AN ALTERNATIVE NORMAL FORM FOR ELLIPTIC CURVE CRYPTOGRAPHY: EDWARDS CURVES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS,
CRYPTOGRAPHY DEPARTMENT
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

KÖKSAL MUŞ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2009

Approval of the thesis:

AN ALTERNATIVE NORMAL FORM FOR ELLIPTIC CURVE CRYPTOGRAPHY: EDWARDS CURVES

submitted by **KÖKSAL MUŞ** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. ERSAN AKYILDIZ ________________
Director, Graduate School of **Applied Mathematics**

Prof. Dr. FERRUH ÖZBUDAK ________________
Head of Department, **Cryptography**

Assoc. Prof. Dr. SEFA FEZA ARSLAN ________________
Supervisor, **Department of Mathematics**

Examining Committee Members:

Assoc. Prof. Dr. ALİ DOĞANAKSOY ________________
Department of Mathematics, METU

Assoc. Prof. Dr. SEFA FEZA ARSLAN ________________
Department of Mathematics, METU

Assoc. Prof. Dr. ALİ AYDIN SELÇUK ________________
Department of Computer Engineering, Bilkent Uni.

Assist. Prof. Dr. ZÜLFÜKAR SAYGI ________________
Department of Mathematics, TOBB ETU

Assist. Prof. Dr. ÇETİN ÜRTİŞ ________________
Department of Mathematics, TOBB ETU

Date: ________________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: KÖKSAL MUŞ

Signature :

ABSTRACT

AN ALTERNATIVE NORMAL FORM FOR ELLIPTIC CURVE CRYPTOGRAPHY:
EDWARDS CURVES

MUŞ, KÖKSAL
M.S., Department of Cryptography
Supervisor : Assoc. Prof. Dr. SEFA FEZA ARSLAN

September 2009, 28 pages

A new normal form $x^2 + y^2 = c^2(1 + x^2y^2)$ of elliptic curves was introduced by M. Harold Edwards in 2007 over the field k having characteristic different than 2. This new form has very special and important properties such that addition operation is strongly unified and complete for properly chosen parameter c . In other words, doubling can be done by using the addition formula and any two points on the curve can be added by the addition formula without exception. D. Bernstein and T. Lange added one more parameter d to the normal form to cover a large class of elliptic curves, $x^2 + y^2 = c^2(1 + dx^2y^2)$ over the same field. In this thesis, an expository overview of the literature on Edwards curves is given. First, the types of Edwards curves over the nonbinary field k are introduced, addition and doubling over the curves are derived and efficient algorithms for addition and doubling are stated with their costs. Finally, known elliptic curves and Edwards curves are compared according to their cryptographic applications. The way to choose the Edwards curve which is most appropriate for cryptographic applications is also explained.

Keywords: Edwards curve, twisted Edwards curve, complete addition, unified addition, cost

ÖZ

ELİPTİK EĞRİ KRİPTOLOJİSİ İÇİN ALTERNATİF ELİPTİK EĞRİ FORMU:
EDWARDS EĞRİLERİ

MUŞ, KÖKSAL
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Doç. Dr. SEFA FEZA ARSLAN

Eylül 2009, 28 sayfa

Harold Edwards tarafından 2007 yılında karakteristiği 2'den farklı olan cisimler üzerinde $x^2 + y^2 = c^2(1 + x^2y^2)$ formunda yeni bir eliptik eğri formu tanımlandı. Uygun seçilen parametreler için yeni form üzerinde tanımlanan toplama işlemi, kriptoloji için önemli olan tam toplama ve bütünleştirilmiş toplama özelliklerine sahiptir. Bir başka deyişle, bu eğri üzerinde bir noktayı kendisiyle toplamak için yeni bir formüle gerek kalmamaktadır. Ayrıca, bu eğri üzerindeki herhangi iki nokta, hiçbir koşul gözetmeksizin, tanımlı toplama işlemi ile toplanabilmektedir. D. Bernstein ve T. Lange, daha çok eliptik eğriyi kapsayabilmek için bu formu $ax^2 + y^2 = c^2(1 + dx^2y^2)$ biçiminde genişletmişlerdir. Bu çalışmada Edwars eğrileri literatürünün genel bir derlemesi yapılmıştır. Öncelikle, karakteristiği ikiden farklı olan cisimler üzerinde Edwards eğrileri tanımlanmış, bu eğriler üzerindeki toplama ve iki katını alma işlemleri ve maaliyetlerinin nasıl hesaplandığı gösterilmiştir. Daha sonra, bilinen eliptik eğrileri ve Edwards eğrileri kriptolojik uygulamalara uygunluk bakımından karşılaştırılmıştır. Ayrıca, Edwards eğrilerinden hangisinin kriptolojik uygulamalar için daha uygun olduğu belirlenmiştir.

Anahtar Kelimeler: Edwards Eğrisi, bükülmüş Edwards Eğrisi, tam toplama, bütünleştirilmiş toplama, işlem maaliyeti

To my family and my lovely wife Sinem.

ACKNOWLEDGMENTS

First of all, I would like to express my deepest sense of gratitude to my supervisor Assoc. Prof. Dr. Sefa Feza ARSLAN for his continous guidance, encouragement and excellent advice throughout this study.

I am also thankful to Onur KOÇAK for his comments and advices for the defence of the thesis.

I want to thank to my examining committee members for spare their valuable times in such a busy time of the year.

I would like to thank IAM administrative staff especially Nejla Erdoğdu and Rukiye Ekinci for their support.

I want to state my deepest thanks to my wife Sinem and my wonderful family, who have raised me to be the person I am today. You have been with me every step of the way, through good times and bad. Thank you for all the unconditional love and support that you have always given me, helping me to succeed and instilling in me the confidence that I am capable of doing anything I put my mind to.

Moreover, I want to thank METU Aikido society and all of my aikido friends including my wife to refresh my mind when I am tried of life.

Last but not the least, I would like to thank Tanja LANGE and Daniel J. BERNSTEIN for introducing me to Edwards Curves in the ECC 2008.

TABLE OF CONTENTS

CHAPTERS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

Introduction

In this thesis, our main object of interest is a new form of elliptic curves called Edwards Curves. These curves were first introduced by M. Harold Edwards in 2007 [1] and is defined as the zero set of $x^2 + y^2 = c^2(1 + x^2y^2)$. The main advantage of this form is that the group law can be stated explicitly on it and it is given by Edwards as :

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Edwards has also proved that every elliptic curve is birationally equivalent to an Edwards curve [1]. Given the importance of elliptic curves in cryptography, it is obvious to estimate that Edwards curves should also be useful in elliptic curve cryptography. Moreover, Edwards curves has many extra features such as cheaper cost operation, strongly unified and complete addition formula which supplies a resistance against the side channel attack.

To understand the importance of Edwards curves in ECC, we first give a short summary of the use of elliptic curves in cryptography. In 1976, Whitfield Diffie and Martin Hellman published a paper [5] in which they introduced an asymmetric-key cryptosystem called Diffie-Hellman key exchange which uses exponentiation in a finite field and its security is based on discrete logarithm problem for finite groups. After a short time, independent of the Diffie-Hellman key exchange, in 1978, Rivest, Shamir and Adleman published a paper [6] about another asymmetric-key cryptosystem called RSA which uses exponentiation modulo a product of two large primes to encrypt and decrypt and its security is based on the difficulty of factoring the product of two large primes. As the computer technology developed, it became necessary to have larger key sizes in order to obtain the required security. In 1986, Neal Koblitz [7] and in 1987, Victor Miller [8] proposed to use elliptic curves in cryptography, independently. In this system, security is based on the discrete logarithm problem and it requires much more smaller key sizes. In the following table given by NSA, it is possible to observe the required key sizes for the same security levels [9].

Symmetric Key Size	RSA and Diffie-Hellman Key Size	Elliptic Curve Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1.1: Key Sizes

Elliptic curve cryptosystems are preferred not only because of their smaller key sizes, but also because of their computational efficiency. This computational efficiency can be observed in the following table for the relevant key sizes [9].

Security Level (bits)	Ratio of DH cost:EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Table 1.2: Computational Efficiency

Elliptic curves are defined as the zero set of the polynomial $y^2 = x^3 + ax + b$ over nonbinary field k, $a, b \in k$, $4a^3 + 27b^2 \neq 0$ and point at infinity. Addition operation on it is defined by the chord and tangent rule and adding a point to itself is called doubling (see figure 1.1.). Identity point of the operation is the point at infinity. Multiplication by an integer constant c is defined as adding the point $c - 1$ times to itself.

In 2007, M. Harold Edwards introduced in [1] a new normal form of elliptic curves (zero set of $x^2 + y^2 = c^2(1 + x^2y^2)$ over a nonbinary field) which are birationally equivalent to elliptic curves. Just after few months, Bernstein and Lange modified the normal form by adding one more parameter (zero set of $x^2 + y^2 = c^2(1 + dx^2y^2)$ over a nonbinary field) which increased the set of birationally equivalent elliptic curves [2].

