



UNIVERSITI PUTRA MALAYSIA

**A NEW "F-LUEG" CRYPTOSYSTEM
AND ITS SECURITY**

CHOO MUN YOONG

FSAS 2002 38

**A NEW “F-LUEG” CRYPTOSYSTEM
AND ITS SECURITY**

By

CHOO MUN YOONG

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in Fulfilment of the Requirement for the Degree of Master of Science**

APRIL 2002



Dedicated To
my family, my committee members
and the church members



Abstract of thesis presented to the Senate of Universiti Putra Malaysia in
fulfilment of the requirement for the degree of Master of Science

A NEW “F-LUEG” CRYPTOSYSTEM AND ITS SECURITY

By

CHOO MUN YOONG

April 2002

Chairman: Mohd Rushdan Md Said, Ph.D.

Faculty : Faculty of Science and Environmental Studies

In this thesis, we present a new public-key cryptosystem and a new digital signature based on the extended Lucas function analogue to ElGamal cryptosystem. We name it “ F-LUEG” cryptosystem.

Chapter 2, we point out how an extended Lucas function can be used in a cryptosystem, which has been presented Md Said in his thesis [Rus]. This extended Lucas function is an extension from Lucas function. In chapter 3, we provide some explanation about ElGamal cryptosystem, which has been presented by T El Gamal in 1985. Finally, from these two cryptosystems, this thesis associate the extended Lucas and ElGamal cryptosystems to develop a new cryptosystem, which is the F-LUEG cryptosystem.



We can discuss the security of F-LUEG cryptosystem in many ways. In chapter 4, F-LUEG is discussed as a one pad time which can achieve perfect secrecy if we choose the key $|K| = |C|$. Chapter 5, we focus upon the security in pseudo-random generators. Since computers generated many random keys, so it is very important to consider the security in pseudo-random generators. Breaking the pseudo-random generator for F-LUEG cryptosystem is equivalent to breaking the ElGamal cryptosystem. Even though an adversary cannot break the F-LUEG cryptosystem, this does not mean the adversary could not obtain some information from the ciphertext. Then in the last chapter, it is shown that, given the ciphertext, it is impossible to guess the least significant bit of plaintext, unless the F-LUEG is broken.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

**SATU SISTEM KRIPTO “F-LUEG” YANG BARU
DAN KESELAMATANNYA**

Oleh

CHOO MUN YOONG

April 2002

Pengerusi : Dr. Mohd Rushdan bin Md. Said

Falkulti : Falkulti Sains dan Pengajian Alam Sekitar

Dalam tesis ini, kami mempersembahkan satu sistem kriptografi kunci awam dan tandatangan digital yang baru. Sistem baru ini berdasarkan kepada penjana Lucas lanjutan dan penjana ElGamal. Kami menamakannya sistem kriptografi F-LUEG.

Dalam bab 2, kami menerangkan bagaimana penjana fungsi lanjutan digunakan dalam sistem kriptografi seperti mana yang ditunjukkan oleh Md Said [Rus]. Penjana fungsi Lucas lanjutan ini adalah kajian lanjutan daripada penjana Lucas. Dalam bab 3, kami menerangkan penjana kriptografi El Gamal yang pernah dipersembahkan oleh T.El Gamal pada 1985. Akhirnya, kami menggabungkan sistem kriptografi fungsi



Lucas lanjutan dengan El Gamal untuk membina satu sistem kripto yang baru, iaitu sistem kripto F-LUEG.

Kita boleh membincangkan keselamatan sistem kripto F-LUEG dari pelbagai aspek. Dalam bab 4, kami membincangkan bahawa F-LUEG adalah satu laluan sahaja, maka ia boleh mencapai keselamatan yang sempurna jika kita memilih kunci $|K| = |C|$. Dalam bab 5, kami memberi tumpuan kepada tahap keselamatan bagi penjana nombor rawak. Oleh sebab komputer boleh menjanakan banyak nombor rawak, jadi adalah penting bagi kita mengkaji keselamatan dalam penjana kerawakan kunci kriptografi. Untuk memecah penjana rawak bagi F-LUEG adalah sama dengan memecah sistem kripto El Gamal. Walaupun musuh tidak dapat memecahkan sistem kripto F-LUEG, ini tidak bermakna musuh tidak boleh mendapatkan maklumat daripada sifer teks. Jadi, dalam bab yang terakhir, kami menunjukkan bahawa tidak ada seorang pun yang boleh mendapatkan maklumat daripada sifer teks kecuali dengan memecahkan F-LUEG.

