Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Education for Pure Sciences

Twisted Edwards Curves for Elliptic Scalar Multiplication Method

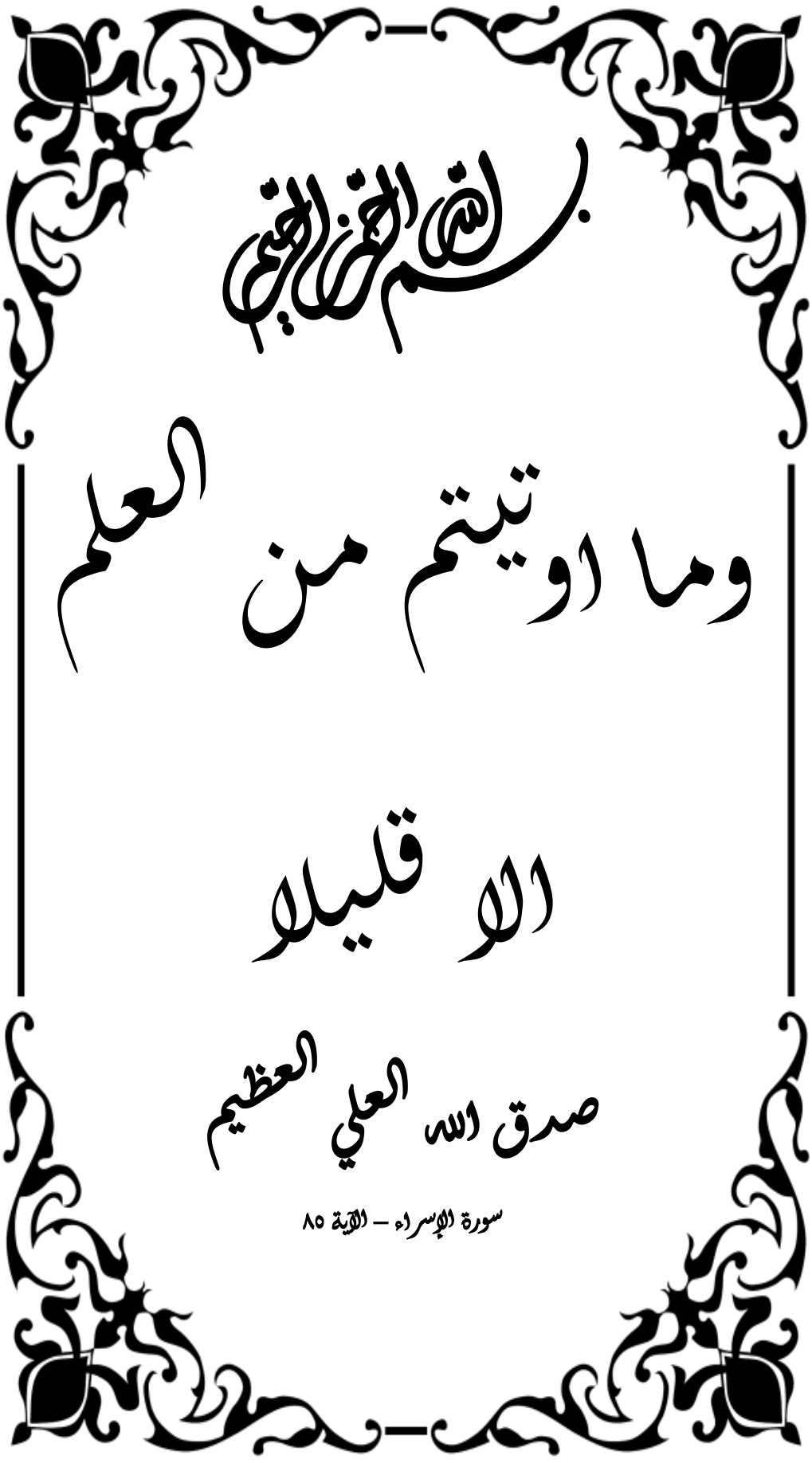
A Dissertation
Submitted to The Council of The College of Education for Pure Sciences in University of Babylon in Partial Fulfillment of The Requirements for the Degree of Doctor of Philosophy in Education / Mathematics
By

Jolan Lazim Theyab Abed

Supervised by

Asst. Prof. Dr. Ruma Kareem K. Ajeena

2021 A.D. 1443 A.H


بسم الله الرحمن الرحيم
وما اوتيتم من العلم
الا قليلا
صدق الله العلي العظيم
سورة الإسراء – الآية ٨٥

DEDICATION

To our greatest and honored prophet Mohamed (God prays on him);

to my master and my master who was slaughtered thirsty in Karbala, the dead man of the abras, al-Husayn ibn Ali(peace be upon him) ;

I dedicate this work.

ACKNOWLEDGEMENT

First, my thanks and gratitude to Allah, the almighty who awarding me the opportunity and health to complete this work.

I would like to thank my supervisor Dr. Ruma Kareem K. Ajeena for her help, encouragement, guidance and support to complete my research work in this dissertation. My prayer for her and I will remember her help and kindness with me. My gratitude and thank fullness for her.

I would like to thank other professors who helped us during the master study. Finally, I'm very thankful to all my family, especially my father and mother.

Jolan Lazim

CONTENTS

List of Tables

Mathematical Symbols

p	Prime number.
F_p	Prime field.
g	Primitive root.
E	Elliptic curve.
O_E	Infinity point on elliptic curve.
Δ	Discriminate of E.
$E(F_p)$	Elliptic curve group over F_p.
$\oplus$	Direct sum.
$\#E(F_p)$	Order of elliptic curve group over F_p.
P_1, P_2	Points on elliptic curve.
t	A scalar.
tP	Scalar multiplication operation.
n	Prime order of P.
$+$	Addition.
$\cdot$	Multiplication.
$\approx$	Approximately.
$\mid$	Division.
$\equiv$	Congruence.
ψ	The efficiently computable endomorphism.
E_d	Edwards curve.
$E_{a,d}$	Twisted Edwards curve.
$\lfloor d \rceil$	the largest integer that is nearest to x .
Mod	Modulo.

$\bmod n$	Arithmetic modulo n.
$\gcd(a,b,c)$	Greatest common divisor of a, b and c

Abbreviations

EEA	Extended Euclidean Algorithm.
GLV	The Gallant-Lambert-Vanstone
GEEA	Generator Extended Euclidean Algorithm.
EC	Elliptic Curve.
E_d	Edward curve.
$E_{a,d}$	Twisted Edward curve.
ECC	Elliptic Curve Cryptosystem.
ISD	Integer Sub-Decomposition.
EGSA	Extended Gram–Schmidt Algorithm.

Publications

The publications of this work are

1. Jolan Lazim Theyab and Ruma Kareem K. Ajeena, The 3-Dimension Integer Sub-Decomposition Method for Edwards Curve Cryptography. In AIP Conference Proceedings (ISSN: 0094-243X) (acceptable for publication)
2. Jolan Lazim_Theyab and_Ruma Kareem K. Ajeena,_ The 3-ISD Method for Twisted Edwards Scalar Multiplication. In AIP Conference Proceedings (acceptable for publication)
3. Jolan Lazim Theyab and Ruma Kareem K. Ajeena, Edwards Scalar Multiplication-Based 3-Integer Sub-Decomposition Method. submitted).

Abstract

Elliptic curve cryptosystem (ECC) is being used nowadays more than ever to fulfill the need for public key cryptosystem. The most time consuming operation in ECC is elliptic curve scalar multiplication (ECSM)**.** The structure of the ECSM involves three mathematical levels: field arithmetic, point arithmetic and scalar arithmetic. The purpose of this work is to study issues that arise in the efficient implementation of ECSM over prime field with special curve. At the point arithmetic level, we introduce three dimensions of integer sub-decomposition (3-ISD) method to compute a scalar multiplication on Edwards curves and twisted Edwards curves defined over the prime field. This methods proven their efficiency in many contexts that compute a scalar multiplication on Edwards curves and twisted Edwards curve , some versions are discussed based on the 3-LLL lattice reduction method and the randomized method to generate the 3-ISD generators. The 3-ISD generators computed by 3-LLL and the randomized method are used to decompose a scalar t in a scalar multiplication tP .

Chapter One

INTRODUCTION

1.1 Introduction

The history of cryptography can be split into two eras: the classical era and the modern era. The turning point between the two occurred when asymetric cryptography was introduced. These new algorithms were revolutionary because they represented the first viable cryptographic schemes where security was based on the theory of numbers; it was the first to enable secure communication between two parties without a shared secret. Cryptography went from being about securely transporting messages around the world to being able to have provably secure communication between any two parties without worrying about someone listening in on the key exchange. The founding idea is that the key you use to encrypt your data can be made public while the key that is used to decrypt your data can be kept private. What you need for an asymetric cryptographic system to work is a set of algorithms that is easy to process in one direction, but difficult to undo. The first, and still most widely used, algorithm introduced was RSA. Its security relies on the fact that multiplying two prime numbers is easy, but factoring the product into its two component primes is difficult. After RSA, researchers explored other mathematics-based cryptographic solutions looking for other algorithms beyond factoring that serve asymetric schemes. Elliptic curve cryptography was then proposed.

This work proposes new version of three dimensions of integer sub-decomposition (3-ISD) method to compute a scalar multiplication on Edwards curves and twisted Edwards curves defined over the prime field

F_p that can be employed by any cryptographer to improve the Edwards or twisted Edwards curve cryptosystems.

On the proposed 3-ISD method, some versions are discussed based on the 3-LLL lattice reduction method and the randomized method to generate the 3-ISD generators. The 3-ISD generators computed by 3-LLL and its extension are used to decompose a scalar t in a scalar multiplication tP on Edwards E_d and twisted Edwards $E_{a,d}$ curves defined over F_p in four versions of Edwards curve E_d and twisted Edwards curve $E_{a,d}$.

On the other hand, other four versions of 3-ISD method are proposed in this work. These versions depended on the randomizational choices of the elements from the range $[1, p-1]$, where p is large prime. These elements are used to generate the 3-ISD generators. The decomposition of a scalar t is done depended on these vectors. These decompositions are performed in similar ways to previous versions that are applied using 3-LLL algorithm. Several experimental results are implemented using Matlab languge for all proposed versions of 3-ISD method.

The comparison between these versions of 3-ISD method based on the randomized generator consider as more fast in compare to the other versions that are depended on 3-LLL algorithms. The distributions of the scalar t in the interval $[1, n-1]$ are discussed by examples. The algorithms to determine all scalars t in interval $[1, n-1]$ that have 3-ISD sub scalars.

Finally, the 3-ISD versions are considered as a bright method for more secure and suitable of the Edwards and twisted Edwards curve cryptographic communications by any cryptographer.

1.2 Previous Studies

In 2007, Edwards [1] presented a normal form $x^2 + y^2 = a^2 + a^2x^2y^2$ for elliptic curves. That allowed giving the addition law. On the elliptic curve also, the j-invariant is defined and the transcendental functions x(t) and y(t) that parameterize are determined.

In 2007, Bernstein and Lange [2], presented the explicit formulas for addition and doubling in coordinates (X : Y : Z). They also introduced the inverted Edwards coordinates ($X_1 : Y_1 : Z_1$) which can be presented as an affine point (Z_1/X_1,Z_1/Y_1) on an Edwards curve. Point, Also their work presented the addition formulas for inverted Edwards coordinates using only 9M+ 1S which are not complete but they are strongly unified. Further, they showed that the doubling formulas used only 3M + 4S, and tripling formulas used only 9M + 4S. Inverted Edwards coordinates saved 1M for each addition, without slowing down doubling or tripling.

In 2007, Bernstein and Lange [3], presented the formulas for group operations on an Edwards curve. The algorithm to compute the doubling used only 3M+ 4S, whereas, the algorithm for mixed addition usesd only 9M + 1S and the algorithm for non-mixed addition uses only 10M + 1S. They also introduced a comparison of different forms of elliptic curves and different coordinate systems for the basic group operations which are doubling, mixed addition, non-mixed addition and unified addition. A higher-level operations what is multi-scalar multiplication is presented as well.

In 2008, Bernstein and Lange [4], studied the pre-computed of elliptic-curve points $2P$, $3P$, $5P$, $7P$, $9P$, . . . , mP in a sliding-window computation. They discussed how many field multiplications are required for the resulting computation of mP and gave the answers of that based on the size

of m, the I/M ratio, the choice of curve the choice of coordinate system, and the choice of addition formulas. Also they compared between these previous analyses.

In 2008,Sagheer [5],We design and implement an elliptic curves public key encryption scheme, in which there is one public encryption key, but many private decryption keys which are distribute through a broadcast channel, the security of the elliptic curves public key.

Also in 2008, Bernstein, et al.[6], introduced the twisted Edwards curves as a generalized case Edwards curves. They showed that the twisted Edwards curves included more curves over finite fields. They also presented the formulas for twisted Edwards curves in projective and inverted coordinates. They showed that the twisted Edwards curves saved the time for many curves that were already expressible as Edwards curves.

In 2009, Morain and François [7], introduced the view of parameterizing elliptic curves given by their j-invariant to compute a complex multiplication (CM). They classified the CM curves that admitted an Edwards or Montgomery form over a finite field and justified the used of isogenous curves.

Also, in same year, Baldwin, Brian, et al [8], presented the implemented results of a reconfigurable elliptic curve processor defined over prime fields F_p. This processor is used to compare a method to compute point addition and point doubling operations on the twisted Edwards curves with the double-and-add algorithm Security levels of both algorithms are also examined and compared.

In 2010 Luk, et at. [9], defined an optimally reduced basis for a lattice in the sense that an optimally reduced as shortest basis in a lattice. Also, they

presented an algorithm for computing an approximation of an optimally reduced basis for a lattice using a novel unimodular transformation.

In 2010 Ibraheem [10], we reduce the calculation by putting the available values of m in two cases, even or odd values. For computations we introduce an algorithm for computing the coefficient as well as finding the values of a and b which makes the elliptic curve that defined on Fp as a supersingular elliptic curve.

Also, in 2010 Moody and Dustin [11], Wu (A mean value formula for elliptic curves, 2010, available at http://eprint.iacr.org/2009/586.pdf) recently devised a definite mean-value formula for the coordinates of the n-division points on an elliptic curve provided in Weierstrass form. On a twisted Edwards elliptic curve, we show a comparable conclusion for the x and y-coordinates.

In 2011, D.J. Bernstein and Lange [12], studied a complete set of addition laws for incomplete Edwards curves given by an equation of the form $ax^2 + y^2 = 1 + dx^2y^2$ with $a \neq d$, a, d, $\in k\backslash\{0\}$. They have combined the Edwards's idea of addition formula and dual addition law which was proposed by Hisil et al.

In 2012 Sagheer, [13], proposes one-way trap-door function defined over Matrices group, We call it Matrices Discrete Logarithm Problem (MDLP) and introduces the first proposed cryptosystems that employ the finite matrices group in the public key cryptosystems.

In 2012 Farashahi, et.al. [14], found an exact formula for the number of Fq-isomorphism classes of Edwards curves, original Edwards curves, and twisted Edwards curves. They discovered a formula for calculating the number of distinct isogeny classes for particular elliptic curve family. For Edwards curves, they were able to accomplish this .

Also, in 2012 Ahmadi, et.al. [15], they count the number of isogeny classes of Edwards curves over odd characteristic finite fields, they also showed that each isogeny class contains a complete Edwards curve, and that an Edwards curve is isogenous to an original Edwards curve over F_q if and only if its group order is divisible by 8 if $q \equiv -1 \pmod 4$, and 16 if $q \equiv 1 \pmod 4$. Furthermore, they gived formulae for the proportion of $d \in F_q \setminus \{0, 1\}$ for which the Edwards curve E_d is complete or original, relative to the total number of d in each isogeny class.

Also, in same year, Hamburg and Mike[16], proposed quicker field arithmetic, a novel point compression algorithm, an improved fixed-base scalar multiplication algorithm, and a new way to verify signatures without inversions or coordinate recovery.

In 2014 Hamburg and Mike [17], proposed that designers describe Edwards curves but use an isogenous twisted Edward to implement scalar multiplications and other operations.

In 2014, Abd ulkareem[18],proposed new encryption algorithm using in RGB image encryption supported by Elliptic Curve Cryptography (ECC) with forward key mixing process. The main advantage of elliptic curves systems is thus their high cryptographic strength relative to the size of the key. The propose scheme is simple, fast and sensitive to the secret key.

Also, in 2014, Ajeena and Kamarulhaili [19], proposed an approach called the integer sub-decomposition (ISD) method for computing the scalar multiplication kP on an elliptic curve E. This approach uses two fast endomorphisms ψ_1 and ψ_2 of E over prime field F_p.

In 2015, Barnard [20], presented a comparison on the Edwards curves, twisted Edwards curves and Montgomery curves. As well, this work discussed the application of the E_d DSA of $E_{a,d}$s.

Also, in same year, Zhe, et al [21], they first introduced a special twisted Edwards curve with an efficiently computable endomorphism and described how said endomorphism be exploited to speed up double-base scalar multiplication.

In 2016, Rao, et al. [22], presented a differential addition formula on Generalized Edwards' Curves that is proposed by Justus and Loebenberger at IWSEC 2010 [15]. Their work introduced an efficient affine differential addition formula of a proposed model on the Binary Edwards Curves by Wu, Tang, and Feng at INDOCRYPT 2012 [16]. A point doubling algorithm on $E_{a,d}$ is provided with different projective coordinates.

In 2017, Farashahi, et al. [23], introduced novel differential addition and doubling formulas for twisted Edwards curves as the main step in Montgomery scalar multiplication. When the specified difference point is in affine form, the formulas are presented with costs of 5M + 4S + 1D, 3M + 7S + 1D, and 3M + 6S + 3D. The expenses of a field multiplication, a field squaring, and a field multiplication by a constant are denoted by M, S, and D, respectively.

In 2018, Skuratovskii [24], constructed a new method for counting the order of an Edwards curve over a finite field. Also, that this method can be applied to the order of elliptic curves due to the birational equivalence between elliptic curves and Edwards curves. they not only find a specific set of coefficients with corresponding field characteristics for which these curves are supersingular, but they additionally find a general formula by which one can determine whether a curve $E_{\mathrm{d}}[F_{\mathrm{p}}]$ is supersingular over this field or not.

Also, in 2018, Vo [25], The fundamental principles of Edwards curves, twisted Edwards curves, and point addition rules on these curves were

presented. The primary result is the parameterization of the Edward curve in the rational field Q with the provided torsion subgroup.

Also, in same year, Ajeena, , and Sanaa [26], suggested a generalized Lagrange-Gauss reduction approach for generating the generators in the ISD method. The results of the generalized Lagrange-Gauss reduction method and the generalized extended Euclidean algorithm were compared. The relationship between the generalized Lagrange-Gauss Reduction and the expanded extended Euclidean Method to compute reduced bases to produce ISD generators in the ISD elliptic scalar algorithm is also discussed.

In 2019, Boudabra and Nitaj [27], they researched Edwards algebraic curves over a finite field, which are one of the most promising supports of sets of points which are used for fast group operations. They constructed a new method for counting the order of an Edwards curve $E_d[F_p]$over a finite field F_p. Also, that this method can be applied to the order of elliptic curves due to the birational equivalence between elliptic curves and Edwards curves. they not only fond a specific set of coefficients with corresponding field characteristics for which these curves are supersingular, but they additionally fond a general formula by which one can determine whether a curve $E_d[F_p]$ is supersingular over this field or not.

In 2020 Skuratovskii and Osadchyy [28], presented a new effective algorithm for the elliptic and Edwards curves order curve counted , additionally obtained. The criterion for supersingularity of these curves.

In 2021 Atnashev et al [29], introducesed fast algorithms for performing group operations on Edwards curves using FFT-based multiplication. Previously known algorithms can use such multiplication too, but better

results can be achieved if particular properties of FFT-based arithmetic are accounted for. The introduced algorithms perform operations in extended Edwards coordinates and in Montgomery single coordinate.

Also, in 2021 Bessalov et al [30], studied an overview of the propertise of three classes of curves in generalized Edwards form $E_{a,d}$ with two parameters is given. The known formulas for the odd degree isogenies on curves Ed with one parameter are generalized to all classes of curves in Edwards form. Methods for bypassing the exceptional points of such curves in PQC cryptosystems like CSIDH are proposed.

Also, in same year, Ajeena [31], has studied a new version of the ISD method for computing a scalar multiplication on elliptic curve defined over prime field has been proposed. This levels is called the soft graphic ISD (SG-ISD) method. Thus, undirected simple graph can be proved as the SG-ISD version.. The computational complexities of the original ISD and proposed SG-ISD methods are determined mathematically on the basis of the counting operations.

1.3 Problem Statement

The computation of a scalar multiplication tP have been done using new versions of the integer sub-decomposition (ISD) in 3-dimention . These versions depend on the sub-decomposition concept of a scalar t in operation tP, where $t \in [1, n-1]$ and P is a point on an Edward curve E_d and twisted Edward curve $E_{a,d}$ defined over the prime field F_p, which has a prime order n.

In other words, a scalar t has been sub-decomposed into t_{11}, t_{12} and t_{21}, t_{22} with $\max\{|t_{11}|, |t_{12}|\} \leq \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \leq \sqrt{n}$. So, the scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1 + t_{21} + t_{22}\lambda_2 \pmod{n},$$

where $\lambda_1, \lambda_2 \in [1, n-1]$ and $\lambda_1 \neq \pm\lambda_2$.

The scalar multiplication tP by using ISD method can be computed by

$$tP \equiv t_{11}P + t_{12}\psi_1(P) + t_{21}P + t_{22}\psi_2(P) \pmod{p},$$

where $\psi_1(P)$ and $\psi_2(P)$ are two efficient computable endomorphisms of E_d and $E_{a,d}$ defined over F_p.

Many researchers have studied the E_d and $E_{a,d}$. All the studies which are proposed previously on the E_d and $E_{a,d}$ depended on the concept of the points addition and doubling laws on Edward curve and Twisted Edward curve to compute a scalar multiplication tP. The decomposition or sub-decomposition of a scalar t in a scalar multiplication tP. So, this work proposes using the decomposition and sub-decomposition, namely 3-ISD method, of a scalar t in a scalar multiplication tP to improve the Edward curve through the computations of tP. The proposed E_d 3-ISD method is benefited from speeding the computations of tP resulting from the sub-decomposition of t and the pre-computations of the endomorphisms of E_d and $E_{a,d}$ defined over a prime field F_p.

In this work also, another proposed to modify the E_d and $E_{a,d}$ is applied based on the randomized vectors to find the 3-ISD generators for speeding the computations of tP on the E_d and $E_{a,d}$, which employed the decomposition of a scalar t into t_1, t_2 and t_3 such that a scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' + t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' + t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\mathrm{mod}\, n).$$

with $\max\{|t_{11}|,|t_{12}|,|t_{13}|\} \le \sqrt{n}$, $\max\{|t_{21}|,|t_{22}|,|t_{23}|\} \le \sqrt{n}$ and $\max\{|t_{31}|,|t_{32}|,|t_{33}|\} \le \sqrt{n}$. where $\lambda_1', \lambda_2', \lambda_1'', \lambda_2'', \hat{\lambda}_1, \hat{\lambda}_2 \in [1,\ n-1]$, and $\lambda_1' \neq \pm\lambda_2', \lambda_1'' \neq \pm\lambda_2'', \hat{\lambda}_1 \neq \pm\hat{\lambda}_2$.

1.4 The Objectives of this Dissertation

The objective of this study is introducing an alternative method different from the previous methods that have been applied on the Edward curve and twisted Edward curve for computing a scalar multiplication tP. This method is called 3-ISD method that uses the efficiently computable endomorphisms of E_d and $E_{a,d}$ depends on the sub-decomposition of the scalar t in tP.

1.5 The Structure of this Dissertation

The outline of this study is as follows: in addition to chapter 1, there are:

- **Chapter 2:** includes the basic facts of the finite fields, this chapter presents an introduction to the elliptic curves over the prime fields, the scalar multiplication on elliptic curves, the efficient computable endomorphisms, the scalar multiplication methods based on the efficient, interleaving method. Also, it explains the Gram-Schmidt Algorithm and lattice reduction Algorithm and introduction to the Edward curves and Twisted Edward curves over the prime fields, representing method of the Edward curves and Twisted Edward curve has been discussed. Finally, simple examples are presented.
- **Chapter 3**: presents a new version of the integer sub-decomposition method on decomposing the Scalar t in 3-dimension. In other words, the 3-ISD generators are generated with 3-dimension to decompose and sub-decompose the Scalar t in a scalar multiplication tP.To generate these generators, the 3-LLL lattice reduction method and

extension of it are used. It explains Four case of 3-ISD method are employed to compute a scalar multiplication tP Edwards and twisted Edwards curves defined over prime field. The security considerations of these case are discussed and determined. As well as, presents the computational complexities of the addition and doubling point on Edwards and twisted Edwards curves.

- **Chapter 4:** In this Chapter, a new version of the integer sub-decomposition method on decomposing the Scalar t in 3-dimension. In other words, the 3-ISD generators are generated with 3-dimension to decompose and sub- decompose the Scalar t in a scalar multiplication tP. To generate these generators, the vectors that have three dimensions that are chosen randomly and each component on each vector is relatively prime is used. Four case of 3-ISD method are employed to compute a scalar multiplication tP Edwards and twisted Edwards curves defined over prime field.
- **Chapter 5:** It includes some computational results on the proposed a schemes.
- **Chapter 6:** Draws the conclusions and future works.

Chapter Two

Mathematical Background

2.1 Introduction

A rich history of elliptic curves motivated many mathematician researchers to use them for solving some problems. For designing the public key cryptosystems. Neal Koblitz and Victor Miller in 1985 proposed the usage of elliptic curves, which are defined over finite fields. The security of the elliptic curve cryptosystems depended on the hardness of solving the elliptic curve discrete logarithm problem [32].

This chapter presents the important facts of elliptic curves defined over a prime field. It first discusses some basic definitions, theorems and examples on finite fields and also several fundamental tools in number theory.

2.2 Introduction to the Finite Fields

In this section, the mathematical concepts related to fields, especially finite fields are discussed as follows.

Definition 2.2.1. (Field). A field is an order triple $(F,\star,\circ)$, where F is nonempty set and $\star$ and $\circ$ are two binary operations of F satisfying the following properties:

- $(F,\star)$ and $\left(F-\{e_1\},\circ\right)$ are abelian groups, where e_1 is identity element of $(F,\star)$.
- For any elements $a,b,c\in F$, then

$$a\circ(b\star c)=(a\circ b)\star(a\circ c) \text{ and } (b\star c)\circ a=(b\circ a)\star(c\circ a),$$

Which is called the distribution law [33].

Definition 2.2.2. (Finite Field or Galois field). A field with finitely many elements is called a finite field. The finite field with p elements is denoted by F_p. Finite fields are also called Galois fields [34].

If a finite field has p elements, and p is prime, then the field is called a prime field, which is defined as follows.

Definition 2.2.3. For a prime p, let F_p be a set $\{0,1,...,p-1\}$ of integers and let $\varphi: Z/(p) \to F_p$ be the mapping defined by $\varphi([a]) = a$ for $a = 0,1,...,p-1$. Then F_p, endowed with the field structure induced by φ, is a finite field, called the Galois field of order p [34].

Example 2.2.1. If $p = 7$, a set with seven elements is

$F_7 = \mathbb{Z}/7\mathbb{Z} = \{\{...,-17,-7,0,7,14,...\}, \{...,-13,-6,1,8,15,...\}$
$,\{...,-12,-5,2,9,16,...\}\ \{...,-11,-4,3,10,17,...\}, \{...,-10,-3,4,11,18,...\}$
$,\{...,-9,-2,5,12,19,...\}, \{...,-8,-1,6,13,20,...\}\}.$

Definition 2.2.4. (The Characteristic of a Field). Let F be a field. The characteristic of F is the least positive integer p such that, $p \cdot 1 = 0$, where 1 is the multiplicative identity of F. If no such p exists, we define the characteristic to be 0 [35].

Example 2.2.2 .

(i) The characteristics of $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are 0.

(ii) The characteristics of the field Z_p is p for any prime p [35].

Example 2.2.3. The ring $F_{17} = Z/17Z$ is a prime field of characteristic 17. The F_{17} has exactly 17 elements. So it is a finite. It is easy to check F_{17} as

a field. Every element in F_{17} is equal to zero under multiplication by 17, thus, the characteristic is 17.

Lemma 2.2.1: Let F be a field.

1. If the characteristic of F is positive, then $char(F)$ is a prime.

2. The finite fields have $char(F) > 0$. By the first part of this lemma, a finite field has a prime characteristic [34].

Theorem 2.2.1 (Primitive Root Theorem). Let p be a prime number. Then there exists an element $g \in F_p^*$ whose powers give every element of F_p^*, i.e.

$$F_p^* = \{1, g, g^2, g^3, \ldots, g^{p-2}\}.$$

Elements with this property are called primitive roots of F_p or generators of F_p^*. They are the elements of F_p^* having order $p-1$ [36].

Example 2.2.4: Suppose $p = 19$ and $F_{19}^* = \{1, 2, \ldots, 18\}$. An element $a = 3$ is a generator root of F_{19}^*, since $a = 3$ generates all elements in F_{19}^*.