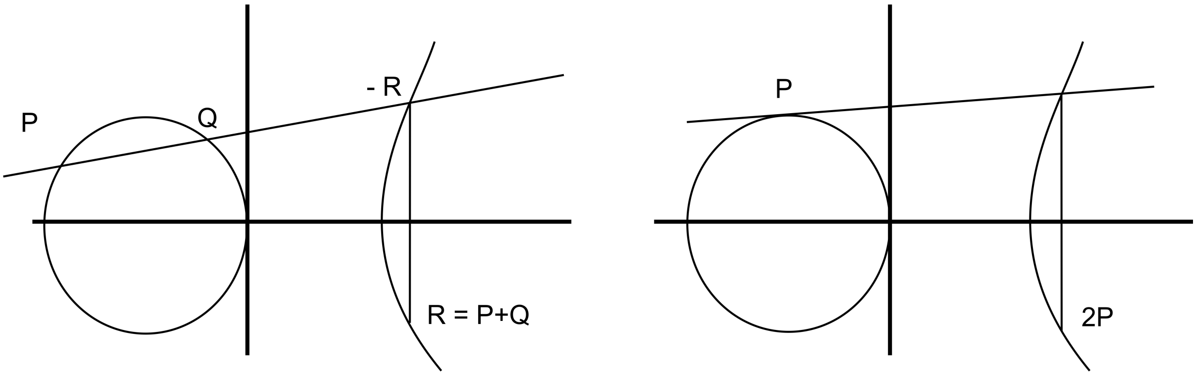

Figure 1.1: Addition and Doubling over Elliptic Curves

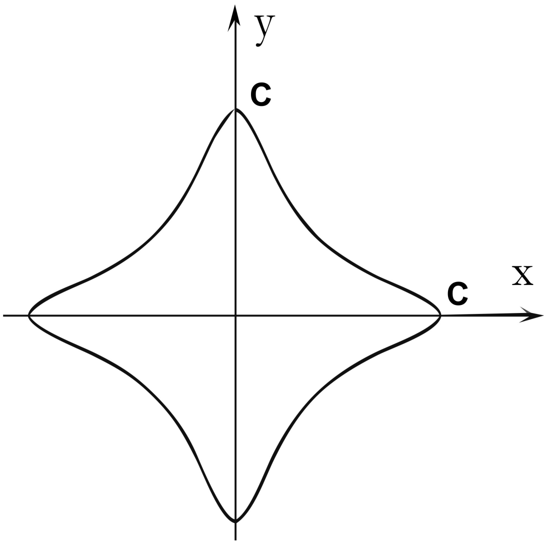

Figure 1.2: Edwards Curve

In its new form, Edwards curve is more suitable for ECC with its extra features. Namely, its complete addition formula gives the advantage that implementations do not require any checking for the points. Its unified addition formula brings the advantage of resistance against side channel attack since addition and doubling can be computed by the same formula.

In Chapter 2, we give the main properties of the Edwards curve by using the more general form of Bernstein and Lange. We explain the addition formula given explicitly by Edwards and modified by Bernstein and Lange. Then, we explain how Bernstein and Lange use homogenous coordinates to obtain efficient addition and doubling operations. At the end of the second chapter, the costs of algorithms are given.

In Chapter 3, first we explain how the inverted Edwards coordinates are introduced in order to get rid of the computation of the inverses. We state the explicit equation and formulas for addition and doubling with these new coordinates. Since, completeness is lost with these new coordinates, the special points are examined separately. We explain how operation costs are reduced by using inverted Edwards coordinates.

In Chapter 4, to cover a larger class of elliptic curves, twisted Edwards curves are defined. The relation between the Edwards curves and twisted Edwards curves are stated. The explicit addition and doubling formulas for twisted Edwards curves are computed by using the related transformations. At the end of the chapter, addition and doubling costs are computed.

In Chapter 5, to make the computation on the twisted Edwards defined in the previous chapter more efficient, the inverted twisted Edwards coordinates are introduced. With this new coordinates, addition and doubling formulas are stated. Again their costs are computed.

In Chapter 6, After stating the birationally equivalence between Montgomery curves and twisted Edwards curves, the results explained in this thesis will compared to previous results in the literature. Then, it is concluded that which elliptic curve should be used for ECC.

Elliptic curve cryptography makes feasible to use public key cryptography on smartcards without mathematical coprocessors, contactless smartcards and wireless communications.

Elliptic curve cryptography provides the same security level with the previous systems such as RSA and Diffie-Hellman with a much more smaller key sizes.

In this thesis, a new form of elliptic curve introduced and its various forms are examined to clarify that what are the advantages and disadvantages of the new normal form.

CHAPTER 2

Edwards Curves

Edwards curves were first defined in [1] by the zero set of the polynomial $x^2+y^2 = c^2\left(1 + x^2y^2\right)$ for $c \in k$, where k is a field having characteristic different than 2. What makes Edwards curves very important is that all elliptic curves with a point of order 4 having characteristic different than 2 can be transformed to Edwards form over the same field or an extension of the original field. The addition law on an Edwards curve is defined in [1] as $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2+x_2y_1}{c(1+x_1x_2y_1y_2)}, \frac{y_1y_2-x_1x_2}{c(1-x_1x_2y_1y_2)}\right)$ and the neutral element is $(0, c)$ with respect to this operation. This addition law on an Edwards curve corresponds to the standard addition law on an elliptic curve. Moreover, if an Edwards curve has a nonsquare parameter d in the field, then addition formula is valid for all pairs of points on the curve without exception, namely it is complete.

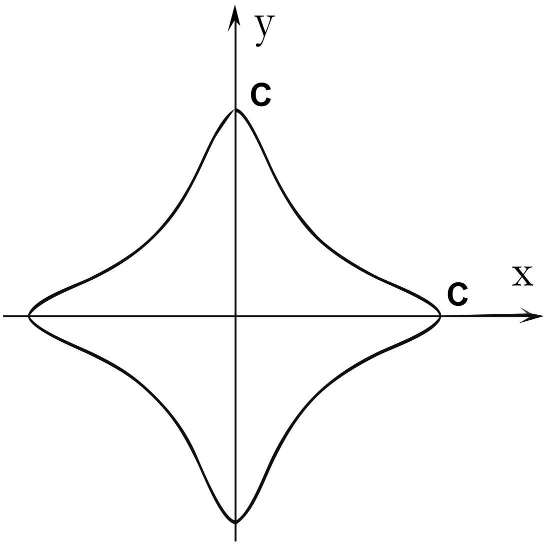

Figure 2.1: Shape of Edwards Curve

To cover a larger class of elliptic curves without extension, the transformation $\overline{x} = cx$ and $\overline{y} = cy$ is applied to the curve equation $\overline{x}^2 + \overline{y}^2 = c^2\left(1 + d\overline{x}^2\overline{y}^2\right)$. The new curve equation is $x^2 + y^2 = 1 + \overline{d}x^2y^2$ where $\overline{d} = dc^4 \neq 1$ [2]. Therefore, $\overline{x}^2 + \overline{y}^2 = c^2\left(1 + d\overline{x}^2\overline{y}^2\right)$ is isomorphic to $x^2+y^2 = 1+\overline{d}x^2y^2$ for all $cd\left(1 - dc^4\right) \neq 0$ over the field k which has characteristic different than 2.

2.1 Transformation to Edwards form:

The following theorem states and proves the relation between elliptic curves and Edwards curves.

Theorem 2.1.1 *[2, Theorem 2.1] Let k be a field in which* $2 \neq 0$. *Let E be an elliptic curve over k such that the group* $E(k)$ *has an element of order 4. Then*

i) There exists $d \in k - \{0, 1\}$ *such that the curve* $x^2 + y^2 = 1 + dx^2y^2$ *is birationally equivalent over k to a quadratic twist of E.*

ii) If $E(k)$ *has a unique element of order 2 then there is a nonsquare* $d \in k$ *such that the curve* $x^2 + y^2 = 1 + dx^2y^2$ *is birationally equivalent over k to a quadratic twist of E.*

iii) If k is finite and $E(k)$ *has a unique element of order 2 then there is a non-square* $d \in k$ *such that the curve* $x^2 + y^2 = 1 + dx^2y^2$ *is birationally equivalent over k to E.*

Later in [3] (Theorem 3.3) Bernstein and Lange et al. proved a stronger version of part (i) saying that an elliptic curve is birationally equivalent to an Edwards curve if and only if it has an element of order 4 and a stronger version of part (iii) cancelling the condition of having a unique element of order 2.

2.2 Edwards Addition Law:

Consider an Edwards curve specified with the given parameters $c, d \in k$ such that $cd(dc^4-1) \neq 0$ over the field k of characteristic different from 2. Addition for the points (x_1, y_1) and (x_2, y_2) which are on the Edwards curve $x^2 + y^2 = c^2(1 + dx^2y^2)$ over k is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{c\,(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c\,(1 - dx_1x_2y_1y_2)}\right).$$

To show that this is a well-defined operation which gives a group structure on the Edwards curve, first it is proved that the addition of two points which are on the Edwards curve is also on the curve. Then, it is shown that Edwards addition and standard addition law on a birationally equivalent elliptic curve gives the same results under certain transformations. Finally, it is proved that when d is a nonsquare over the field k, the Edwards addition law is complete:

Theorem 2.2.1 *[2, Theorem 3.1] Let k be a field in which $2 \neq 0$. Let c, d be nonzero elements of k with $dc^4 \neq 1$. Let x_1, y_1, x_2, y_2 be elements of k such that $x_1^2 + y_1^2 = c^2(1 + dx_1^2y_1^2)$ and $x_2^2 + y_2^2 = c^2(1 + dx_2^2y_2^2)$. Assume that $dx_1x_2y_1y_2 \notin \{-1, 1\}$. Define $x_3 = \frac{x_1y_2+y_1x_2}{c(1+dx_1x_2y_1y_2)}$ and $y_3 = \frac{y_1y_2-x_1x_2}{c(1-dx_1x_2y_1y_2)}$. Then $x_3^2 + y_3^2 = c^2(1 + dx_3^2y_3^2)$.*