ACKNOWLEDGEMENTS

First of all, I would like to give thanks to God who gives me strength and wisdom to complete my thesis. My utmost thanks and deepest gratitude goes to my supervisor, Dr Mohamad Rushdan, and committee members Dr. Mat Rofa, and Prof Dr. Kamel Ariffin, for their encouragement, invaluable advice and guidance throughout the preparation of my thesis.

I would like to express my thanks to my friends: Mun Chau and Peter, who provide me the information that I need for my thesis. I would like to thank Rosy, Tuck Seong, Wai Seong, Tzin Lung, David and Joyce, for allowing me to use their computers.

Appreciation is also given to my caring family for their support and understanding. I also would like to thank Andrew because he has helped me to correct my English grammar in my thesis. Thank you to all my friends for your help and encouragement! Thank you from the bottom of my heart. May God bless and take care all of you!



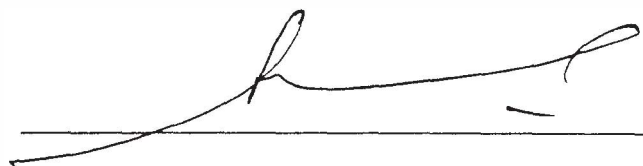
I certify that an Examination Committee met on 13th April 2002 to conduct the final examination of Choo Mun Yoong on his Master thesis entitled “A New “F-LUEG” Cryptosystem and Its Security” in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulation 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Adem Kilicman, Ph.D.
Associate Professor
Faculty Science and Environmental
Universiti Putra Malaysia
(Chairman)

Mohd Rushdan Md.Said, Ph.D.
Faculty Science and Environmental
Universiti Putra Malaysia
(Member)

Kamel Ariffin Mohd Atan, Ph.D.
Professor
Faculty Science and Environmental
Universiti Putra Malaysia
(Member)

Mat Rofa Ismail, Ph.D.
Associate Professor
Faculty Science and Environmental
Universiti Putra Malaysia
(Member)



SHAMSHER MOHAMAD RAMADILI, Ph.D.,
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia
Date: 11 JUL 2002

This thesis submitted to the Senate of Universiti Putra Malaysia has been accepted as fulfilment of the requirement for the degree of the Master.



AINI IDERIS, Ph.D.
Professor/ Dean
School of Graduate Studies,
Universiti Putra Malaysia
Date: **12 SEP 2002**

DECLARATION

I hereby declare that the thesis is based on my original work except for equations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

(CHOO MUN YOONG)

Date :

TABLE OF CONTENTS

	Page
DEDICATION	ii
ABSTRACT	iii
ABSTRAK	v
ACKNOWLEDGEMENTS	vii
APPROVAL	viii
DECLARATION	x
LIST OF SYMBOLS AND ABBEREVIATIONS	xiii
 CHAPTER:	
I INTRODUCTION	1
Objectives	4
 II EXTENDED LUCAS FUNCTION	5
Polynomial	5
The Discriminant	6
Lucas Functions	7
Cubic Equations	11
Third Order Linear Recurrence Relation	14
Cubic Analogue of the Lucas Sequence	15
Properties of the Sequence V_n and U_n	16
 III EL GAMAL CRYPTOSYSTEM	25
The Diffie-Hellman Key Distribution	25
ElGamal Public Key Cryptosystem	27
ElGamal Signature Scheme	31
The Signing Procedure	32
The Verification Procedure	33
The Security of ElGamal Signature	35
The Security of ElGamal Encryption	37



IV	THE F-LUEG PUBLIC KEY CRYPTOSYSTEM	39
	Public-Key Cryptosystem	41
	Public Key System (LUCELG)	44
	New Public Key Cryptosystem (F-LUEG)	44
	Digital Signature Scheme (F-LUEG)	48
	(LUCELG DS)	50
	A New Signature	53
	The Signing Procedure	53
	Verification Procedure	55
	Cryptography Strength (F-LUEG)	59
	Randomized Encryption	60
	Discrete Logarithm Problem	61
	Achieve Perfect Secrecy	63
V	PSEUDORANDOM NUMBER GENERATOR: THE (F-LUEG) CRYPTOSYSTEM	66
	Background	66
	Pseudorandom Objects Generation	68
	Public Key Cryptosystem and Random Trapdoor	69
	Pseudorandom Number Generator on the F-LUEG	
	Cryptosystem	73
	A New Generator for Keeping The F-LUEG Cryptosystem	
	Secure	76
VI	BIT SECURITY OF THE F-LUEG CRYPTOSYSTEM	81
	F-LUEG Bit Security	81
	F-LUEG is a very Efficient Oracle	86
	Binary Search for Inverting F-LUEG	87
VII	CONCLUSIONS AND SUGGESTIONS	90
	Conclusions	93
	Suggestions	93
	 BIBLIOGRAPHY	94
	VITA	97