In other words,

$3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 8, 3^4 \equiv 5, 3^5 \equiv 15, 3^6 \equiv 7, 3^7 \equiv 2, 3^8 \equiv 6, 3^9 \equiv 18, 3^{10} \equiv 16,$
$3^{11} \equiv 10, 3^{12} \equiv 11, 3^{13} \equiv 14, 3^{14} \equiv 4, 3^{15} \equiv 12, 3^{16} \equiv 17, 3^{17} \equiv 13.$

On the other hand, 4 is not a generator of F_{19}, since

$4^0 \equiv 1, 4^1 \equiv 4, 4^2 \equiv 16, 4^3 \equiv 7, 4^4 \equiv 9, 4^5 \equiv 17, 4^6 \equiv 11, 4^7 \equiv 6, 4^8 \equiv 5, 4^9 \equiv 1, 4^{10} \equiv 17,$
$4^{11} \equiv 16, 4^{12} \equiv 7, 4^{13} \equiv 9, 4^{14} \equiv 17, 4^{15} \equiv 11, 4^{16} \equiv 6, 4^{17} \equiv 10.$

Definition 2.2.5. Let p be an odd prime number and let a be a number with $p \nmid a$. We say that a is a quadratic residue modulo p if a is a square modulo p, i.e., if there is a number c so that $c^2 \equiv a \pmod{p}$. If a is not a

square modulo p, i.e., if there exists no such c, then a is called a quadratic non residue modulo p [37].

2.3 The Arithmetic Operations on a Prime Field.

The arithmetical operations, addition, subtraction and multiplication can be computed over a prime field F_p [38]. A simple example with a small value $p = 7$ can be given to explain the arithmetic on F_7. The addition operation can be done by $4 + 5 \pmod 7 \equiv 9 \pmod 7 \equiv 2$.

And, the subtraction computes by $4 - 5 \pmod 7 \equiv -1 \pmod 7 \equiv 6$.
Whereas, the multiplication can be calculated by
$3 \cdot 4 \pmod 7 \equiv 12 \pmod 7 \equiv 5$.

Now, what about computing the division operation over F_p and How to find the value of $a/b \pmod p$ The answer is: it is possible to compute the division operation over F_p by computing the inverse element modulo p which is given in the following relation

$$a/b \pmod p \equiv a \cdot b^{-1} \pmod p, \qquad (2.1)$$

It is easy to compute the inverse element b^{-1} using the extended Euclidean algorithm (EEA) [39].

Definition 2.3.1. Two integers a and b, not both of which are zero, are said to be relatively prime whenever $\gcd(a,b) = 1$ [39].

Definition 2.3.2. The Legendre symbol of *d* is the quantity $\left(\frac{d}{p}\right)$ defined by the rules

$$\left(\frac{d}{p}\right)=\begin{cases}1 \quad if\ d\ is\ a\ quadratic\ residue\ \text{modulo}\ p,\\ -1\ if\ d\ is\ a\ quadratic\ nonresidue\ \text{modulo}\ p,\\ 0 \quad if\ p\mid d.\end{cases} \qquad (2.2)$$

with *p* be an odd prime [37].

2.4 Introduction to Lattice over the Prime Fields

In this section, several mathematical concepts of Lattice that defined over the prime fields are discussed.

2.4.1 Basic Facts on the Lattice over the Prime Fields

Some important definitions, theorems and examples related to Lattice over a prime fields are explained as follows.

Definition 2.4.1.1. Let $\{v_1,v_2,....,v_n\}$ be a set of linearly independent vectors in Z^m, with $m \geq n$. The set $\{v_1,v_2,....,v_n\}$ generates a lattice

$$L=\left\{\sum_{i=1}^{n} l_i v_i : l_i \in Z\right\} \qquad (2.3)$$

of linear combinations which are integers v_i. The vectors $v_1,.....,v_n$. are called a lattice basis. The parameters n and m are the lattice rank and dimension respectively. A lattice has a full rank if $n=m$ [36].

Definition 2.4.1.2. Let $L \subset Z^m$ be a lattice. A sub-lattice is a subset $L' \subset L$ that is a lattice [36].

Definition 2.4.1.3. [36] Let $v, w \in V \subset R^m$ and write v and w using coordinates as $v=(x_1,x_2,....,x_m)$ and $w=(y_1,y_2,....,y_m)$ The dot product of v and w is the quantity

$$v.w = x_1 y_1 + x_2 y_2 + ... + x_m y_m .$$

We say that v and w are orthogonal to one another if $v.w = 0$. The length, or Euclidean norm, of v is the quantity

$$\|v\| = \sqrt{x_1^2 + x_2^2 + ... + x_m^2} .$$

Notice that dot products and norms are related by the formula.

$$v.v = \|v\|^2 .$$

2.4.2 The 3-Dimensional LLL lattice Reduction Method

Suppose $B = \{v_1, v_2, v_3\}$ is a basis of a lattice L where v_1, v_2, v_3 in 3-dimensional coordinates. The aim of using the 3-Dimensional *LLL* algorithm is to transform a basis *B* into better basis, namely as short vectors. In the other words, these vectors are orthogonal to each products

$$v_i \cdot v_j = 0, \forall i \neq j$$

The creation of these better basis can be done by starting to construct Gram–Schmidt Algorithm basis as given in Theorem (2.4.2.1).

Suppose $v_i^* = v_i$ with $i = 1$.

Now, for $i \geq 2$ the v_i^* are computed through the following expression:

$$v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{i,j} v_j^*, \text{ where } \mu_{i,j} = \frac{v_i . v_j^*}{\|v_j^*\|^2} \text{ for } 1 \leq j \leq i-1. \quad (2.4)$$

In Equation (2.4), $\|v_j^*\|^2$ refers to Euclidean norm that is given definition (2.4.1.3).

The vector v_i^*, are elements of the orthogonal basis

$$B^* = \{v_i^* : i = 1,2,3\},$$

for the vector space spanned by

$$B = \{v_i : i = 1,2,3\}.$$

It is easy to see that the lattice is spanned by the basis B and not by B^*.The reason for that is the basis B^* is generated by the Gram–Schmidt method resulting from linear combinations which have non integral coefficients. In spite of, these basis are not same but they have the same determinant. This result can be explained as follows.

Proposition 2.4.2.1. Let $B = \{v_i : i = 1,2,3\}$ be a basis for lattice L and let $B^* = \{v_i^* : i = 1,2,3\}$ be the Gram–Schmidt orthogonal basis then

$$\det(L) = \prod_{i=1}^{3} \|v_i^*\| \tag{2.5}$$

Proof: The proof of this proposition can be seen in [36]

The $det(L)$ in Equation (2.5) should satisfy the condition of the Hadamards inequality [36].

This mean that

$$\det(L) = vol(F) \leq \|v_1\| \|v_2\| \ldots \|v_n\|, \tag{2.6}$$

where $vol(F)$ is the volume of a fundamental domain F for a lattice.

On the other hand, a basis $B^* = \{v_i^* : i = 1,2,3\}$ is considered as a crucial point to give the definition of two conditions. These conditions are size condition and Lovasz condition, which are discussed in Definition (2.4.2.1).

Theorem 2.4.2.1. (Gram–Schmidt Algorithm) Let v_1, v_2, v_3 be a basis for a vector space $V \subset R^m$. The following algorithm creates an orthogonal basis v_1^*, v_2^*, v_3^* for V :

Set $v_1^* = v_1$.

Loop $i = 2, 3$.

compute $\mu_{ij} = v_i v_j^* / \left\| v_j^* \right\|^2$ for $1 \le j < i$.

Set $v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{ij} v_j^*$.

End Loop

The two bases have the property that Span$\{v_1, v_2, v_3\}$ = Span $\{v_1^*, v_2^*, v_3^*\}$ for all $i = 1,2,3$ [36].

Definition 2.4.2.1. Let $B = \{v_i : i = 1,2,3\}$ be a basis for a lattice L and let $B^* = \{v_i^* : i = 1,2,3\}$ Gram–Schmidt orthogonal basis. The basis B is called *LLL* reduced basis if it satisfies the following conditions [36]:

i. $\left| \mu_{i,j} \right| = \dfrac{\left| v_i v_j^* \right|}{\left\| v_j^* \right\|^2} \le \dfrac{1}{2}, \forall 1 \le j < i \le 3.$ (size condition) (2.7)

ii. $\left\| v_i^* \right\|^2 \ge \left(\dfrac{3}{4} - \mu^2_{i,i-1} \right) \left\| v_{i-1}^* \right\|^2, \ \forall 1 < i \le 3.$ (Lovasz condition) (2.8)

The *LLL* reduced basis considers as a good basis and it satisfies the desirable properties. These properties are discussed in theorem (2.4.2.2).

Theorem 2.4.2.2 Let L be a lattice of dimension 3. Any *LLL* reduced basis $B = \{v_1, v_2, v_3\}$ for L has the following properties [36]:

i. $\prod_{i=1}^{3}\|v_i\| \le 2^{3(3-1)/4}.\det(L)$ and

$\|v_j\| \le 2^{(i-1)l2}\|v_i^*\|, \forall 1 \le j \le i \le 3.$

ii. The initial vector v_1 in an LLL reduced basis satisfies

$$\|v_1\| \le 2^{(n-1)/4}|\det L|^{1/n} \text{ and } \quad \|v_1\| \le 2^{(n-1)/2}\min_{0\neq v\in L}\|v\|.$$

Algorithm 2.4.2.2. The 3-dimensional *LLL* lattice reduction algorithm [36].

Input: A lattice L and basis $B = \{v_1, v_2, v_3\}$ for L.

output: A *LLL* reduction basis $\{v_1, v_2, v_3\}$.

1. Use Gram–Schmidt orthogonal algorithm in Theorem (2.4.2.1) to compute $v_1^*, \ldots, v_k^*$

2. put $k = 2$

3. set $v_1^* = v_1$

4. while $k \le n$

5. For $j = 1, 2, \ldots, k-1$

6. compute $v_k = v_k - \lfloor \mu_{k,j} \rceil v_j^*$

7. End for

8. If $\|v_k^*\| \ge \left(\frac{3}{4} - \mu_{k,k-1}^2\right)\|v_{k-1}^*\|^2$ then

9. $k = k + 1$

10. Else

11. swap v_{k-1} and v_k

12. put $k = \max(k\text{-}1, 2)$

13. End If

14. End while

15. Return LLL reduced basis $\{v_1, v_2, \ldots, v_k\}$

2.5 Elliptic Curves over the Prime Fields

In this section, several mathematical concepts of the elliptic curves that defined over the prime fields are discussed.

2.5.1. Basic Facts on the Elliptic Curves over the Prime Fields

Some important definitions, theorems and examples related to the elliptic curves over a prime fields are explained as follows.

Definition 2.5.1.1. Let F_p be a prime field with $p \neq 2,3$. Suppose E is an elliptic curve defined over F_p by

$$E : y^2 \equiv x^3 + ax + b \pmod{p}, \tag{2.9}$$

where $a, b \in F_p$ are coefficients of E.

The set of points on E is

$$E(F_p) = \{(x, y) : x, y \in F_p\} \cup O_E, \tag{2.10}$$

where O_E is an infinitely point [32].

Definition 2.5.1.2. A discriminant Δ of the elliptic curve defined over F_p is given by

$$\Delta \equiv \left(4a^3 + 27b^2\right) \pmod{p} \neq 0 \pmod{p}. \tag{2.11}$$

If $\Delta \neq 0$ then the elliptic curve which is defined in Equation (2.9) has three distinct roots. Otherwise, the formula in Equation (2.11) is not elliptic curve [32].

Example 2.5.1.1. Suppose $p = 41$ and the coefficients a,b are equal to 7 and 5 respectively. Assume E is an elliptic curve defined by

$$E : y^2 \equiv x^3 + 7x + 5 \quad (mod\ 41). \qquad .$$

The discriminant of E is

$$\Delta \equiv (4(7)^3 + 27(5)^2) = 38 \neq 0 \ (mod\ 41).$$

This ensures that the E is elliptic curve over F_{41}. The set of points which lie on E is given by

$$\begin{aligned} E(F_{41}) = \{&(0,28),(0,13),(5,1),(5,40),(8,32),(8,9),(9,10),(9,31),(10,38),(10,3),\\ &(14,10),(14,31),(15,0),(16,20),(16,21),(18,10),(18,31),(23,19),\\ &(23,22),(24,37),(24,4),(25,15),(25,26),(26,16),(26,25),(27,19),(27,22),\\ &(30,14),(30,27),(31,1),(31,40),(32,19),(32,22),(34,33),(34,8),(36,38),(36,3)\\ &(37,35),(37,6),(38,11),(38,30),O_E\}. \end{aligned}$$

These points can be represented in Figure (2.1).

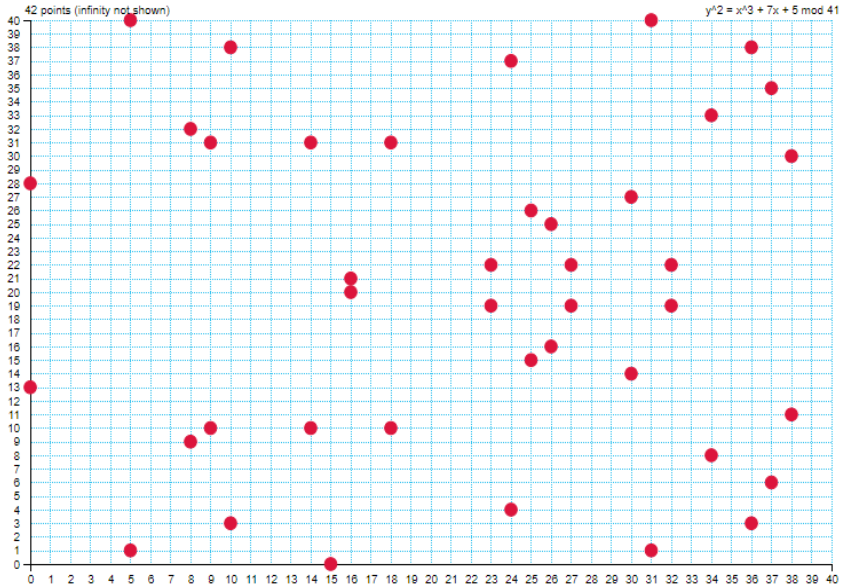


Figure 2.1: The points lying on $E : y^2 \equiv x^3 + 7x + 5$ over F_{41}.

Definition 2.5.1.3. Let p be the characteristic of F_p. An elliptic curve E defined over F_p is supersingular if p divides t, where t is the trace. If p does not divide t, then E is non-supersingular [36].

2.5.2 The Arithmetic Operations on the Elliptic Curves over Prime Fields

The arithmetical operations of the points which are lying on the elliptic curve defined over prime fields as given in Equation (2.9) are explained by the following definitions.

Definition 2.5.2.1 (Point addition) [40]. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2) \in E(F_p)$, where $P_1 \neq \pm P_2$. Then, the sum of P_1 and P_2 is defined by $P_1 + P_2 = (x_3, y_3)$, where

$$\left.\begin{aligned} x_3 &\equiv \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \pmod p \\ y_3 &\equiv \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \pmod p \end{aligned}\right\} \qquad (2.12)$$

Definition 2.5.2.2 (Point doubling) [40].

Let $P = (x_1, y_1) \in E(F_p)$. Then $2P = (x_3, y_3)$, where

$$\left.\begin{aligned} x_3 &\equiv \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \pmod p \\ y_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \pmod p \end{aligned}\right\} \qquad (2.13)$$

Example 2.5.2.2. With the same parameters in the Example (2.5.1.1), suppose the points $P_1 = (14,10)$ and $P_2 = (24,4) \in E(F_{41})$. Using the relation in Equation (2.12), the computation of

$$P_1 + P_2 = (14,10) + (24,4) = (5,1),$$

which is in $E(F_{41})$. Whereas, based on the relation in Equation (2.13), the computation of $2P$ can be done by

$$2P = 2(14,10) = (14,31) \in E(F_{41}).$$

2.5.3 The Group Laws of the Elliptic Curves over Prime Fields.

With an addition operation as defined in Equation (2.12), the set of the points on an elliptic curve E satisfy the abelian group $(E(F_p), +_E)$ axioms: close, additive identity element, associativity, inverse element and commutativity.

The sum point of two points in $E(F_p)$ is a point in $E(F_p)$, so the set $E(F_p)$ is closed under the point addition $+_E$. A point at infinity O_E is considered to use as an identity element. In other words, $P + O_E = O_E + P = P$, where $P = (x_p, y_p)$. The inverse point of P is $-P$, which is defined by $-P = (x_p, -y_p) (\text{mod}\, p)$, since the elliptic curve is defined over F_p. Therefore, $P + (-P) = O_E$. Also $P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$, so, the associativity is verified. Furthermore, the commvtativity on elliptic curve points is verified, namely if $P_1, P_2 \in E(F_p)$ then $P_1 + P_2 \in E(F_p)$, so $P_1 + P_2 = P_2 + P_1 \in E(F_p)$. Hence, $(E(F_p), +_E)$ is abelian group [41].

2.5.4 The Group Order of the Elliptic Curves over Prime Fields.

Let E be an elliptic curve defined over F_p. The number of the points in an elliptic group $E(F_p)$, denoted by $\#E(F_p)$, is called the order of E over F_p. Since the elliptic curve defined in Equation (2.9) has at most two

solutions for each $x \in F_p$, this means that $\#E(F_p) \in [1, 2p-1]$. Hasse's theorem provides a roughly way for determining $\#E(F_p)$ [32].

Theorem 2.5.4.1. (Hasse Theorem). Let E be an elliptic curve defined over F_p. Then

$$p + 1 - 2\sqrt{p} \le \#E(F_p) \le p + 1 + 2\sqrt{p}\,. \qquad (2.14)$$

The interval $[p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}\,]$ is called the Hasse's interval [42]. An alternate formulation of Hasse's theorem is stated by:

If E is defined over F_p, then $\#E(F_p) = p + 1 - t$ where $|t| \le 2\sqrt{p}$. The parameters t is called the trace of E over F_p. Since $2\sqrt{p}$ is a small relative to p, so, it is clear to see $\#E(F_p) \approx p$ [32].

Example 2.5.4.1 (Order of elliptic curve over F_{41}). Suppose E is an elliptic curve over F_{41} defined by

$$E : y^2 \equiv x^3 + 7x + 5 \pmod{41}.$$

Based on the interval [30,54] which is determined by using Equation (2.14), the order of $\#E(F_{41})$ is $\#E(F_{41}) = 41 + 1 + 12 = 54$, where $t = -12$, $|t| = 12 < 12.8$. Hence $\#E(F_{41}) = 54 \approx 41$.

2.5.5 The Group Structure of the Elliptic Curve over F_p.

The group structure of the elliptic curve defined over F_p can be explained by the following theorem:

Theorem 2.5.5.1 (Group structure of an elliptic curve). Let E be an elliptic curve defined over F_p. Then $E(F_p)$ is isomorphic to $Z_{n_1} \oplus Z_{n_2}$, where n_1 and n_2 are uniquely determined positive integers such that n_2 divides both n_1 and $p - 1$ [32].

In this work, one can note that the $\#E(F_p) = n_1 n_2$ with $n_2 = 1$, so the $E(F_p)$ is cyclic group as shown in Example (2.5.1.1) and next Example (2.5.5.1).

Definition 2.5.5.1 (Order of elliptic point). The order of a point P on E defines by the smallest positive integer n such that $nP = O_E$ [32].

Example 2.5.5.1 (Group structure). Suppose E is an elliptic curve defined by

$$E : y^2 = x^3 + 4x + 20$$

over F_{29}. The order of $E(F_{29}), \#E(F_{29}) = 37$. Since 37 is a prime, then $E(F_{29})$ is a cyclic group and any point $E(F_{29})$ is a generator of $E(F_{29})$ except the infinity point O_E. The multiples of the point $P = (1,5)$ generate all the points in $E(F_{29})$ as shown below [32].

$0P = O_E$	$8P = (8,10)$	$16P = (0,22)$	$24P = (16,2)$	$32P = (6,17)$
$1P = (1,5)$	$9P = (14,23)$	$17P = (27,2)$	$25P = (19,16)$	$33P = (15,2)$
$2P = (4,19)$	$10P = (13,23)$	$18P = (2,23)$	$26P = (10,4)$	$34P = (20,26)$
$3P = (20,3)$	$11P = (10,25)$	$19P = (2,6)$	$27P = (13,6)$	$35P = (4,10)$
$4P = (15,27)$	$12P = (19,13)$	$20P = (27,27)$	$28P = (14,6)$	$36P = (1,24)$.
$5P = (6,12)$	$13P = (16,27)$	$21P = (0,7)$	$29P = (8,19)$	
$6P = (17,19)$	$14P = (5,22)$	$22P = (3,28)$	$30P = (24,7)$	
$7P = (24,22)$	$15P = (3,1)$	$23P = (5,7)$	$31P = (17,10)$	

2.6 The Scalar Multiplication on Elliptic Curves.

Suppose E is an elliptic curve defined over a prime field F_p. Let $P \in E(F_p)$ has a prime order n. Assume k is a positive integer, $k \in [1, n-1]$. A scalar multiplication kP on E can be defined by

$$kP = \underbrace{P + P + ... + P}_{k\text{–times}}. \qquad (2.15)$$

A scalar multiplication kP can be computed by the addition and doubling on the Elliptic points on E [32]. For example, a scalar multiplication $9P$ can be calculated by

$$2(4P)+P.$$

Example 2.6.1. Let $p=53$ be a prime number. Suppose E is an elliptic curve defined by $E: y^2 = x^3 + 2x + 1$ over F_{53}. Let $P=(14,11)$ be a generator point lies on E which has a prime order $n=59$.

The computation of the scalar multiplication $10P$, where $t=10\in[1,58]$ can be computed by using Equations (2.12) and (2.13) and as follows

$$\begin{aligned} 10P &= 2(4P)+2P \\ &= (40,2)+(36,6) \\ &= (31,42). \end{aligned}$$

2.7 The Efficient Computable Endomorphisms

The efficient computable endomorphisms ψ of E defined over F_p is given by the following definition:

Definition2.7.1: An endomorphism is a homomorphism $\psi: E(F_p)\to E(F_p)$ that is given by rational function $R_1(x,y)$ and $R_2(x,y)$ such that

$$\psi(P)=\psi(x,y)=(R_1(x,y),\ R_2(x,y)),$$

for all points $P=(x,y)\in E(F_p)$. Since ψ is a homomorphism then $\psi(O_E)=O_E$, where O_E is a point at infinity [42]. There are several cases of efficiently computable endomorphisms [40], this study focuses on the following case:

Suppose E is an elliptic curve defined over F_p. The multiplication by λ, for each integer $\lambda \in [1, n-1]$, forms a map $\psi : E(F_p) \to E(F_p)$ that is defined by

$$\psi : P \to \lambda P. \tag{2.16}$$

This map is an endomorphism of E defined over F_p.

2.8 The Integer Sub-Decomposition Method

For more speeding up of the calculation of a scalar multiplication kP, the integer sub-decomposition (ISD) method has been proposed in 2015 [48] by Ruma Ajeena (also see [15,43,44,45,46,47]). The ISD method depended on using two efficient computable endomorphisms ψ_i, for $i = 1,2$ to compute kP. It employs the sub-decomposition of a scalar k into new sub scalars. The main idea of ISD method can be illustrated as follows.

Suppose E is an elliptic curve defined over F_p as given in Equation (2.9). Let P be a point lies on E which has a prime order n. The scalar $k \in [1, n-1]$ in a scalar multiplication kP is decomposed first into k_1 and k_2 with $\max\{|k_1|,|k_2|\} > \sqrt{n}$. So, the scalar k can be written by

$$k \equiv k_1 + k_2 \pmod{n}, \tag{2.17}$$

based on the generator $\{v_1, v_2\}$ that is computed by the extended Euclidean algorithm (EEA)[39]. Once again, the scalars k_1 and k_2 are sub-decomposed into k_{11}, k_{12} and k_{21}, k_{22} respectively with $\max\{|k_{11}|,|k_{12}|\} \le \sqrt{n}$ and $\max\{|k_{21}|,|k_{22}|\} \le \sqrt{n}$. This sub-decomposition depending on the computation of the ISD generators which are found by the GEEA [48]. So, the scalar k can be rewritten by

$$k \equiv k_{11} + k_{12}\lambda_1 + k_{21} + k_{22}\lambda_2 \pmod{n}, \qquad (2.18)$$

where $\lambda_1, \lambda_2 \in [1, n-1]$ with $\lambda_1 \neq \pm\lambda_2$.

The scalar multiplication kP is computed by using ISD method through the following formula

$$kP \equiv k_{11}\ P + k_{12}\ \psi_1(P) + k_{21}\ P + k_{22}\ \psi_2(P), \qquad (2.19)$$

where $\psi_i(P) = \lambda_i P$ are two efficient computable endomorphisms which are pre-computed by any a scalar multiple algorithm.

2.9 Introduction to the Edward Curves over the Prime Fields

In this section, several mathematical concepts of the Edward curves that defined over the prime fields are discussed.

2.9.1. Basic Facts on the Edward Curves over the Prime Fields

Some important definitions, theorems and examples related to the Edward curves over a prime fields are explained as follows.

Definition 2.9.1.1.[2] Let F_p be a prime field with $p \neq 2,3$. Suppose E_d is an Edward curve defined over F_p in the following equation:

$$E_d : x^2 + y^2 = 1 + d\,x^2 y^2, \text{ where } d \in F_p / \{0, 1\}.$$

Let $P = (x_1,y_1)$ and $Q = (x_2,y_2)$ be two points on E_d. The addition point $P + Q$ is computed by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d\,x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d\,x_1 x_2 y_1 y_2} \right) \qquad (2.20)$$

For addition point, the identity element is a point $O_{Ed} = (0,1)$. The inverse point $-P$ of a point $P = (x_1, y_1)$ is defined by $-P = (-x_1, y_1)$. Some special orders of the points (0, −1) which has order 2 and (1, 0), (−1, 0)

have order 4. The formula of addition point that is defined in Equation (2.20) is known as strongly unified. This return to the reason that the possibility using it for computing the double point as well. Another attractive point that increases the motivation to work with the Edwards is the completeness of the addition point law when *d* is a non-square in F_p. This means that the addition point law can be computed for all points lie on E_d.

Doubling and tripling point in Edwards curve E_d can be performed with the same formula 0f the addition point. With $P = (x_1, y_1) \in E_d(F_p)$, the doubling point is computed by $2P = (x_3, y_3)$,

There $x_3 = \dfrac{2x_1y_1}{x_1^2 + y_1^2}$ and $y_3 = \dfrac{y_1^2 - x_1^2}{2 - x_1^2 - y_1^2}$.

Example 2.9.1.1. Consider the Edwards curve

$$E_7 : x^2 + y^2 = 1 + 7x^2y^2 \pmod{11} \qquad (2.21)$$

The technique to compute all point that satisfying the curve is as follows. First, a square of the elements 0, 1, 2, 3, …, *p*-1 =10 are computed with the prime field F_{11}.

n	0	1	2	3	4	5	6	7	8	9	10
Square (*n*)	0	1	4	9	16	25	36	49	64	81	100
n^2 (mod 11)	0	1	4	9	5	3	3	5	9	4	1

Equation (2.21) of Edwards curve can be rewritten by

$$E_7 : y^2 = \frac{1 - x^2}{1 - 7x^2} \pmod{11}.$$

If $x = 0$ then $y^2 = 1$ which exists in the 3rd row of Table (2.1), so it is a complete square. Since the value 1 in 3rd row corresponds to the values 1

and 10 that are given in 1st row, so the points are (0,1) and (0,10) are lying on E_7. Now, if x =1 then y^2 = 0, this also exists in the 3rd row which corresponds to value 0 in the 1st row, so the point is (1,0) lies on E_7. Similarly, it is possible to calculate the rest of the points. Thus, the set of points which lie on E_d is given by

$$E_7(F_{11}) = \{(0,1),(0,10),(1,0),(2,4),(2,7),(3,3),(3,8),(4,2),(4,9),(7,2),(7,9),$$
$$(8,3),(8,8),(9,4),(9,7),(10,0)\}$$

With another prime number p =13 and d equal to 2, it is easy to define the Edwards curve E_d by

$$E_2 : x^2 + y^2 \equiv 1 + 2x^2y^2 \pmod{13}.$$

The set of points which lie on E_2 is given by

$$E_2(F_{13}) = \{(0,1),(0,12),(1,0),(4,4),(4,9),(9,4),(9,9),(12,0)\}.$$

Example 2.9.1.2. Consider the Edwards curve which is given in example (2.9.1.1) the point addition of the points (2, 4) and (3, 3) is computed by

$$(2,\ 4) + (3,\ 3) = (x_3, y_3),$$

where $$x_3 = \frac{x_1y_2 + x_2y_1}{1 + d\,x_1x_2y_1y_2} = \frac{2.(3) + 3.(4)}{1 + 7.(2).(3).(4).(3)} = 4$$

and $$y_3 = \frac{y_1y_2 - x_1x_2}{1 - d\,x_1x_2y_1y_2} = \frac{4.(3) - (2).(3)}{1 - 7.(2).(3).(4).(3)} = 2.$$

So $(x_3, y_3) = (4,2) \in E_7(F_{11}).$

Doubling point of the point (2, 4) is computed by

$$2P = 2(2,\ 4) = (x_3, y_3),$$

where $$x_3 = \frac{2x_1y_1}{x_1^2 + y_1^2} = \frac{2.(4).(2)}{(4)^2 + (2)^2} = 3$$

and $$y_3 = \frac{y_1^2 - x_1^2}{2 - x_1^2 - y_1^2} = \frac{(4)^2 - .(2)^2}{2 - (4)^2 - (2)^2} = 3.$$

So, $2P = (x_3, y_3) = (3,3) \in E_7(F_{11}).$

Theorem 2.9.1.1. (Order of Edwards Curve). If $p \equiv 3 (\text{mod } 4)$ is a prime and the following condition of supersingularity

$$\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0 (\text{mod } p),$$

is true then the orders of the curves $x^2 + y^2 = 1 + dx^2y^2$ and $x^2 + y^2 = 1 + d^{-1}x^2y^2$ over F_p are equal to

$$\#E_d(F_p) = \begin{cases} p + 1, with \left(\frac{d}{p}\right) = -1, \\ p - 3, with \left(\frac{d}{p}\right) = 1, \end{cases} \tag{2.22}$$

where $\left(\frac{d}{p}\right)$ is a Legendre symbol [24].