Proof. The proof is direct. It is enough to show that the addition point (x_3, y_3) of two points (x_1, y_1) and (x_2, y_2) on the curve satisfies the curve equation, namely,

$$\begin{aligned} x_3^2 + y_3^2 &= c^2(1 + dx_3^2y_3^2) \\ \left[\frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}\right]^2 \left[\frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}\right]^2 &= c^2\left[1 + d[\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}]^2[\frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)}]^2\right] \end{aligned}$$

■

Theorem 2.2.2 *[2, Theorem 3.2] In the situation of previous theorem, let $e = 1 - dc^4$ and let E be the elliptic curve $\frac{1}{e}v^2 = u^3 + (\frac{4}{e} - 2)u^2 + u$. For each $i \in \{1, 2, 3\}$ define P_i as follows: $P_i = \infty$ if $(x_i, y_i) = (0, c)$; $P_i = (0, 0)$ if $(x_i, y_i) = (0, -c)$; and $P_i = (u_i, v_i)$ if $x_i = 0$, where $u_i = \frac{(c+y_i)}{(c-y_i)}$ and $v_i = \frac{2c(c+y_i)}{(c-y_i)x_i}$. Then $P_i \in E(k)$ and $P_1 + P_2 = P_3$.*

Proof. Similar proof will be given in Chapter 6. For the detailed proof of this theorem, you can see [2]. ■

Theorem 2.2.3 *[2, Theorem 3.3] Let k be a field in which $2 \neq 0$. Let c, d, e be nonzero elements of k with $e = 1 - dc^4$. Assume that d is not a square in k. Let x_1, y_1, x_2, y_2 be elements of k such that $x_1^2 + y_1^2 = c^2(1 + dx_1^2y_1^2)$ and $x_2^2 + y_2^2 = c^2(1 + dx_2^2y_2^2)$. Then $dx_1x_2y_1y_2 \neq 1$ and $dx_1x_2y_1y_2 \neq 1$.*

Homogenous Coordinates Leading to Efficient Group Operations:

2.2.1 Addition:

Since finding the inverse of an element is too expensive in a finite field, Edwards addition formula is adapted to homogenous coordinates. Homogenous Edwards curve equation is $(X^2+Y^2)Z^2 = c^2(Z^4+dX^2Y^2)$ and every point $(X : Y : Z)$ with $Z \neq 0$ on the homogenous Edwards curve corresponds to the point $(\frac{X}{Z}, \frac{Y}{Z})$ on the Edwards curve. The neutral element is $(0 : c : 1)$ and the inverse of $(X : Y : Z)$ is $(-X : Y : Z)$.

Addition formula on homogenous coordinates: Since every point $(X : Y : Z)$ corresponds to the point $(\frac{X}{Z}, \frac{Y}{Z})$ when $Z \neq 0$, we can replace x by $\frac{X}{Z}$ and y by $\frac{Y}{Z}$ in the addition formula : $x_3 = \frac{x_1y_2+y_1x_2}{c(1+dx_1x_2y_1y_2)}$ and $y_3 = \frac{y_1y_2-x_1x_2}{c(1-dx_1x_2y_1y_2)}$.

$(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}) + (\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}) = (\frac{X_3}{Z_3}, \frac{Y_3}{Z_3})$ where $(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3})$ corresponds to the point $(X_3 : Y_3 : Z_3)$.

Substitute the point to the additon formula:

$$\frac{X_3}{Z_3} = \frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{c(1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2})} = \frac{\frac{X_1Y_2+Y_1X_2}{Z_1Z_2}}{c(1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2})}$$

Write $X_1Y_2 + Y_1X_2$ as $(X_1+Y_1)(X_2+Y_2) - X_1X_2 - Y_1Y_2$ then

$$\frac{X_3}{Z_3} = \frac{\frac{(X_1+Y_1)(X_2+Y_2)-X_1X_2-Y_1Y_2}{Z_1Z_2}}{c(1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2})} = Z_1Z_2\frac{(X_1+Y_1)(X_2+Y_2) - X_1X_2 - Y_1Y_2}{c(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)}.$$

$$\text{Similarly, } \frac{Y_3}{Z_3} = Z_1Z_2\frac{Y_1Y_2 - X_1X_2}{c(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}.$$

$$\begin{aligned}
\text{So, } X_3 &= Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)((X_1+Y_1)(X_2+Y_2) - X_1X_2 - Y_1Y_2),\\
Y_3 &= Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2),\\
Z_3 &= c(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2). \qquad (2.1)
\end{aligned}$$

The following algorithm allows us to compute $(X_3 : Y_3 : Z_3)$ which is the addition of two given points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$, in homogenous coordinates with the cost of 10M+1S+1C+1D+7a operations. (The cost of operations are represented by some symbols, specifically, M for multiplication, S for squaring, C for multiplication by c, D for multiplication by d and a for addition/subtraction.)

$A = Z_1 \cdot Z_2$; $B = A^2$; $C = X_1 \cdot X_2$; $D = Y_1 \cdot Y_2$; $E = dC \cdot D$; $F = B - E$; $G = B + E$;
$X_3 = A \cdot F \cdot [(X_1+Y_1) \cdot (X_2+Y_2) - C - D]$; $Y_3 = A \cdot G \cdot (D - C)$; $Z_3 = cF \cdot G$.

2.2.2 Doubling:

Since addition formula is complete, doubling can be computed directly from the addition formula. But, since the added points are the same, doubling operation can be more efficient than addition.

$$\begin{aligned} x_3 &= \frac{2x_1y_1}{c(1+dx_1^2y_1^2)} = \frac{2x_1y_1}{(x_1^2+y_1^2)/c} = \frac{2cx_1y_1}{x_1^2+y_1^2}, \\ y_3 &= \frac{y_1^2-x_1^2}{c(1-dx_1^2y_1^2)} = \frac{c(y_1^2-x_1^2)}{2c^2-(x_1^2+y_1^2)}. \end{aligned} \tag{2.2}$$

By similar transformations,

$(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}) + (\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}) = (\frac{X_3}{Z_3}, \frac{Y_3}{Z_3})$ where $(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3})$ corresponds to the point $(X_3 : Y_3 : Z_3)$:

$$\begin{aligned} X_3 &= c[(X_1+Y_1)^2 - X_1^2 - Y_1^2][(X_1^2+Y_1^2) - 2c^2Z_1^2], \\ Y_3 &= c(X_1^2+Y_1^2)(X_1^2-Y_1^2), \\ Z_3 &= (X_1^2+Y_1^2)[(X_1^2+Y_1^2) - 2c^2Z_1^2]. \end{aligned} \tag{2.3}$$

By using the following operations, a point can be doubled with a cost of 3M+4S+3C+6a.
$B = (X_1 + Y_1)^2$; $C = X_1^2$; $D = Y_1^2$; $E = C + D$; $H = (cZ_1)^2$; $J = E - 2H$;
$X_3 = c(B - E) \cdot J$; $Y_3 = cE \cdot (C - D)$; $Z_3 = E \cdot J$

CHAPTER 3

Inverted Edwards Curves

It can be seen that homogenous coordinates can be used to make the addition more efficient on an Edwards curve. Inverting these coordinates make addition even more efficient, because this makes the computations 1M efficient than Edwards coordinates for each addition without slowing down doubling and tripling. But changing the coordinates result with the loss of completeness. Thus, some points should be considered separately. In spite of the loss of completeness, it is still strongly unified, in other words, doubling can be computed via the same formula.

As a notation, (X, Y, Z) will be used for inverted Edwards coordinates for not confusing it with homogenous Edwards coordinates $(X : Y : Z)$.

In inverted Edwards coordinates (X, Y, Z) represent the point $(x, y) = (\frac{Z}{X}, \frac{Z}{Y})$. Hence, in the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$, x is replaced by $\frac{Z}{X}$ and y is replaced by $\frac{Z}{Y}$ to find the inverted Edwards curve equation.

$$\begin{aligned} (\frac{Z}{X})^2 + (\frac{Z}{Y})^2 &= 1 + d(\frac{Z}{X})^2(\frac{Z}{Y})^2 = 1 + d(\frac{Z^4}{X^2Y^2}) \\ Z^2(X^2 + Y^2) &= X^2Y^2 + dZ^4 \qquad (3.1) \end{aligned}$$

where $XYZ \neq 0$. (Recall that, in homogenous coordinates, $(X : Y : Z) = (\lambda X : \lambda Y : \lambda Z)$ for any $\lambda \neq 0$).

Just by using three multiplication, homogenous Edwards coordinates can be converted to inverted Edwards coordinates. If $(X : Y : Z)$ is a point on projective Edwards coordinates, the point $(YZ : XZ : XY)$ is a point on the inverted Edwards coordinates. The same transformation applied to the inverted Edwards coordinates gives the original homogenous coordinates. (In other words, $(X^2YZ : XY^2Z : XYZ^2) = XYZ(X : Y : Z) = (X : Y : Z)$ if $\lambda = XYZ \neq 0$.)