LIST OF SYMBOLS AND ABBREVIATIONS

p	Prime Number
Z	Ring of Integers
C	Field of Complex Numbers
F	Ring or Field
$F[x]$	Ring of Polynomial with Coefficient in F
\prod	Product
\sum	Summation
$\det A$	Determinant A
\exp	Exponential
mod	Modulo
DES	Data Encryption Standard
DHP	Diffie-Hellman Protocol
DH	Diffie-Hellman
DL	Discrete Logarithm
DLP	Discrete Logarithm Problem
ELGMA	El Gamal Cryptosystem
F-L	Fibonacci Lucas
GF	Galois field
ISO	International Standards Organization



LUC Lucas
RSA Rivest, Shamir and Adleman



CHAPTER I

INTRODUCTION

Cryptography is the art of providing secure communication over insecure channels. Historically, cryptology has been used almost exclusively, in military and diplomats. Due to the computer revolution, cryptography has gone public and become a necessity to be used for personal, financial, commercial and technological information. Cryptography today might be summed up as the study of techniques and applications that dependent upon the existence of a difficult problem. Cryptanalysis is the study of how to defeat cryptographic mechanisms, and cryptology (from the Greek *kryptos logos*, meaning “ hidden word”) is the discipline of cryptography and cryptanalysis combined. However, the protection of the communication has been the emphasis of the cryptography in history and is only one part of today’s cryptography. Cryptography is the study of mathematical systems for solving two kinds of security problems: privacy and authentication. Cryptography was used as a tool to protect national secret and strategies. Beginning with the work of Feistel at IBM in the early 1970s, the Data Encryption Standard, DES, is the most well known cryptography mechanism in history. It remains the standard for securing electronic commerce for many financial institutions around the world.

The purpose of a cryptosystem is to encipher an intelligible cleartext, thus producing an unintelligible ciphertext. The receiver must be able to decipher the ciphertext, and recover the cleartext. However, the cryptanalysts are unable to decrypt the cipher text. We can classify cryptosystems in many ways. For this thesis, however, we consider two ways; restricted use cryptosystems and general use cryptosystems. A cryptosystem is restricted if its security is based on keeping the secret of the enciphering and deciphering algorithms. For example, Caesar cipher is a restricted use cryptosystem, which replaces each letter in the plaintext with the third following letter in the alphabet. For example, the word "cleartext" becomes "fohduwhaw". Restricted systems are not used in modern context because it is easy for cryptanalysts to decrypt the ciphertext. A cryptosystem is called general use cryptosystem if its security lies not in the secrecy of the enciphering and deciphering algorithms, but of the secret key such as RSA and ElGamal.

In the 1970s, a class of cryptosystem known as "public key" system was developed by Rivest, Shamir and Adleman [Rsa]. These are the systems, which the decryption key is not the same as the encryption key. The encryption key can be presented to the world, but the decryption key is to be kept secret. Let say you wish to receive encryption e-mail from your girl friend, Alice. You send her your public key. Alice writes a passionate love letter, encrypt it with your public key

and send it back to you. You decrypt it with your secret key. If your other friend Mei Cheng intercept it then there is no way she can decrypt it because she cannot use public key to decrypt it. Decryption can only be performed with the private key.

The development in the history of cryptography came, when Diffie and Hellman published “ New Direction in Cryptography” [Dh] in 1976. They gave a new concept for a key exchange, which is based on the intractability of the discrete logarithm problem. Although they did not show a practical way to generate a public-key encryption, but the idea is clear. Merkle independently discovered a similar idea [Merk]. In 1978, Rivest, Shamir, and Adleman discovered the first practical public-key encryption and signature scheme, known as RSA. The RSA scheme is based on the intractability of factoring large integers. In such system, each user selects a private key from which she obtains a pair of algorithms. It was made available to everyone as her public enciphering algorithm, and she keeps secret the other one, which is the corresponding algorithm.

