Efficient Lucas Public-Key Cryptosystems

Guang Gong & Lein Harn
Department of Computer Networking
University of Missouri - Kansas City
Kansas City, MO 64110
TEL:(816)235-2367
FAX:(816)235-5159
Email:HARN@CSTP.UMKC.EDU

Abstract

The Lucas sequence (or equivalently, Dickson polynomial) has important applications in cryptology. In the first part of this paper, we will investigate distribution properties of Lucas sequences over $GF(p)$ where p is a prime, and over Z_n where n is a product of two primes. We will show that all elements of the Lucas sequence can be classified into two disjoint subsets according to their Legendre symbols. In the second part, we will show how to utilize those distinct properties of Lucas sequences to design Lucas public-key cryptographic algorithms. The performance of these cryptosystems is more efficient than cryptosystems based on the exponential function.

I. Introduction

The exponential function has played an important role in most public-key cryptosystems, such as the RSA scheme [1], the Diffie-Hellman public-key distribution scheme [2], the ElGamal scheme [3], the DSA [4], etc. For an exponential function over Z_n, we can write $f_\alpha(x)=\alpha^x$ $,x\in Z_n$, where α is a fixed element in Z_n. The element α^x can be regarded as the xth term in the linear recurring sequence with the minimal polynomial $f(x)=x-\alpha$ and the initial state is 1. Here we list some well-known properties of the exponential function:

(i) α^x satisfies a commutative law: $\alpha^{xy}=\alpha^{yx}$, $x,y\in Z_n$.

(ii) Homomorphism: $\alpha^{x+y}=\alpha^x\alpha^y$.

(iii) If n is a prime number, we write p instead of n. Given $\alpha, b\in Z_p$ and $a^x=b$, where x is an unknown variable in Z_p, then solving the exponent x is equivalent to solve the discrete logarithm in Z_p. It can be solved in time $L_p[1/3;\ (64/9)^{1/3}+O(1)]$, for $p\rightarrow\infty$, where $L_p[u,v]=\exp(v(\log p^u(\log\log p)^{1-u})$ [5].

(iv) Let the order of α be t. Then α^x is a one-to-one and onto (bijective) map from $S=\{0,1,\ldots,t-1\}$ to $\{\alpha^x|x\in S\}$.

Property (i) has been used in the Diffie-Hellman public-key distribution scheme, property (ii) has been used in the ElGamal digital signature scheme, property (iii) has been used for building a one-way trapdoor function, and property (iv) has been used for ensuring the system's maximal security especially when the order t is a large integer.

In 1984, Muller and Nobauer [6-7] proposed public-key cryptosystems based on Lucas sequences (or equivalently, Dickson polynomials) over Z_n. Smith [8-9] improved Muller and Nobauer's public-key systems in 1993. Since then, a series of papers [10-15] studied Lucas sequences and their applications in cryptology.

A Lucas sequence can be represented as $V=\{V_k\}_{k\geq 0}$ which elements are given by

$$V_k=\xi V_{k-1}-V_{k-2},\ n\geq 2,\ \text{in } Z_n \qquad (1)$$

with $\xi\in Z_n$, $V_0=2$, and $V_1=\xi$ [6]. We also denote V as V(ξ). A Lucas sequence in Z_n is a 2nd-order linear recurring sequence over Z_n with the minimal polynomial $f(x)=x^2-\xi x+1$ and the initial state $(V_0,V_1)=(2,\xi)$. We also list similar properties of the Lucas sequence:

(i) The index function of a Lucas sequence satisfies a commutative law [6]: $V_x(V_y(\xi))=V_{xy}(\xi)=V_y(V_x(\xi))$.

(ii) $V_{x+y} = V_x V_y - V_{x-y}$

(iii) Given ξ, $\beta \in Z_n$ and $V_k(\xi) = \beta$ where k is an unknown variable, we define the discrete index problem as to solve the index k in the equation $V_k(\xi) = \beta$. Suppose that n is a prime number and $f(x) = x^2 - \xi x + 1$ is a reducible polynomial over $GF(p)$, then solving the discrete index problem can be changed into solving the discrete logarithm problem in $GF(p)$ [13]. If $f(x) = x^2 - \xi x + 1$ is an irreducible polynomial over $GF(p)$, then solving the discrete index problem can be changed into solving the discrete logarithm in $GF(p^2)$. According to the reference [13], the best scheme to solve the discrete logarithm in $GF(p^2)$ needs running time $Lp[1/3; (128/9)^{1/3} + O(1)]$.