3.1 Addition:

To obtain addition formula for inverted Edwards coordinates, Edwards coordinates can be converted to inverted Edwards coordinates by placing $(\frac{Z_i}{X_i})$ and $(\frac{Z_i}{Y_i})$ for $i = 1, 2$ in the addition formula. Since addition formula for inverted Edwards coordinates does not preserve completeness, special points namely $X_iY_iZ_i = 0$ for $i = 1, 2$ should be considered separately. The addition formula for inverted Edwards coordinates is obtained as follows:

$(\frac{x_1y_2+x_2y_1}{c(1+dx_1x_2y_1y_2)}, \frac{y_1y_2-x_1x_2}{c(1-dx_1x_2y_1y_2)})$ where $(x_1, y_1) = (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$ and $(x_2, y_2) = (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2})$

$$\begin{aligned}
(\frac{Z_3}{X_3}, \frac{Z_3}{Y_3}) &= (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1}) + (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2}) = (\frac{\frac{Z_1}{X_1}\cdot\frac{Z_2}{Y_2} + \frac{Z_2}{X_2}\cdot\frac{Z_1}{Y_1}}{1 + d\frac{Z_1}{X_1}\frac{Z_2}{X_2}\frac{Z_1}{Y_1}\frac{Z_2}{Y_2}}, \frac{\frac{Z_1}{Y_1}\cdot\frac{Z_2}{Y_2} - \frac{Z_1}{X_1}\cdot\frac{Z_2}{X_2}}{1 - d\frac{Z_1}{X_1}\frac{Z_2}{X_2}\frac{Z_1}{Y_1}\frac{Z_2}{Y_2}}) \\
&= (\frac{(X_2Y_1 + X_1Y_2)Z_1Z_2}{X_1X_2Y_1Y_2 + dZ_1^2Z_2^2}, \frac{(X_1X_2 - Y_1Y_2)Z_1Z_2}{X_1X_2Y_1Y_2 - dZ_1^2Z_2^2})
\end{aligned}$$

$$\begin{aligned}
\text{Therefore, } X_3 &= (X_1X_2 - Y_1Y_2)(X_1X_2Y_1Y_2 + dZ_1^2Z_2^2), \\
Y_3 &= (X_2Y_1 + X_1Y_2)(X_1X_2Y_1Y_2 - dZ_1^2Z_2^2), \\
Z_3 &= (X_1X_2 - Y_1Y_2)(X_2Y_1 + X_1Y_2)Z_1Z_2. \qquad (3.2)
\end{aligned}$$

The following algorithm allows to compute addition efficiently at 9M+1S+1D+7a cost:
$A = Z_1 \cdot Z_2; B = dA^2; C = X_1 \cdot X_2; D = Y_1 \cdot Y_2; E = C \cdot D; H = C - D;$
$I = (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D; X_3 = (E + B) \cdot H; Y_3 = (E - B) \cdot I; Z_3 = A \cdot H \cdot I.$

Special points: The addition formula for inverted Edwards coordinates is not valid only for the points which are on the curve but not satisfy $XYZ \neq 0$. The only points which do not satisfy the condition are $(0, 1), (0, -1), (1, 0)$ and $(-1, 0)$ on the Edwards curve. These points represent the special points of inverted Edwards coordinates $(1, 0, 0), (-1, 0, 0), (0, 1, 0)$ and $(0, -1, 0)$, respectively. For algorithmic reasons, the point $(0, \mp 1, 0)$ in inverted Edwards coordinates corresponds to the point $(\pm 1, 0)$. So, the special cases of addition are $Z = 0$ and $XY = 0$.

Addition of special points $Z_1 = 0$ or $Z_2 = 0$ then $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_1X_2 - Y_1Y_2, X_2Y_1 + X_1Y_2, Z_1 + Z_2)$.

There are four special cases that addition gives a special point as a result:

(A) $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (\pm 1, 0, 0)$:

Suppose addition of two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) is equal to the point $(\pm 1, 0, 0)$ in inverted Edwards coordinates. The corresponding points in Edwards coordinates are $(x_1, y_1) = (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$, $(x_2, y_2) = (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2})$ and $(0, \pm 1)$, respectively. By using the addition formula for Edwards coordinates, it can be said that $x_2y_1 + x_1y_2 = 0$, in other words $(x_2, y_2) = (-x_1, y_1)$ or $(x_2, y_2) = (x_1, -y_1)$.

(A-i) If $(x_2, y_2) = (-x_1, y_1)$ is true, then the equality $(\frac{Z_2}{X_2}, \frac{Z_2}{Y_2}) = (-\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$ is valid and it leads to the conditions that $Z_2X_1 = -Z_1X_2$ and $Z_2Y_1 = Z_1Y_2$. Note also that, these conditions are equivalent to the conditions $X_1Y_2 + X_2Y_1 = 0$ and $Y_2Z_1 = Y_1Z_2$ in [4](Chapter 4, page 6). If the conditions $Z_2X_1 = -Z_1X_2$ and $Z_2Y_1 = Z_1Y_2$ are placed to the Edwards addition formula after replacing $(x_1, y_1) = (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$, $(x_2, y_2) = (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2})$, one can deduce that result of the addition is $(0, 1)$. This means that it is equal to the point $(1, 0, 0)$ in inverted Edwards coordinates.

(A-ii) Similarly, if $(x_2, y_2) = (x_1, -y_1)$ is true, then the equality $(\frac{Z_2}{X_2}, \frac{Z_2}{Y_2}) = (\frac{Z_1}{X_1}, -\frac{Z_1}{Y_1})$ is valid and it leads to the conditions that $Z_2X_1 = Z_1X_2$ and $Z_2Y_1 = -Z_1Y_2$. Note also that, these conditions are equivalent to the conditions $X_1Y_2 + X_2Y_1 = 0$ and $Y_2Z_1 = -Y_1Z_2$ in [4](Chapter 4, page 6). If the conditions $Z_2X_1 = Z_1X_2$ and $Z_2Y_1 = -Z_1Y_2$ are placed to the Edwards addition formula after replacing $(x_1, y_1) = (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$, $(x_2, y_2) = (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2})$, one can deduce that result of the addition is $(0, -1)$. It means that, it is equal to the point $(-1, 0, 0)$ in inverted Edwards coordinates.

(B) $(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (0, \pm 1, 0)$:

Suppose addition of two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) on the inverted Edwards coordinates is equal to the point $(0, \pm 1, 0)$ in inverted Edwards coordinates. The corresponding points in Edwards coordinates are $(x_1, y_1) = (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$, $(x_2, y_2) = (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2})$ and $(\mp 1, 0)$. By using the addition formula for Edwards coordinates, it can be said that $y_1y_2 - x_1x_2 = 0$, in other words $(x_2, y_2) = (y_1, x_1)$ or $(x_2, y_2) = (-y_1, -x_1)$.

(B-i) If $(x_2, y_2) = (y_1, x_1)$ is true, then the equality $(\frac{Z_2}{X_2}, \frac{Z_2}{Y_2}) = (\frac{Z_1}{Y_1}, \frac{Z_1}{X_1})$ is valid and it leads to the conditions that $Z_2Y_1 = Z_1X_2$ and $Z_2X_1 = Z_1Y_2$. Note also that, these conditions are equivalent to the conditions $X_1X_2 - Y_1Y_2 = 0$ and $Y_2Z_1 = -Y_1Z_2$ in [4](Chapter 4, page 6). If the conditions $Z_2Y_1 = Z_1X_2$ and $Z_2X_1 = Z_1Y_2$ are placed to the Edwards addition formula after replacing $(x_1, y_1) = (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1})$, $(x_2, y_2) = (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2})$, one can deduce that result of the addition is $(1,0)$. This means that it is equal to the point $(0,-1,0)$ in inverted Edwards coordinates.

(B-ii) If $(x_2,y_2) = (-y_1,-x_1)$ is true, then the equality $(\frac{Z_2}{X_2},\frac{Z_2}{Y_2}) = (-\frac{Z_1}{Y_1},-\frac{Z_1}{X_1})$ is valid and it leads to the conditions that $-Z_2Y_1 = Z_1X_2$ and $Z_2X_1 = -Z_1Y_2$. Note also that, these conditions are equivalent to the conditions $X_1X_2 - Y_1Y_2 = 0$ and $Y_2Z_1 = X_1Z_2$ in [4](Chapter 4, page 6). If the conditions $-Z_2Y_1 = Z_1X_2$ and $Z_2X_1 = -Z_1Y_2$ are placed to the Edwards addition formula after replacing $(x_1,y_1) = (\frac{Z_1}{X_1},\frac{Z_1}{Y_1})$, $(x_2,y_2) = (\frac{Z_2}{X_2},\frac{Z_2}{Y_2})$, one can deduce that result of the addition is $(-1,0)$. This means that it is equal to the point $(0,1,0)$ in inverted Edwards coordinates.

3.2 Doubling:

Since the addition formula for inverted Edwards curves is unified, it is valid for doubling. But, adding two points has an advantage to make the operation more efficient. So, doubling formula is much more efficient than the addition formula. For example, since X_1 and X_2 are the same and X_1^2 is already computed, computation of $X_1 \cdot X_2$ is unnecessary. The efficient doubling formula for inverted Edwards coordinates is as follows:

$$(X_3,Y_3,Z_3) = (X_1,Y_1,Z_1) + (X_1,Y_1,Z_1) = (\frac{2X_1Y_1Z_1^2}{X_1^2Y_1^2 + dZ_1^4}, \frac{(X_1^2 - Y_1^2)Z_1^2}{X_1^2Y_1^2 - dZ_1^4})$$

$$\begin{aligned} \text{Then, } X_3 &= (X_1^2Y_1^2 + dZ_1^4)(X_1^2 - Y_1^2), \\ Y_3 &= 2X_1Y_1(X_1^2Y_1^2 - dZ_1^4), \\ Z_3 &= 2X_1Y_1Z_1^2(X_1^2 - Y_1^2). \end{aligned} \tag{3.3}$$

$A = X_1^2$; $B = Y_1^2$; $C = Z_1^2$; $D = X_1 \cdot Y_1$; $E = D + D$; $F = A - B$; $G = C^2$; $H = dG$; $X_3 = (D^2 + H) \cdot F$; $Y_3 = (D^2 - H) \cdot E$; $Z_3 = E \cdot F \cdot G$.