ElGamal introduced another class of powerful and practical public-key scheme in 1985 and it is based on the discrete logarithm problem. One of the most significant contributions provided by public-key cryptography is the digital signature by ElGamal [Elg] in 1985. In 1991 the first international standard for

digital signatures (ISO/IEC 9796) was adopted. It is based on the RSA public-key scheme. In 1994 the U.S Government adopted the Digital Signature Standard, a mechanism based on the ElGamal public-key scheme. Many cryptosystems developed in America are being protected by the government policy. So we need to develop a strong cryptosystem for our own country to protect our country's information such as extended LUC cryptosystem.

This thesis is divided into six chapters. In the first part, the extended Lucas cryptosystem and ElGamal cryptosystem, which are discussed by [Rus], [Elg], [Lip] is presented. From these two cryptosystems, we associate the extended Lucas cryptosystem and ElGamal by referring to the paper by [Smith]. We name this new cryptosystem as "F-LUEG" cryptosystem. In the last part, we investigate the security of the cryptosystem through two aspects; that is security in pseudorandom number generator and bit security. In chapter 5, we discuss a new generator, which is secure to use in F-LUEG cryptosystem. For an adversary to break the pseudorandom number generator, the adversary must break the ElGamal cryptosystem. Finally, in the last chapter, we show that no information can be obtained from the ciphertext, unless the F-LUEG is broken.



CHAPTER II

EXTENDED LUCAS FUNCTION

After the LUC public-key cryptosystem by Smith and Lennon [Luc], Wang Liping and Zhau Jinjun [Lip] presented public-key cryptosystems, which were the extension from LUC cryptosystem. The LUC cryptosystem was based on the second-order linear recurrence, however the extended LUC cryptosystem was based on the use of third-order linear recurrences. In their papers, they presented the new public-key cryptosystems based on the third-order linear recurrences.

Polynomial

If 'x' is a variable, 'n' is a non-negative integer and $T_0, T_1, T_2, \dots, T_n$ are given constants of which T_n is not zero, then

$$T(x) = T_n x^n + T_{n-1} x^{n-1} + \dots + T_0 \quad (2.1)$$

is a polynomial of degree 'n'. If $T(x) = 0$, when 'x' has any one of the 'n' distinct value a_1, a_2, \dots, a_n as the roots,

$$T_n x^n + T_{n-1} x^{n-1} + \dots + T_0 = 0$$

$$T(x) = T_n (x - a_1) (x - a_2) \dots (x - a_n)$$

$$= T_n \prod_{i=1}^n (x - a_i) .$$

If $T_n = 1$, the polynomial is called monic polynomial of degree 'n'. The relations between the roots and the coefficient of the equation $f(x)$ are as follows[Rus]:

$$T_{n-1} = - \sum_{i=1}^n a_i$$

$$T_{n-2} = \sum_{i < j} a_i a_j$$

$$T_{n-3} = - \sum_{i < j < k} a_i a_j a_k$$

$$T_0 = (-1)^n a_1 a_2 \dots a_n$$

The Discriminant

Suppose F is a field and f is a polynomial in $F[x]$ and X_1, \dots, X_n are the roots of f in a splitting field extension of F . We define

$$\begin{aligned} \Delta(X_1, \dots, X_n) &= \prod_{1 \leq i < j \leq n} (X_i - X_j) \in Z[X_1, \dots, X_n]. \\ &= (X_1 - X_2)(X_2 - X_3)(X_3 - X_4) \dots (X_{n-1} - X_n) \end{aligned}$$

Every permutation of X_1, \dots, X_n permutes the factors $X_i - X_j$ among themselves, changing the sign of them. So, Δ is either left unchanged or changed into its opposite by a permutation, and Δ^2 is a symmetric polynomial. We define

$\Delta(X_1, \dots, X_n)^2 = D(P_1, \dots, P_n)$ for some polynomial D with integer coefficient, the discriminant of the generic polynomial of degree n . If f has a repeated root, then $\Delta(X_1, \dots, X_n) = 0$. Otherwise, f is separable and $\Delta(X_1, \dots, X_n) \neq 0$.

Definition: 2.1 The discriminant of a polynomial $f(x) \in F[x]$ is $D = \Delta(X_1, \dots, X_n)^2$

In degree 2, we readily have:

$$D = \Delta(X_1, X_2)^2 = (X_1 - X_2)^2 = X_1^2 + X_2^2 - 2X_1X_2$$

For degree 3, we have:

$$\begin{aligned} D = \Delta(X_1, X_2, X_3)^2 &= (X_1 - X_2)(X_1 - X_3)(X_2 - X_3) \\ &= (X_1^2 X_2 + X_2^2 X_3 + X_3^2 X_1) - (X_1 X_2^2 + X_2 X_3^2 + X_3 X_1^2) \end{aligned}$$

Lucas functions

Lucas functions are examples of second order linear recurrences. If $a_1, a_2, a_3, \dots, a_m$, are integers, then

$$T_n = a_1 T_{n-1} + a_2 T_{n-2} + \dots + a_m T_{n-m}$$

is a sequence of integers $\{T_n\}$ for $n \geq m$.