By comparing these basic properties, we can say that if the index function of Lucas sequence has the same bijective property as the exponential function, all cryptographic systems based on the exponential function can be converted into cryptosystems based on the Lucas sequence. Unfortunately, the bijective property of the Lucas sequence has never been discussed in the open literature.

In section II, we will prove that the index functions of the Lucas sequence $\mathrm{V}(\xi)$ over $GF(p)$ with period t is a bijective map from $S = \{0, 1, \ldots, \lfloor t/2 \rfloor\}$ to $\{V_x(\xi) | x \in S\}$. Therefore the index function of Lucas sequence over $GF(p)$ is a bijective map if we only consider elements in the first half period (we call the "folding period" of the Lucas sequence). We will also investigate distribution properties of Lucas sequences over Z_n where n is a product of two primes. We will show that all elements of the Lucas sequence can be classified into two disjoint subsets according to their Legendre symbols.

The evaluation of the Lucas function $(V_x(m), V_{x+1}(m))$ needs $2\log_2 n$ multiplications [7,8], where n is the modulus. On the other hand, the evaluation of the exponential function m^x needs $1.5\log_2 n$ multiplications. In order to improve the efficiency of Lucas-type cryptosystems, we should realize that Lucas sequence is generated by an irreducible polynomial of degree 2 and we should utilize a state, which consists of two consecutive elements, instead of just a single element. Unfortunately, all current-existing Lucas-type cryptosystems only utilize a single element each time. Thus, these Lucas-type schemes are less efficient than schemes based on exponential functions, such as the RSA scheme and the ElGamal scheme. In section III, we propose Lucas public-key cryptographic schemes which utilize two elements. These proposed schemes are more efficient than schemes based on the exponential function. In addition, we show that Lucas function is the most suitable candidate for designing cryptosystems based on two different security assumptions.

Remark. Reader is referring to see [16] for some basic theories of finite fields and linear recurring sequences over finite fields .

II. Distribution Properties of Lucas Sequences

Since Lucas sequences over $GF(p)$ are 2nd-order linear recurring sequences over $GF(p)$, we will take a different approach to investigate the distribution properties of Lucas sequences. The following Theorem states a relationship between elements in $GF(p^2)$ and coefficients of the minimal polynomial of Lucas sequence over $GF(p)$.

Theorem 1. Let ω be a primitive element of $GF(p^2)$ and $f(x) = x^2 - \xi x + 1 \in \mathrm{Z}_p[x]$. Then, it is either

Case 1. the polynomial $f(x)$ is reducible over $GF(p)$ and $\xi \neq \pm 2$ if and only if

$$\xi = \alpha + \alpha^{-1} \text{ where } \alpha = \omega^{r(p+1)} (0 < r < p-1); \quad (2)$$

or

Case 2. the polynomial $f(x)$ is irreducible over $GF(p)$ if and only if

$$\xi = \beta + \beta^{-1} \text{ where } \beta = \omega^{s(p-1)} \ (0 < s < p+1). \quad (3)$$

Proof.

Case 1. Suppose that (2) is true. Since $\alpha^{p-1} = \omega^{r(p+1)(p-1)} = 1$, we have $\alpha \in GF(p)$, and $f(x) = (x-\alpha)(x-\alpha^{-1})$. So $f(x)$ is reducible over $GF(p)$.

If $f(x)$ is reducible over $GF(p)$ and we let α_i, i =1, 2, be two roots of $f(x)$ in $GF(p)$, we have

$\xi = \alpha_1 + \alpha_2$ and $\alpha_1\alpha_2 = 1$. Consequently $\alpha_2 = \alpha_1^{-1}$. Since $\alpha_1 \in GF(p)$, and ω^{p+1} is a primitive element of $GF(p)$, there exists a positive integer r such that $\alpha_1 = \omega^{r(p+1)}$.

Case 2. Suppose that (3) is true. Since $\beta = \omega^{s(p-1)}$, we have $\beta \notin GF(p)$. This concludes that $f(x)$ is irreducible over $GF(p)$.