Example 2.9.1.3. The number of Edward curve points over F_{11} when $d = 2$ is equal to $\#E_2(F_{11}) = \#E_{2^{-1}}(F_{11}) = p + 1 = 12.$

Since

$$E_2(F_{11}) = \{(0,1),(0,10),(1,0),(3,4),(3,7),(4,3),(4,8),(7,3),(7,8),$$
$$(8,4),(8,7),(10,0)\},$$

and

$$E_{2^{-1}}(F_{11}) = E_6(F_{11}) = \{(0,1),(0,10),(1,0),(2,5),(2,6),(5,2),(5,9),(6,2),(6,9),$$
$$(9,5),(9,6),(10,0)\}.$$

2.9.2. The Twisted Edward Curves over the Prime Field

The Twisted Edwards curve $E_{a,d}$ over F_p is discussed as follows.

Definition 2.9.2.1. [5] Let F_p be a prime field with $p \neq 2$. The Twisted Edwards curve $E_{a,d}$ over F_p is defined by

$$E_{a,d} : ax^2 + y^2 = 1 + d\ x^2 y^2 \qquad (2.23)$$

where a and d are non-zero elements and $a \neq d$. The twisted Edwards curve $E_{a,d}$ is an Edwards curve E_d with $a = 1$. Suppose $P = (x, y)$ lies on $E_{a,d}$. Since the $E_{a,d}$ is an E_d, so the identity point is (0,1) which means that $(x, y) + (0,1) = (x, y)$, for all point $P = (x, y)$ lies on $E_{a,d}$. The inverse of $P = (x, y)$ is also defined by $-P = (-x, y)$. The sum point $P + Q$ for two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ which are lying on $E_{a,d}$ is defined by

$$P + Q = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right) \qquad (2.24)$$

The sum $P + Q$ is also a point in $E_{a,d}(F_p)$ which is defined over a prime field F_p.

Doubling and tripling point on Twisted Edwards curve $E_{a,d}$ can be performed with the same formula of the addition point with $P = (x_1, y_1) \in E_{a,d}(F_p)$, Edwards the doubling point is computed by $2P = (x_3, y_3)$,

Where $x_3 = \dfrac{2x_1 y_1}{a x_1^2 + y_1^2}$ and $y_3 = \dfrac{y_1^2 - a x_1^2}{2 - a x_1^2 - y_1^2}$.

Theorem 2.9.2.1. (Properties the order of E_d and $E_{a,d}$ [24]).

- If $\left(\frac{d}{p}\right)=1$, then the orders $\#E_d\left(F_p\right)=\#E_{d-1}\left(F_p\right)$.
- If $\left(\frac{d}{p}\right)=-1$, then E_d and E_{d-1} are pair of twisted Edwards. In the other words, the orders of curves E_d and E_{d-1} satisfy

$$\#E_d\left(F_p\right)+\#E_{d-1}\left(F_p\right)=2p+2.$$

Example 2.9.2.1. Let E_d Edwards curve over the field F_p with $d=4$ and $p=11$, Then based Theorem(2.9.2.1), if $\left(\frac{d}{p}\right)=1$ then the number of Edwards points equal to $\#E_d\left(F_p\right)=\#E_{d-1}\left(F_p\right)=\#E_3\left(F_{11}\right)=\#E_4\left(F_{11}\right)=12.$

Also, Using the same Theorem(2.9.2.1), if $\left(\frac{d}{p}\right)=-1$ then the number of Edwards points equal to $\#E_7\left(F_{11}\right)+\#E_8\left(F_{11}\right)=24,$

Since with $d=7$ and $p=11$, the order $\#E_7\left(F_{11}\right)=16$ and the order $\#E_8\left(F_{11}\right)=8,$ so $\#E_7\left(F_{11}\right)+\#E_8\left(F_{11}\right)=16+8=24.$

Example(2.9.2.2): Consider the Twisted Edwards curve

$$E_{3,7}: 3x^2+y^2=1+7x^2y^2 \pmod{11} \qquad (2.25)$$

The technique to compute all point that satisfying the curve is as follows. First, a square of the elements 0, 1, 2, 3, …, p-1 =10 are computed with the prime field F_{11} as given in Table (2.1).

Equation (2.25) of $E_{a,b}$ can be rewritten by

$$E_{3,7}: y^2 = \frac{1-3x^2}{1-7x^2} \pmod{11}.$$

If $x = 0$ then $y^2 = 1$ which exists in the 3rd row of Table (2.1), so it is a complete square. Since the value 1 in 3rd row corresponds to the values 1 and 10 that are given in 1st row, so the points are (0,1) and (0,10) are lying on $E_{3,7}$. Now, if $x = 1$ then $y^2 = 4$, this also exists in the 3rd row which corresponds to value 0 in the 1st.

row, so the point is (1,2) lies on $E_{3,7}$. Similarly, it is possible to calculate the rest of the points. Thus, the set of points which lie on $E_{a,d}$ is given by

$$E_{3,7}(F_{11}) = \{(0,1),(0,10),(1,2),(1,9),(2,0),(4,5),(4,6),(7,5),(7,6),$$
$$(9,0),(10,2),(10,9)\}.$$

Example 2.9.2.3: Consider the Twisted Edwards curve $E_{a,d}$ which is given in Example (2.9.2.2). The addition point of the points (7, 5) and (10, 2) is computed by

$$(7,\ 5)+(10,\ 2)=(x_3, y_3),$$

Where $x_3 = \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2} = \frac{7.(2)+10.(5)}{1+7.(7).(5).(10).(2)} = 7$

and $y_3 = \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} = \frac{2.(5)-3.(7).(10)}{1-7.(7).(5).(10).(2)} = 6.$

So, $(7,5)+(10,2)=(7,6).$

Doubling point of the (1, 9) is computed by

$$2P = 2(1,9) = (x_3, y_3),$$

Where $x_3 = \frac{2x_1y_1}{ax_1^2 + y_1^2} = \frac{2.(1).(9)}{3.(1)^2 + (9)^2} = 1$

and $y_3 = \frac{y_1^2 - x_1^2}{2 - ax_1^2 - y_1^2} = \frac{(9)^2 - 3.(1)^2}{2 - 3.(1)^2 - (9)^2} = 2.$

So, $2P = (1,2).$

Chapter Three

The Twisted Edwards 3-ISD Method Using the 3-LLL Lattice Reduction Algorithm

3.1 Introduction

In this Chapter, a new version of the integer sub-decomposition method on decomposing the scalar t in 3-dimension. In other words, the 3-ISD generators are generated with 3-dimension to decompose and sub-decompose the Scalar t in a scalar multiplication tP.To find generate these generators, the 3-LLL lattice reduction method and extension of it are used.

Four cases of 3-ISD method are employed to compute a scalar multiplication tP Edwards and twisted Edwards curves defined over prime field. The security considerations of these case are discussed and determined in this chapter as well.

3.2 The Extended LLL Lattice Reduction Method.

The lattice bases with dimension 3 can be reduced using the Lenstra, Lenstra and Lov´asz algorithm, which is known by the LLL or L_3 algorithm as discussed in Chapter (2), Section (2.4.2). The extension of the LLL algorithm has been proposed in this section as a main to compute the generators in the proposed 3-ISD method. The 3-ISD method is used to compute a scalar multiplication tP on Edwards or Twisted Edwards curve defined over a prime field. The extended LLL lattice reduction algorithm needs first to extend the Gram–Schmidt method, that is considered as a key point for it.

3.2.1. The Extended Gram–Schmidt Method

The extended Gram–Schmidt method is proposed in this section. This extension is useful to propose the extended LLL lattice reduction method .The extended Gram–Schmidt is explained by the following theorem.

Theorem 3.2.1.1. (The Extended Gram–Schmidt Algorithm)

Let $B_1 = \{v_1, v_2, v_3\}$, $B_2 = \{s_1, s_2, s_3\}$ and $B_3 = \{r_1, r_2, r_3\}$ are bases for a vector space $V \subset R^m$.

The Extended Gram–Schmidt Algorithm (EGSA) is used to create the orthogonal bases $B_1^* = \{v_1^*, v_2^*, v_3^*\}, B_2^* = \{s_1^*, s_2^*, s_3^*\}$ and $B_3^* = \{r_1^*, r_2^*, r_3^*\}$ for V through

1. $v_1^* = v_1$, $s_1^* = s_1$ and $r_1^* = r_1$
2. For $i = 2,3$
3. For $j = 1,2$
4. Compute $\mu_{ij} = \dfrac{v_i . v_j^*}{\|v_j^*\|^2}$, $\mu'_{ij} = \dfrac{s_i . s_j^*}{\|s_j^*\|^2}$, and $\mu''_{ij} = \dfrac{r_i . r_j^*}{\|r_j^*\|^2}$,
5. Compute $v_i^* = v_i - \sum_{j=1}^{2} \mu_{ij} v_j^*$, $s_i^* = s_i - \sum_{j=1}^{2} \mu'_{ij} s_j^*$ and
$$r_i^* = r_i - \sum_{j=1}^{2} \mu''_{ij} r_j^*.$$
6. End for
7. End for
8. Return B_1^*, B_2^*, B_3^* . ■

Example 3.2.1.1. (The Extended Gram–Schmidt Algorithm)

Let $B_1 = \{v_1 = (28,0,-21),\ v_2 = (14,-7,35),\ v_3 = (21,7,7)\}$,

$B_2 = \{s_1 = (6,57,-12),\ s_2 = (9,18,6),\ s_3 = (6,-3,12)\}$

and $B_3 = \{r_1 = (9,12,27),\ r_2 = (9,27,9),\ r_3 = (18,18,18)\}$.

are bases for a vector space $V \subset R^3$.

$v_1^* = v_1 = (28,0,-21),\ s_1^* = s_1 = (6,57,-12)$ and $r_1^* = r = (9,12,27)$

If $i = 2,3$ and $j = 1,2$ compute $\mu_{i,j} = \dfrac{v_i . v_j^*}{\|v_j^*\|^2}$, $\mu'_{i,j} = \dfrac{s_i . s_j^*}{\|s_j^*\|^2}$, and

$\mu''_{i,j} = \dfrac{r_i . r_j^*}{\|r_j^*\|^2}$

$\mu_{2,1} = \dfrac{-343}{1225} \approx -0.28,\ \mu'_{2,1} = \dfrac{1008}{3429} \approx 0.294,\ \mu''_{2,1} = \dfrac{648}{954} \approx 0.679.$

Compute $v_i^* = v_i - \sum_{j=1}^{2} \mu_{i,j} v_j^*,\ s_i^* = s_i - \sum_{j=1}^{2} \mu'_{i,j} s_j^*,$ and

$r_i^* = r_i - \sum_{j=1}^{2} \mu''_{i,j} r_j^*.$

$v_2^* = (14,-7,35) - \dfrac{-343}{1225}(28,0,-21)$ $\quad s_2^* = (9,18,6) - \dfrac{1008}{3429}(6,57,-12)$

$v_2^* = (14,-7,35) + (0.28)(28,0,-21)$, $s_2^* = (9,18,6) - (0.29)(6,57,-12)$ and

$v_2^* = (21.84,-7,29.21)$ $\quad s_2^* = (7.236,1.242,9.528)$

$$r_2^* = (9,27,9) - \frac{648}{954}(9,12,27)$$

$$r_2^* = (9,27,9) - (0.679)(9,12,27)$$

$$r_2^* = (2.889,18.852,-9.333)$$

$$v_3^* = (21,7,7) - \frac{441}{1225}(28,0,-21) - \frac{613.48}{1373.96}(21.84,-7,29.12)$$
$$v_3^* = (21,7,7) - (0.36)(28,0,-21) - (0.447)(21.84,-7,29.12)$$
$$v_3^* = (1.158,10.129,-13.577)$$

$$s_3^* = (6,-3,12) - \frac{-279}{3429}(6,57,-12) - \frac{154.026}{144.685}(7.236,1.242,9.528)$$
$$s_3^* = (6,-3,12) - (0.0814)(6,57,-12) - (1.065)(7.236,1.242,9.528)$$
$$s_3^* = (-1.2179,0.3171,0.8759)$$

$$r_3^* = (18,18,18) - \frac{864}{954}(9,12,27) - \frac{223.344}{450.849}(2.889,18.852,-9.333)$$
$$r_3^* = (18,18,18) - (0.9057)(9,12,27) - (0.4955)(2.889,18.852,-9.333)$$
$$r_3^* = (8.418,-2.209,-1.829)$$

$B_1^* = \{v_1^* = (28,0,-21),\ v_2^* = (21.84,-7,29.21),\ v_3^* = (1.158,10.129,-13.577)\}$
$B_2^* = \{s_1^* = (6,57,-12),\ s_2^* = (7.236,1.242,9.528),\ s_3^* = (-1.2179,0.3171,0.8759)\}$
$B_3^* = \{r_1^* = (9,12,27),\ r_2^* = (2.889,18.852,-9.333),\ r_3^* = (8.418,-2.209,-1.829)\}.$

Algorithm 3.2.2.1 .The Extended LLL Lattice reduction algorithm.

Input: A lattice L and basis $B_1 = \{v_1, v_2, v_3\}$, $B_2 = \{s_1, s_2, s_3\}$, and

$B_3 = \{t_1, t_2, t_3\}$ for L.

output: A LLL reduction basis $\{B_1, B_2, B_3\}$.

1. Use Gram–Schmidt orthogonal algorithm Theorem (2.4.2.1) to compute B_1^*, B_2^*, B_3^*
2. put $k = 2$
3. set $v_1^* = v_1$, $s_1^* = s_1$, and $r_1^* = r_1$
4. while $k \leq n$
5. For $j = 1,2,\ldots,k-1$

6. Compute $v_k = v_k - \lfloor \mu_{k,j} \rceil v_j^*, s_k = s_k - \lfloor \mu_{k,j} \rceil s_j^*$ and

   $r_k = r_k - \lfloor \mu_{k,j} \rceil r_j^*$.

7. End for,

8. If $\|v_k^*\| \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right)\|v_{k-1}^*\|^2$, $\|s_k^*\| \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right)\|s_{k-1}^*\|^2$ and

   $\|r_k^*\| \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right)\|r_{k-1}^*\|^2$ then

9. $k = k + 1$

10. Else

11. Swap v_{k-1} and v_k

12. put k = max (k-1,2)

13. End If

14. End while

15. Return LLL reduced basis $\{B_1^*, B_2^*, B_3^*\}$

3.3 The 3-ISD Edwards Scalar Multiplication Method

This section proposed another version of the integer sub-decomposition method for computing a scalar multiplication tP on Edwards curve E_d defined over a prime F_p. This version with the 3 dimension of ISD generators $\{B_1^*, B_2^*\}$ that are generated using the extended LLL reduction algorithm, when $B_1^* = \{v_1^*, v_2^*, v_3^*\}$, $B_2^* = \{v_4^*, v_5^*, v_6^*\}$ and with v_i^* for $i = 1,2,...,6$ are vectors have 3 dimension.

Suppose t is scalar in scalar multiplication tP, when $t \in [1, n-1]$ and n is a prime order of a point P which lies on Edwards curve E_d defined over prime field F_p. The Basic idea of 3-ISD method is to use first generator $B = \{v_1, v_2, v_3\}$, with three vector $v_1 = (a_1, b_1, c_1)$, $v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$ that are the short vectors are generated using the 3-LLL

lattice reduction Algorithm (2.4.2.2) to decompose a scalar t by t_1 and t_2 such that

$$t \equiv t_1 + t_2\lambda_1 \pmod{n}, \tag{3.1}$$

with $\max\{|t_1|,|t_2|\} > \sqrt{n}$ and $\lambda_1, \lambda_2 \in [1, n-1]$ the scalars t_1 and t_2 are computed

$$t_1 = t + a_1b_1 - a_2b_2 - a_3b_3 \pmod{n} \text{ and } t_2 = t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod{n}. \tag{3.2}$$

Then, the application of the extended LLL lattice reduction algorithm (3.2.2.1), The scalars t_1 and t_2 are sub–decomposed again into t_{11}, t_{12} and t_{21}, t_{22} respectively. The sub-decomposition is proved as follows.

Theorem 3.3.1. Suppose E_d is an Edwards curve (or twisted Edwards curve) defined over F_p. Let $t \in [1, n-1]$ with n is a prime order of a point P which lies on E_d. Then, 3-ISD scalar multiplication is defined by

$$tP \equiv t_{11}\ P + t_{12}\ \psi_1(P) + t_{21}\ P + t_{22}\ \psi_2(P) \pmod{p},$$

where $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$ are two efficiently computable endomorphisms of Edwards curve E_d defined over F_p.

Proof.

Let $B = \{v_1, v_2, v_3\}$, be a first generator of ISD method with three vector $v_1 = (a_1, b_1, c_1)$, $v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$ that are the short vectors are generated using the 3-LLL lattice reduction Algorithm (2.4.2.2).

Suppose $t \in [1, n-1]$ is a scalar in a scalar multiplication tP. Based on a generator B, a scalar t is decomposed into the scalars t_1 and t_2. In other words, t is rewritten by

$$t \equiv t_1 + t_2\lambda \pmod{n},$$

with $\max\{|t_1|,|t_2|\} > \sqrt{n}$ and $\lambda \in [1, n-1]$.

Now, with other 3-ISD generators $B_1^* = \{v'_1, v'_2, v'_3\}$ and $B_2^* = \{v''_1, v''_2, v''_3\}$, where $v'_1 = (a'_1, b'_1, c'_1)$, $v'_2 = (a'_2, b'_2, c'_2)$, $v'_3 = (a'_3, b'_3, c'_3)$ and $v''_1 = (a''_1, b''_1, c''_1)$, $v''_2 = (a''_2, b''_2, c''_2)$, $v''_3 = (a''_3, b''_3, c''_3)$, that are obtained using the extended 3-LLL lattice reduction algorithm (3.2.2.1), the scalars t_1 and t_2 are sub-decomposed into t_{11}, t_{12} and t_{21}, t_{22}, namely

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \text{ and } t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n}, \tag{3.3}$$

where

$$t_{11} \equiv t_1 + a'_1 b'_1 - a'_2 b'_2 - a'_3 b'_3 \pmod{n}, \quad t_{12} \equiv t_{11} + b'_1 c'_1 - b'_2 c'_2 - b'_3 c'_3 \pmod{n} \tag{3.4}$$

and

$$t_{21} \equiv t_2 + a''_1 b''_1 - a''_2 b''_2 - a''_3 b''_3 \pmod{n}, \quad t_{22} \equiv t_{21} + b''_1 c''_1 - b''_2 c''_2 - b''_3 c''_3 \pmod{n} \tag{3.5}$$

with $\max\{|t_{11}|, |t_{12}|\} \le \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \le \sqrt{n}$. So, the scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1 + t_{21} + t_{22}\lambda_2 \pmod{n}. \tag{3.6}$$

The scalar multiplication tP using the 3-ISD method is computed by

$$tP \equiv t_{11} P + t_{12} \psi_1(P) + t_{21} P + t_{22} \psi_2(P) \pmod{p}, \tag{3.7}$$

where $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$ are two efficiently computable endomorphisms of Edwards curve E_d defined over F_p. ■

The 3-ISD Edwards scalar multiplication can be implemented using Algorithm (3.3.1).

Algorithm (3.3.1): The 3-ISD Edwards Scalar Multiplication tP.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$ and $P \in E_d(p)$.

Output: 3-ISD Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$.

   computation stage:
2. Run 3-LLL lattice reduction Algorithm (2.4.2.2) to find the first 3-ISD generator $\{v_1, v_2, v_3\} \ni v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$.
3. Choose randomly a scalar $t \in [1, n-1]$.
4. Use the 3-ISD generator $\{v_1, v_2, v_3\}$ to decompose t into t_1 and t_2 such that $t_1 = t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n}$ and $t_2 = t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n}$ with $\max\{|t_1|, |t_2|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1, \lambda_2 \in [1, n-1]$.
6. Run the extended 3-LLL lattice reduction Algorithm (3.2.2.1) to find the two 3-ISDgenerator $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$.
7. Use extended 3-LLL lattice reduction Algorithm (3.2.2.1) sub-decompose t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that $t_1 = t_{11} + t_{12}\lambda_1 \pmod{n}$ and $t_2 = t_{21} + t_{22}\lambda_2 \pmod{n}$, where $\max\{|t_{11}|, |t_{12}|\} \le \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \le \sqrt{n}$.
8. Compute tP 3-ISD Edwards scalar multiplication tP by $tP \equiv t_{11} P + t_{12} \psi_1(P) + t_{21} P + t_{22} \psi_2(P) \pmod{p}$
9. Return tP.

Example 3.3.1. (The 3- ISD Edwards Scalar Multiplication Method)

Let $p = 1171$ be a prime number. Suppose E_d is an Edwards curve defined by $E_2 : x^2 + y^2 = 1 + 2x^2 y^2 \pmod{1171}$, with $d = 2$ over F_{1171}.

Let $P = (7, 766)$ be a point on E_2 has prime order $n = 293$.

Using the 3-LLL lattice reduction algorithm (3.2.2.1), the first 3-ISD generator $\{v_1, v_2, v_3\}$ is computed, where $v_1 = (21,1,57), v_2 = (-57,29,29)$ and $v_3 = (-81,-122,30)$.

Suppose $t = 292 \in [1,292]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n} \equiv 215 \pmod{293}$$

and

$$t_2 \equiv t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n} \equiv 77 \pmod{293},$$

where $\max\{215,77\} > \sqrt{n} = \sqrt{293} = 17.11$.

Now, Using the extended 3-LLL lattice reduction algorithm (3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, when

$$v_1' = (1,9,-7), v_2' = (11,3,7), v_3' = (-20,19,25)$$

and

$$v_1'' = (18,30,-12), v_2'' = (-28,21,30), v_3'' = (37,-15,47).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \equiv (-15) + 12(68) \pmod{293}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv 2 + 10(154) \pmod{293}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$tP = (1076,941) + (556,245) + (884,538) + (44,666)$$
$$= (328,603) + (480,417)$$
$$= (859,802),$$

Where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$t_{11}P = -15(7,766) = (1076,941)$, $t_{12}\psi_1(P) = 12(562,1070) = (556,245)$,

$t_{21}P = 2(7,766) = (884,532)$ and $t_{22}\psi_2(P) = 10(937,248) = (44,666)$.

with $\psi_1(P) = \lambda_1 P = 68(7,766) = (562,1070)$

and $\psi_2(P) = \lambda_2 P = 154(7,766) = (937,248)$.

are two efficiently computable endomorphisms that are pre-computed.

Example 3.3.2. (The 3- ISD Edwards scalar multiplication method)

Let $p = 1867$ be a prime number. Suppose E_d is an Edwards curve defined by $E_2 : x^2 + y^2 = 1 + 2x^2y^2 (\text{mod} 1867)$, with $d = 2$ over F_{1171}. Let $P = (3,317)$ be a point on E_2 has prime order $n = 467$.

Using the 3-LLL lattice reduction algorithm (2.4.2.2), the first 3-ISD generator $\{v_1, v_2, v_3\}$ is computed, when $v_1 = (11,37,-17)$, $v_2 = (23,34,85)$ and $v_3 = (121,-48,3)$.

Suppose $t = 463 \in [1,466]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 (\text{mod}\, n) \equiv 292 (\text{mod}\, 467)$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 (\text{mod}\, n) \equiv 171 (\text{mod}\, 467),$$

where $\max\{292,171\} > \sqrt{n} = \sqrt{467} = 21.61$.

Now, Using the extended 3-LLL lattice reduction algorithm (3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, when

$$v_1' = (7, 17, -7),\ v_2' = (30, -7, -14),\ v_3' = (53, 3, 85)$$

and

$$v_1'' = (9, -2, 15),\ v_2'' = (-35, 13, 16),\ v_3'' = (-11, -56, -4).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_1 + t_{12}\lambda_1 \pmod{n} \equiv (-5) + (-10)(17) \pmod{467}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv (-8) + (-3)(96) \pmod{467}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (994,\ 68) + (1327, 509) + (1298, 1494) + (524, 1280) \\ &= (1070, 555) + (1528, 1113) \\ &= (1211, 1387). \end{aligned}$$

where $t_{11}P$, $t_{12}\psi_1(P)$, $t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$t_{11}P = -5(3, 317) = (994, 68)$, $t_{12}\psi_1(P) = (-10)(340, 1375) = (1327, 509)$,

$t_{21}P = (-8)(3, 317) = (1298, 1494)$ and

$t_{22}\psi_2(P) = (-3)(1626, 1039) = (524, 1280)$.

with $\psi_1(P) = \lambda_1 P = 17(3, 317) = (340, 1375)$

and $\psi_2(P) = \lambda_2 P = 96(3, 317) = (1626, 1039)$.

are two efficiently computable endomorphisms that are pre-computed.

Some other experimental results of the 3-ISD Edwards Scalar multiplication are seen in Chapter (5), Table (5.1).

3.4 The 3-ISD Twisted Edwards Scalar Multiplication Method

This section proposes to use another kind of the elliptic curve which is called twisted Edwards curve $E_{a,d}$ defined over prime field F_p to perform the scalar multiplication operation tP of a point P lies on it. Here the proposed 3-ISD method has been applied as follows. Suppose $E_{a,d}$ is a Twisted Edwards curve defined by

$$E_{a,d} : ax^2 + y^2 \equiv 1 + dx^2 y^2 \pmod{P} \tag{3.8}$$

Let P is a point lies on $E_{a,d}$ which has a prime order n. Assume t is a scalar in the range $[1, n-1]$ which is a scalar in scalar multiplication tP $v_3 = (a_3, b_3, c_3)$, that computed using the $E_{a,d}$ defined over F_p.

Based on the 3-ISD idea that is proposed in the previous case, a scalar t is decomposed first in to t_1 and t_2 with $\max\{|t_1|, |t_2|\} > \sqrt{n}$ which is computed using Equation (3.2),based on the first ISD generator that is generated using the 3-LLL lattice reduction Algorithm (2.4.2.2).

The application of the extended 3-LLL Algorithm (3.2.2.1) out puts the two 3-ISD generators that are used to sub-decompose t_1 and t_2 in to sub-scalar t_{11}, t_{12} and t_{21}, t_{22} respectively.

These sub-scalar are computed using the relations in Equation(3.4) and (3.5).with the conditions $\max\{|t_{11}|, |t_{12}|\} \le \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \le \sqrt{n}$.

Now, Twisted Edwards the scalar multiplication tP using 3-ISD method can be computed using the expression that is defined in Equation (3.7).The computation of the last equation needs the Per-computed values of two efficiently computable endomorphisms $\psi_1(P)=\lambda_1 P$ and $\psi_2(P)=\lambda_2 P$ of $E_{a,d}$ defined over F_p, where $\lambda_1,\lambda_2 \in [1,n-1]$ and P lies on $E_{a,d}$.

The 3-ISD twisted Edwards scalar multiplication can be implemented using Algorithm (3.4.1).

Algorithm (3.4.1): The 3-ISD Twisted Edwards Scalar Multiplication tP.

Input: The primes p,a and $n, \lambda \in [1,n-1],\ d \neq 0,1, a \neq d$ and $P \in E_{a,d}(p)$.

Output: 3-ISD Twisted Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism $\psi_1(P)=\lambda_1 P$ and $\psi_2(P)=\lambda_2 P$.

computation stage:

2. Run 3-LLL lattice reduction Algorithm (2.4.2.2) to find the first 3-ISD generator $\{v_1,v_2,v_3\} \ni v_1=(a_1,b_1,c_1), v_2=(a_2,b_2,c_2)$ and $v_3=(a_3,b_3,c_3)$.
3. Choose randomly a scalar $t \in [1,n-1]$.
4. Use the 3-ISD generator $\{v_1,v_2,v_3\}$ to decompose t into t_1 and t_2 such that $t_1 = t + a_1b_1 - a_2b_2 - a_3b_3 \pmod n$ and $t_2 = t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod n$ with $\max\{|t_1|,|t_2|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1,\lambda_2 \in [1,n-1]$.
6. Run the extended 3-LLL lattice reduction Algorithm (3.2.2.1) to find the two 3-ISDgenerator $\{v'_1,v'_2,v'_3\}$ and $\{v''_1,v''_2,v''_3\}$.
7. Use extended 3-LLL lattice reduction Algorithm (3.2.2.1) sub-decompose t_1 and t_2 into t_{11},t_{12} and t_{21},t_{22} respectively such that

$t_1 = t_{11} + t_{12}\lambda_1 (\mathrm{mod}\, n)$ and $t_2 = t_{21} + t_{22}\lambda_2 (\mathrm{mod}\, n)$, where $\max\{|t_{11}|, |t_{12}|\} \le \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \le \sqrt{n}$.

8. Compute tP 3-ISD Edwards scalar multiplication tP by $tP \equiv t_{11}\, P + t_{12}\, \psi_1(P) + t_{21}\, P + t_{22}\, \psi_2(P) \pmod{p}$
9. Return tP.