Then, the cost is 5M+5S+1D+4a. But, replacing the term $X_1^2Y_1^2$ by $(X_1^2 + Y_1^2)Z_1^2 - dZ_1^4$ makes the computation 1S+2M-2a more efficient. New formula and algorithm are as follow:

$$\begin{aligned} X_3 &= (X_1^2 + Y_1^2)(X_1^2 - Y_1^2); \\ Y_3 &= 2X_1Y_1(X_1^2 + Y_1^2 - 2dZ_1^2); \\ Z_3 &= 2X_1Y_1(X_1^2 - Y_1^2). \end{aligned} \tag{3.4}$$

$A = X_1^2$; $B = Y_1^2$; $C = A+B$; $D = A-B$; $E = (X_1+Y_1)^2-C$; $X_3 = C\cdot D$; $Y_3 = E\cdot(C\cdot -2d\cdot Z_1^2)$; $Z_3 = D\cdot E$. Hence, the new cost is 3M+4S+1D+6a.

3.3 Tripling:

The direct computation of tripling can be done first doubling the point then adding it to the point itself. But, its cost is the cost of addition and doubling, namely 13M+5S+1D+13a. By using equailities from the curve equation, tripling cost can be reduced to 9M+4S+1D+10a:

$A = X_1^2$; $B = Y_1^2$; $C = Z_1^2$; $D = A + B$; $E = 4(D - d\cdot C)$; $H = 2D\cdot(B - A)$; $P = D^2 - A\cdot E$; $Q = D^2 - B\cdot E$; $X_3 = (H + Q)\cdot Q\cdot X_1$; $Y_3 = (H - P)\cdot P\cdot Y_1$; $Z_3 = P\cdot Q\cdot Z_1$.

If S/M is small then there is an alternative for tripling with the cost 7M+7S+1D+17a by the following algorithm:

$A = X_1^2$; $B = Y_1^2$; $C = Z_1^2$; $D = A + B$; $E = 4(D - d\cdot C)$; $H = 2D\cdot(B - A)$; $P = D^2 - A\cdot E$; $Q = D^2 - B\cdot E$; $X_3 = (H + Q)\cdot Q\cdot[(Q + X_1)^2 - Q^2 - A]$; $Y_3 = 2(H - P)\cdot P\cdot Y_1$; $Z_3 = P\cdot[(Q + Z_1)^2 - Q^2 - C]$.

Special points: It is true for all special points that $3(X_1, Y_1, 0) = (X_1, -Y_1, 0)$.

CHAPTER 4

Twisted Edwards Curves

Twisted Edwards curves are defined in [Twst] by the equation $ax^2 + y^2 = 1 + dx^2y^2$ over a field k which has characteristic different than 2 and with distinct nonzero parameters a and $d \in k$. Twisted Edwards curve with the fixed parameters a, d are represented by $E_{E,a,d}$ where sub E indicates that it is a twisted Edwards curve.

For the parameter $a = 1$, every twisted Edwards curve is an Edwards curve.

Addition of two points (x_1, y_1) and (x_2, y_2) on $E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is given by $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2})$. The element $(0, 1)$ is the neutral element and the inverse of (x_1, y_1) is $(-x_1, y_1)$ for the addition operation.

Every twisted Edwards curve $E_{E,a,d}$ is a quadratic twist of the Edwards curve $E_{E,1,\frac{d}{a}}$. There is an isomorphism from $E_{E,a,d} : a\bar{x}^2 + \bar{y}^2 = 1 + d\bar{x}^2\bar{y}^2$ to $E_{E,1,\frac{d}{a}} : x^2 + y^2 = 1 + \frac{d}{a}x^2y^2$ defined by $(\bar{x}, \bar{y}) \mapsto$(x,y)=$(\sqrt{a}\bar{x}, \bar{y})$ over the field $k(\sqrt{a})$. If a is a square then twisted Edwards curve and Edwards curve are isomorphic over the field k. In other words, for a square a, the quadratic twist $E_{E,\bar{a},\bar{d}}$ where $\frac{\bar{d}}{\bar{a}} = \frac{d}{a}$ of an Edwards curve $E_{E,1,\frac{d}{a}}$ is isomorphic to the Edwards curve $E_{E,1,\frac{d}{a}}$ itself.

Addition of two points $(\bar{x}_1, \bar{y}_1)$ and $(\bar{x}_2, \bar{y}_2)$ on the twisted Edwards curve $E_{E,a,d}$ for square a corresponds to the addition of (x_1, y_1) and (x_2, y_2) on the Edwards curve $E_{E,1,\frac{d}{a}}$ which are the transformed points of $(\bar{x}_1, \bar{y}_1)$ and $(\bar{x}_2, \bar{y}_2)$. Therefore, group structure on twisted Edwards curve can be checked in a way that points are transformed to $E_{E,1,\frac{d}{a}}$. Then, corresponding points are added on $E_{E,1,\frac{d}{a}}$. The resulting point transformed back to a point on $E_{E,a,d}$. If addition of the points and transformed point are the same for arbitrary points on $E_{E,a,d}$ then addition operation on twisted Edwards curve defines the same group structure with the Edwards curve. (Note that, in Chapter 2(Edwards), it is proved that addition operation defines a group structure on Edwards curve).

$$\begin{tikzcd}
E_{E,a,d} & E_{E,1,\frac{d}{a}} \\
(x_1, y_1) \arrow[r] & (\bar{x}_1, \bar{y}_1) \\
+ & + \\
(x_2, y_2) \arrow[r] & (\bar{x}_2, \bar{y}_2) \\
\shortparallel\, ? & \shortparallel \\
(x_3, y_3) & (\bar{x}_3, \bar{y}_3) \arrow[l]
\end{tikzcd}$$

To obtain the addition formula on the twisted Edwards curve, we first take two points (x_1, y_1) and (x_2, y_2) on the twisted Edwards curve $E_{E,a,d}$. By using the map $(x, y) \longmapsto (\bar{x}, \bar{y}) = (x\sqrt{a}, y)$. The points (x_1, y_1) and (x_2, y_2) are transformed to the points $(\bar{x_1}, \bar{y_1}) = (x_1\sqrt{a}, y_1)$ $(\bar{x_2}, \bar{y_2}) = (x_1\sqrt{a}, y_1)$ on the Edwards curve $E_{E,1,\frac{d}{a}}$, respectively. Addition of $(\bar{x_1}, \bar{y_1})$ and $(\bar{x_2}, \bar{y_2})$ is $(\bar{x_3}, \bar{y_3}) = (\sqrt{a}\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2})$. Transforming $(\bar{x_3}, \bar{y_3})$ by the inverse transformation $(\bar{x}, \bar{y}) \longmapsto (x, y) = (\frac{\bar{x}}{\sqrt{a}}, \bar{y})$ results with $(x_3, y_3) = (\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2})$ on the $E_{E,a,d}$.

Moreover, there is a birational isomorphism between $E_{E,a,d}$ and $E_{E,d,a}$ given by the rational map $(\bar{x}, \bar{y}) \mapsto (x, y) = (\bar{x}, \frac{1}{\bar{y}})$. More generally, $E_{E,a,d}$ is a quadratic twist of $E_{E,\bar{d},\bar{a}}$ if $\frac{a}{d} = \frac{\bar{a}}{\bar{d}}$ is satisfied.

Homogenous Coordinates Leading to Efficient Group Operations: We have seen that addition formula for twisted Edwards curve is given by $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2})$ for the points (x_1, y_1) and (x_2, y_2) on the twisted Edwards curve for a square $a \in k$ and non-square $d \in k$. As stated above, twisted Edwards curve addition formula coincides with the Edwards addition formula. In other words, it is valid for all pairs and also for doubling. Similar to Edwards curve, transforming to homogenous coordinates reduces the cost of the addition operation on the curve, since addition in homogenous coordinates does not require the inverse elements of the denominators.

A point (x_1, y_1) in twisted Edwards coordinates represented by the point $(X_1 : Y_1 : Z_1)$ for $x_1 = \frac{X_1}{Z_1}$ and $y_1 = \frac{Y_1}{Z_1}$ where $Z_1 \neq 0$.

To find the homogenous twisted Edwards coordinates, replace x by $\frac{X}{Z}$ and y by $\frac{Y}{Z}$ in twisted

Edwards curve:

$$a(\frac{X}{Z})^2 + (\frac{Y}{Z})^2 = 1 + d(\frac{X}{Z})^2(\frac{Y}{Z})^2$$

Hence, the homogenous twisted Edwards curve equation is $(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$.