If $f(x)$ is irreducible over $GF(p)$ and we let β_i , i =1, 2, be roots of $f(x)$ in the extension $GF(p^2)$ of $GF(p)$, we have $\xi = \beta_1 + \beta_2$ and $\beta_1\beta_2 = 1$. These two roots of $f(x)$ are conjugate with respect to $GF(p)$. We can write $\beta_2 = \beta_1^p$. So $\beta_1^{p+1} = 1$. Thus the order of β_1 divides p + 1. Since $\omega^{p-1}$is an element with order p + 1 in $GF(p^2)$, then there exists a positive integer $s \in \{1,\ldots,p\}$ such that $\beta_1 = \omega^{s(p-1)}$. Q.E.D.

Lemma 1. Let $\mathbb{V}(\xi)$ and $\mathbb{V}(\zeta)$ be two Lucas sequences over $GF(p)$ with periods $p-1$ and p +1 respectively, then $V_{(p-1)/2}(\xi) = V_{(p+1)/2}(\zeta) = -2$.

Proof. Let ω be a primitive element of $GF(p^2)$, $\alpha = \omega^{p+1}$ and $\beta = \omega^{p-1}$. From Theorem 1, we can write

$$V_k(\xi) = \alpha^k + \alpha^{-k},\ \xi = \alpha + \alpha^{-1},\ k = 0,1,\ldots \qquad (4)$$

$$V_k(\zeta) = \beta^k + \beta^{-k},\ \varsigma = \beta + \beta^{-1},\ k = 0,1,\ldots \qquad (5)$$

Since $\omega^{\pm(p^2-1)/2} = -1$, we have

$$\begin{aligned} V_{(p-1)/2}(\xi) &= \alpha^{(p-1)/2} + \alpha^{-(p-1)/2} \\ &= \omega^{(p+1)(p-1)/2} + \omega^{-(p+1)(p-1)/2} \\ &= \omega^{(p^2-1)/2} + \omega^{-(p^2-1)/2} = -2 \end{aligned}$$

Similarly, we have $V_{(p+1)/2}(\zeta) = -2$. Q.E.D.

From the proof of the above Lemma, we have the following result immediately.

Corollary 1. For any Lucas sequence $\mathbb{V}(\xi)$ over $GF(p)$ with period t, we have $V_{\lfloor t/2\rfloor}(\xi) = -2$.

Lemma 2. With notations in Theorem 1 and Lemma 1, letting

$IR = \{\omega^{(p-1)i} + \omega^{-(p-1)i} \mid 1 \le i < (p+1)/2\}$ and $R = \{\omega^{(p+1)i} + \omega^{-(p+1)i} \mid 1 \le i < (p-1)/2\}$,

then $GF(p) = IR \cup R \cup \{2,-2\}$.

Proof.

For $\xi \in GF(p)$ and $\xi \ne \pm 2$, we construct a polynomial $f(x) = x^2 - \xi x + 1$.

(i) If $f(x)$ is reducible over $GF(p)$, according to Theorem 1, there exists a positive integer r with $0 < r < p-1$, such that $\xi = \omega^{(p-1)r} + \omega^{-(p-1)r}$. Notice that

$$\omega^{(p+1)i} + \omega^{-(p+1)i} = \omega^{(p+1)(p+1-i)} + \omega^{-(p+1)(p+1-i)},\quad 0 < i < (p-1)/2. \qquad (6)$$

Therefore we can write

$$\xi = \omega^{(p+1)r} + \omega^{-(p+1)r},\ 0 < r < (p-1)/2,$$

which shows that $\xi \in R$.

(ii) If $f(x)$ is irreducible over $GF(p)$, and since

$$\omega^{(p-1)i} + \omega^{-(p-1)i} = \omega^{(p-1)(p-1-i)} + \omega^{-(p-1)(p-1-i)},\quad 0 < i < (p+1)/2. \qquad (7)$$

Similarly, we can write

$$\xi = \omega^{(p-1)r} + \omega^{-(p-1)r},\ 0 < r < (p+1)/2,$$

which gives $\xi \in IR$.

By combing (i) and (ii), we have

$$\forall \xi \in GF(p) \Rightarrow \xi \in IR \cup R \cup \{2,-2\}.$$

That's
$$GF(p) \subset IR \cup R \cup \{2,-2\}. \qquad (8)$$

Since $|R| \le (p-1)/2 - 1$ and $|IR| \le (p+1)/2 - 1$, then

$$|IR \cup R \cup \{2,-2\}| \le |IR| + |R| + 2$$
$$\le \frac{p+1}{2} - 1 + \frac{p-1}{2} - 1 + 2 = p = |GF(p)|. \qquad (9)$$

Together with (8) yields that

$$GF(p) = IR \cup R \cup \{2,-2\}.$$

Q.E.D.