Example 3.4.1. (The 3- ISD Twisted Edwards scalar multiplication method)

Let $p = 1171$ be a prime number. Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{16,2}: 16x^2 + y^2 = 1 + 2x^2y^2 (\mathrm{mod} 1171)$, with $d = 2$ and $a = 16$ over F_{1171}. Let $p = (1169, 3)$ be a generator point lies on $E_{16,2}$ has prime order $n = 149$.

Using the 3-LLL lattice reduction Algorithm (2.4.2.2), the first 3-ISD generator $\{v_1, v_2, v_3\}$ is computed, when $v_1 = (-16, -5, -17), v_2 = (16, -2, -14)$ and $v_3 = (-6, -25, -3)$.

Suppose $t = 118 \in [1, 148]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 (\mathrm{mod}\, n) \equiv 80 (\mathrm{mod} 149)$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 (\mathrm{mod}\, n) \equiv 38 (\mathrm{mod} 149),$$

Where $\max\{80, 38\} > \sqrt{n} = \sqrt{149} = 12.21$.

Now, Using the extended 3-LLL lattice reduction Algorithm (3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$, when

$$v_1' = (16,-3,15),\ v_2' = (-26,12,31),\ v_3' = (-11,-58,-3)$$

and

$$v_1'' = (7,-3,19),\ v_2'' = (-30,14,8),\ v_3'' = (-21,-56,3).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \equiv 4 + 9(25) \pmod{149}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv 6 + 5(66) \pmod{149}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (957,745) + (871,621) + (662,1140) + (340,549) \\ &= (1033,504) + (929,730) \\ &= (567,1120). \end{aligned}$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$t_{11}P = 4(1169,3) = (957,745), t_{12}\psi_1(P) = 9(422,857) = (871,621),$

$t_{21}P = 6(1169,3) = (668,1140)$ and $t_{22}\psi_2(P) = 5(685,44) = (340,549).$

with $\psi_1(P) = \lambda_1 P = 25(1169,3) = (422,857)$

and $\psi_2(P) = \lambda_2 P = 66(1169,3) = (685,44).$

are two efficiently computable endomorphisms that are pre-computed.

Example 3.4.2. (The 3- ISD Twisted Edwards scalar multiplication method)

Let $p = 2011$ be a prime number. Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{64,2} : 64x^2 + y^2 = 1 + 2x^2y^2 \pmod{2011}$, with $d = 2$ and $a = 64$ over F_{2011}. Let $P = (9,1318)$ be a generator point lies on $E_{64,2}$ has prime order $n = 163$.

Using the 3-LLL lattice reduction Algorithm (2.4.2.2), the first 3-ISD generator $\{v_1, v_2, v_3\}$ is computed, when $v_1 = (20,6,14), v_2 = (6,18,-14)$ and $v_3 = (-42,38,48)$.

Suppose $t = 159 \in [1,162]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 \pmod{n} \equiv 137 \pmod{163}$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod{n} \equiv 22 \pmod{163},$$

where $\max\{137, 22\} > \sqrt{n} = \sqrt{163} = 12.76$.

Now, Using the extended 3-LLL lattice reduction algorithm (3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, where

$$v_1' = (-22,11,11),\ v_2' = (6,-3,35),\ v_3' = (-26,-53,2)$$

and

$$v_1'' = (5,12,25),\ v_2'' = (-37,6,-4),\ v_3'' = (-35,-74,42).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \,(\text{mod } n) \equiv 2 + 8(78)\,(\text{mod}163)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \,(\text{mod } n) \equiv (-4) + 5(103)\,(\text{mod}163).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (1311,\ 1750) + (878,\ 689) + (1825,32) + (216,1286) \\ &= (1795,1286) + (285,1158) \\ &= (1825,32). \end{aligned}$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$t_{11}P = 2(9,1318) = (1311,1750),\ \ t_{12}\psi_1(P) = 8(1920,1427) = (878,689),$

$t_{21}P = (-4)(9,1318) = (1825,32)$ and $t_{22}\psi_2(P) = 5(1299,606) = (216,1286).$

With $\psi_1(P) = \lambda_1 P = 78(9,1318) = (1920,1427)$

and $\psi_2(P) = \lambda_2 P = 103(9,1318) = (1299,606).$

are two efficiently computable endomorphisms that are pre-computed.

Several experimental results of the 3-ISD Twisted Edwards scalar multiplication are in implemented Chapter (5), Table (5.2).

3.5 New Type of 3-ISD Method.

The new type of 3-ISD method is discussed first to compute a scalar multiplication tP, when P is a point lies on Edwards curve E_d defined over prime field F_p. And later, this type also will be explained on lies on Twisted Edwards curve $E_{a,d}$ defined over prime field F_p.

3.5.1 Edwards Scalar Multiplication Based 3-ISD Computation Method.

Let $v_1=(a_1,b_1,c_1), v_2=(a_2,b_2,c_2)$ and $v_3=(a_3,b_3,c_3)$ be the short vectors that form a first 3-ISD generator $\{v_1,v_2,v_3\}$ which is a better basis that is computed using the 3-dimensioal *LLL* lattice reduction method.

Suppose E_d is an Edwards curve defined over F_p. Let P be a point lies on E_d defined over F_p. A scalar $t \in [1, n-1]$ in tP can be decomposed with new type of the decomposition. This type of the decomposition can be proved as follows.

Theorem 3.5.1.1. Suppose E_d is an Edwards curve (or twisted Edwards curve) defined over F_p. Let $t \in [1, n-1]$ with n is a prime order of a point P which lies on E_d. Then, 3-ISD scalar multiplication is defined by

$$tP \equiv (t_{11}+t_{21}+t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P),$$

where $\psi_1'(P)=\lambda_1'P$, $\psi_2'(P)=\lambda_2'P$, $\psi_1''(P)=\lambda_1''P$, $\psi_2''(P)=\lambda_2''P$, $\hat{\psi}_1(P)=\hat{\lambda}_1P$ and $\hat{\psi}_2(P)=\hat{\lambda}_2P$ are efficiently computable endomorphisms of Edwards curve E_d defined over F_p.

Proof.

Suppose E_d is an Edwards curve defined over F_p. Let P be a point lies on E_d defined over F_p. A scalar $t \in [1, n-1]$, where n is a prime order of P.

Based on a first 3-ISD generator $\{v_1,v_2,v_3\}$ that is formed using the 3-LLL algorithm with $v_1=(a_1,b_1,c_1), v_2=(a_2,b_2,c_2)$ and $v_3=(a_3,b_3,c_3)$, a scalar t is decomposed into new scalars t_1, t_2 and t_3, namely t can be written by

$$t \equiv t_1 + t_2\lambda_1 + t_3\lambda_2 \pmod{n} \qquad (3.9)$$

with $\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$, when $\lambda_1, \lambda_2 \in [1, n-1]$.

The scalar t_1, t_2 and t_3 are computed by

$$t_1 = t - d_1 a_1 - d_2 a_2 - d_3 a_3,\ t_2 = t - d_1 b_1 - d_2 b_2 - d_3 b_3 \tag{3.10}$$

and

$$t_3 = d_1 c_1 + d_2 c_2 + d_3 c_3 \tag{3.11}$$

.

where

$$d_1 = \lfloor -b_3 t / n \rceil,\ \ d_2 = \lfloor b_2 t / n \rceil \text{ and } d_3 = \lfloor b_1 t / n \rceil.$$

Now, the extended *LLL* lattice reduction algorithm is used to compute nine vectors.

$$v_1' = (a_1', b_1', c_1'),\ v_2' = (a_2', b_2', c_2'),\ v_3' = (a_3', b_3', c_3')$$

$$v_1'' = (a_1'', b_1'', c_1''), v_2'' = (a_2'', b_2'', c_2''), v_3'' = (a_3'', b_3'', c_3'')$$

and

$$\hat{v_1} = (\hat{a}_1, \hat{b_1}, \hat{c_1}), \hat{v_2} = (\hat{a}_2, \hat{b_2}, \hat{c}_2), \hat{v_3} = (\hat{a}_3, \hat{b_3}, \hat{c}_3)$$

These vectors form the ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. Using these generators, the scalars t_1, t_2 and t_3 are sub-decomposed again into new sub-scalars $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$, and t_{31}, t_{32}, t_{33} respectively. In the other words, the scalars t_1, t_2 and t_3 are written by

$$t_1 \equiv t_{11} + t_{12}\lambda_1^{'} + t_{13}\lambda_2^{'} (\text{mod } n),\ \ t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod}\, n) \tag{3.12}$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda_1} + t_{33}\hat{\lambda_2} (\text{mod}). \tag{3.13}$$

where

$$t_{11} \equiv t_1 - d_1'a_1' - d_2'a_2' - d_3'a_3' (\mathrm{mod}\, n),\ t_{12} \equiv t_{11} - d_1'b_1' - d_2'b_2' - d_3'b_3' \ (\mathrm{mod}\, n),$$
$$t_{13} \equiv d_1'c_1' + d_2'c_2' + d_3'c_3' \ (\mathrm{mod}\, n)$$

(3.14)

$$t_{21} \equiv t_2 - d_1''a_1'' - d_2''a_2'' - d_3''a_3'' (\mathrm{mod}\, n),\ t_{22} \equiv t_{21} - d_1''b_1'' - d_2''b_2'' - d_3''b_3'' \ (\mathrm{mod}\, n),$$
$$t_{23} \equiv d_1''c_1'' + d_2''c_2'' + d_3''c_3'' \ (\mathrm{mod}\, n)$$

(3.15)

and

$$t_{31} \equiv t_3 - \hat{d}_1\hat{a}_1 - \hat{d}_2\hat{a}_2 - \hat{d}_3\hat{a}_3 (\mathrm{mod}\, n),\ t_{32} \equiv t_{31} - \hat{d}_1\hat{b}_1 - \hat{d}_2\hat{b}_2 - \hat{d}_3\hat{b}_3 \ (\mathrm{mod}\, n),$$
$$t_{33} \equiv \hat{d}_1\hat{c}_1 + \hat{d}_2\hat{c}_2 + \hat{d}_3\hat{c}_3 \ (\mathrm{mod}\, n)$$

(3.16)

with $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \le \sqrt{n},\ \max\{|t_{21}|, |t_{22}|, |t_{23}|\} \le \sqrt{n}$

and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \le \sqrt{n}.$

The parameters d_i', d_i'' and $\hat{d}_i$ for $i = 1,2,3$ are computed by

$$d_1' = \lfloor -b_3't / n \rceil,\ d_2' = \lfloor b_2't / n \rceil,\ d_3' = \lfloor b_1't / n \rceil,$$

$$d_1'' = \lfloor -b_3''t / n \rceil,\ d_2'' = \lfloor b_2''t / n \rceil,\ d_3'' = \lfloor b_1''t / n \rceil,$$

and $\hat{d}_1 = \lfloor -\hat{b}_3t / n \rceil,\ \hat{d}_2 = \lfloor \hat{b}_2t / n \rceil,\ \hat{d}_3 = \lfloor \hat{b}_1t / n \rceil.$

The scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' + t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' + t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\mathrm{mod}\, n). \quad (3.17)$$

The Edwards scalar multiplication tP using the 3-ISD method is computed by

$$
\begin{aligned}
tP \equiv\, & t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\
& t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\
\equiv\, & \left(t_{11} + t_{21} + t_{31}\right)P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\
& t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P),
\end{aligned}
\tag{3.18}
$$

where $\psi_1^{'}(P) = \lambda_1^{'}P$, $\psi_2^{'}(P) = \lambda_2^{'}P$, $\psi_1^{''}(P) = \lambda_1^{''}P$, $\psi_2^{''}(P) = \lambda_2^{''}P$, $\hat{\psi}_1(P) = \hat{\lambda}_1 P$ and

$\hat{\psi}_2(P) = \hat{\lambda}_2 P$ are efficiently computable endomorphisms of Edwards curve E_d defined over F_p. ■

The 3-ISD Edwards scalar multiplication can be implemented using Algorithm (3.5.1.1).

Algorithm (3.5.1.1): Edwards Scalar Multiplication Based 3-ISD Computation tP.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$ and $P \in E_d(p)$.

Output: 3-ISD Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism

   $\psi_1'(P) = \lambda_1'P, \psi_2'(P) = \lambda_2'P, \psi_1''(P) = \lambda_1''P, \psi_2''(P) = \lambda_2''P, \hat{\psi}_1(P) = \hat{\lambda}_1 P$ and

   $\hat{\psi}_2(P) = \hat{\lambda}_2 P$.

   computation stage:

2. Run 3-LLL lattice reduction Algorithm (2.4.2.2) to find the first 3-ISD generator $\{v_1, v_2, v_3\} \ni v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and

   $v_3 = (a_3, b_3, c_3)$.

3. Choose randomly a scalar $t \in [1, n-1]$.

4. Use the 3-ISD generator $\{v_1, v_2, v_3\}$ to decompose t into t_1 and t_2 such that $t_1 = t + a_1b_1 - a_2b_2 - a_3b_3 \pmod{n}$ and $t_2 = t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod{n}$ with $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1', \lambda_2', \lambda_1'', \lambda_2'', \hat{\lambda}_1, \hat{\lambda}_2 \in [1, n-1]$.
6. Run the extended 3-LLL lattice reduction Algorithm (3.2.2.1) to find the two 3-ISDgenerator $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$.
7. Use extended 3-LLL lattice reduction Algorithm (3.2.2.1) sub-decompose t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that $t_1 = t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' \pmod{n}, t_2 = t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' \pmod{n}$ and $t_3 = t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \pmod{n}$, where $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \le \sqrt{n}$ $\max\{|t_{21}|, |t_{22}|, |t_{23}|\} \le \sqrt{n}$ and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \le \sqrt{n}$.
8. Compute *tP* 3-ISD Edwards scalar multiplication *tP* by

$$\begin{aligned} tP &\equiv t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\ &\equiv (t_{11} + t_{21} + t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P), \end{aligned}$$

9. Return *tP*.

Example 3.5.1.1 (Edwards Scalar Multiplication Based New Type of 3-ISD Method).

With a prime number $p = 1171$, **s**uppose $v_1 = (17, 17, -17), v_2 = (34, 51, 68)$ and $v_3 = (85, -68, -17)$ are three vectors computed using the 3-dimensioal *LLL* lattice reduction Algorithm (2.4.2.2).

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 188 \in [1, 292]$.

The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 \,(\mathrm{mod}\, n) \equiv 20 \,(\mathrm{mod}\, 293),$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 \,(\mathrm{mod}\, n) \equiv 21 \,(\mathrm{mod}\, 293),$$

and

$$t_3 \equiv d_1 c_1 + d_2 c_2 + d_3 c_3 \,(\mathrm{mod}\, n) \equiv 147 \,(\mathrm{mod}\, 293),$$

Where $\max\{20, 21, 147\} > \sqrt{n} = \sqrt{293} = 17.11$ and

$$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(-68)188 / 293 \rceil = 44,\ d_2 = \lfloor b_2 t / n \rceil = \lfloor (51)188 / 293 \rceil = 33,$$

$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (17)188 / 293 \rceil = 11.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* lattice reduction Algorithm (2.4.2.2) to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (3, 21, -3),\ v_2' = (14, 4, 16), v_3' = (16, -3, -15),$$
$$v_1'' = (5, 5, -5),\ v_2'' = (10, 15, 20),\ v_3'' = (25, -20, 5),$$

and

$$\hat{v_1} = (3, 13, -1),\ \hat{v_2} = (14, 4, 14),\ \hat{v_3} = (16, -3, -4).$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\mathrm{mod}\ n) \equiv 4 + 7(16) + (-15)(65) (\mathrm{mod}\, 293),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\mathrm{mod}\ n) \equiv 6 + (-14)(8) + 15(28) \,(\mathrm{mod}\, 293).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\mathrm{mod}\ n) \equiv 1 + (-12)(26) + (-2)(64) (\mathrm{mod}\, 293).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (749,710)+(459,69)+(903,514),+(220,526)+(712,69)+\\ &\quad (81,1054)+(7,766)+(701,196)+(744,18)\\ &= (630,404) \end{aligned}$$

when

$$\psi_1'(P)=\lambda_1'P=16(7,766)=(178,910),\ \ \psi_2'(P)=\lambda_2'P=65(7,766)=(51,1125),$$

$$\psi_1''(P)=\lambda_1''P=8(7,766)=(50,528),\quad \psi_2''(P)=\lambda_2''P=28(7,766)=(266,509)$$

$$\hat{\psi}_1(P)=\hat{\lambda}_1P=26(7,766)=(1048,904),\ \hat{\psi}_2(P)=\hat{\lambda}_2P=64(7,766)=(611,540).$$

$$t_{11}P=4(7,766)=(749,710),\ t_{12}\psi_1'(P)=7(178,910)=(459,69),$$
$$t_{13}\psi_2'(P)=-15(51,1125)=(903,514)$$

$$t_{21}P=6(7,766)=(220,526),\ \ t_{22}\psi_1''(P)=-14(50,528)=(712,69),$$
$$t_{23}\psi_2''(P)=15(266,509)=(81,1054)$$

$$t_{31}P=1(7,766)=(7,766),\quad t_{32}\hat{\psi}_1(P)=-12(1048,904)=(701,196),$$
$$t_{33}\hat{\psi}_2(P)=2(611,540)=(744,18)$$

are six efficiently computable endomorphisms that are pre-computed.

Example 3.5..1.2. (Edwards Scalar Multiplication Based New Type of 3-ISD method).

with a prime number $p=2083$, **s**uppose $v_1=(-17,7,7), v_2=(18,6,-61)$ and $v_3=(-21,-61,25)$ are three vectors computed using the 3-dimensioal *LLL* lattice reduction Algorithm (2.4.2.2).

So, the first generator of 3-ISD method is $\{v_1,v_2,v_3\}$ using to decompose a scalar $t=517\in[1,520]$.

The scalars t_1,t_2 and t_3 are computed by

$$t_1\equiv t-a_1d_1-a_2d_2-a_3d_3\,(\mathrm{mod}\,n)\equiv 30\,(\mathrm{mod}\ 521),$$
$$t_2\equiv t_1-b_1d_1-b_2d_2-b_3d_3\,(\mathrm{mod}\,n)\equiv 476\,(\mathrm{mod}\ 521),$$

and $$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \,(\text{mod}\, n) \equiv 20 \,(\text{mod } 521),$$

where $\max\{30, 467, 20\} > \sqrt{n} = \sqrt{521} = 22.83.$ and

$$d_1 = \lfloor -b_3 t \,/\, n \rceil = \lfloor -(-61)517 / 521 \rceil = 61,\ d_2 = \lfloor b_2 t \,/\, n \rceil = \lfloor (6)517 / 521 \rceil = 6$$

$$d_3 = \lfloor b_1 t \,/\, n \rceil = \lfloor (7)517 / 521 \rceil = 7.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm (3.2.2.1) to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (3, 21, -15),\ v_2' = (14, 4, 23),\ v_3' = (16, -3, -20),$$
$$v_1'' = (-29, 11, 11),\ v_2'' = (12, -3, 35),\ v_3'' = (-18, -53, 10).$$

and

$$\hat{v_1} = (11, -3, 10),\ \hat{v_2} = (-26, 12, 31),\ \hat{v_3} = (-11, -58, -4)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 14 + 17(8) + (-20)(6) (\text{mod } 521),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv (-9) + (-16)(64) + 2(229) (\text{mod } 512).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv (-2) + (4)(8) + (20)(260) (\text{mod } 521).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (359, 722) + (1125, 1026) + (676, 1064), +(1953, 1275) + (1851, 677) + \\ &\quad (1645, 233) + (219, 927) + (1227, 1975) + (135, 1640) \\ &= (1719, 2068) \end{aligned}$$

where

$$\psi_1'(P) = \lambda_1' P = 8(2076,469) = (1171,764),\ \ \psi_2'(P) = \lambda_2' P = 6(2076,469) = (638,1974),$$

$$\psi_1''(P) = \lambda_1'' P = 64(2076,469) = (1286,1763),\ \ \psi_2''(P) = \lambda_2'' P = 229(2076,469) = (767,1356)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 8(2076,469) = (1171,764),\ \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 260(2076,469) = (104,1114).$$

$$t_{11}P = 14(2076,469) = (359,722),\ t_{12}\psi_1'(P) = 17(1171,764) = (1125,1026),$$

$$t_{13}\psi_2'(P) = -20(638,1974) = (676,1064)$$

$$t_{21}P = -9(2076,469) = (1953,1275),\ \ t_{22}\psi_1''(P) = -16(1286,1763) = (1851,677),$$

$$t_{23}\psi_2''(P) = 2(767,1356) = (1645,233)$$

$$t_{31}P = -2(2076,469) = (219,927),\ \ t_{32}\hat{\psi}_1(P) = 4(1171,764) = (1227,1975),$$

$$t_{33}\hat{\psi}_2(P) = 20(1004,1114) = (135,1640)$$

are six efficiently computable endomorphisms that are pre-computed. Some implemented results of Edward scalar multiplication with new type of decomposition are implanted in Chapter (5) ,Table (5.3).

3.5.2 Twisted Edwards Scalar Multiplication Based 3-ISD Method.

Let $v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$ the short vectors that form a better basis which is computed using the 3-dimensioal *LLL* lattice reduction method.

A scalar $t \in [1, n-1]$ in the Twisted Edwards curve $E_{a,d}$, where n is a prime order of a point P which lies on Twisted Edwards curve $E_{a,d}$ defined over prime field F_p. A scalar multiplication tP can be decomposed into new scalars t_1, t_2 and t_3

Such that

$$t \equiv t_1 + t_2\lambda_1 + t_3\lambda_2 \pmod{n}$$

with $\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$,

with $\lambda_1, \lambda_2 \in [1, n-1]$ and at least one of these scalar t_i, for $i = 1,2,3$ lies outside the range $\sqrt{n}$ on the interval $[1, n-1]$.

where t_1, t_2 and t_3 are computed by

$$t_1 = t - d_1a_1 - d_2a_2 - d_3a_3,\ t_2 = t - d_1b_1 - d_2b_2 - d_3b_3$$

and

$$t_3 = d_1c_1 + d_2c_2 + d_3c_3$$

So, the parameters $d_1 = \lfloor -b_3t / n \rceil$, $d_2 = \lfloor b_2t / n \rceil$ and $d_3 = \lfloor b_1t / n \rceil$.

Now, the 3-dimensioal *LLL* lattice reduction method selection of six vectors has been done. These vectors are

$$v_1' = (a_1', b_1', c_1'),\ v_2' = (a_2', b_2', c_2'), v_3' = (a_3', b_3', c_3')$$

$$v_1'' = (a_1'', b_1'', c_1''),\ v_2'' = (a_2'', b_2'', c_2''),\ v_3'' = (a_3'', b_3'', c_3'')$$

and

$$\hat{v_1} = (\hat{a}_1, \hat{b_1}, \hat{c}_1),\ \hat{v_2} = (\hat{a}_2, \hat{b_2}, \hat{c}_2), \hat{v_3} = (\hat{a}_3, \hat{b_3}, \hat{c}_3)$$

that form the ISD generators $\{v_1', v_2', v_3'\}, \{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. The scalars t_1, t_2 and t_3 will be sub-decomposed again into new sub-scalars $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively. In the other words, the scalars t_1, t_2 and t_3 are written by

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n),\ t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod} n) \text{ and}$$

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\text{mod}).$$

where

$$t_{11} \equiv t_1 - d_1'a_1' - d_2'a_2' - d_3'a_3' (\text{mod} n),\ t_{12} \equiv t_{11} - d_1'b_1' - d_2'b_2' - d_3'b_3' \ (\text{mod} n),$$
$$t_{13} \equiv d_1'c_1' + d_2'c_2' + d_3'c_3' \ (\text{mod} n)$$

$$t_{21} \equiv t_2 - d_1''a_1'' - d_2''a_2'' - d_3''a_3'' (\text{mod} n),\ t_{22} \equiv t_{21} - d_1''b_1'' - d_2''b_2'' - d_3''b_3'' \ (\text{mod} n),$$
$$t_{23} \equiv d_1''c_1'' + d_2''c_2'' + d_3''c_3'' \ (\text{mod} n)$$

and

$$t_{31} \equiv t_3 - \hat{d}_1\hat{a}_1 - \hat{d}_2\hat{a}_2 - \hat{d}_3\hat{a}_3 (\text{mod} n),\ t_{32} \equiv t_{31} - \hat{d}_1\hat{b}_1 - \hat{d}_2\hat{b}_2 - \hat{d}_3\hat{b}_3 \ (\text{mod} n),$$
$$t_{33} \equiv \hat{d}_1\hat{c}_1 + \hat{d}_2\hat{c}_2 + \hat{d}_3\hat{c}_3 \ (\text{mod} n)$$

with $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \le \sqrt{n}, \max\{|t_{21}|, |t_{22}|, |t_{23}|\} \le \sqrt{n}$ and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \le \sqrt{n}.$

So, the scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' + t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' + t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\text{mod} n).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &\equiv t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\ &\equiv (t_{11} + t_{21} + t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \end{aligned}$$

Where $\psi_1'(P) = \lambda_1'P, \psi_2'(P) = \lambda_2'P, \psi_1''(P) = \lambda_1''P, \psi_2''(P) = \lambda_2''P$ and $\hat{\psi}_1(P) = \hat{\lambda}_1P, \hat{\psi}_2(P) = \hat{\lambda}_2P.$ are six efficiently computable endomorphisms of Twisted Edwards curve $E_{a,d}$ defined over F_p.

Algorithm (3.5.2.1): Twisted Edwards Scalar Multiplication Based 3-ISD Computation tP.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$, $a \neq d$ and $P \in E_d(p)$.

Output: 3-ISD Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism
   $\psi_1'(P) = \lambda_1' P, \psi_2'(P) = \lambda_2' P, \psi_1''(P) = \lambda_1'' P, \psi_2''(P) = \lambda_2'' P, \hat{\psi}_1(P) = \hat{\lambda}_1 P$ and
   $\hat{\psi}_2(P) = \hat{\lambda}_2 P$.

   computation stage:
2. Run 3-LLL lattice reduction Algorithm (2.4.2.2) to find the first 3-ISD generator $\{v_1, v_2, v_3\} \ni v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$.
3. Choose randomly a scalar $t \in [1, n-1]$.
4. Use the 3-ISD generator $\{v_1, v_2, v_3\}$ to decompose t into t_1 and t_2 such that $t_1 = t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n}$ and $t_2 = t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n}$ with $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1', \lambda_2', \lambda_1'', \lambda_2'', \hat{\lambda}_1, \hat{\lambda}_2 \in [1, n-1]$.
6. Run the extended 3-LLL lattice reduction Algorithm (3.2.2.1) to find the two 3-ISDgenerator $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$.
7. Use extended 3-LLL lattice reduction Algorithm (3.2.2.1) sub-decompose t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that $t_1 = t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' \pmod{n}, t_2 = t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' \pmod{n}$ and $t_3 = t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \pmod{n}$, where $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \leq \sqrt{n}$ $\max\{|t_{21}|, |t_{22}|, |t_{23}|\} \leq \sqrt{n}$ and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \leq \sqrt{n}$.

8. Compute tP 3-ISD Edwards scalar multiplication tP by

$$\begin{aligned} tP &\equiv t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\ &\equiv (t_{11} + t_{21} + t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P), \end{aligned}$$

9. Return tP.

Example 3.5.2.1 (Twisted Edwards Scalar Multiplication Based New Type of 3-ISD Method).

With a prime number $p = 1171$, **s**uppose $v_1 = (20,6,14), v_2 = (6,18,-14)$ and $v_3 = (-42,38,50)$ are three vectors computed using the 3-dimensioal *LLL* lattice reduction Algorithm (2.4.2.2).

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 147 \in [1,148]$.

The scalars t_1, t_2 and t_3 are computed by

$$\begin{aligned} t_1 &\equiv t - a_1d_1 - a_2d_2 - a_3d_3 \pmod{n} \equiv 137 \pmod{149}, \\ t_2 &\equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \pmod{n} \equiv 61 \pmod{149}, \end{aligned}$$

and

$$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \pmod{n} \equiv 98 \pmod{149},$$

where

$d_1 = \lfloor -b_3t / n \rceil = \lfloor -(38)147 / 149 \rceil = 37$, $d_2 = \lfloor b_2t / n \rceil = \lfloor (30)147 / 149 \rceil = 18$ and

$$d_3 = \lfloor b_1t / n \rceil = \lfloor (6)147 / 149 \rceil = 6.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm

(3.2.2.1) to generate the 3-ISD generators $\{v'_1, v'_2, v'_3\}$, $\{v''_1, v''_2, v''_3\}$ and $\{\hat{v}_1, \hat{v}_2, \hat{v}_3\}$. These vectors are

$$v'_1 = (9, -3, 10),\ v'_2 = (-24, 12, 31), v'_3 = (-22, -58, -7),$$
$$v''_1 = (-26, 12, 9),\ v''_2 = (10, -3, 31),\ v''_3 = (-22, -53, -2),$$

and

$$\hat{v}_1 = (16, 30, -11),\ \hat{v}_2 = (-27, 21, 29),\ \hat{v}_3 = (38, -15, 45)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda'_1 + t_{13}\lambda'_2 (\text{mod } n) \equiv 7 + 9(5) + (-2)(32) (\text{mod} 149),$$
$$t_2 \equiv t_{21} + t_{22}\lambda''_1 + t_{23}\lambda''_2 (\text{mod } n) \equiv 8 + (6)(3) + 8(23) (\text{mod} 149).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv 3 + (7)(9) + (4)(8) (\text{mod} 149).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (625,163) + (266,1077) + (119,1051), + (343,382) + (993,648) + \\ &\quad (948,539) + (311,501) + (266,1077) + (340,549) \\ &= (802,1050) \end{aligned}$$

where

$$\psi'_1(P) = \lambda'_1 P = 5(1169,3) = (1110,983),\ \psi'_2(P) = \lambda'_2 P = 32(1169,3) = (340,549),$$

$$\psi''_1(P) = \lambda''_1 P = 3(1169,3) = (311,501),\quad \psi''_2(P) = \lambda''_2 P = 23(1169,3) = (269,1032)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 9(1169,3) = (1004,109),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 8(1169,3) = (343,382).$$

$$t_{11}P = 7(1169,3) = (625,163),\ t_{12}\psi'_1(P) = 9(1110,983) = (266,1077),$$

$$t_{13}\psi'_2(P) = -2(340,549) = (119,1051)$$

$$t_{21}P = 8(1169,3) = (343,382),\ t_{22}\psi_1''(P) = 6(311,501) = (993,648),$$

$$t_{23}\psi_2''(P) = 8(269,1032) = (948,539)$$

$$t_{31}P = 3(1169,3) = (311,501),\ t_{32}\hat{\psi}_1(P) = 7(1004,109) = (266,1077),$$

$$t_{33}\hat{\psi}_2(P) = 4(343,382) = (340,549)$$

are six efficiently computable endomorphisms that are pre-computed.

