A QUALITATIVE STUDY OF FAMILIES OF EDWARDS CURVES AND THEIR APPLICATIONS IN CRYPTOGRAPHY

RESEARCH MANAGEMENT INSTITUTE (RMI)
UNIVERSITI TEKNOLOGI MARA
40450 SHAH ALAM, SELANGOR
MALAYSIA

BY :

NURUL 'AZWA BT KAMARUDIN
NURUL AIN BT MUSTAKIM

SEPTEMBER 2012

UNIVERSITI TEKNOLOGI MARA

PEMENANG Anugerah Kualiti Perdana Menteri 2008

Surat Kami : 600-RMI/SSP/DANA 5/3/Dsp (272 /2011)
Tarikh : 8 Jun 2011

UNIT PENULISAN & PENERBITAN (UPENA) DITERIMA DAN DIREKOD 15 JUN 2011 T.T. ..... UiTM Kampus Melaka

Pn Nurul 'Azwa Kamarudin
Fakulti Sains Komputer dan Matematik
Universiti Teknologi MARA Cawangan Melaka
KM. 26, Jalan Lendu
78000 Alor Gajah, Melaka

Y. Brs. Profesor./Tuan/Puan

KELULUSAN PERMOHONAN DANA KECEMERLANGAN 06/2011

Tajuk Projek	:	Edward Curves and Its Applications in Cryptography
Kod Projek	:	600-RMI/SSP/DANA 5/3/Dsp (272 /2011)
Kategori Projek	:	Kategori F (2011)
Tempoh	:	15 Jun 2011 – 14 Jun 2012 (12 bulan)
Jumlah Peruntukan	:	RM 5,000.00
Ketua Projek	:	Pn Nurul 'Azwa Kamarudin

Dengan hormatnya perkara di atas adalah dirujuk.

2. Sukacita dimaklumkan pihak Universiti telah meluluskan cadangan penyelidikan Y. Brs Profesor/tuan/puan untuk membiayai projek penyelidikan di bawah Dana Kecemerlangan UiTM.

3. Bagi pihak Universiti kami mengucapkan tahniah kepada Y. Brs. Profesor/tuan/puan kerana kejayaan ini dan seterusnya diharapkan berjaya menyiapkan projek ini dengan cemerlang.

4. Peruntukan kewangan akan disalurkan melalui tiga (3) peringkat berdasarkan kepada laporan kemajuan serta kewangan yang mencapai perbelanjaan lebih kurang 50% dari peruntukan yang diterima.

Peringkat Pertama	20%
Peringkat Kedua	40%
Peringkat Ketiga	40%

5. Untuk tujuan mengemaskini, pihak Y. Brs. Profesor/tuan/puan adalah diminta untuk melengkapkan semula kertas cadangan penyelidikan sekiranya perlu, mengisi borang setuju terima projek penyelidikan dan menyusun perancangan semula bajet yang baru seperti yang diluluskan. Sila lihat lampiran bagi tatacara tambahan untuk pengurusan projek.

Sekian, harap maklum.

"SELAMAT MENJALANKAN PENYELIDIKAN DENGAN JAYANYA"

Yang benar

DR OSKAR HASDINOR HASSAN
Ketua Penyelidikan (Sains Sosial dan Pengurusan)

/RS_

4. Enhanced Research Title and Objectives

Original Title as Proposed:
Edwards Curves and Its Applications in Cryptography

Improved/Enhanced Title:
A Qualitative Study Of Families Of Edwards Curves And Their Applications In Cryptography

Original Objectives as Proposed:

- To give detail overview of Edwards curve in cryptography
- To identify the applications of Edwards curves in cryptography

Improved/Enhanced Objectives:

- To give detail overview of families of Edwards curves in cryptography i.e. important properties of the Edward Curves' families
- To identify the applications of families of Edwards curves in cryptography.

5. Report

5.1 Proposed Executive Summary

Cryptography or Cryptology is the practice and study of hiding information, as well as the applications of cryptography include ATM cards, computer passwords, and electronic commerce. In cryptology, there are many types of scheme used in encrypting a message so that is can be sent to a particular receiver from a particular sender without the third party knowing the content of the message known as cryptosystem. For example, RSA, DES (Data Encryption Standard), Symmetric Key Cryptography and many more. Among those cryptosystems, there are three types of public key cryptographic systems that are currently considered both secure and efficient, that are classified according to the mathematical problems upon which they are based, are: the Integer Factorization Systems (of which the RSA algorithm is the most well known example), the Discrete logarithm Systems (such as the US Government's Digital Signature Algorithm), and the Elliptic Curve Cryptosystem (ECC). From the previous research, many focused on elliptic curve and its applications in mobile communication. This paper describes briefly the basic concept of an Edward curve, one of the special form of elliptic curves used in cryptography, from the definition of the ordinary elliptic curve that is defined by Weierstrass equation to several curves defined by a new form of equations and also the Edward curve itself. This includes operations of points on Edward curve, important properties of the Edward Curve with some example to show the applications in cryptography. It is important to know the properties of Edward Curve as this will encourage further studies in this area and might be useful in wireless communication.

5.2 Enhanced Executive Summary

Cryptography is the science of hiding information and its applications include ATM cards, computer passwords and electronic commerce in this modern world. There are many types of scheme used in encrypting a message so that it can be sent to a particular receiver from a particular sender without the third party knowing the content of the message known as cryptosystem. For example, RSA, DES (Data Encryption Standard), Symmetric Key Cryptography. Among those cryptosystems, there are three types of public key cryptographic systems that are currently considered both secure and efficient, classified according to the mathematical problems upon which they are based: the Integer Factorization Systems (of which the RSA algorithm is the most well known example), the Discrete logarithm Systems (such as the US Government's Digital Signature Algorithm) and the Elliptic Curve Cryptosystem (ECC). Many previous researches focused on elliptic curve and its applications in mobile communication. The purpose of the qualitative study is to explore and develop basic understanding of the properties of the families of Edwards curves, one of the special forms of elliptic curves, and their applications in cryptography, using grounded theory approach, in which the data are hand-analyzed, coded and grouped into themes under study. It is important to distinguish the properties of each member in the families of Edward curves as to encourage further studies and may be useful in wireless and mobile communication.