Let QR_p represents the set of all integers between 1 and p - 1 that are quadratic residue modulo p, and QNR_p represents the set of all integers between 1 and p - 1 that are quadratic nonresidue modulo p. The Legendre symbol is defined as $J(a/p)$ =1 if $a \in QR_p$ or $J(a/p)$ = -1 if $a \in QNR_p$. From Lemma 2 and Theorem 1, the following result comes immediately.

Theorem 2. With notations in Lemma 2, we have

(i) $R \cap IR = \varnothing$.

(ii) $\xi \in R \Leftrightarrow J\left(\dfrac{\xi^2-4}{p}\right)=1 \Leftrightarrow$

$f(x)=x^2-\xi x+1$ is reducible over *GF*(*p*)

$\Leftrightarrow per(\mathrm{V}(\xi)) \mid p-1$.

(iii) $\xi \in IR \Leftrightarrow J\left(\dfrac{\xi^2-4}{p}\right)=-1$

$\Leftrightarrow f(x)=x^2-\xi x+1$ is irreducible over *GF*(*p*) $\Leftrightarrow per(\mathrm{V}(\xi)) \mid p+1$.

Corollary 2. Let $\mathrm{V}(\xi)$ be a Lucas sequence over $GF(p)$ with period *t*. Then

$$\pi\colon k \rightarrow V_k(\xi),\ k=0,1,\ldots,\left\lfloor \frac{t}{2} \right\rfloor$$

is a bijective map from $S=\{k \mid k=0,1,\ldots,\lfloor t/2 \rfloor\}$ to $L=\{V_k(\xi) \mid k \in S\}$.

Proof. We only need to prove $V_k(\xi) \neq V_{k'}(\xi)$ for $0 \le k \neq k' \le \lfloor t/2 \rfloor$.

Case 1. $t \mid p$ -1. Thus the minimal polynomial $f(x)=x^2-\xi x+1$ of $\mathrm{V}(\xi)$ is reducible over $GF(p)$. From Theorem 1, we can write $\xi=\omega^{(p+1)r}+\omega^{-(p+1)r}$, $0<r<(p-1)/2$. Thus elements of $\mathrm{V}(\xi)$ can be represented as

$$V_k(\xi)=\alpha^k+\alpha^{-k}, \text{ where } \alpha=\omega^{(p+1)r},$$
$$0<r<(p-1)/2.$$

Consequently, $V_k(\xi) \in R \cup \{2,-2\}$ for any k with $0 \le k \le \lfloor t/2 \rfloor$. From Theorem 2 - (i),

$$V_k(\xi) \neq V_{k'}(\xi) \text{ if } 0 \le k \neq k' \le \lfloor t/2 \rfloor. \quad (10)$$

Case 2. $t \mid p$ + 1. Similarly, by using Theorem 1 and Theorem 2 - (i), we have $L \subset IR \cup \{2,-2\}$ which implies (10) is also true. Q.E.D.

Remark. If V is a Lucas sequence over Z_n with period *t*, then $V_k = V_{t-k}$, $0 < k < \lfloor t/2 \rfloor$ (see [15]). Together with Corollary 2, we have the following corollary.

Corollary 3. For any Lucas sequence V over *GF*(*p*), each element in *GF*(*p*) either appears two times exactly in one period of V or doesn't appear.

Corollary 4. Let $\mathrm{V}(\xi)$ and $\mathrm{V}(\zeta)$ be two Lucas sequences over *GF*(*p*) with the same period *t*. Let $L(z)=\{V_k(z) \mid 0 \le k \le \lfloor t/2 \rfloor\}$, then

$$L(\xi)=L(\zeta).$$

They are either a subset of *IR* or *R* .

Proof. From Remarks of Theorem 1 and Corollary 2, the result comes immediately.

Next we want to generalize Corollary 2 to Lucas sequences over Z_n.

Theorem 3. Let $\mathrm{V}(\xi)$ be a Lucas sequence over Z_n with period *t*, where $n=pq$ and p, q are two primes, $S=\{k \mid k=1,1,2,\ldots,\lfloor t/2 \rfloor\}$ and $L=\{V_k(\xi) \mid k \in S\}$. For the following map from S to L

$$\pi\colon k \rightarrow V_k(\xi),\ k \in S$$

there has at most two different *k* and *k*' in S such that $V_k(\xi)=V_{k'}(\xi)$.