Example 3.5.2.2 (Twisted Edwards Scalar Multiplication Based New Type of 3-ISD method).

With a prime number $p = 2083$, **s**uppose $v_1 = (15,-6,10), v_2 = (-26,11,28)$ and $v_3 = (-11,-56,-9)$ are three vectors computed using the 3-dimensioal *LLL* lattice reduction Algorithm (2.4.2.2).

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$using to decompose a scalar $t = 246 \in [1,256]$.

The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1d_1 - a_2d_2 - a_3d_3 \pmod{n} \equiv 170 \pmod{257},$$
$$t_2 \equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \pmod{n} \equiv 111 \pmod{257},$$

and $$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \pmod{n} \equiv 222 \pmod{257},$$

where $\max\{170,111,222\} > \sqrt{n} = \sqrt{257} = 16.$ and

$d_1 = \lfloor -b_3t / n \rceil = \lfloor -(-56)246 / 257 \rceil = 54,\ d_2 = \lfloor b_2t / n \rceil = \lfloor (11)246 / 257 \rceil = 11$ and $d_3 = \lfloor b_1t / n \rceil = \lfloor (-6)246 / 257 \rceil = -6.$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm (3.2.2.1) to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (-20,10,9),\ v_2' = (6,-3,35), v_3' = (-21,-53,2),$$
$$v_1'' = (-47,19,17),\ v_2'' = (29,3,59),\ v_3'' = (-47,-105,27),$$

and

$$\hat{v_1} = (21,6,14),\ \hat{v_2} = (5,18,-14),\ \hat{v_3} = (-41,38,36)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 1 + 16(16) + (2)(85) (\text{mod } 257),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv 3 + (-15)(4) + 12(14) (\text{mod } 257).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv 12 + (-11)(5) + (1)(8) (\text{mod } 257).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (13,1295) + (2070,1295) + (1219,238), +(325,1646) + (1558,1109) + \\ &\quad (1471,1655) + (274,1529) + (1262,955) + (2061,744) \\ &= (1539,1804) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 16(13,1295) = (114,158),\ \ \psi_2'(P) = \lambda_2' P = 85(13,1295) = (87,62),$$
$$\psi_1''(P) = \lambda_1'' P = 4(13,1295) = (1242,1703),\ \ \psi_2''(P) = \lambda_2'' P = 14(13,1295) = (1210,1568)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 5(13,1295) = (1321,732),\ \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 1(13,1295) = (13,1295).$$

$$t_{11}P = 1(13,1295) = (13,1295),\ t_{12}\psi_1'(P) = 16(114,158) = (2070,1295),$$
$$t_{13}\psi_2'(P) = 2(87,62) = (1219,238)$$

$$t_{21}P = 3(13,1295) = (325,1646),\ t_{22}\psi_1''(P) = -15(1242,1703) = (1558,1109),$$
$$t_{23}\psi_2''(P) = 12(1210,1568) = (1471,1655)$$

$$t_{31}P = 12(13,1295) = (274,1529),\ t_{32}\hat{\psi}_1(P) = -11(1321,732) = (1262,955),$$
$$t_{33}\hat{\psi}_2(P) = 8(13,1295) = (2061,744)$$

are six efficiently computable endomorphisms that are pre-computed.

More implemented results of twisted Edward curve can be seen in Chapter (5) in Table (5.4).

3.6 The Distribution of a Scalar *t* in the Interval [1, *n*-1]

This section discussed four cases of the distribution of scalar t in the scalar multiplication tP that is computed using the 3-ISD method which is applied on Edwards curve and Twisted Edwards curve defined over the prime fields.

The decomposition of a scalar t on these cases depended on using the 3-LLL lattice reduction algorithm and its extended algorithm to generate 3-ISD generators. The cases are discussed as follows.

3.6.1 Enumerating the Scalars in Interval [1, *n*-1] Using 3- ISD Edwards or Twisted Edwards Curve Method.

Suppose E_d is an Edwards curve and $E_{a,d}$ twisted Edwards curve defined F_p which is respectively given by

$$E_d : x^2 + y^2 = 1 + d\,x^2 y^2 (\mathrm{mod}\, p),\ E_{a,d} : ax^2 + y^2 = 1 + d\,x^2 y^2 (\mathrm{mod}\ p)$$

and $P = (x, y)$ is a point lies on E_d or $E_{a,d}$ The order of P is a prime number n and let t is scalar of an Edward or twisted Edwards curve scalar multiplication tP. This section discusses the procedure of sieving scalar t in $[1, n-1]$, which satisfy the 3-ISD method that explained in section (3.3) and section(3.4). The sieving process for computing the scalar multiplication tP on Edward curve over F_p. The decomposed

scalars t_1 and t_2 of 3-ISD scalar t satisfy the condition $\max\{|t_1|,|t_2|\} > \sqrt{n}$. The sieving process begins by writing down all the scalars t starting from 1 into $n-1$ which enumerates all the 3-ISD scalars t in interval $[1,n-1]$. The next step is to check all scalars t_1 and t_2 such that $t_1,t_2 < t$ with $t_1,t_2 \neq 0$ and $\max\{|t_1|,|t_2|\} > \sqrt{n}$. All scalars t with decompositions that do not satisfy the conditions are crossed off. The results of sieving process of scalars t that lie in the $[1,n-1]$ interval are determined based on the following cases of new scalars t_1 and t_2 values from t decomposition. These cases are as follows.

i. The decomposition of t into t_1 and t_2 resulted in $\min\{|t_1|,|t_2|\} = 1$ or $\max\{|t_1|,|t_2|\} = t$.

ii. The decomposition of t into t_1 and t_2 leads to $\max\{|t_1|,|t_2|\} > t$.

iii. The decomposition of t into t_1 and t_2 yields $\max\{|t_1|,|t_2|\} \leq \sqrt{n}$.

iv. The decomposition of t into t_1 and t_2 produces $\max\{|t_1|,|t_2|\} > \sqrt{n}$.

Repeating this process with cross off all cases i, ii and iii gives a list of the scalars up to *n*-1. These scalars lie outside the range $\sqrt{n}$ on the interval $[1,n-1]$. Scalars t with such a property represent 3-ISD used for the successful computation of the 3-ISD Edwards scalar multiplication tP. Using Algorithm (3.6.1), all the scalars satisfying the 3-ISD decomposition in the $[1,n-1]$ are determined. This algorithm is performed with input (n,v_1,v_2,v_3). to output the 3-ISD correct values of multipliers t.

Algorithm 3.6.1. 1.The Distribution of multiplier t in the 3-ISD Edwards scalar multiplication tP over a prime field.

Input : A prime n, vectors v_1= (a_1, b_1, c_1), v_2= (a_2, b_2, c_2) and v_3= (a_3, b_3, c_3).

Output : The list of the 3-ISD correct values of multiplier t.

1. For $t = 1$ to $n - 1$ do
2. Compute t_1
3. Compute t_2
4. If values of t_1 and t_2 satisfy the relation $t \equiv t_1 + t_2 \pmod{n}$ then
5. if $\min\{|t_1|, |t_2|\} = 1$ or $\max(\{|t_1|, |t_2|\} = t$ then
6. stop and go to step 1 to choose new value t.
7. Else if $(\max\{|t_1|, |t_2|\} > t\}$ then
8. stop and go to step 1 to choose new value of t.
9. Else if $(\max\{|t_1|, |t_2|\} \leq \sqrt{n}\}$ then
10. stop and go to step 1 to choose new value of t.
11. Else if $(\max\{|t_1|, |t_2|\} > \sqrt{n}\}$ then
12. return 3-ISD scalar t.
13. Else $t \geq n$
14. stop and go to step 1 to choose new value of t.
15. End if
16. Else
17. stop and go to step 1 to choose new value of t.
18. End if
19. End for
20. Return the list of the 3-ISD correct values of multiplier t.

Example 3.6.1.1. (Distributing the 3-ISD Edwards Scalar Multiplication Method)

Let $p = 1171$ be a prime number. **S**uppose $E_2 : x^2 + y^2 \equiv 1 + 2x^2y^2 \pmod{1171}$, with $d = 2$ is Edwards curve defined over F_{1171}. Let $P = (7, 766)$ be a point on E_2 has prime order $n = 293$.

Using the 3-LLL lattice reduction algorithm (2.4.2.2), the first 3-ISD generator $\{v_1, v_2, v_3\}$ is computed, when $v_1 = (-16, -6, -17), v_2 = (16, -3, -14)$ and $v_3 = (10, -18, 14)$.

Suppose $t = 133 \in [1, 292]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 \pmod{n} \equiv 95 \pmod{293}$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod{n} \equiv 38 \pmod{293},$$

where $\max\{95, 38\} > \sqrt{n} = \sqrt{293} = 17.11$.

Now, Using the extended 3-LLL lattice reduction algorithm (3.2.2.1), others six vectors are computed to generate 3-ISD generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, when

$$v_1' = (16, -3, 15),\ v_2' = (-26, 12, 31), v_3' = (-11, -58, -3)$$

and

$$v_1'' = (-23, 11, 13), v_2'' = (6, -3, 35),\ v_3'' = (-24, -53, 1).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \equiv (14) + 9(9) \pmod{293}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv -4 + 4(157) \pmod{293}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (447,1027) + (123,904) + (422,710) + (981,842) \\ &= (224,1025) + (429,434) \\ &= (1065,148), \end{aligned}$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 14(7,766) = (447,1027),\ t_{12}\psi_1(P) = 9(162,41) = (123,904),$$

$$t_{21}P = -4(7,766) = (422,710) \text{ and } t_{22}\psi_2(P) = 4(735,743) = (981,842).$$

with $$\psi_1(P) = \lambda_1 P = 225(7,766) = (162,41)$$

and $$\psi_2(P) = \lambda_2 P = 157(7,766) = (37,246).$$

are two efficiently computable endomorphisms that are pre-computed.

With another value $t = 187 \in [1,292]$ the decomposition into can be done scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n} \equiv 149 \pmod{293}$$

and

$$t_2 \equiv t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n} \equiv 38 \pmod{293},$$

Where $\max\{149,38\} > \sqrt{n} = \sqrt{293} = 17.11.$

Now, using the extended 3-LLL lattice reduction algorithm(3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$, when

$$v_1' = (20,6,14), v_2' = (6,18,-13), v_3' = (-42,38,47)$$

and

$$v_1'' = (-23,11,13), v_2'' = (6,-3,35),\ v_3'' = (-24,-53,1).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 (\text{mod}\, n) \equiv (-1) + 109(-4) (\text{mod}\, 293)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2\ (\text{mod}\ n) \equiv -4 + 4(157) (\text{mod}\, 293).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (1164,766) + (517,351) + (422,710) + (981,842) \\ &= (256,900) + (429,434) \\ &= (451,141), \end{aligned}$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = -(7,766) = (1164,766),\ t_{12}\psi_1(P) = -4(119,1144) = (517,351),$$

$$t_{21}P = -4(7,766) = (422,710) \text{ and } t_{22}\psi_2(P) = 4(735,743) = (981,842).$$

with $$\psi_1(P) = \lambda_1 P = 109(7,766) = (119,1144)$$

and $$\psi_2(P) = \lambda_2 P = 157(7,766) = (37,246).$$

are two efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [57,292]$ that have 3-ISD sub-scalars.

Example 3.6.1.2. (Distributing the 3-ISD Twisted Edwards Scalar Multiplication Method)

Let $p = 1171$ be a prime number. Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{16,2}: 16x^2 + y^2 = 1 + 2x^2y^2 \pmod{1171}$, with $d = 2$ and $a = 16$ over F_{1171}. Let $p = (1169,3)$ be a generator point lies on $E_{16,2}$ has prime order $n = 149$.

Using the 3-LLL lattice reduction algorithm (2.4.2.2), the first 3-ISD generator $\{v_1, v_2, v_3\}$ is computed, when $v_1 = (14,37,-17), v_2 = (20,34,85)$ and $v_3 = (121,-48,5)$.

Suppose $t = 91 \in [1,148]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 \pmod{n} \equiv 75 \pmod{149}$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod{n} \equiv 16 \pmod{149},$$

where $\max\{75,16\} > \sqrt{n} = \sqrt{149} = 12.21$.

Now, Using the extended 3-LLL lattice reduction algorithm (3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, when

$$v_1' = (-23,11,13),\ v_2' = (6,-3,35),\ v_3' = (-24,-53,1)$$

and

$$v_1'' = (7,12,25),\ v_2'' = (-41,6,-4),\ v_3'' = (-35,-74,42).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \equiv (2) + 7(53) \pmod{149}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv (-9) + (-4)(31) \pmod{149}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (64,644) + (300,621) + (167,109) + (606,212) \\ &= (598,743) + (24,707) \\ &= (906,978). \end{aligned}$$

where $t_{11}P$, $t_{12}\psi_1(P)$, $t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$t_{11}P = 2(1169,3) = (64,644)$, $t_{12}\psi_1(P) = 7(633,640) = (300,621)$,

$t_{21}P = (-9)(1169,3) = (167,109)$ and $t_{22}\psi_2(P) = (-4)(685,44) = (606,212)$.

with $\psi_1(P) = \lambda_1 P = 53(1169,3) = (633,640)$

and $\psi_2(P) = \lambda_2 P = 31(1169,3) = (269,1032)$.

are two efficiently computable endomorphisms that are pre-computed.

With another value $t = 94 \in [1,148]$ the decomposition into can be done scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n} \equiv 78 \pmod{149}$$

and

$$t_2 \equiv t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n} \equiv 16 \pmod{149},$$

where $\max\{78,16\} > \sqrt{n} = \sqrt{149} = 12.21$.

Now, Using the extended 3-LLL lattice reduction algorithm (3.2.2.1), others six vectors are computed to generate 3-IDS generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$, when $v'_1 = (5,12,25)$, $v'_2 = (-37,6,-4)$, $v'_3 = (-35,-74,42)$ and

$v_1'' = (7,12,25),\ v_2'' = (-41,6,-4),\ v_3'' = (-35,-74,42).$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 (\mathrm{mod}\, n) \equiv (5) + 10(52) (\mathrm{mod} 149)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \ (\mathrm{mod}\ n) \equiv (-9) + (-4)(31) (\mathrm{mod} 149).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (1110,983) + (300,621) + (167,109) + (606,212) \\ &= (872,919) + (24,707) \\ &= (902,1032). \end{aligned}$$

where $t_{11}P$, $t_{12}\psi_1(P)$, $t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$t_{11}P = 5(1169,3) = (1110,983),\ t_{12}\psi_1(P) = 10(177,348) = (300,621),$

$$t_{21}P = (-9)(1169,3) = (167,109) \text{ and}$$
$$t_{22}\psi_2(P) = (-4)(269,1032) = (606,212).$$

with $\psi_1(P) = \lambda_1 P = 52(1169,3) = (177,348)$

and $\psi_2(P) = \lambda_2 P = 31(1169,3) = (269,1032).$

are two efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [18,148]$ that have 3-ISD sub-scalars.

3.6.2 Enumerating the Scalars in Interval [1, *n*-1] Using New Type 3-ISD Edwards or twisted Edwards curve Method.

Suppose E_d is an Edwards curve and $E_{a,d}$ twisted Edwards curve defined F_p which is respectively given by

$$E_d : x^2 + y^2 = 1 + d\,x^2 y^2 (\mathrm{mod}\, p),\ E_{a,d} : ax^2 + y^2 = 1 + d\,x^2 y^2 (\mathrm{mod}\ p)$$

and $P = (x, y)$ is a point lies on E_d or $E_{a,d}$ The order of P is a prime number n and let t is scalar of an Edward or twisted Edwards curve scalar multiplication tP. This section discusses the procedure of sieving scalar t in $[1, n-1]$, which satisfy the 3-ISD method that explained in section (3.5.1)and section (3.5.2). The sieving process for computing the scalar multiplication tP on Edward curve twisted Edwards curve over F_p. The decomposed scalars t_1, t_2 and t_3 of 3-ISD scalar t satisfy the condition $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$. The sieving process begins by writing down all the scalars t starting from 1 into $n-1$ which enumerates all the 3-ISD scalars t in interval $[1, n-1]$. The next step is to check all scalars t_1 and t_2 such that $t_1, t_2, t_3 < t$ with $t_1, t_2, t_3 \neq 0$ and $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$. All scalars t with decompositions that do not satisfy the conditions are crossed off. The results of sieving process of scalars t that lie in the $[1, n-1]$ interval are determined based on the following cases of new scalars t_1, t_2 and t_3 values from t decomposition. These cases are as follows.

i. The decomposition of t into t_1, t_2 and t_3 resulted in $\min\{|t_1|, |t_2|, |t_3|\} = 1$ or $\max\{|t_1|, |t_2|, |t_3|\} = t$.

ii. The decomposition of t into t_1, t_2 and t_3 leads to $\max\{|t_1|, |t_2|, |t_3|\} > t$.

iii. The decomposition of t into t_1,t_2 and t_3 yields $\max\{|t_1|,|t_2|,|t_3|\} \le \sqrt{n}$.

iv. The decomposition of t into t_1,t_2 and t_3 produces $\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$.

Repeating this process with cross off all cases i, ii and iii gives a list of the scalars up to n-1. These scalars lie outside the range $\sqrt{n}$ on the interval $[1,n-1]$. Scalars t with such a property represent 3-ISD used for the successful computation of the 3-ISD Edwards scalar multiplication tP. Using Algorithm (3.6.2.1), all the scalars satisfying the 3-ISD decomposition in the $[1,n-1]$ are determined. This algorithm is performed with input (n,v_1,v_2,v_3). to output the 3-ISD correct values of multipliers t.

Algorithm 3.6.2.1. The Distribution of multiplier t in the New Type

3-ISD Edwards and twisted Edwards curve scalar multiplication tP over a prime field.

Input : A prime n, vectors v_1= (a_1, b_1, c_1), v_2= (a_2, b_2, c_2) and v_3= (a_3, b_3, c_3).

Output : The list of the 3-ISD correct values of multiplier t.

1. For $t=1$ to $n-1$ do
2. Compute t_1
3. Compute t_2
4. Compute t_3
5. If values of t_1,t_2 and t_3 satisfy the relation $t \equiv t_1 + t_2\lambda_1 + t_3\lambda_2 \pmod{n}$ then
6. if $\min\{|t_1|,|t_2|,|t_3|\} = 1$ or $\max\{|t_1|,|t_2|,|t_3|\} = t$ then
7. stop and go to step 1 to choose new value t.

8. Else if $(\max\{|t_1|,|t_2|,|t_3|\} > t\}$ then

9. stop and go to step 1 to choose new value of t.

10. Else if $(\max\{|t_1|,|t_2|,|t_3|\} \le \sqrt{n}\}$ then

11. stop and go to step 1 to choose new value of t.

12. Else if $(\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}\}$ then

13. return 3-ISD scalar t.

14. Else $t > n$

15. stop and go to step 1 to choose new value of t.

16. End if

17. Else

18. stop and go to step 1 to choose new value of t.

19 End if

20. End for

21. Return the list of the 3-ISD correct values of multiplier t.

Example 3.6.2.1. (Distributing Edwards Scalar Multiplication based new Type of 3-ISD Method).

With a prime number $p = 1171$, **s**uppose $v_1 = (-23,11,9), v_2 = (7,-3,35)$ and $v_3 = (-25,-53,1)$ are three vectors computed using the 3-dimensioal *LLL* lattice reduction Algorithm (2.4.2.2).

So, the first generator of 3-ISD method is $\{v_1,v_2,v_3\}$using to decompose a scalar $t = 157 \in [1,292]$.

The scalars t_1,t_2 and t_3 are computed by

$$t_1 \equiv t - a_1d_1 - a_2d_2 - a_3d_3 \,(\mathrm{mod}\, n) \equiv 86 (\mathrm{mod}\, 293),$$
$$t_2 \equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \,(\mathrm{mod}\, n) \equiv 90 (\mathrm{mod}\, 293),$$

and

$$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \,(\mathrm{mod}\, n) \equiv 274 (\mathrm{mod}\, 293),$$

where $\max\{86,90,724\} > \sqrt{n} = \sqrt{293} = 17.11$ and

$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(-53)157/293 \rceil = 28,\ d_2 = \lfloor b_2 t / n \rceil = \lfloor (-3)157/293 \rceil = -2,$

$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (11)157/293 \rceil = 6.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm (3.2.2.1) to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (-27,10,3),\ v_2' = (7,-3,40), v_3' = (-25,-53,1),$$
$$v_1'' = (3,21,-3),\ v_2'' = (14,4,16),\ v_3'' = (12,-3,-2),$$

and

$$\hat{v_1} = (-12,3,3),\ \hat{v_2} = (5,1,17),\ \hat{v_3} = (-6,26,19).$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod}\, n) \equiv 14 + 10(5) + (11)(2) (\text{mod}\, 293),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod}\, n) \equiv 1 + (-6)(8) + (1)(137) (\text{mod}\, 293)$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod}\ n) \equiv -1 + (-8)(3) + (2)(3) (\text{mod}\, 293).$$

The scalar multiplication *tP* using the 3-ISD method is computed by

$$\begin{aligned} tP &= (447,1027) + (223,850) + (970,585), + (7,766) + (994,1000) + \\ &\quad (778,471) + (1164,766) + (106,148) + (220,526) \\ &= (753,484) \end{aligned}$$

when

$$\psi_1'(P)=\lambda_1'P=5(7,766)=(650,926),\ \psi_2'(P)=\lambda_2'P=2(7,766)=(884,532),$$
$$\psi_1''(P)=\lambda_1''P=8(7,766)=(50,528),\quad \psi_2''(P)=\lambda_2''P=137(7,766)=(778,471)$$

$$\hat{\psi}_1(P)=\hat{\lambda}_1P=3(7,766)=(230,136),\ \hat{\psi}_2(P)=\hat{\lambda}_2P=3(7,766)=(230,136).$$

$$t_{11}P=14(7,766)=(447,1027),\ t_{12}\psi_1'(P)=10(650,926)=(223,850),$$
$$t_{13}\psi_2'(P)=11(884,532)=(970,585)$$

$$t_{21}P=1(7,766)=(7,766),\ t_{22}\psi_1''(P)=-6(50,528)=(994,1000),$$
$$t_{23}\psi_2''(P)=1(778,471)=(778,471)$$

$$t_{31}P=-1(7,766)=(1164,766),\quad t_{32}\hat{\psi}_1(P)=-8(230,136)=(106,148),$$
$$t_{33}\hat{\psi}_2(P)=2(230,136)=(220,526)$$

are six efficiently computable endomorphisms that are pre-computed.

With another value $t=207\in[1,293]$ the decomposition into can be done scalars t_1,t_2 and t_3 such that

$$t_1\equiv t-a_1d_1-a_2d_2-a_3d_3\ (\mathrm{mod}\,n)\equiv 100(\mathrm{mod}\,293),$$
$$t_2\equiv t_1-b_1d_1-b_2d_2-b_3d_3\ (\mathrm{mod}\,n)\equiv 249(\mathrm{mod}\,293),$$

and

$$t_3\equiv d_1c_1+d_2c_2+d_3c_3\ (\mathrm{mod}\,n)\equiv 151(\mathrm{mod}\,293),$$

where $\max\{100,249,151\}>\sqrt{n}=\sqrt{293}=17.11$ and

$$d_1=\lfloor -b_3t/n\rceil=\lfloor -(-53)207/293\rceil=37,\ d_2=\lfloor b_2t/n\rceil=\lfloor(-3)207/293\rceil=-2,$$

$$d_3=\lfloor b_1t/n\rceil=\lfloor(11)207/293\rceil=8.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm (3.2.2.1) to generate the 3-ISD generators $\{v_1',v_2',v_3'\}$, $\{v_1'',v_2'',v_3''\}$ and $\{\hat{v}_1,\hat{v}_2,\hat{v}_3\}$. These vectors are

$$v_1' = (-27,3,-3),\ v_2' = (8,4,20), v_3' = (2,-23,9),$$
$$v_1'' = (-16,-5,-17),\ v_2'' = (16,-2,-14),\ v_3'' = (-6,-25,-8),$$

and

$$\hat{v_1} = (-12,-6,-1),\ \hat{v_2} = (16,-2,-14),\ \hat{v_3} = (-6,-25,-3).$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11},t_{12},t_{13},t_{21},t_{22},t_{23}$ and t_{31},t_{32},t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod}\, n) \equiv 13 + 8(4) + (11)(5) (\text{mod}\, 293),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod}\, n) \equiv 7 + (5)(8) + (-4)(96) (\text{mod}\, 293)$$

and $t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod}\ n) \equiv 12 + (13)(5) + (10)(66) (\text{mod}\, 293).$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (16,181) + (983,384) + (499,15), +(443,548) + (341,165) + \\ &\quad (1011,1132) + (447,1027) + (51,1125) + (684,175) \\ &= (306,123) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 4(7,766) = (749,710),\ \ \psi_2'(P) = \lambda_2' P = 11(7,766) = (703,693),$$
$$\psi_1''(P) = \lambda_1'' P = 5(7,766) = (650,926),\quad \psi_2''(P) = \lambda_2'' P = 96(7,766) = (268,514)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 5(7,766) = (650,926),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 66(7,766) = (68,238).$$

$$t_{11}P = 13(7,766) = (16,181),\ t_{12}\psi_1'(P) = 8(749,710) = (983,384),$$
$$t_{13}\psi_2'(P) = 5(703,693) = (499,15)$$

$$t_{21}P = 7(7,766) = (443,548),\ \ t_{22}\psi_1''(P) = 8(650,926) = (341,165),$$
$$t_{23}\psi_2''(P) = -4(268,514) = (1011,1132)$$

$$t_{31}P = 12(7,766) = (447,1027),\quad t_{32}\hat{\psi}_1(P) = 13(650,926) = (51,1125),$$
$$t_{33}\hat{\psi}_2(P) = 10(68,238) = (684,175)$$

are six efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [49,292]$ that have 3-ISD sub-scalars.

Example 4.5.2.2 (Twisted Edwards Scalar Multiplication based new Type of 3-ISD Method).

With a prime number $p = 1171$, **s**uppose $v_1 = (20,6,14), v_2 = (6,18,-14)$ and $v_3 = (-42,38,50)$ are three vectors computed using the 3-dimensioal *LLL* lattice reduction Algorithm (2.4.2.2).

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 112 \in [1,148]$.

The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 \pmod{n} \equiv 73 \pmod{149},$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 \pmod{n} \equiv 57 \pmod{149},$$

and

$$t_3 \equiv d_1 c_1 + d_2 c_2 + d_3 c_3 \pmod{n} \equiv 131 \pmod{149},$$

where $\max\{73,57,131\} > \sqrt{n} = \sqrt{149} = 12.21.$ and

$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(38)112/149 \rceil = 29$, $d_2 = \lfloor b_2 t / n \rceil = \lfloor (18)112/149 \rceil = 14$ and

$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (6)112/149 \rceil = 5.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm (3.2.2.1) to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (-26,12,9),\ v_2' = (11,-3,31),\ v_3' = (-22,-53,-8),$$
$$v_1'' = (13,19,-3),\ v_2'' = (15,6,16),\ v_3'' = (20,-5,-3),$$

and $\hat{v_1} = (-21,11,11),\ \hat{v_2} = (6,-3,35),\ \hat{v_3} = (-20,-53,4)$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11},t_{12},t_{13},t_{21},t_{22},t_{23}$ and t_{31},t_{32},t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod}\, n) \equiv (-2) + 1(4) + (6)(136)(\text{mod}149),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod}\, n) \equiv 10 + (-5)(32) + (5)(101)(\text{mod}149)$$

and $t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod}\ n) \equiv -5 + (-1)(18) + (5)(1)(\text{mod}149).$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (1107,644) + (957,745) + (299,919), + (589,896) + (427,832) + \\ &\quad (954,97) + (61,983) + (178,648) + (1110,983) \\ &= (234,1050) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 4(1169,3) = (957,745), \ \ \psi_2'(P) = \lambda_2' P = 136(1169,3) = (264,469),$$
$$\psi_1''(P) = \lambda_1'' P = 32(1169,3) = (340,549), \quad \psi_2''(P) = \lambda_2'' P = 101(1169,3) = (1147,707)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 18(1169,3) = (993,648), \ \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 1(1169,3) = (1169,3).$$

$$t_{11}P = -2(1169,3) = (1107,644), \ t_{12}\psi_1'(P) = 1(957,745) = (957,745),$$
$$t_{13}\psi_2'(P) = 6(264,469) = (299,919)$$

$$t_{21}P = 10(1169,3) = (589,896), \ t_{22}\psi_1''(P) = -5(311,501) = (427,832),$$
$$t_{23}\psi_2''(P) = 5(1147,707) = (954,97)$$

$$t_{31}P = -5(1169,3) = (61,983), \ t_{32}\hat{\psi}_1(P) = -1(993,648) = (178,648),$$
$$t_{33}\hat{\psi}_2(P) = 5(1169,3) = (1110,983)$$

are six efficiently computable endomorphisms that are pre-computed.