4.0.1 Addition:

Similarly, addition formula in the homogenous twisted Edwards coordinates for the given points (x_1, y_1) and $(x_2, y_2$ on the twisted Edwards coordinates is the following:

$$\begin{aligned}
(x_1, y_1) + (x_2, y_2) &= (\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}) \\
(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}) + (\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}) &= (\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{Y_1}{Z_1}\frac{X_2}{Z_2}}{1 + d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_2}{Z_2}\frac{Y_1}{Z_1}}, \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - a\frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_2}{Z_2}\frac{Y_1}{Z_1}}) \\
&= (\frac{Z_1Z_2(X_1Y_2 + X_2Y_1)}{Z_1^2Z_2^2 + dX_1X_2Y_1Y_2}, \frac{Z_1Z_2(Y_1Y_2 - aX_1X_2)}{Z_1^2Z_2^2 - dX_1X_2Y_1Y_2}). \qquad (4.1)
\end{aligned}$$

$$\begin{aligned}
\text{Thus, } X_3 &= Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(X_1Y_2 + X_2Y_1), \\
&= Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2], \\
Y_3 &= Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - aX_1X_2), \\
Z_3 &= (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2). \qquad (4.2)
\end{aligned}$$

The following algorithm gives the addition in homogenous Edwards coordinates in 10M+1S+2D+7a: $A = Z_1 \cdot Z_2$; $B = A^2$; $C = X_1 \cdot X_2$; $D = Y_1 \cdot Y_2$; $E = dC - D$; $F = B - E$; $G = B + E$; $X_3 = A \cdot F \cdot [(X_1 + Y_1) \cdot (X_2 + Y_2) - C - D]$; $Y_3 = A \cdot G \cdot (D - aC)$; $Z_3 = F \cdot G$.

4.0.2 Doubling:

Doubling means adding a point with itself, so that $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$. Hence, in the addition formula, if $(X_2 : Y_2 : Z_2)$ is replaced by $(X_1 : Y_1 : Z_1)$, then the formula is the following:

$$\begin{aligned}
X_3 &= Z_1^2(Z_1^4 - dX_1^2Y_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2], \\
Y_3 &= Z_1^2(Z_1^4 + dX_1^2Y_1^2)(Y_1^2 - aX_1^2), \\
Z_3 &= (Z_1^4 + dX_1^2Y_1^2)(Z_1^4 - dX_1^2Y_1^2). \qquad (4.3)
\end{aligned}$$

To convert the formulas much more efficient form, replace $Z_1^4 - dX_1^2Y_1^2$ by $-Z_1^2(aX_1^2 + Y_1^2 - 2Z_1^2)$ and $(Z_1^4 + dX_1^2Y_1^2)$ by $Z_1^2(aX_1^2 + Y_1^2)$ in X_3, Y_3 and Z_3.

Note that: $Z_1^4 - dX_1^2Y_1^2 = 2Z_1^4 - (Z_1^4 + dX_1^2Y_1^2) = 2Z_1^4 - (aX_1^2 + Y_1^2)Z_1^2 = -Z_1^2(aX_1^2 + Y_1^2 - 2Z_1^2)$.

$$\begin{aligned} \text{Thus, } X_3 &= -Z_1^4(aX_1^2 + Y_1^2 - 2Z_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2], \\ Y_3 &= -Z_1^4(aX_1^2 + Y_1^2)(aX_1^2 - Y_1^2), \\ Z_3 &= -Z_1^4(aX_1^2 + Y_1^2)(aX_1^2 + Y_1^2 - 2Z_1^2). \qquad (4.4) \end{aligned}$$

Choose λ as $\lambda = -Z_1^4 \neq 0$, then the following formulas give the doubling formula in homogenous Edwards coordinates:

$$\begin{aligned} X_3 &= (aX_1^2 + Y_1^2 - 2Z_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2], \\ Y_3 &= (aX_1^2 + Y_1^2)(aX_1^2 - Y_1^2), \\ Z_3 &= (aX_1^2 + Y_1^2)(aX_1^2 + Y_1^2 - 2Z_1^2). \qquad (4.5) \end{aligned}$$

The following algorithm gives the doubling operation at a cost 3M+4S+1D+7a:

$B = (X_1 + Y_1)^2$; $C = X_1^2$; $D = Y_1^2$; $E = aC$; $F = E + D$; $H = Z_1^2$; $J = F - 2H$;
$X_3 = (B - C - D) \cdot J$; $Y_3 = F \cdot (E - D)$; $Z_3 = F \cdot J$.

4.1 Alternative Addition and Doubling formulas:

Some applications have more doubling than addition. For such cases, using the curve $E_{E,1,\frac{d}{a}}$ instead of the twisted Edwards curve $E_{E,a,d}$ is more appropriate, since doubling is 1 addition and 1 doubling cheaper on $E_{E,1,\frac{d}{a}}$ while addition is 1 doubling expensive.

4.1.1 Alternative Addition:

Addition formula for $E_{E,1,\frac{d}{a}}$ can be obtained by homogenization of the curve equation and homogenization of the formulas:

$E_{E,1,\frac{d}{a}} : x^2 + y^2 = 1 + \frac{d}{a}x^2y^2$ and the points (x_1, y_1) and (x_2, y_2) are on the curve. And, addition formula is $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2 + x_2y_1}{1 + \frac{d}{a}x_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - \frac{d}{a}x_1x_2y_1y_2})$.

So, addition formula for homogenized coordinates can be found by replacing (x_i, y_i) by $(\frac{X_i}{Z_i}, \frac{Y_i}{Z_i})$ for $i = 1, 2$ as the following:

Curve equation in the homogenous coordinates is $aZ^2(X^2 + Y^2) = aZ^4 + dX^2Y^2$. The points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ represent the points $(x_1, y_1) = (\frac{X_1}{Z_1}, \frac{Y_1}{Z_1})$ and $(x_2, y_2) = (\frac{X_2}{Z_2}, \frac{Y_2}{Z_2})$, respectively.

$$\begin{aligned}
(x_1, y_1) + (x_2, y_2) &= (\frac{x_1y_2 + x_2y_1}{1 + \frac{d}{a}x_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - \frac{d}{a}x_1x_2y_1y_2}) \\
(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}) + (\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}) &= \left(\frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{X_2}{Z_2}\frac{Y_1}{Z_1}}{1 + \frac{d}{a}\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}, \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - \frac{d}{a}\frac{X_1}{Z_1}\frac{X_2}{Z_2}\frac{Y_1}{Z_1}\frac{Y_2}{Z_2}}\right) \\
&= \left(\frac{aZ_1Z_2(X_1Y_2 + X_2Y_1)}{aZ_1^2Z_2^2 + dX_1X_2Y_1Y_2}, \frac{aZ_1Z_2(Y_1Y_2 - X_1X_2)}{aZ_1^2Z_2^2 - dX_1X_2Y_1Y_2}\right). \qquad (4.6)
\end{aligned}$$

Then, addition of the points is $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ where

$$\begin{aligned}
X_3 &= aZ_1Z_2(aZ_1^2Z_2^2 - dX_1X_2Y_1Y_2)[(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2], \\
Y_3 &= aZ_1Z_2(aZ_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2), \\
Z_3 &= (aZ_1^2Z_2^2 - dX_1X_2Y_1Y_2)(aZ_1^2Z_2^2 + dX_1X_2Y_1Y_2). \qquad (4.7)
\end{aligned}$$

And the following algorithm is the addition of two points on the curve $E_{E,1,\frac{d}{a}}$
with $10M + 1S + 3D + 7a$:
$A = Z_1 \cdot Z_2; B = aA^2; H = aA; C = X_1 \cdot X_2; D = Y_1 \cdot Y_2; E = dC \cdot D;$
$F = B - E; G = B + E; X_3 = H \cdot F \cdot [(X_1 + Y_1) \cdot (X_2 + Y_2) - C - D];$
$Y_3 = H \cdot G \cdot (D - C); Z_3 = F \cdot G.$

4.1.2 Alternative Doubling:

$(X_3 : Y_3 : Z_3)$,doubling of $(X_1 : Y_1 : Z_1)$, can be found from alternative addition formula of twisted Edwards coordinates by replacing $(X_2 : Y_2 : Z_2)$ by $(X_1 : Y_1 : Z_1)$ as the following:

$$\begin{aligned}
X_3 &= aZ_1^2(aZ_1^4 - dX_1^2Y_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2], \\
Y_3 &= aZ_1^2(aZ_1^4 + dX_1^2Y_1^2)(Y_1^2 - X_1^2), \\
Z_3 &= (aZ_1^4 - dX_1^2Y_1^2)(aZ_1^4 + dX_1^2Y_1^2). \qquad (4.8)
\end{aligned}$$

In the formulas, $aZ_1^4 - dX_1^2Y_1^2$ can be replaced by $aZ_1^2(2Z_1^2 - X_1^2 - Y_1^2)$ and $aZ_1^2 + dX_1^2Y_1^2$ can be replaced by $aZ_1^2(X_1^2 + Y_1^2)$ in X_3, Y_3 and Z_3. Note that, first can be found as the following and latter is from the homogenized form of $E_{E,1,\frac{d}{a}}$:

$$\begin{aligned} aZ_1^4 - dX_1^2Y_1^2 &= 2aZ_1^2 - Z_1^2 - dX_1^2Y_1^2 = 2aZ_1^2 - (Z_1^2 + dX_1^2Y_1^2) \\ &= aZ_1^2(2Z_1^2 - X_1^2 - Y_1^2) \end{aligned}$$

The new formula is the following:

$$\begin{aligned} X_3 &= a^2Z_1^4(2Z_1^2 - X_1^2 - Y_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2], \\ Y_3 &= a^2Z_1^4(X_1^2 + Y_1^2)(Y_1^2 - X_1^2), \\ Z_3 &= a^2Z_1^4(2Z_1^2 - X_1^2 - Y_1^2)(X_1^2 + Y_1^2). \end{aligned} \tag{4.9}$$

The more efficient form of alternative doubling formula can be obtained by cancelling $a^2Z_1^4$ from X_3, Y_3 and Z_3 since it is on homogenized coordinates and $a^2Z_1^4 \neq 0$.

$$\begin{aligned} X_3 &= (2Z_1^2 - X_1^2 - Y_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2], \\ Y_3 &= (X_1^2 + Y_1^2)(Y_1^2 - X_1^2), \\ Z_3 &= (2Z_1^2 - X_1^2 - Y_1^2)(X_1^2 + Y_1^2). \end{aligned} \tag{4.10}$$

The following algorithm computes the doubling on homogenized twisted Edwards coordinates with the cost of 3M+4S+1D+6a:

$A = X_1^2$; $B = Y_1^2$; $C = Z_1^2$; $D = 2C$; $E = A + B$; $F = B - A$; $G = D - E$;
$X_3 = G \cdot [(X_1 + Y_1)^2 - E]$; $Y_3 = E \cdot F$; $Z_3 = G \cdot E$.

