton, FL: CRC Press.

SHANNON, C. E. 1949. Communication theory of secrecy system. *Bell Syst. Tech. J.* **28:** 656-715.

SHANNON, C.E. 1984. A mathematical theory of communication. *Bell Syst. Tech. J.* **27:** 379-423 (July),623-656 (Oct.) .

TIGNOL, J.P. 1988. *Galois' Theory of Algebraic Equations.* Longman Group UK Limited.