Corollary 5. We use same notations as in the Theorem 3 and let $T=\{0,1,2,\ldots,p+q\}$, then

$$\pi\colon k \rightarrow V_k(\xi),\ k \in T$$

is a bijective mapping.

Above results can be derived based on the Corollary 2 and the Chinese Remainder Theorem . The proof will be given in the full paper.

III. Efficient Lucas Public-Key Cryptosystems

Generally speaking, there are two types of Lucas cryptosystems. The first type of Lucas system is over Z_p, where p is a large prime. Thus, it is the extension of the well-known Diffie-Hellman [2] or ElGamal cryptosystem [3]. The second type od Lucas cryptosystem is over Z_n, where n is the product of two large primes. Thus, it is the extension of the well-known RSA cryptosystem [1]. In the following, we will show how to utilize those distinct properties of Lucas sequences that we have derived in section II to design Lucas-type public-key cryptographic algorithms. The performance of these cryptosystems is more efficient than cryptosystems based on the exponential function.

A . *Diffie-Hellman-type Lucas Public-Key Distribution Scheme over Z_n*

Diffie-Hellman-type public-key distribution scheme based on Lucas sequences was proposed by Smith [11] in 1994. But, this scheme is less efficient than the original Diffie-Hellman scheme [2].

Proposed scheme: In our Diffie-Hellman-type scheme, there are public parameters (n, ξ), where $n = pq$, p and q are two large primes randomly selected by a trusted party, and $f(x) = x^2 - \xi x + 1$ is a polynomial over Z_n. The trusted party can destroy these p and q after publishing the parameter n. Each user i needs to randomly select a secret key $x_i \in [1, n-1]$ and to compute a public key $y_i = (V_{x_i}(\xi), V_{x_i+1}(\xi))$.

Let us assume that users A and B want to share a common secret key $K_{A,B}$. Then A needs to access B's public key $y_B = (V_{x_B}(\xi), V_{x_B+1}(\xi))$ and to use his secret key x_A to compute $(V_{x_A}(V_{x_B}(\xi)), V_{x_A+1}(V_{x_B}(\xi)))$ and $(V_{x_A}(V_{x_B+1}(\xi)), V_{x_A+1}(V_{x_B+1}(\xi)))$. Similarly, B needs to access A's public key $y_A = (V_{x_A}(\xi), V_{x_A+1}(\xi))$ and to use his secret key x_B to compute $(V_{x_B}(V_{x_A}(\xi)), V_{x_B+1}(V_{x_A}(\xi)))$ and $(V_{x_B}(V_{x_A+1}(\xi)), V_{x_B+1}(V_{x_A+1}(\xi)))$.

Theorem 4: The common secret key between A and B is $K_{A,B} = (K_1, K_2, K_3, K_4)$, where

$$K_1 = V_{x_A}(V_{x_B}(\xi)) = V_{x_B}(V_{x_A}(\xi)),$$
$$K_2 = V_{x_A+1}(V_{x_B}(\xi)) = V_{x_B}(V_{x_A+1}(\xi)),$$
$$K_3 = V_{x_A}(V_{x_B+1}(\xi)) = V_{x_B+1}(V_{x_A}(\xi)),$$

and $K_4 = V_{x_A+1}(V_{x_B+1}(\xi)) = V_{x_B+1}(V_{x_A+1}(\xi))$.

Proof: It is obvious. Q.E.D.

Security: Since all computations are over Z_n, these four subkeys (K_1, K_2, K_3, K_4) are all independent without knowing secret primes p and q.. The security of this proposed scheme is based on the factoring problem. Complete discussion of the security will be given in the full paper.

Discussion: According to [13], the factoring problem over Z_n and the discrete logarithm problem over Z_p have the same level of security if the sizes of p and n are the same. We need to point out that, in our scheme, the size of the common secret key is $4\log_2 n$ bits; but in the original Diffie-Hellman scheme, the size of the common secret key is $\log_2 p$ bits.

B. *RSA-type Lucas Public-Key Cryptosystem Over Z_n*

In 1984, Muller and Nobauer [6, 7] proposed public-key cryptosystems based on Lucas sequences (or equivalently, Dickson polynomials) over Z_n, where n is the product of two large primes. Smith [8, 9] improved Muller and Nobauer's public-key system in 1993.