With another value $t = 113 \in [1,148]$ the decomposition into can be done scalars t_1, t_2 and t_3 such that

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 (\text{mod}\, n) \equiv 74(\text{mod}149),$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 (\text{mod}\, n) \equiv 59(\text{mod}149),$$

and

$$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \,(\text{mod}\, n) \equiv 129 (\text{mod} 149),$$

where $\max\{73,57,131\} > \sqrt{n} = \sqrt{149} = 12.21.$ and

$d_1 = \lfloor -b_3 t \,/\, n \rceil = \lfloor -(38)113/149 \rceil = 26,\ d_2 = \lfloor b_2 t \,/\, n \rceil = \lfloor (18)113/149 \rceil = 14$ and

$$d_3 = \lfloor b_1 t \,/\, n \rceil = \lfloor (6)113/149 \rceil = 6.$$

Now, others extended nine the short vectors that form a better basis which are computed using the 3- *LLL* extended lattice reduction Algorithm (3.2.2.1) to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (-26,12,9),\ v_2' = (11,-3,31), v_3' = (-22,-53,-8),$$
$$v_1'' = (14,18,-3),\ v_2'' = (15,6,16),\ v_3'' = (20,-5,-3),$$

and $\hat{v_1} = (16,-3,15),\ \hat{v_2} = (-26,12,29),\ \hat{v_3} = (-11,58,-4)$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod}\, n) \equiv -1 + 2(8) + (6)(134) (\text{mod} 149),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod}\, n) \equiv 10 + (-3)(8) + (5)(104) (\text{mod} 149)$$

and $t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod}\ n) \equiv 3 + (8)(8) + (9)(40) (\text{mod} 149).$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (2,3) + (377,200) + (885,654), + (589,896) + (785,71) + \\ &\quad (300,621) + (311,501) + (1052,1051) + (45,178) \\ &= (320,1053) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 8(1169,3) = (343,382),\ \ \psi_2'(P) = \lambda_2' P = 134(1169,3) = (401,691),$$
$$\psi_1''(P) = \lambda_1'' P = 8(1169,3) = (343,382),\quad \psi_2''(P) = \lambda_2'' P = 104(1169,3) = (905,1077)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 8(1169,3) = (343,382),\ \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 40(1169,3) = (182,776).$$

$$t_{11}P = -1(1169,3) = (2,3),\ t_{12}\psi_1'(P) = 2(343,382) = (377,200),$$
$$t_{13}\psi_2'(P) = 6(401,691) = (885,654)$$

$$t_{21}P = 10(1169,3) = (589,896),\ \ t_{22}\psi_1''(P) = -3(343,382) = (785,71),$$
$$t_{23}\psi_2''(P) = 5(905,1077) = (300,621)$$

$$t_{31}P = 3(1169,3) = (311,501),\ t_{32}\hat{\psi}_1(P) = 8(343,382) = (1052,1051),$$
$$t_{33}\hat{\psi}_2(P) = 9(182,776) = (45,178)$$

are six efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [41,148]$ that have 3-ISD sub-scalars.

Chapter Four

The Twisted Edwards 3-ISD Method Using the Randomized Generators

4.1 Introduction

In this Chapter, a new version of the integer sub-decomposition method on decomposing the Scalar t in 3-dimension. In other words, the 3-ISD generators are generated with 3-dimension to decompose and sub-decompose the Scalar t in a scalar multiplication tP.To generate these generators, the vectors that have three dimensions that are chosen randomly and each component on each vector is relatively prime is used.

Four case of 3-ISD method are employed to compute a scalar multiplication tP Edwards and twisted Edwards curves defined over prime field. The security considerations of these case are discussed and determined in this chapter as well.

4.2 The 3-ISD Edwards Scalar Multiplication Method Based on the Randomized Generators

In this section, Suppose v_1, v_2 and v_3 are vectors that have three dimensions that are chosen randomly from the range $[1, p-1]$. Based on 3-dimensions of the coordinates of the vectors that form the first 3-ISD generator, the scalar $t \in [1, n-1]$ can be decomposed into two scalars t_1 and t_2 as defined in Equation (3.1) by

$$t = t_1 + t_2\lambda \pmod{n}, \text{ with } \max\{|t_1|, |t_2|\} > \sqrt{n},$$

where t_1 and t_2, as given in Equation (3.2), are computed by

$$t_1 = t + a_1b_1 - a_2b_2 - a_3b_3 \pmod{n} \text{ and } t_2 = t_1 + b_1c_1 - b_2c_2 - b_3c_3 \pmod{n}.$$

Now, a random selection of six vectors has been done. These vectors are

$$v'_1 = (a'_1, b'_1, c'_1), v'_2 = (a'_2, b'_2, c'_2),\ v'_3 = (a'_3, b'_3, c'_3)$$

and $$v''_1 = (a''_1, b''_1, c''_1), v''_2 = (a''_2, b''_2, c''_2), v''_3 = (a''_3, b''_3, c''_3)$$

that form the ISD generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$. The scalars t_1 and t_2 will be sub-decomposed again into new sub-scalars t_{11}, t_{12} and t_{21}, t_{22} respectively. In the other words, the scalars t_1 and t_2 are written by

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \text{ and } t_2 \equiv t_{21} + t_{22}\lambda_1 \pmod{n},$$

where $t_{11} \equiv t_1 + a''_1b'_1 - a'_2b'_2 - a'_3b'_3 \pmod{n}$, $t_{12} \equiv t_{11} + b'_1c'_1 - b'_2c'_2 - b'_3c'_3 \pmod{n}$

and $t_{21} \equiv t_2 + a''_1b''_1 - a''_2b''_2 - a''_3b''_3 \pmod{n}$, $t_{22} \equiv t_{21} + b''_1c''_1 - b''_2c''_2 - b''_3c''_3 \pmod{n}$

with $\max\{|t_{11}|, |t_{12}|\} \le \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \le \sqrt{n}$. So, the scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1 + t_{21} + t_{22}\lambda_2 \pmod{n}.$$

The scalar multiplication tP using the 3-ISD method is computed by

$$tP \equiv t_{11}P + t_{12}\psi_1(P) + t_{21}P + t_{22}\psi_2,$$

Where $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$ are two efficiently computable endomorphisms of Edwards curve E_d defined over F_p.

The 3-ISD Edwards scalar multiplication tP based on randomized vectors that are used to generate the 3-ISD generators can be implemented using Algorithm (4.2.1).

Algorithm (4.2.1): The 3-ISD Edwards Scalar multiplication tP based on randomized Generators.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$ and $P \in E_d(p)$.

Output: 3-ISD Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$.

computation stage:

2. Choose randomly the elements $a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3, c_3$ from the rang $[1, p-1]$ to generate the vectors $v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$ that forms a first 3-ISD generator $\{v_1, v_2, v_3\}$.
3. Choose randomly a scalar $t \in [1, n-1]$.
4. Use the 3-ISD generator $\{v_1, v_2, v_3\}$ to decompose t into t_1 and t_2 such that $t_1 = t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n}$ and $t_2 = t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n}$ with $\max\{|t_1|, |t_2|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1, \lambda_2 \in [1, n-1]$.
6. Randomly Select some elements from the range $[1, p-1]$ to generator the vector $v_1' = (a_1', b_1', c_1'), v_2' = (a_2', b_2', c_2'), v_3' = (a_3', b_3', c_3'), v_1'' = (a_1'', b_1'', c_1'')$, $v_2'' = (a_2'', b_2'', c_2'')$ and $v_3'' = (a_3'', b_3'', c_3'')$ to form the two 3-ISDgenerator $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$.
7. Use 3-ISD randomized generator to sub-decompose t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that $t_1 = t_{11} + t_{12}\lambda_1 \pmod{n}$ and $t_2 = t_{21} + t_{22}\lambda_1 \pmod{n}$, where $\max\{|t_{11}|, |t_{12}|\} \leq \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \leq \sqrt{n}$.
8. Compute tP 3-ISD Edwards scalar multiplication tP by $tP \equiv t_{11} P + t_{12} \psi_1(P) + t_{21} P + t_{22} \psi_2(P) \pmod{p}$
9. Return tP.

Example 4.2.1. (The 3- ISD Edwards Scalar Multiplication Method Using the Randomized Generators)

Let $P = 1171$ be a prime number. Suppose E_d is an Edwards curve defined by $E_2 : x^2 + y^2 = 1 + 2x^2y^2 (\text{mod} 1171)$, with $d = 2$ over F_{1171}. Let $P = (7,766)$ be a point on E_2 has prime order $n = 293$.

Suppose $v_1 = (37,65,31)$, $v_2 = (21,47,6)$ and $v_3 = (17,33,19)$ are three vectors are chosen randomly. The elements on each vector are selected from the interval [1,1170].

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$.

Suppose $t = 290 \in [1,290]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 (\text{mod}\, n) \equiv 268 (\text{mod}\, 293)$$

and

$$t_2 \equiv t_1 + a_1c_1 - a_2c_2 - a_3c_3 (\text{mod}\, n) \equiv 22 (\text{mod}\, 293)$$

where $\max\{268,22\} > \sqrt{n} = \sqrt{293} = 17.11$.

Now, others six vectors are chosen randomly from the interval [1,1170] to generate the 3-ISD generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$, where

$v'_1 = (22,11,31)$, $v'_2 = (11,14,19)$, $v'_3 = (7,8,9)$

and

$$v''_1 = (11,13,12),\ v''_2 = (10,9,29),\ v''_3 = (7,10,47).$$

These generators are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \,(\text{mod } n) \equiv 7 + 10(114)\,(\text{mod } 293)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \,(\text{mod } n) \equiv 5 + 16(56)\,(\text{mod } 293).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (443,548) + (188,384) + (650,926) + (333,489) \\ &= (183,277) + (970,585) \\ &= (941,136), \end{aligned}$$

Where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 7(7,766) = (443,548),\ t_{12}\psi_1(P) = 10(1106,237) = (188,384),$$

$$t_{12}P = 5(7,766) = (650,926) \text{ and } t_{22}\psi_2(P) = 16(127,296) = (333,489).$$

with $\psi_1(P) = \lambda_1 P = 114(7,766) = (1106,237)$

and $\psi_2(P) = \lambda_2 P = 56(7,766) = (127,296).$

are two efficiently computable endomorphisms that are pre-computed.

Example 4.2.2. (The 3- ISD Edwards Scalar Multiplication Method Using the Randomized Generators)

Let $P = 1867$ be a prime number. Suppose E_d is an Edwards curve defined by $E_2 : x^2 + y^2 = 1 + 2x^2y^2 (\text{mod} 1171)$, with $d = 2$ over F_{1171}. Let $P = (7,766)$ be a point on E_2 has prime order $n = 467$.

Suppose $v_1 = (47,57,72)$, $v_2 = (27,65,39)$ and $v_3 = (37,55,59)$ are three vectors are chosen randomly. The elements on each vector are selected from the interval [1,1866].

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$.

Suppose $t = 459 \in [1,466]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \,(\mathrm{mod}\, n) \equiv 282 \,(\mathrm{mod}\, 467)$$

and

$$t_2 \equiv t_1 + a_1 c_1 - a_2 c_2 - a_3 c_3 \,(\mathrm{mod}\, n) \equiv 177 \,(\mathrm{mod}\, 467)$$

where $\max\{282,177\} > \sqrt{n} = \sqrt{467} = 21.61.$

Now, others six vectors are chosen randomly from the interval [1,1866] to generate the 3-ISD generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, where

$$v_1' = (101,113,85),\ v_2' = (12,17,29),\ v_3' = (27,10,117)$$

and

$$v_1'' = (10,11,17),\ v_2'' = (12,17,5), v_3'' = (7,10,11).$$

These generators are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \,(\mathrm{mod}\ n) \equiv 13 + 16(46) \,(\mathrm{mod}\, 467)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \ (\mathrm{mod}\ n) \equiv 13 + 5(313) \,(\mathrm{mod}\, 467).$$

Then, the ISD scalar multiplication can be computed by

$$\begin{aligned} tP &= (960,1178)+(732,1287)+(960,1178)+(1050,1217) \\ &= (872,667)+(910,132) \\ &= (970,331) \end{aligned}$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 13(3,317) = (950,1178),\ t_{12}\psi_1(P) = 13(821,1644) = (732,1287),$$
$$t_{12}P = 13(3,317) = (960,1178) \text{ and } t_{22}\psi_2(P) = 5(1493,1769) = (1050,1217).$$

with $$\psi_1(P) = \lambda_1 P = 114(7,766) = (1106,237)$$

and $$\psi_2(P) = \lambda_2 P = 56(7,766) = (127,296).$$

are two efficiently computable endomorphisms that are pre-computed.

Some other experimental results of the 3-ISD Edwards Scalar Multiplication that is created based on the randomized 3-ISD generators can be seen in Chapter (5) in Table (5.6).

4.3 The 3-ISD Twisted Edwards Scalar Multiplication Method Based on the Randomized Generators

Suppose three dimension vectors v_1, v_2 and v_3 are chosen randomly from the range $[1, P-1]$. These vectors form the first 3-ISD generator $\{v_1, v_2, v_3\}$ where $v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$. Let t be a scalar lies within the range $[1, n-1]$ where n is a prime order of a point P which lies on twisted Edwards curve $E_{a,d}$ defined over a prime field F_p. Based on 3-dimension of the coordinates of the vectors that form the first generator, a scalar t can be decomposed into two scalars t_1 and t_2 such that

$$t = t_1 + t_2\lambda \pmod{n} \text{ with } \max\{|t_1|, |t_2|\} > \sqrt{n},$$

where t_1 and t_2 are computed as given in Equation (3.3).

Now, a random selection of six vectors has been done as before.

to form the 3- ISD generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$. The scalars t_1 and t_2 will be sub-decomposed again into new sub-scalars t_{11}, t_{12} and t_{21}, t_{22} respectively. In the other words, the scalars t_2 and t_2 are written by

$$t_1 \equiv t_{11} + t_{12}\lambda_1 (\mathrm{mod}\, n) \text{ and } t_2 \equiv t_{21} + t_{22}\lambda_1 \pmod{n},$$

Where t_{11}, t_{12} and t_{21}, t_{22} respectively are computed as shown in Equations (3.4) and (3.5),

with $\max\{|t_{11}|, |t_{12}|\} \leq \sqrt{n}$ and $\max\{|t_{21}|, |t_{22}|\} \leq \sqrt{n}$.

So, the scalar *t* can be written by

$$t \equiv t_{11} + t_{12}\lambda_1 + t_{21} + t_{22}\lambda_2 (\mathrm{mod}\, n).$$

The scalar multiplication *tP* using the 3-ISD method is computed by

$$tP \equiv t_{11}P + t_{12}\psi_1(P) + t_{21}P + t_{22}\psi_2,$$

Where $\psi_1(P) = \lambda_1 P$, $\psi_2(P) = \lambda_2 P$ are two efficiently computable endomorphisms of Twisted Edwards curve $E_{a,d}$ defined over F_p.

The 3-ISD Edwards scalar multiplication *tP* based on randomized vectors that are used to generate the 3-ISD generators can be implemented using Algorithm (4.3.1).

Algorithm (4.3.1): The 3-ISD Twisted Edwards Scalar multiplication *tP* based on randomized Generators.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$ and $P \in E_{a,d}(p)$.

Output: 3-ISD Twisted Edwards scalar multiplication *tP*.

pre computation stage:

1. Computing the endomorphism $\psi_1(P) = \lambda_1 P$ and $\psi_2(P) = \lambda_2 P$.

computation stage:

2. Choose randomly the elements $a_1,b_1,c_1,a_2,b_2,c_2,a_3,b_3,c_3$ from the rang $[1,p-1]$ to generate the vectors $v_1=(a_1,b_1,c_1),v_2=(a_2,b_2,c_2)$ and $v_3=(a_3,b_3,c_3)$ that forms a first 3-ISD generator $\{v_1,v_2,v_3\}$.
3. Choose randomly a scalar $t\in[1,n-1]$.
4. Use the 3-ISD generator $\{v_1,v_2,v_3\}$ to decompose t into t_1 and t_2 such that $t_1=t+a_1b_1-a_2b_2-a_3b_3\,(\mathrm{mod}\,n)$ and $t_2=t_1+b_1c_1-b_2c_2-b_3c_3\,(\mathrm{mod}\,n)$ with $\max\{|t_1|,|t_2|\}>\sqrt{n}$.
5. Choose randomly $\lambda_1,\lambda_2\in[1,n-1]$.
6. Randomly Select some elements from the range $[1,p-1]$ to generator the vector $v_1'=(a_1',b_1',c_1'),v_2'=(a_2',b_2',c_2'),v_3'=(a_3',b_3',c_3'),v_1''=(a_1'',b_1'',c_1'')$, $v_2''=(a_2'',b_2'',c_2'')$ and $v_3''=(a_3'',b_3'',c_3'')$ to form the two 3-ISDgenerator $\{v_1',v_2',v_3'\}$ and $\{v_1'',v_2'',v_3''\}$.
7. Use 3-ISD randomized generator to sub-decompose t_1 and t_2 into t_{11},t_{12} and t_{21},t_{22} respectively such that $t_1=t_{11}+t_{12}\lambda_1(\mathrm{mod}\,n)$ and $t_2=t_{21}+t_{22}\lambda_1(\mathrm{mod}\,n)$, where $\max\{|t_{11}|,|t_{12}|\}\le\sqrt{n}$ and $\max\{|t_{21}|,|t_{22}|\}\le\sqrt{n}$.
8. Compute *tP* 3-ISD Twisted Edwards scalar multiplication *tP* by $tP\equiv t_{11}\,P+t_{12}\;\psi_1(P)+t_{21}\,P+t_{22}\;\psi_2(P)\;(\mathrm{mod}\;p)$
9. Return *tP*.

Example 4.3.1. (The 3- ISD Twisted Edwards Scalar Multiplication Method Based on the Randomized Generators)

Let $p=1171$ be a prime number. Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{16,2}:16x^2+y^2=1+2x^2y^2(\mathrm{mod}1171)$, with $d=2$ and $a=16$ over F_{1171}. Let $p=(1169,3)$ be a generator point lies on $E_{16,2}$ has prime order $n=149$.

Suppose $v_1 = (16,13,12), v_2 = (11,21,15)$ and $v_3 = (17,18,9)$ are three vectors are chosen randomly. The elements on each vector are relative prime to each other. So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$.

Suppose $t = 144 \in [1,148]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \,(\mathrm{mod}\, n) \equiv 113 (\mathrm{mod}\, 149)$$

and

$$t_2 \equiv t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \,(\mathrm{mod}\, n) \equiv 31 (\mathrm{mod} 149),$$

where $\max\{113,31\} > \sqrt{n} = \sqrt{149} = 12.21.$

Now, others six vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$, where

$$v_1' = (15,19,10), v_2' = (14,37,19), v_3' = (17,10,9)$$

and

$$v_1'' = (6,19,23), v_2'' = (11,37,29), v_3'' = (18,10,11).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 (\mathrm{mod}\, n) \equiv 8 + 1(105) (\mathrm{mod} 149)$$

and $$t_2 \equiv t_{21} + t_{22}\lambda_2 \,(\mathrm{mod}\, n) \equiv 5 + 4(81) (\mathrm{mod} 149).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$tP = (343,382) + (793,1053) + (1110,983) + (685,44)$$
$$= (391,399) + (299,919)$$
$$= (948,539)$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 8(1169,3) = (343,382), t_{12}\psi_1(P) = 1(793,1053) = (793,1053),$$

$$t_{12}P = 5(1169,3) = (1110,983) \text{ and } t_{22}\psi_2(P) = 4(217,97) = (685,44).$$

with $\psi_1(P) = \lambda_1 P = 105(1169,3) = (793,1053)$

and $\psi_2(P) = \lambda_2 P = 81(1169,3) = (217,97).$

are two efficiently computable endomorphisms that are pre-computed

Example 4.3.2. (The 3- ISD Twisted Edwards Scalar Multiplication Method Based on the Randomized Generators)

Let $p = 2011$ be a prime number. Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{64,2}: 64x^2 + y^2 = 1 + 2x^2y^2 (\text{mod}\, 2011)$, with $d = 2$ and $a = 64$ over F_{2011}. Let $P = (9,1318)$ be a generator point lies on $E_{64,2}$ has prime order $n = 163$.

Suppose $v_1 = (14,13,12), v_2 = (11,21,15)$ and $v_3 = (17,18,11)$ are three vectors are chosen randomly. The elements on each vector are relative prime to each other. So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$.

Suppose $t = 158 \in [1,162]$. A scalar $t = 158$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 (\text{mod}\, n) \equiv 129 (\text{mod}\, 163)$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 (\text{mod}\, n) \equiv 29 (\text{mod} 163),$$

where $\max\{129,29\} > \sqrt{n} = \sqrt{163} = 12.77.$

Now, others six vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1', v_2', v_3'\}$ where

$$v_1' = (21,19,11),\ v_2' = (14,37,19),\ v_3' = (17,10,32)$$

and

$$v_1'' = (18,19,11),\ v_2'' = (14,37,19),\ v_3'' = (17,10,32).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 (\bmod n) \equiv 3 + 4(113) (\bmod 163)$$

and $$t_2 \equiv t_{21} + t_{22}\lambda_2 \ (\bmod\ n) \equiv 9 + 10(2) (\bmod 163).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (744,1901) + (827,1120) + (1508,1036) + (114,630) \\ &= (1335,748) + (1873,211) \\ &= (76,580) \end{aligned}$$

where $t_{11}P, t_{12}\psi_1(P), t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 3(9,1318) = (744,1901),\ t_{12}\psi_1(P) = 4(1366,1256) = (827,1120),$$

$$t_{12}P = 9(9,1318) = (1508,1036) \text{ and } t_{22}\psi_2(P) = 2(1311,1750) = (114,630).$$

with $$\psi_1(P) = \lambda_1 P = 113(9,1318) = (1366,1256)$$

and $$\psi_2(P) = \lambda_2 P = 2(9,1318) = (1311,1750).$$

are two efficiently computable endomorphisms that are pre-computed.

Several experimental results of the 3-ISD Twisted Edwards scalar multiplication are in implemented Chapter (5), Table (5.6).

4.4 Another Type of 3-ISD Method Based the Randomized Generators

Another type of 3-ISD method is discussed first to compute a scalar multiplication tP, when P is a point lies on Edwards curve E_d defined over prime field F_p. And later, this type also will be explained on lies on Twisted Edwards curve $E_{a,d}$ defined over prime field F_p.

4.4.1 Edwards Scalar Multiplication Based the randomized 3-ISD Generators.

Suppose v_1, v_2 and v_3 are vectors that have three dimensions that are chosen randomly from the range $[1, p-1]$. Suppose E_d is an Edwards curve defined over F_p. Let P be a point lies on E_d defined over F_p. A scalar $t \in [1, n-1]$ in tP can be decomposed with another type of the decomposition. A scalar t is decomposed into new scalars t_1, t_2 and t_3, as given in Equation (3.10) and (3.11) that explained Section (3.5.1).

where $\lambda_1, \lambda_2 \in [1, n-1]$.

The scalar t_1, t_2 and t_3 are computed using the formulas that are given in Equation (3.12) and(3.13).

where

$$d_1 = \lfloor -b_3 t / n \rceil, \quad d_2 = \lfloor b_2 t / n \rceil \text{ and } d_3 = \lfloor b_1 t / n \rceil.$$

Now, a random selection of nine vectors $v'_1, v'_2, v'_3, v''_1, v''_2, v''_3, \hat{v}_1, \hat{v}_2, \hat{v}_3$ has been done.

These vectors form the ISD generators $\{v_1',v_2',v_3'\}$, $\{v_1'',v_2'',v_3''\}$ and $\{\hat{v}_1,\hat{v}_2,\hat{v}_3\}$. Using these generators, the scalars t_1,t_2 and t_3 are sub-decomposed again into new sub-scalars $t_{11},t_{12},t_{13},t_{21},t_{22},t_{23}$, and t_{31},t_{32},t_{33} respectively. In the other words, the scalars t_1,t_2 and t_3 are written as before by

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n),\ \ t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \text{ and}$$

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\text{mod}).$$

where

$$t_{11} \equiv t_1 - d_1'a_1' - d_2'a_2' - d_3'a_3' (\text{mod } n),\ \ t_{12} \equiv t_{11} - d_1'b_1' - d_2'b_2' - d_3'b_3' \ (\text{mod } n),$$
$$t_{13} \equiv d_1'c_1' + d_2'c_2' + d_3'c_3' \ (\text{mod } n)$$
$$t_{21} \equiv t_2 - d_1''a_1'' - d_2''a_2'' - d_3''a_3'' (\text{mod } n),\ \ t_{22} \equiv t_{21} - d_1''b_1'' - d_2''b_2'' - d_3''b_3'' \ (\text{mod } n),$$
$$t_{23} \equiv d_1''c_1'' + d_2''c_2'' + d_3''c_3'' \ (\text{mod } n)$$

and

$$t_{31} \equiv t_3 - \hat{d}_1\hat{a}_1 - \hat{d}_2\hat{a}_2 - \hat{d}_3\hat{a}_3 (\text{mod } n),\ \ t_{32} \equiv t_{31} - \hat{d}_1\hat{b}_1 - \hat{d}_2\hat{b}_2 - \hat{d}_3\hat{b}_3 \ (\text{mod } n),$$
$$t_{33} \equiv \hat{d}_1\hat{c}_1 + \hat{d}_2\hat{c}_2 + \hat{d}_3\hat{c}_3 \ (\text{mod } n)$$

with $\max\{|t_{11}|,|t_{12}|,|t_{13}|\} \le \sqrt{n}$, $\max\{|t_{21}|,|t_{22}|,|t_{23}|\} \le \sqrt{n}$ and $\max\{|t_{31}|,|t_{32}|,|t_{33}|\} \le \sqrt{n}$.

The parameters d_i',d_i'' and $\hat{d}_i$ for $i = 1,2,3$ are computed by

$$d_1' = \lfloor -b_3't / n \rceil,\ d_2' = \lfloor b_2't / n \rceil,\ d_3' = \lfloor b_1't / n \rceil,$$

$$d_1'' = \lfloor -b_3''t / n \rceil,\ d_2'' = \lfloor b_2''t / n \rceil,\ d_3'' = \lfloor b_1''t / n \rceil,$$

and

$$\hat{d}_1 = \lfloor -\hat{b}_3t / n \rceil,\ \hat{d}_2 = \lfloor \hat{b}_2t / n \rceil,\ \hat{d}_3 = \lfloor \hat{b}_1t / n \rceil.$$

The scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' + t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' + t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\mathrm{mod}\, n).$$

The Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP \equiv & t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ & t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\ \equiv & (t_{11} + t_{21} + t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ & t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P), \end{aligned}$$

where $\psi_1'(P) = \lambda_1' P$, $\psi_2'(P) = \lambda_2' P$, $\psi_1''(P) = \lambda_1'' P$, $\psi_2''(P) = \lambda_2'' P$, $\hat{\psi}_1(P) = \hat{\lambda}_1 P$ and $\hat{\psi}_2(P) = \hat{\lambda}_2 P$ are efficiently computable endomorphisms of Edwards curve E_d defined over F_p.

Edwards Scalar Multiplication tP Based the randomized 3-ISD Generators can be implemented using Algorithm (4.4.1.1).

Algorithm (4.4.1.1): The 3-ISD Edwards Scalar Multiplication tP Based on Randomized Generators.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$ and $P \in E_d(p)$.

Output: 3-ISD Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism $\psi_1'(P) = \lambda_1' P, \psi_2'(P) = \lambda_2' P, \psi_1''(P) = \lambda_1'' P, \psi_2''(P) = \lambda_2'' P, \hat{\psi}_1(P) = \hat{\lambda}_1 P$ and $\hat{\psi}_2(P) = \hat{\lambda}_2 P$.

   computation stage:

2. Choose randomly the elements $a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3, c_3$ from the rang $[1, p-1]$ to generate the vectors $v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$ that forms a first 3-ISD generator $\{v_1, v_2, v_3\}$.
3. Choose randomly a scalar $t \in [1, n-1]$.