CHAPTER 5

Inverted Twisted Edwards Curves

A point (x_1, y_1) in the inverted twisted Edwards coordinates is represented by the point (X_1, Y_1, Z_1) for $x_1 = \frac{Z_1}{X_1}$ and $y_1 = \frac{Z_1}{Y_1}$ where $X_1 Y_1 Z_1 \neq 0$.

To find the homogenous inverted twisted Edwards coordinates, replace x by $\frac{Z}{X}$ and y by $\frac{Z}{Y}$ in the twisted Edwards curve equation $ax^2 + y^2 = 1 + dx^2y^2$ such that $XYZ \neq 0$:

$$a(\frac{Z}{X})^2 + (\frac{Z}{Y})^2 = 1 + d(\frac{Z}{X})^2(\frac{Z}{Y})^2$$

Thus, the inverted twisted Edwards curve equation is $(X^2 + aY^2)Z^2 = X^2Y^2 + dZ^4$.

5.1 Addition:

Addition formula in the inverted twisted Edwards curve is similar to the one in the inverted Edwards coordinates:

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= (\frac{Z_1}{X_1}, \frac{Z_1}{Y_1}) + (\frac{Z_2}{X_2}, \frac{Z_2}{Y_2}) = \left(\frac{\frac{Z_1}{X_1}\frac{Z_2}{Y_2} + \frac{Z_1}{Y_1}\frac{Z_2}{X_2}}{1 + d\frac{Z_1}{X_1}\frac{Z_2}{X_2}\frac{Z_2}{Y_2}\frac{Z_1}{Y_1}}, \frac{\frac{Z_1}{Y_1}\frac{Z_2}{Y_2} - a\frac{Z_1}{X_1}\frac{Z_2}{X_2}}{1 - d\frac{Z_1}{X_1}\frac{Z_2}{X_2}\frac{Z_2}{Y_2}\frac{Z_1}{Y_1}} \right) \\ &= \left(\frac{Z_1Z_2(X_1Y_2 + X_2Y_1)}{X_1X_2Y_1Y_2 + dZ_1^2Z_2^2}, \frac{Z_1Z_2(X_1X_2 - aY_1Y_2)}{X_1X_2Y_1Y_2 - dZ_1^2Z_2^2} \right).\end{aligned}$$

$$\begin{aligned} Thus, X_3 &= (X_1X_2Y_1Y_2 + dZ_1^2Z_2^2)(X_1X_2 - aY_1Y_2), \\ Y_3 &= (X_1X_2Y_1Y_2 - dZ_1^2Z_2^2)(X_1Y_2 + X_2Y_1), \\ Z_3 &= Z_1Z_2(X_1Y_2 + X_2Y_1)(X_1X_2 - aY_1Y_2). \end{aligned} \tag{5.1}$$

In Y_3, if $(X_1Y_2 + X_2Y_1)$ is replaced by $(X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2$ then the following algorithm gives the additon in the inverted twisted Edwards coordinates with the cost of

9M+1S+2D+7a:

$A = Z_1 \cdot Z_2$; $B = dA^2$; $C = X_1 \cdot X_2$; $D = Y_1 \cdot Y_2$; $E = C \cdot D$; $H = C - aD$;
$I = (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D$; $X_3 = (E + B) \cdot H$; $Y_3 = (E - B) \cdot I$; $Z_3 = A \cdot H \cdot I$.

5.2 Doubling:

By using the addition formula, doubling formula can be found by replacing X_2 by X_1, Y_2 by Y_1 and Z_2 by Z_1:

$$\begin{aligned} X_3 &= (X_1^2Y_1^2 + dZ_1^4)(X_1^2 - aY_1^2), \\ Y_3 &= (X_1^2Y_1^2 - dZ_1^4)(2X_1Y_1), \\ Z_3 &= Z_1^2(2X_1Y_1)(X_1^2 - aY_1^2). \end{aligned} \tag{5.2}$$

Doubling formula can be computed in a much more efficient form if $(X_1^2Y_1^2 + dZ_1^4)$ is replaced by $(X_1^2+aY_1^2)Z_1^2$ in X_3, $2X_1Y_1$ is replaced by $(X_1+Y_1)^2-X_1^2-Y_1^2$ in both Y_3 and Z_3, $(X_1^2Y_1^2-dZ_1^4)$ is replaced by $(X_1^2Y_1^2 + dZ_1^4 - 2dZ_1^4)$ and $X_1^2Y_1^2 + dZ_1^4$ is replaced by $(X_1^2 + aY_1^2 - 2dZ_1^2)Z_1^2$ in Y_3. Finally, Z_1^2 can be cancelled from X_3, Y_3 and Z_3, since $Z_1^2 \neq 0$. Thus, efficient formula for doubling formula is the following:

$$\begin{aligned} X_3 &= (X_1^2 + aY_1^2)(X_1^2 - aY_1^2), \\ Y_3 &= [(X_1 + Y_1)^2 - X_1^2 - Y_1^2](X_1^2 + aY_1^2 - 2dZ_1^2), \\ Z_3 &= (X_1^2 - aY_1^2)[(X_1 + Y_1)^2 - X_1^2 - Y_1^2]. \end{aligned} \tag{5.3}$$

The following algorithm gives the doubling algorithm in the inverted twisted Edwards coordinates with the cost of 3M+4S+2D+6a:

$A = X_1^2$; $B = Y_1^2$; $U = aB$; $C = A + U$; $D = A - U$; $E = (X_1 + Y_1)^2 - A - B$;
$X_3 = C \cdot D$; $Y_3 = E \cdot (C - 2dZ_1^2)$; $Z_3 = D \cdot E$.

CHAPTER 6

Montgomery Curves and Twisted Edwards Curves

Montgomery curves are defined by the equation $Bv^2 = u^3 + Au^2 + u$ over a nonbinary field k where $A \in k - \{-2, 2\}$ and $B \in k - \{0\}$. As a notation, it is represented by $E_{M,A,B}$.

Theorem 6.0.1 *[3, Theorem 3.2] Fix a field k with char$(k) \neq 2$.*

- *Every twisted Edwards curve over k is birationally equivalent over k to a Montgomery curve.*
- *Conversely, every Montgomery curve over k is birationally equivalent over k to a twisted Edwards curve.*

Proof.

- Fix distinct nonzero elements $a, d \in k$. The twisted Edwards curve $E_{E,a,d}$ is birationally equivalent to the Montgomery curve $E_{M,A,B}$, where $A = \frac{2(a+d)}{(a-d)}$ and $B = \frac{4}{a-d}$. The birational equivalence from $E_{E,a,d}$ to $E_{M,A,B}$ defined by the map $(x, y) \mapsto (u, v) = (\frac{1+y}{1-y}, \frac{1+y}{(1-y)x})$ with inverse map $(u, v) \mapsto (x, y) = (\frac{u}{v}, \frac{u-1}{u+1})$.

  For the given transformation, A and B are defined for all a, d except for $a = d$.
  If $A = 2$ then $a + d = a - d$ so $d = 0$; if $A \neq -2$ then $a + d = d - a$ so $a = 0$. So, $A = 2$ and $A = -2$ are contradictions. Thus, $E_{M,A,B}$ is a Montgomery curve.

  There are some exceptional cases such as $y = 1$ and $x = 0$ on $E_{E,a,d}$ and for inverse transformation, $v = 0$ and $u = -1$ on $E_{M,A,B}$. Since these points are finitely many, they don't disturb the birational equivalence.

- Fix $A \in k - \{-2,2\}$ and $B \in k - \{0\}$. The Montgomery curve $E_{M,A,B}$ is birationally equivalent to the twisted Edwards curve $E_{E,a,d}$, where $a = \frac{A+2}{B}$ and $d = \frac{A-2}{B}$.

  Note that, since $B \neq 0$, a and d are defined; since $A \neq -2$, $a \neq 0$; since $A \neq 2$, $d \neq 0$; and $a \neq d$. Thus, $E_{E,a,d}$ is a twisted Edwards curve.

  By i and ii, $A = 2\frac{a+d}{a-d} = 2\frac{\frac{A+2}{B}+\frac{A-2}{B}}{\frac{A+2}{B}-\frac{A-2}{B}} = A$ and $B = \frac{4}{a-d} = \frac{4}{\frac{A+2}{B}-\frac{A-2}{B}} = B$.

  Hence $E_{E,a,d}$ is birationally equivalent to $E_{M,A,B}$ by i and ii.

Exceptional Points for the Birational Equivalence: Birational equivalence between $E_{M,A,B}$ and $E_{E,a,d}$ defined by the map $(u,v) \mapsto (x,y) = (\frac{u}{v}, \frac{u-1}{u+1})$ is undefined at finitely many points namely at the points $u+1=0$ or $v=0$.