In Muller and Nobauer scheme, the receiver has secret keys (p, q, d) and public keys (n, e), where $n = pq$, p and q are two large primes, $ed \bmod \ell(n) = 1$, $\ell(n) = (p-1)(p+1)(q-1)(q+1)$, To send an encrypted message to the receiver the ciphertext is $c = V_e(m)$ in Z_n. The ciphertext can be recovered by the intended receiver by computing $V_d(V_e(m)) = V_{de}(m) = V_1(m) = m$ in Z_n. The problem of this algorithm is that in order to satisfy the equation $ed \bmod \ell(n) = 1$ the deciphering key becomes too large. Thus, it slows down the deciphering speed.

In 1993, Smith [8, 9] realized that the size of the deciphering key can be reduced by selecting four message-dependent deciphering keys as $ed_i \equiv 1 \bmod R_i$ $(1 \le i \le 4)$ where R_i $(1 \le i \le 4)$ are given in Table 1. Notice that the period of the Lucas sequence $V(m)$ over Z_n is a factor of one of numbers R_i, $1 \le i \le 4$. Smith deciphering algorithm needs to compute four values

$$V_{d_i}(V_e(m)) = V_{d_ie}(m) = m_i,\ 1 \le i \le 4,$$

then determine which one is the right message m according to a specific format. The problem of this algorithm is that it needs to repeat the same deciphering procedure four times.

Proposed scheme: First, we would like to show how to utilize Theorem 2 and Corollary 4 that we have derived in section II to speed up the deciphering process by four times.

From Theorem 2-(ii), -(iii) and Corollary 4, we know that Legendre symbols of m^2-4 and $\left(V_e(m)\right)^2-4$ for both primes p and q are the same. Thus, the intended receiver can use the ciphertext $V_e(m)$ to determine the periods of both $V_e(m)$ mod p and $V_e(m)$ mod q instead of using the message m. Therefore the proper deciphering key can be determined uniquely in terms of the ciphertext. We list this procedure in Table 1. For example, if

$$J\left(\frac{\left(V_e(m)\right)^2-4}{p}\right)=1 \text{ and } J\left(\frac{\left(V_e(m)\right)^2-4}{q}\right)=-1,$$

then the decipher key is d_2. i.e.,

$$V_{d_2}\left(V_e(m)\right)=V_{d_2e}(m)=V_1(m)=m.$$

So this approach speeds up Smith's deciphering algorithm four times.

We assume that the receiver has secret keys (p,q,d_1,d_2,d_3,d_4) and public keys (n, e), where $n = pq$, p and q are two large primes, $ed_i \equiv 1 \bmod R_i$ $(1 \le i \le 4)$, where $R_i(\ 1 \le i \le 4)$ are given in Table 1. To send an encrypted message $m=(m_1,m_2)$ to the receiver, the ciphertext is computed as

$m_{12}=m_1 \oplus m_2$, where $\oplus$ is the exclusive-or operation

$$\left(V_e(m_{12}), V_{e+1}(m_{12})\right),$$

$$c_1=V_e(m_{12}), \text{ and}$$

$$c_2=V_{e+1}(m_{12})\cdot m_1.$$

We want to point out that all computations are computed in Z_n. Ciphertext $c=(c_1,c_2)$ is sent to the intended receiver.

To decrypt the ciphertext $c=(c_1,c_2)$, the receiver uses his secret key (p, q) to determine Legendre symbols of both $J(\frac{c_1^2-4}{p})$ and $J(\frac{c_1^2-4}{q})$. Then, according to Table 1, the receiver selects a proper deciphering key d_i such that $ed_i \equiv 1 \bmod R_i$ and computes

$$\left(V_{d_i}(c_1), V_{d_i+1}(c_1)\right),$$

$$m_{12}'=V_{d_i}(c_1),$$

$$m_1'=\left(V_{d_i+1}(c_1)\right)^{-1}\cdot c_2, \text{ and}$$

$$m_2'=m_{12}\oplus m_1'.$$

Theorem 5: $(m_1',m_2')=(m_1,m_2)$.
Proof: it is obvious. Q.E.D.

Discussion: In the encryption (or decryption) operation, each encryption can encrypt $2\log_2 n$-bit message. Thus, it requires 1 multiplication per 1-bit message. The RSA scheme requires 1.5 multiplications per 1-bit message.