4. Use the 3-ISD generator $\{v_1, v_2, v_3\}$ to decompose t into t_1, t_2 and t_3 such that $t_1 = t - d_1a_1 - d_2a_2 - d_3a_3 \pmod{n}, t_2 = t - d_1b_1 - d_2b_2 - d_3b_3 \pmod{n}$ and $t_3 = d_1c_1 + d_2c_2 + d_3c_3 \pmod{n}$ with $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1', \lambda_2', \lambda_1'', \lambda_2'', \hat{\lambda}_1, \hat{\lambda}_2 \in [1, n-1]$.
6. Randomly Select some elements from the range $[1, p-1]$ to generator the vector $v_1' = (a_1', b_1', c_1'), v_2' = (a_2', b_2', c_2'), v_3' = (a_3', b_3', c_3'), v_1'' = (a_1'', b_1'', c_1''),$ $v_2'' = (a_2'', b_2'', c_2'')$ and $v_3'' = (a_3'', b_3'', c_3'')$ to form the two 3-ISDgenerator $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$.
7. Use 3-ISD randomized generator to sub-decompose t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that $t_1 = t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' \pmod{n}, t_2 = t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' \pmod{n}$ and $t_3 = t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \pmod{n}$ where $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \le \sqrt{n}, \max\{|t_{21}|, |t_{22}|, |t_{23}|\} \le \sqrt{n}$ and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \le \sqrt{n}$.
8. Compute tP 3-ISD Edwards scalar multiplication tP by
$$\begin{aligned} tP &\equiv t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\ &\equiv (t_{11} + t_{21} + t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P), \end{aligned}$$
9. Return tP.

Example 4.4.1.1. (Edwards Scalar Multiplication Based Another Type of the randomized 3-ISD Generators).

With a prime number $p = 1171$, suppose $v_1 = (17, 12, 23), v_2 = (34, 51, 68)$ and $v_3 = (85, 68, 17)$ are three vectors are chosen randomly. So, the first

generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 250 \in [1, 292]$. The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 \pmod{n} \equiv 62 \pmod{293},$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 \pmod{n} \equiv 178 \pmod{293},$$

and $$t_3 \equiv d_1 c_1 + d_2 c_2 + d_3 c_3 \pmod{n} \equiv 70 \pmod{293},$$

Where $\max\{62, 178, 70\} > \sqrt{n} = \sqrt{293} = 17.11$ and

$$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(68)250 / 293 \rceil = -58, \; d_2 = \lfloor b_2 t / n \rceil = \lfloor (51)250 / 293 \rceil = 44$$
$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (12)250 / 293 \rceil = 10.$$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}, \{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (14, 8, 13), v_2' = (34, 51, 68), v_3' = (85, 68, 17),$$

$$v_1'' = (8, 29, 12), v_2'' = (19, 12, 18), \; v_3'' = (55, 21, 3)$$

and

$$\hat{v_1} = (9, 12, 17), \hat{v_2} = (19, 25, 18), \hat{v_3} = (17, 43, 23)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 7 + 8(265) + (14)(292) (\text{mod } 293),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv 9 + (-11)(287) + 12(292) (\text{mod } 293).$$

and $$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \; (\text{mod } n) \equiv (-7) + 12(36) + 7(292) (\text{mod } 293).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$tP = (443,\ 548) + (1065,\ 148) + (12,\ 186) + (391,\ 944) + (188,\ 384) + (573,\ 576) + (728,\ 548) + (234,\ 248) + (728,\ 548) = (373,\ 825)$$

where

$$\psi_1'(P) = \lambda_1' P = 3(7,766) = (230,136),\ \psi_2'(P) = \lambda_2' P = 65(7,766) = (51,1125),$$
$$\psi_1''(P) = \lambda_1'' P = 9(7,766) = (391,944),\ \psi_2''(P) = \lambda_2'' P = 65(7,766) = (127,296)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 36(7,766) = (912,581),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 292(7,766) = (1164,766).$$

$$t_{11}p = 7(7,766) = (443,548),\ t_{12}\psi_1'(p) = 8(230,136) = (1065,148),$$
$$t_{13}\psi_2'(p) = 14(51,1125) = (12,186)$$

$$t_{21}p = 9(7,766) = (391,944),\ t_{22}\psi_1''(p) = -8(51,1125) = (68,238),$$
$$t_{23}\psi_2''(p) = 12(1164,766) = (724,1027)$$

$$t_{31}p = -7(7,766) = (443,548) = (728,548),\ t_{32}\hat{\psi}_1(p) = 12(912,581) = (234,248),$$
$$t_{33}\hat{\psi}_2(p) = 7(1164,766) = (728,548)$$

are six efficiently computable endomorphisms that are pre-computed.

Example 4.4.1.2. (Edwards Scalar Multiplication Based Another Type randomized 3-ISD Generators).

With a prime number $p = 1867$, **s**uppose $v_1 = (44,12,23), v_2 = (27,51,39)$ and $v_3 = (37,68,17)$ are three vectors are chosen randomly. The elements on each vector are relative prime to each other.

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 458 \in [1,466]$.

The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 \pmod{n} \equiv 211 \pmod{467},$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 \pmod{n} \equiv 276 \pmod{467},$$

and $$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \,(\mathrm{mod}\, n) \equiv 438 \,(\mathrm{mod}\, 467),$$

where $\max\{211, 276, 438\} > \sqrt{n} = \sqrt{467} = 21.61.$ and

$$d_1 = \lfloor -b_3 t \,/\, n \rceil = \lfloor -(68)458 / 467 \rceil = -67,\ d_2 = \lfloor b_2 t \,/\, n \rceil = \lfloor (51)458 / 467 \rceil = 50$$
$$d_3 = \lfloor b_1 t \,/\, n \rceil = \lfloor (12)458 / 467 \rceil = 12.$$

Now, others nine vectors are chosen randomly to general the ISD generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (43, 57, 72),\ v_2' = (27, 65, 39),\ v_3' = (37, 55, 44),$$
$$v_1'' = (16, 18, 17),\ v_2'' = (13, 27, 38),\ v_3'' = (22, 17, 3).$$

and $$\hat{v_1} = (22, 18, 17),\ \hat{v_2} = (13, 31, 38),\ \hat{v_3} = (24, 16, 5)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\mathrm{mod}\ n) \equiv 8 + (-14)(20) + (8)(2) (\mathrm{mod}\, 467),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\mathrm{mod}\ n) \equiv (-14) + (14)(9) + 4(41) (\mathrm{mod}\, 467).$$

and $t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\mathrm{mod}\ n) \equiv (-17) + 16(8) + (-2)(70) (\mathrm{mod}\, 467).$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (569, 1494) + (1272, 679) + (109, 1008) + (1509, 199) + (364, 455) \\ &\quad (1050, 1217) + (1527, 1375) + (1075, 991) + (773, 1086) \\ &= (969, 1049) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 20(3, 317) = (1348, 1615),\ \ \psi_2'(P) = \lambda_2' P = 2(3, 317) = (154, 1089),$$
$$\psi_1''(P) = \lambda_1'' P = 9(3, 317) = (898, 1049),\ \ \psi_2''(P) = \lambda_2'' P = 41(3, 317) = (1463, 1830),$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 8(3, 317) = (569, 1494),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 90(3, 317) = (1566, 899).$$

$$t_{11}p = 8(3,317) = (569,1494),\ t_{12}\psi_1'(p) = (-14)(1348,1615) = (1272,679),$$
$$t_{13}\psi_2'(p) = 8(1546,1089) = (109,1008)$$

$$t_{21}p = (-14)(3,317) = (1509,199),\ t_{22}\psi_1''(p) = 14(898,1049) = (364,455),$$
$$t_{23}\psi_2''(p) = 4(1463,1830) = (1050,1217)$$

$$t_{31}p = 16(569,1494) = (1075,991),\ t_{32}\hat{\psi}_1(p) = 16(569,1494) = (1075,991),$$
$$t_{33}\hat{\psi}_2(p) = (-2)(1566,899) = (773,1086)$$

are six efficiently computable endomorphisms that are pre-computed.

Some implemented results of Edward scalar multiplication with another type of decomposition are implanted in Chapter (5) ,Table (5.7).

4.4.2 Twisted Edwards Scalar Multiplication Based the Randomized 3-ISD Generators.

Suppose v_1, v_2 and v_3 are vectors that have three dimensions that are chosen randomly from the range $[1, p-1]$. Suppose $E_{a,d}$ is Twisted Edwards curve defined over F_p. Let P be a point lies on E_d defined over F_p. A scalar $t \in [1, n-1]$ in tP can be decomposed with another type of the decomposition. A scalar t is decomposed into new scalars t_1, t_2 and t_3, as given in Equation (3.10) and (3.11) that explained Section (3.5.1).

where $\lambda_1, \lambda_2 \in [1, n-1]$.

The scalar t_1, t_2 and t_3 are computed using the formulas that are given in Equation (3.12) and (3.13)

So, the parameters $d_1 = \lfloor -b_3 t / n \rceil, d_2 = \lfloor b_2 t / n \rceil$ and $d_3 = \lfloor b_1 t / n \rceil$.

Now, a random selection of nine vectors $v_1', v_2', v_3', v_1'', v_2'', v_3'', \hat{v}_1, \hat{v}_2, \hat{v}_3$. has been done.

That form the 3-ISD generators $\{v'_1, v'_2, v'_3\}, \{v''_1, v''_2, v''_3\}$ and $\{\hat{v}_1, \hat{v}_2, \hat{v}_3\}$. The scalars t_1, t_2 and t_3 will be sub-decomposed again into new sub-scalars $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$, and t_{31}, t_{32}, t_{33} respectively. In the other words, the scalars , t_1, t_2 and t_3 are written as before by

$$t_1 \equiv t_{11} + t_{12}\lambda'_1 + t_{13}\lambda'_2 (\text{mod } n),\ t_2 \equiv t_{21} + t_{22}\lambda''_1 + t_{23}\lambda''_2 (\text{mod } n) \text{ and}$$

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\text{mod}). \text{ where}$$

$$t_{11} \equiv t_1 - d'_1 a'_1 - d'_2 a'_2 - d'_3 a'_3 (\text{mod } n),\ t_{12} \equiv t_{11} - d'_1 b'_1 - d'_2 b'_2 - d'_3 b'_3 \ (\text{mod } n),$$
$$t_{13} \equiv d'_1 c'_1 + d'_2 c'_2 + d'_3 c'_3 \ (\text{mod } n)$$

$$t_{21} \equiv t_2 - d''_1 a''_1 - d''_2 a''_2 - d''_3 a''_3 (\text{mod } n),\ t_{22} \equiv t_{21} - d''_1 b''_1 - d''_2 b''_2 - d''_3 b''_3 \ (\text{mod } n),$$
$$t_{23} \equiv d''_1 c''_1 + d''_2 c''_2 + d''_3 c''_3 \ (\text{mod } n)$$

and

$$t_{31} \equiv t_3 - \hat{d}_1 \hat{a}_1 - \hat{d}_2 \hat{a}_2 - \hat{d}_3 \hat{a}_3 (\text{mod } n), t_{32} \equiv t_{31} - \hat{d}_1 \hat{b}_1 - \hat{d}_2 \hat{b}_2 - \hat{d}_3 \hat{b}_3 \ (\text{mod } n),$$
$$t_{33} \equiv \hat{d}_1 \hat{c}_1 + \hat{d}_2 \hat{c}_2 + \hat{d}_3 \hat{c}_3 \ (\text{mod } n)$$

with $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \leq \sqrt{n}, \{|t_{21}|, |t_{22}|, |t_{23}|\} \leq \sqrt{n}$ and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \leq \sqrt{n}$.

So, the scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda'_1 + t_{13}\lambda'_2 + t_{21} + t_{22}\lambda''_1 + t_{23}\lambda''_2 + t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\text{mod } n).$$

The scalar multiplication tP using the 3-ISD method is computed is given in Equation (3.19),

where $\psi'_1(P) = \lambda'_1 P, \psi'_2(P) = \lambda'_2 P, \psi''_1(P) = \lambda''_1 P, \psi''_2(P) = \lambda''_2 P$ and

$\hat{\psi}_1(P) = \hat{\lambda}_1 P, \hat{\psi}_2(P) = \hat{\lambda}_2 P$ are six efficiently computable endomorphisms of Edwards curve E_d defined over F_p.

Twisted Edwards Scalar Multiplication tP Based the randomized 3-ISD Generators can be implemented using Algorithm (4.2.1).

Algorithm (4.4.2.1): The 3-ISD Twisted Edwards Scalar Multiplication tP Based on Randomized Generators.

Input: The primes p and n, $\lambda \in [1, n-1]$, $d \neq 0,1$ and $P \in E_{a,d}(p)$.

Output: 3-ISD Edwards scalar multiplication tP.

pre computation stage:

1. Computing the endomorphism $\psi_1'(P) = \lambda_1' P, \psi_2'(P) = \lambda_2' P, \psi_1''(P) = \lambda_1'' P, \psi_2''(P) = \lambda_2'' P, \hat{\psi}_1(P) = \hat{\lambda}_1 P$ and $\hat{\psi}_2(P) = \hat{\lambda}_2 P$.

   computation stage:

2. Choose randomly the elements $a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3, c_3$ from the rang $[1, p-1]$ to generate the vectors $v_1 = (a_1, b_1, c_1), v_2 = (a_2, b_2, c_2)$ and $v_3 = (a_3, b_3, c_3)$ that forms a first 3-ISD generator $\{v_1, v_2, v_3\}$.
3. Choose randomly a scalar $t \in [1, n-1]$.
4. Use the 3-ISD generator $\{v_1, v_2, v_3\}$ to decompose t into t_1, t_2 and t_3 such that $t_1 = t - d_1 a_1 - d_2 a_2 - d_3 a_3 \pmod{n}, t_2 = t - d_1 b_1 - d_2 b_2 - d_3 b_3 \pmod{n}$ and $t_3 = d_1 c_1 + d_2 c_2 + d_3 c_3 \pmod{n}$ with $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$.
5. Choose randomly $\lambda_1', \lambda_2', \lambda_1'', \lambda_2'', \hat{\lambda}_1, \hat{\lambda}_2 \in [1, n-1]$.
6. Randomly Select some elements from the range $[1, p-1]$ to generator the vector $v_1' = (a_1', b_1', c_1'), v_2' = (a_2', b_2', c_2'), v_3' = (a_3', b_3', c_3'), v_1'' = (a_1'', b_1'', c_1''),$ $v_2'' = (a_2'', b_2'', c_2'')$ and $v_3'' = (a_3'', b_3'', c_3'')$ to form the two 3-ISDgenerator $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$.
7. Use 3-ISD randomized generator to sub-decompose t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that $t_1 = t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' \pmod{n}, t_2 = t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' \pmod{n}$ and $t_3 = t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \pmod{n}$ where $\max\{|t_{11}|, |t_{12}|, |t_{13}|\} \leq \sqrt{n}, \max\{|t_{21}|, |t_{22}|, |t_{23}|\} \leq \sqrt{n}$ and $\max\{|t_{31}|, |t_{32}|, |t_{33}|\} \leq \sqrt{n}$.

8. Compute *tP* 3-ISD Twisted Edwards scalar multiplication *tP* by

$$\begin{aligned} tP &\equiv t_{11}P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{21}P + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{31}P + t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P) \\ &\equiv (t_{11} + t_{21} + t_{31})P + t_{12}\psi_1'(P) + t_{13}\psi_2'(P) + t_{22}\psi_1''(P) + t_{23}\psi_2''(P) + \\ &\quad t_{32}\hat{\psi}_1(P) + t_{33}\hat{\psi}_2(P), \end{aligned}$$

9. Return *tP*.

Example 4.4.2.1. (Twisted Edwards Scalar Multiplication Based Another Type of the randomized 3-ISD Generators).

With a prime number $p = 1171$, **s**uppose $v_1 = (71,97,31), v_2 = (79,28,91)$ and $v_3 = (91,71,55)$ are three vectors are chosen randomly.

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$using to decompose a scalar $t = 142 \in [1,148]$.

The scalars t_1, t_2 and t_3 are computed by

$$\begin{aligned} t_1 &\equiv t - a_1d_1 - a_2d_2 - a_3d_3 \,(\mathrm{mod}\, n) \equiv 127 \,(\mathrm{mod}\, 149), \\ t_2 &\equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \,(\mathrm{mod}\, n) \equiv 62 \,(\mathrm{mod}\, 149), \end{aligned}$$

and

$$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \,(\mathrm{mod}\, n) \equiv 102 \,(\mathrm{mod}\, 149),$$

where $\max\{127,62,102\} > \sqrt{n} = \sqrt{149} = 12.20.$ and

$$d_1 = \lfloor -b_3t / n \rceil = \lfloor -(71)142 / 149 \rceil = -68,\ d_2 = \lfloor b_2t / n \rceil = \lfloor (28)142 / 149 \rceil = 27,$$
$$d_3 = \lfloor b_1t / n \rceil = \lfloor (97)142 / 149 \rceil = 92.$$

$\max\{127,62,102\} > \sqrt{n} = \sqrt{149} = 12.20.$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}, \{v_1'', v_2'', v_3''\}$, and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$, These vectors are

$$v_1' = (35,18,23),\ v_2' = (30,44,39),\ v_3' = (21,64,16),$$
$$v_1'' = (35,18,19),\ v_2'' = (31,44,41), v_3'' = (21,64,11),$$

and

$$\hat{v_1} = (59,10,23),\ \hat{v_2} = (21,44,51),\ \hat{v_3} = (41,64,12)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11},t_{12},t_{13},t_{21},t_{22},t_{23}$ and t_{31},t_{32},t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 1 + (-2)(2) + (10)(13) (\text{mod} 149),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv 4 + (-5)(2) + 4(17) (\text{mod} 149).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv (-7) + 6(4) + 6(39) (\text{mod} 149).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (1169,\ 3) + (214,745) + (596,282) + (957,745) + (582,896) + (231,84) \\ &\quad + (546,163) + (386,71) + (119,1051) \\ &= (546,\ 163) \end{aligned}$$

where

$$\psi_1'(P) = \lambda_1' P = 2(1169,3) = (64,644),\ \ \psi_2'(P) = \lambda_2' P = 13(1169,3) = (907,469),$$
$$\psi_1''(P) = \lambda_1'' P = 2(1169,3) = (64,644),\ \ \psi_2''(P) = \lambda_2'' P = 17(1169,3) = (231,84)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 4(1169,3) = (957,745),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 39(1169,3) = (1103,423).$$

$$t_{11}p = 1(1169,3) = (1169,3),\ t_{12}\psi_1'(p) = (-2)(64,644) = (214,745),$$
$$t_{13}\psi_2'(p) = 10(907,469) = (596,282)$$

$$t_{21}p = 4(1169,3) = (957,745),\ t_{22}\psi_1''(p) = -5(589,896) = (582,896),$$
$$t_{23}\psi_2''(p) = 4(316,255) = (231,84)$$

$$t_{31}p = -7(1169,3) = (546,163),\ t_{32}\hat{\psi}_1(p) = 6(957,745) = (386,71),$$
$$t_{33}\hat{\psi}_2(p) = 6(1103,423) = (119,1051)$$

are six efficiently computable endomorphisms that are pre-computed.

Example 4.4.2.2. (Twisted Edwards Scalar Multiplication Based Another Type of the randomized 3-ISD Generators).

With a prime number $p = 1867$, suppose $v_1 = (77,23,32), v_2 = (37,65,49)$ and $v_3 = (49,18,21)$ are three vectors are chosen randomly.

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 138 \in [1,150]$.

The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1d_1 - a_2d_2 - a_3d_3 \pmod{n} \equiv 121 \pmod{151},$$
$$t_2 \equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \pmod{n} \equiv 57 \pmod{151},$$

and

$$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \pmod{n} \equiv 111 \pmod{151},$$

where $\max\{121,57,111\} > \sqrt{n} = \sqrt{151} = 12.29.$ and

$$d_1 = \lfloor -b_3t / n \rceil = \lfloor -(18)138/151 \rceil = -7,\ d_2 = \lfloor b_2t / n \rceil = \lfloor (65)138/151 \rceil = 59,$$
$$d_3 = \lfloor b_1t / n \rceil = \lfloor (23)138/151 \rceil = 21.$$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}, \{v_1'', v_2'', v_3''\}$, and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$, These vectors are

$$v_1' = (46,23,25),\ v_2' = (36,44,39), v_3' = (56,62,19),$$
$$v_1'' = (11,17,25),\ v_2'' = (26,11,39),\ v_3'' = (59,60,19),$$

and $\hat{v_1} = (13,10,25),\ \hat{v_2} = (11,15,35), \hat{v_3} = (58,60,17)$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 2 + (6)(8) + (4)(131) (\text{mod} 151),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv (3) + (-10)(5) + (-3)(66) (\text{mod} 151).$$

and $t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv (-9) + (-3)(6) + 8(5) (\text{mod} 151).$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (797,1212) + (1770,1767) + (1379,1607) + (1582,1679) + (637,471) + \\ &\quad (1590,862) + (1207,400) + (1163,317) + (1180,1199) \\ &= (1180,1199). \end{aligned}$$

where

$$\psi_1'(P) = \lambda_1' P = 8(1864,1140) = (1026,509), \ \psi_2'(P) = \lambda_2' P = 131(1864,1140) = (430,32),$$

$$\psi_1''(P) = \lambda_1'' P = 5(1864,1140) = (585,1119),$$
$$\psi_2''(P) = \lambda_2'' P = 66(1864,1140) = (1545,1033)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 6(1864,1140) = (1207,400), \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 5(1864,1140) = (585,119).$$

$$t_{11}p = 2(1864,1140) = (797,1212), \ t_{12}\psi_1'(p) = (6)(1026,509) = (1770,1767),$$
$$t_{13}\psi_2'(p) = 4(430,32) = (1379,1607)$$

$$t_{21}p = 3(1864,1140) = (1582,1679), \ t_{22}\psi_1''(p) = (-10)(585,1119) = (637,471),$$
$$t_{23}\psi_2''(p) = (-3)(1545,1033) = (1590,862)$$

$$t_{31}p = -9(1864,1140) = (1207,400), \ t_{32}\hat{\psi}_1(p) = -3(1764,1613) = (1163,317),$$
$$t_{33}\hat{\psi}_2(p) = 8(585,1119) = (1180,1199)$$

are six efficiently computable endomorphisms that are pre-computed.

More implemented results of twisted Edward curve with another type of 3-ISD Method can be seen in Chapter (5) in Table (5.8).

4.5 The Distribution of a Scalar t Based on Randomized Vectors in the Interval [1, n-1]

Two cases of the distribution of scalar t in the scalar multiplication tP that is computed using the 3-ISD method based on the randomized choices of the vectors are discussed in this Section. The computations are done on Edwards curve and twisted Edwards curve defined over the prime fields. The decomposition of a scalar t on these cases depended on using three vectors are chosen randomly. The cases are discussed as follows.

4.5.1 Enumerating the Scalars Using 3-ISD Edwards or Twisted Edwards Method Based the Randomized Vectors in Interval [1, n-1].

Suppose E_d is an Edwards curve and $E_{a,d}$ twisted Edwards curve defined F_p which is respectively given by

$$E_d : x^2 + y^2 = 1 + d\,x^2 y^2 (\mathrm{mod}\, p),\quad E_{a,d} : ax^2 + y^2 = 1 + d\,x^2 y^2 (\mathrm{mod}\ p)$$

and $P = (x, y)$ is a point lies on E_d or $E_{a,d}$ The order of P is a prime number n and let t is scalar of an Edward or twisted Edwards curve scalar multiplication tP. This section discusses the procedure of sieving scalar t in $[1, n-1]$, which satisfy the 3-ISD method that explained in section (4.3) and section (4.4). The sieving process for computing the scalar multiplication tP on Edward curve twisted Edwards curve over F_p. The decomposed scalars t_1 and t_2 of 3-ISD scalar t satisfy the condition $\max\{|t_1|, |t_2|\} > \sqrt{n}$. The sieving process begins by writing down all the scalars t starting from 1 into $n-1$ which enumerates all the 3-ISD scalars t in interval $[1, n-1]$. The next step is to check all scalars t_1 and t_2 such that $t_1, t_2 < t$ with $t_1, t_2 \neq 0$ and $\max\{|t_1|, |t_2|\} > \sqrt{n}$. All scalars t with decompositions that do not satisfy the conditions are crossed off. The results of sieving process of scalars t that lie in the $[1, n-1]$ interval are

determined based on the following cases of new scalars t_1 and t_2 values from t decomposition. These cases are as follows.

i. The decomposition of t into t_1 and t_2 resulted in $\min\{|t_1|,|t_2|\}=0.$ or $\max\{|t_1|,|t_2|\}=t.$

ii. The decomposition of t into t_1 and t_2 leads to $\max\{|t_1|,|t_2|\}>t.$

iii. The decomposition of t into t_1 and t_2 yields $\max\{|t_1|,|t_2|\}\leq\sqrt{n}.$

iv. The decomposition of t into t_1 and t_2 produces $\max\{|t_1|,|t_2|\}>\sqrt{n}.$

Repeating this process with cross off all cases i, ii and iii gives a list of the scalars up to *n*-1. These scalars lie outside the range $\sqrt{n}$ on the interval $[1,n-1]$. Scalars t with such a property represent 3-ISD used for the successful computation of the 3-ISD Edwards scalar multiplication tP. Using Algorithm (3.6.1.1), all the scalars satisfying the 3-ISD decomposition in the $[1,n-1]$ are determined. This algorithm is performed with input (n,v_1,v_2,v_3). to output the 3-ISD correct values of multipliers t.

Example 4.5.1.1. (Distributing the 3-ISD scalars on Edwards curve Based on Randomized vectors)

Let $p=1171$ be a prime number. **S**uppose $E_2: x^2+y^2\equiv 1+2x^2y^2 \pmod{1171}$, with $d=2$ is Edwards curve defined over F_{1171}. Let $P=(7,766)$ be a point on E_2 has prime order $n=293$ So, the first 3-ISD generator $\{v_1,v_2,v_3\}$ is computed, when $v_1=(28,12,23), v_2=(29,37,25)$ and $v_3=(33,14,17)$.

Suppose $t=195\in[1,292]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1\equiv t+a_1b_1-a_2b_2-a_3b_3 \pmod{n}\equiv 168 \pmod{293}$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 \,(\mathrm{mod}\, n) \equiv 27 \,(\mathrm{mod}\, 293),$$

where $\max\{168, 27\} > \sqrt{n} = \sqrt{293} = 17.11.$

Now, others six vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$. These vectors are

$$v_1' = (10,11,18), v_2' = (12,17,5), v_3' = (7,10,11)$$

and

$$v_1'' = (23,11,18), v_2'' = (12,17,5), v_3'' = (7,10,11).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \,(\mathrm{mod}\ n) \equiv (4) + 7(149) \,(\mathrm{mod}\, 293)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \,(\mathrm{mod}\ n) \equiv 6 + 9(100) \,(\mathrm{mod}\, 293).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (749,710) + (900,915) + (220,526) + (924,218) \\ &= (467,1053) + (318,545) \\ &= (152,817). \end{aligned}$$

where $t_{11}P$, $t_{12}\psi_1(P)$, $t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 4(7,766) = (749,710),\ t_{12}\psi_1(P) = 7(256,900) = (900,915),$$

$$t_{21}P = 6(7,766) = (220,526) \text{ and } t_{22}\psi_2(P) = 9(1049,580) = (924,218).$$

with $$\psi_1(P) = \lambda_1 P = 149(7,766) = (256,900)$$

and $$\psi_2(P) = \lambda_2 P = 100(7,766) = (1049,580).$$

are two efficiently computable endomorphisms that are pre-computed.

Suppose $t = 200 \in [1,292]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \pmod{n} \equiv 147 \pmod{293}$$

and

$$t_2 \equiv t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \pmod{n} \equiv 53 \pmod{293},$$

where $\max\{147,53\} > \sqrt{n} = \sqrt{293} = 17.11.$

Now, others six vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$ These vectors are

$$v_1' = (43,56,72), v_2' = (26,65,39), v_3' = (37,55,59)$$

and

$$v_1'' = (30,15,11), v_2'' = (16,17,4), v_3'' = (17,13,8).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \equiv 4 + 149(7) \pmod{293}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv 6 + 9(100) \pmod{293}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (884,532) + (1089,956) + (1107,1081) + (798,825) \\ &= (300,642) + (837,976) \\ &= (648,297). \end{aligned}$$

where $t_{11}P$, $t_{12}\psi_1(P)$, $t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 2(7,766) = (884,532),\ t_{12}\psi_1(P) = 12(1033,627) = (1089,956),$$

$$t_{21}P = 10(7,766) = (1107,1081) \text{ and } t_{22}\psi_2(P) = 3(459,69) = (798,825).$$

with $$\psi_1(P) = \lambda_1 P = 183(7,766) = (1033,627)$$

and $$\psi_2(P) = \lambda_2 P = 112(7,766) = (459,69).$$

are two efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [36,292]$ that have 3-ISD sub-scalars that are got based on the randomized choices of the vectors to generate the 3-ISD generators.

Example 4.5.1.2. (Distributing the 3-ISD scalars on Twisted Edwards curve Based on Randomized vectors)

Let $p = 1171$ be a prime number. Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{16,2}: 16x^2 + y^2 = 1 + 2x^2y^2 (\text{mod}1171)$, with $d = 2$ and $a = 16$ over F_{1171}. Let $P = (1169,3)$ be a generator point lies on $E_{16,2}$ has prime order $n = 149$.

suppose $v_1 = (16,33,14)$, $v_2 = (11,22,15)$ and $v_3 = (17,18,8)$ are three vectors are chosen randomly. The elements on each vector are relative prime to each other. So, the first generator of 3-ISD method Is $\{v_1, v_2, v_3\}$.