- The point $(0,0)$ on $E_{M,A,B}$ corresponds to the one of the points of order 2 on $E_{E,a,d}$ specifically $(0,-1)$. Other order 2 point corresponds to the point at infinity.

- If $(A+2)(A-2)$ is a square in other words ad is a square then there are two points with $v = 0$, namely $(\frac{-A\pm\sqrt{(A+2)(A-2)}}{2}, 0)$. These points are order 2 and corresponds to two points of order 2 at infinity on the desingularization of $E_{E,a,d}$.

- If $\frac{A-2}{B}$ is a square in other words d is a square then there are two points with $u = -1$, namely $(-1, \pm\sqrt{\frac{A-2}{B}}$. These order 4 points correspond to two points of order 4 at infinity on the desingularization of $E_{E,a,d}$.

■

6.1 Edwards Curves versus Montgomery Curves:

Montgomery form of elliptic curves were first introduced for speeding up the Pollard and Elliptic curve methods of integer factorization [10]. Moreover, Montgomery form of elliptic curve implementations are faster than Weierstrass form of elliptic curves [11],[12],[13] and [14]. Later, Bernstein and Lange showed in [2] (Chapter 5,page 13) that Edwards form of elliptic curves are faster than not only the Montgomery form of elliptic curves but also Hessian, Jacobi intersection type of elliptic curves. More specifically, Edwards form addition is as faster as the Hessian form of elliptic curves which is the speed leader of addition operation and Edwards form doubling is as faster as the Jacobi intersection doubling operation which is the speed leader of doubling. The tables 6.1 and 6.2 [2] (Chapter 5,page 13) compare the cost of addition and doubling operations with the form of well known elliptic curves in the literature. Note that, in the table, the column (a,b) shows the costs for the platform that the cost of 1S is equal to aM and the cost of 1D is equal to the cost bM.

Coordinate System	Addition	(1,1)	(0.8,0.5)	(0.8,0)
Doche/Icart/Kohel 2	12M+5S+1D	18M	16.5M	16M
Doche/Icart/Kohel 3	11M+6S+1D	18M	16.3M	15.8M
Jacobian	11M+5S	16M	15M	15M
Jacobi Intersection	13M+2S+1D	16M	15.1M	14.6M
Projective	12M+2S	14M	13.6M	13.8M
Jacobi quartic	10M+3S+1D	14M	12.9M	12.4M
Hessian	12M	12M	12M	12M
Edwards	10M+1S+1D	12M	11.3M	10.8M

Table 6.1: Addition Operation Comparison Table

Coordinate System	Addition	(1,1)	(0.8,0.5)	(0.8,0)
Projective	5M+6S+1D	12M	10.3M	9.8M
Projective if $a = -3$	7M+3S	10M	9.4M	9.4M
Hessian	7M+1S	8M	7.8M	7.8M
Doche/Icart/Kohel 3	2M+7S+2D	11M	8.6M	7.6M
Jacobian	1M+8S+1D	10M	7.9M	7.4M
Jacobian if $a = -3$	3M+5S	8M	7M	7M
Jacobi quartic	2M+6S+2D	10M	7.8M	6.8M
Jacobi Intersection	3M+4S	7M	6.2M	6.2M
Edwards	3M+4S	7M	6.2M	6.2M
Doche/Ikart/Kohel 2	2M+5S+2D	9M	7M	6M

Table 6.2: Doubling Operation Comparison Table

Edwards curves also have unified addition property which is the property that addition and doubling can be computed by the same formula. Moreover, for non-square parameter d, Edwards curve addition operation has the completeness property which is the property that addition can be applied to any point pair on the Edwards curve without any check. Thus, for implementation issues, Edwards curves are more reasonable than other form of elliptic curves.

Coordinate System	Addition	Doubling
Edwards	10M+1S+7a+1C+1D	3M+4S+6a+3C
Inverted Edwards	9M+1S+7a+1D	3M+4S+6a+1D
Twisted Edwards	10M+1S+7a+2D	3M+4S+7a+1D
Twisted E. (Alternative)	10M+1S+7a+3D	3M+4S+6a+1D
Inverted Twisted E.	9M+1S+7a+2D	3M+4S+6a+2D

Table 6.3: Edwards Curves Comparison Table

6.2 Edwards Curves versus Twisted Edwards Curves:

From the table, it can be observed that inverted coordinates are more efficient. When it is needed to make a choice between the inverted Edwards coordinates and twisted Edwards coordinates for elliptic curve cryptography implementation in the efficiency point of view, it can be said that Edwards curve should be chosen. But, by more detailed analyse, one can realise that, 1D in Edwards coordinates is multiplication by curve parameter d and 2D in Twisted Edwards coordinate is multiplication by twisted Edwards curve parameters a and d. Most of the time, curve parameter d can be written as $\frac{\bar{d}}{\bar{a}}$ in the finite field k. As mentioned in Chapter 2, the Edwards curve $E_{E,1,d}$ where $d = \frac{\bar{d}}{\bar{a}}$ is birationally equivalent to the twisted Edwards curve $E_{E,\bar{d},\bar{a}}$. Over the finite field, in general, big number can be written as a division of two small number. In our situation, multiplying with two small integer instead of one big integer is cheaper over the finite field k. The following example shows the advantage of the twisted Edwards curve instead of edwards curve. The Edwards curve $E_{E,1,\frac{121665}{121666}} : x^2+y^2 = 1+\frac{121665}{121666}x^2y^2$ over the field $p = 2^{255}-19$ which is birationally equivalent to the Curve25519 the speed leader of Diffie-Hellman before the occurrence of the Edwards curve in the literature is isomorphic to the twisted Edwards curve $E_{E,121666,121665} : 121666x^2+y^2 = 1+121665x^2y^2$. For an addition over the curves, the former curve consist an multiplication by the curve parameter $\frac{121665}{121666} \equiv 20800338683988658368647408995589388737092878452977063003340006470870624536394 \bmod(2^{255}-19)$ and the latter has two multiplication by the curve parameters 121666 and 121665 $\bmod(2^{255}-19)$. Therefore, the addition and doubling operations can be regarded as cheaper over the inverted twisted Edwards coordinates. Moreover, inverted twisted Edwards coordinates are birationally equivalent to more elliptic curves than inverted Edwards curves. Thus, inverted twisted Edwards coordinates can be regarded as the more appropriate form of elliptic curve for elliptic curve cryptography.

CHAPTER 7

Conclusion

In recent years, there has been an increase in the number of applications which use ECC. The applications are mostly used in low capacity platforms such as contactless smart cards. Thus, it is important to define ECC computations with high efficiencies and with low costs as much as possible without losing the security level. This makes Edwards curves an important area of research.

In this work, we have given an expository overview of the literature on Edwards curves. The Edwards curves were defined in 2007 by M. Harold Edwards, and modified and applied to ECC by D. Bernstein and T. Lange. In chapter 1, a brief information on the importance of ECC has been given. In chapter 2,3,4 and 5, types of Edwards curves have been introduced, explicit formulas for addition and doubling have been explained and cost of the operations have been stated. In the last chapter, it is explained why the Edwards curves are more suitable for ECC then any other known elliptic curve forms. It has been also stated how to understand which Edwards curve is the best for the implementation issues.

REFERENCES

[1] H. M. Edwards, *A Normal Form For Elliptic Curves*, Bull. Amer. Math. Soc., Volume 44, Number 3, pp. 393422, July 2007.

[2] D. J. Bernstein, T. Lange, *Faster Addition and Doubling on Elliptic Curves*, Advances in Cryptology ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2008, pp. 29-50, Springer Berlin-Heidelberg, Nov. 2007.

[3] D. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, *Twisted Edwards curves*, In Progress in Cryptology - AFRICACRYPT 2008, pp. 389-405, 2008.

[4] D. J. Bernstein, T. Lange, *Inverted Edwards Coordinates*, AIn: Bozta¸s, S., Lu, H.-F.(eds.) AAECC 2007. LNCS, vol. 4851, pp. 2027. Springer, Heidelberg, 2007.

[5] W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, vol. 22, issue 6, pp. 644-654, 1976.

[6] R. L. Rivest, A. Shamir, and L. Adelman. *On Digital Signatures and Public Key Cryptosystems*, MIT Laboratory for Computer Science Technical Memorandum 82, 1977.

[7] N. Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation, vol. 48, no. 177, pp. 203-209, AMS, 1987.

[8] V. S. Miller,*Use of Elliptic Curves in Cryptography*, 218 on Advances in cryptology - CRYPTO 85, Lecture Notes in Computer Science, pp. 417-426, Springer-Verlag, 1986.

[9] NSA-National Security Agency, *The Case for Elliptic Curve Cryptography*, http://www.nsa.gov/business/programs/elliptic_curve.shtml, last visited at Agust 30, 2009.

[10] P.L. Montgomery, *Speeding the Pollard and Elliptic Curve Methods of Factorizations*, Math. Comp. 48, pp. 243-264, 1987.

[11] K. Takauchi, K. Koyama, *Fast Computation of Elliptic Curve Cryptosystems*, SCIS'99, pp. 281-284, 1999.

[12] T. Izu, *Elliptic Curve Exponentiation for Cryptosystem*, SCIS'99, W4-1.1, pp. 275-280, 1999.

[13] T. Izu, *Elliptic Curve Exponentiation without y-coordinate*, Technical report of IEICE, ISEC98-86, pp. 93-98, 1999.

[14] K. Ohgishi, R. Sakai, M. Kasahara, *Elliptic Curve Signature Scheme with no y-coordinate*, SCIS'99, W4-1.3, pp. 285-287, 1999.