Security: Since $V_e(m_{12})=m_{12}^e+m_{12}^{-e}$, we have $(m_{12}^e)^2-V_e(m_{12})m_{12}^e+1=0$. To solve m_{12}^e without knowing the factoring of n is computational infeasible. In addition, to solve m_{12} from m_{12}^e needs to solve the discrete logarithm. On the other hand, since $V_{e+1}(m_{12})=m_{12}V_e(m_{12})-V_{e-1}(m_{12})$, it is infeasible to derive $V_{e+1}(m_{12})$ without knowing m_{12} and $V_{e-1}(m_{12})$. In addition, since $c_2=V_{e+1}(m_{12})\cdot m_1$, the attacker can derive $V_{e+1}(m_{12})$ with the knowledge of m_1. But, to derive m_{12} from $V_{e+1}(m_{12})$ needs a proper deciphering key d_i. We will include the complete discussion of the security analysis in the full paper.

C. Lucas Public-Key Cryptosystem Based on Two Cryptographic Assumptions

One common feature among all existing cryptosystems, such as RSA [1] and the ElGamal cryptosystem [3], is that the security is based on just one cryptographic assumption, such as factoring or discrete logarithms. Although these cryptographic assumptions appear secure today, it is still very likely that a clever cryptanalyst will discover an efficient way in the future to factor integers or to compute discrete logarithms. Thus, cryptosystems based on the corresponding assumption will surrender their security suddenly. To enhance security is the major motivation for developing cryptosystems based on multiple cryptographic assumptions. This is due to the common belief that it is very unlikely that multiple cryptographic assumptions would simultaneously become easy to solve.

In 1988, McCurley [17] proposed the first cryptosystem based on two dissimilar assumptions, both of which appear to be hard. Instead of using an arithmetic modulus p in the original Diffie-Hellman public-key distribution scheme and in the ElGamal cryptosystem, it uses a modulus n that is a product of two primes. Breaking the system requires the factoring of n into two primes, p and q, and the ability to solve discrete logarithm problems in subgroups of Z_p and Z_q. Thus, it is impossible to select proper moduli, p and q, to achieve the same difficulty for these two assumptions. This results in two disadvantages: (1) larger key size; and (2) longer computation time. In 1994, Harn [18] proposed a public-key cryptosystem based on two assumptions by selecting a special modulus $p=2p'q'+1$, where p, p' and q' are all primes. He and Kiesler [19] had a proposal to enhance the security of ElGamal's signature scheme with two assumptions. But, the security of the proposed scheme has been disproved in [20, 21].

Lucas-type cryptosystem with two assumptions: Horster et al. [22] has proposed a Lucas-type signature scheme in 1995. As a result of their scheme, the signature generation (one evaluation of Lucas function) and signature verification (three evaluations of a Lucas function) are slightly less efficient than that of the original ElGamal signature scheme over GF(p). In this paper, we propose a generalization of the ElGamal scheme which requires only two evaluations of a Lucas function in signature verification.

System setup: Each user selects two large primes, p and q, where $p+1=2p'$, $q+1=2q'$, p' and q' are primes, and computes $n=pq$. Then selects $0,1 \neq \xi \in [2,n-1]$ such that $V_{p'}(\xi) \neq 2$, $V_{q'}(\xi) \neq 2$, $V_{p+1}(\xi) = 2$, and $V_{q+1}(\xi) = 2$. i.e. $f(x) = x^2 - \xi x + 1$ is an irreducible polynomial over $GF(p)$ and $GF(q)$. Each user selects x, with $0<x<n-1$, as his private key and computes $y= V_x(\xi)$ as his public key. (ξ, n, y) are each user's public keys and (p, q, p', q', x) are each user's secret keys.

Signature generation: If the user wants to sign the message $m \in [1, n\text{-}1]$, he chooses a random integer $k \in [1, n\text{-}1]$, computes $r= V_k(\xi)$ *mod* n, and solve the signature equation, $x=(m'+r)k+s \ mod\ (p+1)(q+1)$, for the parameter s, where $m'=h(m)$, and $h(.)$ is a public-known one-way hash function. The tuple (r, s) is the signature.

Signature verification: Any verifier can check if $y^2 + V_{m'+r}^2(\xi) + V_s^2(\xi) = yV_{m'+r}(\xi)V_s(\xi) + 4 \mod$. The correctness of this verification can be easily checked according to Theorem 1 in [22].