We must define T_0, T_1, \dots, T_{m-1} independently, in order to use the defining equation. This equation is called an m 'th order linear recurrence relation. A sequence defined by a first-order linear recurrence relations made up of numbers which are a constant (T_0) times successive powers of a_1 . Sequence satisfying higher order linear relations can be thought of as generalization of powers, so it

is not surprising that generalizations of the RSA systems to some of these sequences is possible. So the general second-order linear recurrence relation, is defined by

$$T_n = PT_{n-1} - QT_{n-2} \quad (2.2)$$

where P and Q are relatively prime integers and $T_0 = a$ and $T_1 = b$ are the initial values. If we take $P=1$ and $Q=-1$, then the sequence of integers obtained by choosing $T_0=0$, $T_1=1$ is the well - known Fibonacci sequence. It is easy to find the general form of a sequence from the second-order linear recurrence. Let α , β be the roots of the quadratic equation

$$x^2 - Px + Q = 0. \quad (2.3)$$

If c_1 and c_2 are any numbers, then the sequence $\{c_1\alpha^n + c_2\beta^n\}$ has the property that

$$\begin{aligned} P\{c_1\alpha^{n-1} + c_2\beta^{n-1}\} - Q\{c_1\alpha^{n-2} + c_2\beta^{n-2}\} &= c_1\alpha^{n-2}(P\alpha - Q) + c_2\beta^{n-2}(P\beta - Q) \\ &= c_1\alpha^{n-2}(\alpha^2) + c_2\beta^{n-2}(\beta^2) \\ &= c_1\alpha^n + c_2\beta^n \end{aligned}$$

So this sequence satisfies the second-order linear recurrence relation (2.2), and it is not difficult to see that any sequence $\{T_n\}$ satisfying (2.2) must be of the form $\{c_1\alpha^n + c_2\beta^n\}$, where

$$T_0 = c_1 + c_2, T_1 = c_1\alpha + c_2\beta$$

If T_0 and T_1 are integers, then by (2.2), all terms in the sequence will be integers, even though α, β, c_1, c_2 are probably not integers, and may be not real. There are two particular solutions of the general second-order linear recurrence relation.

They are denoted by $\{U_n\}$ and $\{V_n\}$, and are defined by

$$U_n = \frac{(\alpha^n - \beta^n)}{(\alpha - \beta)}, \text{ so } c_1 = \frac{1}{(\alpha - \beta)} = -c_2$$

$$V_n = \alpha^n + \beta^n, \text{ so } c_1 = 1 = c_2$$

where $\alpha \neq \beta$ because when $\alpha = \beta$, $\{U_n\}$ is undefined.

These will both be the sequence of integers, since we have:

$$U_0 = 0, U_1 = 1, V_0 = 2, \text{ and } V_1 = P.$$

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 that their dependence on P and Q . They were first discussed by Lucas [Lucas] in 1875, but their theory was extended by Lehmer [Leh]. If N is any number, then

$$U_n(P \bmod N, Q \bmod N) \equiv U_n(P, Q) \bmod N$$

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

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

So the stated result follows by induction. Similarly

$$V_n(P \bmod N, Q \bmod N) \equiv V_n(P, Q) \bmod N.$$

The roots of (2.3) satisfies the equations

$$\alpha + \beta = P, \quad \alpha\beta = Q$$

The discriminant of 2.3, $D = P^2 - 4Q$, can be expressed in terms of the roots of the quadratic equation by:

$$D = (\alpha - \beta)^2.$$

Consider the linear recurrence relation created by using $V_k(P, Q)$ for P and Q^k for Q :

$$T_n = V_k(P, Q)T_{n-1} - Q^k T_{n-2}.$$

The roots of the corresponding quadratic equation, α' and β' , must satisfy

$\alpha' + \beta' = V_k(P, Q) = \alpha^k + \beta^k$ and $\alpha'\beta' = Q^k = \alpha^k\beta^k$, so we must have $\alpha' = \alpha^k$ and $\beta' = \beta^k$. This means that

$$V_n(V_k(P, Q), Q^k) = (\alpha^k)^n + (\beta^k)^n = \alpha^{nk} + \beta^{nk} = V_{nk}(P, Q)$$