Discussion: Breaking this system requires: (1) factoring n into two large primes, and (2) solving the discrete logarithm problem in two subgroups of Z_{p^2} and Z_{q^2}. If we select two large primes, p and q, with 614 bits each, then their product is 1228-bit long. According to [13], the difficulty of solving the discrete logarithm problem in the subgroup of Z_{p^2}, with a 614-bit prime p, is equivalent to the difficulty of factoring a 1024-bit composite integer. Thus, in our proposed system, it is possible to reduce the difference between security levels for these two assumptions and to maintain the efficiency of the implementation.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, " A method for obtaining digital signatures and public key cryptosystems," *CACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. on Inform. Theory*, vol. IT-22, pp. 644-654, Nov. 1976.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[4] NIST, A proposed federal information processing standard for digital signature standard (DSS), Federal Register 56 (1991), 42980-42982.

[5] D. Gordon, "Discrete logarithms in *GF(p)* using the number field sieves," *SIAM J. Disc Math.* **6** , pp. 124-138, 1993.

[6] W. B. Muller, W. Nobauer, "Cryptanalysis of the Dickson-scheme," *Proceedings of Eurocrypt '85,* Springer-Verlag, pp. 71-76, 1985.

[7] W. Nobauer, "Cryptanalysis of a public-key cryptosystem based on Dickson polynomials," *Mathematica Slovaca* **38** (1989), pp. 309-323.

[8] P. Smith, "LUC public-key encryption," *Dr. Dobb's Journal*, pp. 44-49, January 1993.

[9] P. Smith, M. J. J. Lennon, "LUC: a new public key system," *Proceedings of the Ninth IFIP*

Int. Symp. on Computer Security (1993), pp. 103-117.

[10] E. Bach, "Comments on Peter Smith's LUC public-key encryption system," manuscript, March 1993.

[11] P. Smith, C. Skinner, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms," Proceedings of Asiacrypt '94, pp. 298-306, Nov. 1994.

[12] R. Lidl, G.L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics 65, John Wiley & Sons, Inc., 1993.

[13] D. Bleichenbacher, W. Bosma, A.K. Lenstra, "Some Remarks on Lucas-Based Cryptosystems," *Advances in Cryptology-Crypto '95, Lecture Notes in Computer Science*, vol. 963, Springer-Verlag, pp. 386-396, Aug. 1995.

[14] H. Postl, "Fast evaluation of Dickson polynomials," *Contributions to General Algebra* 6, Verlag Holder-Pichler-Tempsky, Wien-Verlag B.G. Teubner, Stuttgart, pp. 223-225, 1988.

[15] S.-M. Yen, C.-S. Laih, "Fast algorithms for LUC digital signature computation," *IEE Proc. Comput. Digit. Tech.*, vol. 142, no. 2, pp. 165-169, March 1995.

[16] R. Lidl, H. Niederreiter, "Finite Fields," in *Encyclopedia of Mathematics and its Applications*, vol. 20. Reading, MA: Addison-Wesley, 1983.

[17] K. S. McCurley, "A Key Distribution System Equivalent to Factoring," *Journal of Cryptology*, Vol. 1, No. 2, pp. 95-106, 1988.

[18] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms", *IEE Proc.-Comput. Digit. Tech.*, Vol. 141, No. 3, pp. 193-195, May, 1994.

[19] J. He, and T. Kiesler, "Enhancing the security of ElGamal's signature scheme', *IEE Proc.-Comput. Digit. Tech., Vol. 141, No. 4*, pp. 249-252, July 1994.

[20] L. Harn, "Comments on enhancing the security of ElGamal's signature scheme", *IEE Proceedings - Computers and Digital Techniques*, Vol. 142, No. 5, p. 376, Sep. 1995.

[21] N. Y. Lee and T. Hwang, "The security of He and Kiesler's signature schemes," *IEE Proceedings - Computers and Digital Techniques*, Vol. 142, No. 5, pp. 370-372, Sep. 1995.

[22] P. Horster, M. Michels and H. Petersen, "Digital signature schemes based on Lucas functions," *Proceedings of the Communications and Multimedia Security Conference*, IFIP TC-6 and TC-11, Graz, Austria, Sep. pp. 20-21, 1995.

Table 1

$J\left(\frac{\left(V_e(m)\right)^2-4}{p}\right)$	$J\left(\frac{\left(V_e(m)\right)^2-4}{q}\right)$	*deciphering key*	R_i
1	1	d_1	$R_1=(p-1)(q-1)$
1	−1	d_2	$R_2=(p-1)(q+1)$
−1	1	d_3	$R_3=(p+1)(q-1)$
−1	−1	d_4	$R_4=(p+1)(q+1)$