Suppose $t = 90 \in [1,148]$ can be decomposed into scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1b_1 - a_2b_2 - a_3b_3 (\text{mod}\, n) \equiv 70 (\text{mod}149)$$

and

$$t_2 \equiv t_1 + b_1c_1 - b_2c_2 - b_3c_3 (\text{mod}\, n) \equiv 20 (\text{mod}149),$$

Where $\max\{70,20\} > \sqrt{n} = \sqrt{149} = 12.21.$

Now, others six vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$ and $\{v_1'', v_2'', v_3''\}$. These vectors are

$$v_1' = (29,15,11),\ v_2' = (16,17,4),\ v_3' = (18,13,7)$$

and

$$v_1'' = (75,61,13),\ v_2'' = (15,37,30),\ v_3'' = (17,10,12).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \pmod{n} \equiv -1 + 5(44) \pmod{149}$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \pmod{n} \equiv (-4) + (6)(4) \pmod{149}.$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (2,3) + (299,919) + (214,745) + (386,71) \\ &= (443,711) + (369,1050) \\ &= (605,907). \end{aligned}$$

Where $t_{11}P, t_{12}\psi_1(P), t_{21}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = -1(1169,3) = (2,3),\ t_{12}\psi_1(P) = 5(378,1053) = (299,919),$$

$$t_{21}P = (-4)(1169,3) = (214,745) \text{ and } t_{22}\psi_2(P) = 6(957,745) = (386,71).$$

with $$\psi_1(P) = \lambda_1 P = 44(1169,3) = (378,1053)$$

and $$\psi_2(P) = \lambda_2 P = 4(1169,3) = (957,745).$$

are two efficiently computable endomorphisms that are pre-computed.

With another value $t = 103 \in [1,148]$ the decomposition into can be done scalars t_1 and t_2 such that

$$t_1 \equiv t + a_1 b_1 - a_2 b_2 - a_3 b_3 \,(\mathrm{mod}\, n) \equiv 68 \,(\mathrm{mod} 149)$$

and

$$t_2 \equiv t_1 + b_1 c_1 - b_2 c_2 - b_3 c_3 \,(\mathrm{mod}\, n) \equiv 35 \,(\mathrm{mod} 149),$$

Where $\max\{68,35\} > \sqrt{n} = \sqrt{149} = 12.21.$

Now, others six vectors are chosen randomly to general the 3-IDS generators $\{v'_1, v'_2, v'_3\}$ and $\{v''_1, v''_2, v''_3\}$. These vectors are

$$v'_1 = (27,17,11),\ v'_2 = (17,36,23),\ v'_3 = (19,11,9)$$

and

$$v''_1 = (11,17,24),\ v''_2 = (12,36,31),\ v''_3 = (19,12,16).$$

These generators, are used to sub-decompose the scalars t_1 and t_2 into t_{11}, t_{12} and t_{21}, t_{22} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1 \,(\mathrm{mod}\ n) \equiv 4 + 9(123) \,(\mathrm{mod} 149)$$

and

$$t_2 \equiv t_{21} + t_{22}\lambda_2 \ (\mathrm{mod}\ n) \equiv (9) + (3)(108) \,(\mathrm{mod} 149).$$

Now, the Edwards scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (957,745) + (291,1011) + (1004,109) + (265,978) \\ &= (955,364) + (948,539) \\ &= (119,1051). \end{aligned}$$

where $t_{11}P$, $t_{12}\psi_1(P)$, $t_{12}P$ and $t_{22}\psi_2(P)$ are computed by

$$t_{11}P = 4(1169,3) = (957,745),\ t_{12}\psi_1(P) = 9(893,572) = (291,1011),$$

$$t_{21}P = (9)(1169,3) = (1004,109) \text{ and } t_{22}\psi_2(P) = (3)(234,333) = (265,978).$$

with $$\psi_1(P) = \lambda_1 P = 123(1169,3) = (893,572)$$

and $$\psi_2(P) = \lambda_2 P = 108(1169,3) = (234,333).$$

are two efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [33,148]$ that have 3-ISD sub-scalars which are obtained based on the randomized choices of the vectors that generate the 3-ISD generators.

4.5.2 Enumerating the Scalars Using Another Type 3-ISD Edwards or Twisted Edwards Method Based the Randomized Vectors in Interval [1, *n*-1].

Suppose E_d is an Edwards curve and $E_{a,d}$ twisted Edwards curve defined F_p which is respectively given by

$$E_d : x^2 + y^2 = 1 + d\,x^2 y^2 (\text{mod}\, p),\ E_{a,d} : ax^2 + y^2 = 1 + d\,x^2 y^2 (\text{mod}\ p)$$

and $P = (x, y)$ is a point lies on E_d or $E_{a,d}$ The order of P is a prime number n and let t is scalar of an Edward or twisted Edwards curve scalar multiplication tP. This section discusses the procedure of sieving scalar t in $[1, n-1]$, which satisfy the 3-ISD method that explained in section(4.3)and section(4.4). The sieving process for computing the scalar multiplication tP on Edward curve twisted Edwards curve over F_p. The decomposed scalars t_1, t_2 and t_3 of 3-ISD scalar t satisfy the condition $\max\{|t_1|, |t_2|, |t_3|\} > \sqrt{n}$. The sieving process begins by writing down all the scalars t starting from 1 into $n-1$ which enumerates all the 3-ISD scalars t in interval $[1, n-1]$. The next step is to check all scalars t_1 and t_2

such that $t_1,t_2,t_3 < t$ with $t_1,t_2,t_3 \neq 0$ and $\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$. All scalars t with decompositions that do not satisfy the conditions are crossed off. The results of sieving process of scalars t that lie in the $[1,n-1]$ interval are determined based on the following cases of new scalars t_1,t_2 and t_3 values from t decomposition. These cases are as follows.

i. The decomposition of t into t_1,t_2 and t_3 resulted in $\min\{|t_1|,|t_2|,|t_3|\} = 1$ or $\max\{|t_1|,|t_2|,|t_3|\} = t$.

ii. The decomposition of t into t_1,t_2 and t_3 leads to $\max\{|t_1|,|t_2|,|t_3|\} > t$.

iii. The decomposition of t into t_1,t_2 and t_3 yields $\max\{|t_1|,|t_2|,|t_3|\} \leq \sqrt{n}$.

iv. The decomposition of t into t_1,t_2 and t_3 produces $\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$.

Repeating this process with cross off all cases i, ii and iii gives a list of the scalars up to n-1. These scalars lie outside the range $\sqrt{n}$ on the interval $[1,n-1]$. Scalars t with such a property represent 3-ISD used for the successful computation of the 3-ISD Edwards scalar multiplication tP. Using Algorithm (3.6.2.1), all the scalars satisfying the 3-ISD decomposition in the $[1,n-1]$ are determined. This algorithm is performed with input (n,v_1,v_2,v_3). to output the 3-ISD correct values of multipliers t.

Example 4.5.2.1. (Distributing the scalars on Edwards curve Based Another Type of 3-ISD Method with Randomized Generators).

With a prime number $p = 1171$, suppose $v_1 = (55,31,24), v_2 = (37,11,17)$ and $v_3 = (11,13,28)$ are three vectors are chosen randomly. The elements on each vector are relative prime to each other. So, the first generator of 3-ISD method Is $\{v_1,v_2,v_3\}$. So, the first generator of 3-ISD method is

$\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 159 \in [1, 292]$. The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 \,(\mathrm{mod}\, n) \equiv 135 (\mathrm{mod}\, 293),$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 \,(\mathrm{mod}\, n) \equiv 260 (\mathrm{mod}\, 293),$$

and

$$t_3 \equiv d_1 c_1 + d_2 c_2 + d_3 c_3 \,(\mathrm{mod}\, n) \equiv 57 \,(\mathrm{mod}\, 293),$$

where $\max\{135, 260, 57\} > \sqrt{n} = \sqrt{293} = 17.11$ and

$$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(13)159 / 293 \rceil = -7,\ d_2 = \lfloor b_2 t / n \rceil = \lfloor (11)159 / 293 \rceil = 6,$$

$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (31)159 / 293 \rceil = 17.$$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (18, 13, 25),\ v_2' = (33, 51, 68),\ v_3' = (85, 68, 17),$$
$$v_1'' = (41, 57, 72),\ v_2'' = (27, 65, 39),\ v_3'' = (37, 55, 42),$$

and

$$\hat{v_1} = (28, 54, 41),\ \hat{v_2} = (33, 65, 72),\ \hat{v_3} = (47, 57, 10).$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\mathrm{mod}\ n) \equiv 10 + 4(32) + (12)(73) (\mathrm{mod}\, 293),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\mathrm{mod}\ n) \equiv (-12) + (15)(1) + (-3)(12) \,(\mathrm{mod}\, 293).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\mathrm{mod}\ n) \equiv 5 + (6)(2) + (9)(37) (\mathrm{mod}\, 293).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$tP = (1107,1081) + (427,18) + (941,136), +(724,1027) + (272,1001) + (259,581) + (650,926) + (447,1027) + (341,165) = (2,592)$$

when

$$\psi_1'(P) = \lambda_1' P = 32(7,766) = (983,384),\ \psi_2'(P) = \lambda_2' P = 73(7,766) = (911,1085),$$
$$\psi_1''(P) = \lambda_1'' P = 1(7,766) = (7,766),\quad \psi_2''(P) = \lambda_2'' P = 12(7,766) = (447,1027)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 2(7,766) = (884,532),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 37(7,766) = (872,1151).$$

$$t_{11}P = 10(7,766) = (1107,1081),\ t_{12}\psi_1'(P) = 4(983,384) = (427,18),$$
$$t_{13}\psi_2'(P) = 12(911,1085) = (941,136)$$

$$t_{21}P = -12(7,766) = (724,1027),\ t_{22}\psi_1''(P) = 15(7,766) = (272,1001),$$
$$t_{23}\psi_2''(P) = -3(447,1027) = (259,581)$$

$$t_{31}P = 5(7,766) = (650,926),\quad t_{32}\hat{\psi}_1(P) = 6(884,532) = (447,1027),$$
$$t_{33}\hat{\psi}_2(P) = 9(872,1151) = (341,165)$$

are nine efficiently computable endomorphisms that are pre-computed.

With another value $t = 236 \in [1,293]$ the decomposition into can be done scalars t_1, t_2 and t_3 such that

$$t_1 \equiv t - a_1 d_1 - a_2 d_2 - a_3 d_3 \pmod{n} \equiv 178 \pmod{293},$$
$$t_2 \equiv t_1 - b_1 d_1 - b_2 d_2 - b_3 d_3 \pmod{n} \equiv 27 \pmod{293},$$

and

$$t_3 \equiv d_1 c_1 + d_2 c_2 + d_3 c_3 \pmod{n} \equiv 31 \pmod{293},$$

where $\max\{178,27,31\} > \sqrt{n} = \sqrt{293} = 17.11$ and

$$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(13)236/293 \rceil = -10,\ d_2 = \lfloor b_2 t / n \rceil = \lfloor (11)236/293 \rceil = 9,$$

$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (31)236/293 \rceil = 25.$$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (23,12,13),\ v_2' = (8,32,37), v_3' = (25,53,43),$$
$$v_1'' = (52,37,29),\ v_2'' = (37,11,12),\ v_3'' = (11,13,10),$$

and

$$\hat{v_1} = (12,41,51),\ \hat{v_2} = (60,11,15),\ \hat{v_3} = (66,10,11).$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 1 + -8(8) + (2)(267) (\text{mod } 293),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv 9 + (-4)(2) + (13)(2) (\text{mod } 293).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv 12 + (2)(3) + (8)(258) (\text{mod } 293).$$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (7,766) + (560,540) + (189,49), + (391,944) + (1121,528) + \\ &\quad (947,1025) + (447,1027) + (220,526) + (16,181) \\ &= (208,788) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 8(7,766) = (50,528),\ \ \psi_2'(P) = \lambda_2' P = 267(7,766) = (123,904),$$
$$\psi_1''(P) = \lambda_1'' P = 2(7,766) = (884,532),\quad \psi_2''(P) = \lambda_2'' P = 2(7,766) = (884,532)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 3(7,766) = (230,136),\ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 258(7,766) = (235,974).$$

$$t_{11}P = 1(7,766) = (7,766),\ t_{12}\psi_1'(P) = -8(611,540) = (560,540),$$
$$t_{13}\psi_2'(P) = 2(123,904) = (189,49)$$

$$t_{21}P = 9(7,766) = (391,944),\ t_{22}\psi_1''(P) = -4(884,532) = (1121,528),$$
$$t_{23}\psi_2''(P) = 13(884,532) = (947,1025)$$

$$t_{31}P = 12(7,766) = (447,1027),\quad t_{32}\hat{\psi}_1(P) = 2(230,136) = (220,526),$$
$$t_{33}\hat{\psi}_2(P) = 8(235,974) = (16,181)$$

are six efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [49,292]$ that have 3-ISD sub-scalars which are obtained based on the randomized choices of the vectors that generate the 3-ISD generators.

Example 4.5.1.4. (Twisted Edwards Scalar multiplication based new Type of 3-ISD method).

With a prime number $p = 1171$, Suppose $E_{a,d}$ is an Twisted Edwards curve defined by $E_{16,2}: 16x^2 + y^2 = 1 + 2x^2y^2 \pmod{1171}$, with $d = 2$ and $a = 16$ over F_{1171}. Let $p = (1169,3)$ be a generator point lies on $E_{16,2}$ has prime order $n = 149$.

Suppose $v_1 = (46,23,25)$, $v_2 = (36,44,39)$ and $v_3 = (56,18,21)$ are three vectors are chosen randomly. The elements on each vector are relative prime to each other.

So, the first generator of 3-ISD method is $\{v_1, v_2, v_3\}$ using to decompose a scalar $t = 78 \in [1,148]$. The scalars t_1, t_2 and t_3 are computed by

$$t_1 \equiv t - a_1d_1 - a_2d_2 - a_3d_3 \pmod{n} \equiv 35 \pmod{149},$$
$$t_2 \equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \pmod{n} \equiv 91 \pmod{149},$$

and

$$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \pmod{n} \equiv 101 \pmod{149},$$

where $\max\{35,91,101\} > \sqrt{n} = \sqrt{149} = 12.21$. and

$d_1 = \lfloor -b_3 t / n \rceil = \lfloor -(18)78/149 \rceil = -9,\ d_2 = \lfloor b_2 t / n \rceil = \lfloor (44)78/149 \rceil = 23$ and

$$d_3 = \lfloor b_1 t / n \rceil = \lfloor (23)78/149 \rceil = 12.$$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (12,18,17),\ v_2' = (13,51,19), v_3' = (17,18,35),$$
$$v_1'' = (61,15,33),\ v_2'' = (59,5,33),\ v_3'' = (66,7,38),$$

and

$$\hat{v_1} = (76,29,32),\ \hat{v_2} = (37,66,49),\ \hat{v_3} = (49,18,21)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into$t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv 8 + (-8)(10) + (2)(128) (\text{mod} 149),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv 11 + (-7)(4) + 11(64) (\text{mod} 149).$$

and

$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv 7 + (5)(8) + (6)(9) (\text{mod} 149).$$

The scalar multiplication *tP* using the 3-ISD method is computed by

$$\begin{aligned} tP &= (343,382) + (138,504) + (1044,603), + (744,832) + (893,572) + \\ &\quad (234,333) + (625,163) + (182,776) + (35,1101) \\ &= (872,919) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 10(1169,3) = (589,896),\ \ \psi_2'(P) = \lambda_2' P = 128(1169,3) = (401,961),$$
$$\psi_1''(P) = \lambda_1'' P = 4(1169,3) = (957,745),\ \ \psi_2''(P) = \lambda_2'' P = 64(1169,3) = (1052,1051)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 8(1169,3) = (343,382),\ \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 9(1169,3) = (1004,109).$$

$$t_{11}P = 8(1169,3) = (343,382),\ t_{12}\psi_1'(P) = -8(589,896) = (138,504),$$
$$t_{13}\psi_2'(P) = 2(401,961) = (1044,603)$$

$$t_{21}P = 11(1169,3) = (744,832),\ t_{22}\psi_1''(P) = -7(957,745) = (893,572),$$
$$t_{23}\psi_2''(P) = 11(1052,1051) = (234,333)$$

$$t_{31}P = 7(1169,3) = (625,163),\ t_{32}\hat{\psi}_1(P) = 5(343,382) = (182,776),$$
$$t_{33}\hat{\psi}_2(P) = 6(1004,109) = (35,1101)$$

are six efficiently computable endomorphisms that are pre-computed.

With another value $t = 115 \in [1,148]$ the decomposition into can be done scalars t_1, t_2 and t_3 such that

$$t_1 \equiv t - a_1d_1 - a_2d_2 - a_3d_3 \pmod{n} \equiv 76 \pmod{149},$$
$$t_2 \equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 \pmod{n} \equiv 66 \pmod{149},$$

and $$t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 \pmod{n} \equiv 122 \pmod{149},$$

where $\max\{76,66,122\} > \sqrt{n} = \sqrt{149} = 12.21.$ and

$d_1 = \lfloor -b_3t / n \rceil = \lfloor -(71)115/149 \rceil = -55,\ d_2 = \lfloor b_2t / n \rceil = \lfloor (28)115/149 \rceil = 22$ and

$$d_3 = \lfloor b_1t / n \rceil = \lfloor (97)115/149 \rceil = 75.$$

Now, others nine vectors are chosen randomly to general the 3-IDS generators $\{v_1', v_2', v_3'\}$, $\{v_1'', v_2'', v_3''\}$ and $\{\hat{v_1}, \hat{v_2}, \hat{v_3}\}$. These vectors are

$$v_1' = (29,32,17),\ v_2' = (33,17,39), v_3' = (37,55,54),$$
$$v_1'' = (30,31,18),\ v_2'' = (33,17,35),\ v_3'' = (37,55,54),$$

and $$\hat{v_1} = (4,12,29),\ \hat{v_2} = (19,13,38),\ \hat{v_3} = (56,62,17)$$

Using these generators, one can sub-decompose the scalars t_1, t_2 and t_3 into $t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23}$ and t_{31}, t_{32}, t_{33} respectively such that

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\text{mod } n) \equiv -1 + 11(32) + (-6)(21) (\text{mod} 149),$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\text{mod } n) \equiv 4 + (-9)(5) + 8(32) (\text{mod} 149).$$

and $t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \ (\text{mod } n) \equiv 4 + (2)(8) + (3)(34) (\text{mod} 149).$

The scalar multiplication tP using the 3-ISD method is computed by

$$\begin{aligned} tP &= (2,3) + (35,1101) + (327,231), + (957,745) + (905,1077) + \\ &\quad (1044,603) + (957,745) + (377,200) + (669,928) \\ &= (589,896) \end{aligned}$$

when

$$\psi_1'(P) = \lambda_1' P = 32(1169,3) = (340,549), \ \psi_2'(P) = \lambda_2' P = 21(1169,3) = (770,961),$$
$$\psi_1''(P) = \lambda_1'' P = 5(1169,3) = (1110,983), \quad \psi_2''(P) = \lambda_2'' P = 32(1169,3) = (340,549)$$

$$\hat{\psi}_1(P) = \hat{\lambda}_1 P = 8(1169,3) = (343,382), \ \hat{\psi}_2(P) = \hat{\lambda}_2 P = 34(1169,3) = (998,906).$$

$$t_{11}P = -1(1169,3) = (2,3), \ t_{12}\psi_1'(P) = 11(340,549) = (35,1101),$$
$$t_{13}\psi_2'(P) = -7(770,961) = (327,231)$$

$$t_{21}P = 4(1169,3) = (957,745), \ t_{22}\psi_1''(P) = -9(1110,983) = (905,1077),$$
$$t_{23}\psi_2''(P) = 8(340,549) = (1044,603)$$

$$t_{31}P = 4(1169,3) = (957,745), \ t_{32}\hat{\psi}_1(P) = 2(343,382) = (377,200),$$
$$t_{33}\hat{\psi}_2(P) = 3(998,906) = (669,928)$$

are nine efficiently computable endomorphisms that are pre-computed.

All the scalar $t \in [44,148]$ that have 3-ISD sub-scalars which are obtained based on the randomized choices of the vectors that generate the 3-ISD generators.

Chapter Five

The Computational Results of the Proposed Versions of the 3-ISD Method

In this chapter, some other computational results are presented as follows.

5.1 The Experimental Results of the Edwards Scalar Multiplication Using 3 -ISD Algorithm

Some simple computations of the Edward Scalar multiplication based on 3-ISD algorithm are presented. The experimental samples with different values of a prime p are chosen. The computational results to computed a scalar multiplication tP are shown in Tables (5.1).

5.2 The Experimental Results of the Twisted Edwards Scalar Multiplication Based 3 -ISD Algorithm

Some simple computations of the twisted Edward curve 3-ISD algorithm (3.4.1.1)are discussed. The experimental samples with different values of a prime p are chosen. The computational results for computing tP are shown in Tables (5.2).

Table 5.1: The experimental results of the Edward scalar multiplication 3–ISD algorithm.

p	d	n	λ_1	λ_2	3-ISD generators	t
1171	2	293	68	154	$\{v_1' = (1,9,-7), v_2' = (11,3,7), v_3' = (-20,19,25)\}$, $\{v_1'' = (18,30,-12), v_2'' = (-28,21,30), v_3'' = (37,-15,47)\}$	292
1867	2	467	17	96	$\{v_1' = (7,17,-7), v_2' = (30,-7,-14), v_3' = (53,3,85)\}$, $\{v_1'' = (9,-2,15), v_2'' = (-35,13,16), v_3'' = (-11,-56,-4)\}$	463
2011	2	503	410	183	$\{v_1' = (3,21,-16), v_2' = (14,4,25), v_3' = (16,-3,-21)\}$, $\{v_1'' = (2,18,-14), v_2'' = (22,6,14), v_3'' = (-41,38,57)\}$	498
2083	2	521	80	19	$\{v_1' = (26,30,-5), v_2' = (29,-15,40), v_3' = (-34,21,22)\}$, $\{v_1'' = (20,30,-5), v_2'' = (-29,21,22), v_3'' = (35,-15,40)\}$	516
2251	2	563	252	250	$\{v_1' = (-10,-6,-16), v_2' = (7,19,-1), v_3' = (20,-5,-15)\}$, $\{v_1'' = (-15,-5,-17), v_2'' = (17,-2,-14), v_3'' = (-7,-24,-1)\}$	558
7603	5	1901	840	1073	$\{v_1' = (32,30,-10), v_2' = (23,-15,45), v_3' = (-41,21,18)\}$, $\{v_1'' = (18,30,-12), v_2'' = (-29,21,17), v_3'' = (37,-15,47)\}$	1868

$P = (x, y)$	t_{11}	t_{12}	t_{21}	t_{22}	tP
(7, 766)	-15	12	2	10	(859, 802)
(3, 317)	-5	-10	-8	-3	(1211,1387)
(2004, 750)	2	6	1	14	(811, 1961)
(2076, 469)	8	-4	3	–9	(699, 823)
(2244, 656)	-20	20	–17	16	(877, 1162)
(22, 108)	14	11	21	9	(709, 3040)

Table 5.2: The experimental results of the Twisted Edward scalar multiplication 3–ISD algorithm.

p	$E_{a,d}(a,d)$	n	λ_1	λ_2	3-ISD generators	t
1171	(2,16)	149	25	66	$\{v_1' = (16,-3,15), v_2' = (-26,12,31), v_3' = (-11,-58,-3)\}$, $\{v_1'' = (7,-3,19), v_2'' = (-30,14,8), v_3'' = (-21,-56,3)\}$	118
1867	(2,110)	151	46	57	$\{v_1' = (2,12,27), v_2' = (-31,6,-7), v_3' = (-37,-74,40)\}$, $\{v_1'' = (-17,8,8), v_2'' = (13,16,32), v_3'' = (-13,-68,42)\}$	150
2011	(2,64)	163	78	103	$\{v_1' = (-22,11,11), v_2' = (6,-3,35), v_3' = (-26,-53,2)\}$, $\{v_1'' = (5,12,25), v_2'' = (-37,6,-4), v_3'' = (-35,-74,42)\}$	159
2083	(2,49)	257	8	30	$\{v_1' = (-26,11,6), v_2' = (6,-3,30), v_3' = (-26,-53,2)\}$, $\{v_1'' = (-22,11,9), v_2'' = (6,-3,31), v_3'' = (-26,-53,1)\}$	186
2251	(2,122)	139	52	112	$\{v_1' = (-23,27,11), v_2' = (-6,-19,37), v_3' = (-39,-23,-25)\}$, $\{v_1'' = (-23,27,11), v_2'' = (-2,-19,35), v_3'' = (-39,-23,-24)\}$	138
7603	(5,141)	631	205	389	$\{v_1' = (2,18,-10), v_2' = (22,6,13), v_3' = (-37,38,43)\}$, $\{v_1'' = (2,18,-14), v_2'' = (22,6,14), v_3'' = (-45,44,64)\}$	610

$P = (x, y)$	t_{11}	t_{12}	t_{21}	t_{22}	tP
(1169, 3)	4	9	6	5	(567, 1120)
(1864, 1140)	5	9	11	3	(212,21)
(9, 1318)	2	8	-4	5	(1825, 32)
(13, 1295)	8	13	14	2	(1894, 833)
(2, 890)	2	10	6	-1	(2249, 890)
(4, 4221)	8	9	10	13	(1747, 6409)

5.3 The Experimental Results of Edwards Scalar Multiplication Based New Type of 3-ISD Method

Some simple computations of the Edward Scalar multiplication based on 3-ISD algorithm are presented. The experimental samples with different values of a prime p are chosen. The computational results to computed a scalar multiplication tP are shown in Tables (5.3).

5.4 The Experimental Results of Twisted Edwards Scalar Multiplication Based New Type of 3-ISD Method

Some simple computations of the twisted Edward curve 3-ISD algorithm (3.5.2.1)are discussed. The experimental samples with different values of a prime p are chosen. The computational results for computing tP are shown in Tables (5.4).

Table 5.3: The experimental results of the Edward scalar multiplication 3–ISD with new type of decomposition.

P	d	n	λ_1'	λ_2'	λ_1''	λ_2''	$\hat{\lambda}_1$	$\hat{\lambda}_2$	3-ISD generators	t
1171	2	293	16	65	8	28	26	64	$\{v_1'=(3,21,-3), v_2'=(14,4,16), v_3'=(16,-3,-15)\}$, $\{v_1''=(5,5,-5), v_2''=(10,15,20), v_3''=(25,-20,5)\}$, $\{\hat{v_1}=(3,13,-1), \hat{v_2}=(14,4,14), \hat{v_3}=(16,-3,-4)\}$.	188
1867	2	467	16	103	32	358	8	113	$\{v_1'=(3,21,-3), v_2'=(14,4,23), v_3'=(16,-3,-20)\}$, $\{v_1''=(3,21,-3), v_2''=(14,4,16), v_3''=(16,-3,-11)\}$, $\{\hat{v_1}=(2,18,-14), \hat{v_2}=(22,6,14), \hat{v_3}=(-49,38,37)\}$.	438
2011	2	503	2	280	8	7	32	157	$\{v_1'=(-24,11,6), v_2'=(7,-3,32), v_3'=(-25,-53,-9)\}$, $\{v_1''=(3,13,-3), v_2''=(20,4,16), v_3''=(17,-3,-15)\}$, $\{\hat{v_1}=(2,18,-14), \hat{v_2}=(22,6,14), \hat{v_3}=(-40,38,29)\}$.	412
2083	2	521	8	6	64	229	8	260	$\{v_1'=(3,21,-3), v_2'=(14,4,23), v_3'=(16,-3,-20)\}$, $\{v_1''=(-29,11,11), v_2''=(12,-3,35), v_3''=(-18,-53,10)\}$, $\{\hat{v_1}=(11,-3,10), \hat{v_2}=(-26,12,31), \hat{v_3}=(-11,-58,-4)\}$.	517
2251	2	563	66	8	72	12	113	4	$\{v_1'=(-54,14,13), v_2'=(11,46,73), v_3'=(-28,-80,26)\}$, $\{v_1''=(3,19,-3), v_2''=(14,6,16), v_3''=(21,-5,-6)\}$, $\{\hat{v_1}=(10,19,-3), \hat{v_2}=(14,6,20), \hat{v_3}=(21,-5,-7)\}$.	560
7603	5	1901	1403	129	1475	4	1790	2	$\{v_1'=(6,21,24), v_2'=(-39,6,-6), v_3'=(-37,-74,31)\}$, $\{v_1''=(-24,11,3), v_2''=(6,-3,47), v_3''=(-26,-53,2)\}$, $\{\hat{v_1}=(-29,11,4), \hat{v_2}=(11,-4,46), \hat{v_3}=(-21,-52,3)\}$.	1861

$P=(x,y)$	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{23}	t_{33}	tP
$(7,766)$	4	7	-15	6	-14	15	1	-12	-2	$(630,404)$
$(3,317)$	10	13	-20	12	17	-17	9	-5	-5	$(1707, 1347)$
$(2004, 750)$	-17	7	13	17	19	-14	16	-6	9	$(837,1214)$
$(2076,469)$	14	17	-20	-9	-16	2	-2	4	20	$(1719,2068)$
$(2244,656)$	4	-19	3	20	4	-6	20	-16	-10	$(1201,474)$
$(22,108)$	28	-4	42	18	11	5	2	9	34	$(3739,3281)$

Table 5.4: The experimental results of the twisted Edward scalar multiplication3–ISD with new type of decomposition.

p	$E_{a,d}(a,d)$	n	λ_1'	λ_2'	λ_1''	λ_2''	$\hat{\lambda}_1$	$\hat{\lambda}_2$	3-ISD generators	t
1171	(2,16)	149	5	32	3	23	9	8	$\{v_1'=(9,-3,10), v_2'=(-24,12,31), v_3'=(-22,-58,-7)\}$, $\{v_1''=(-26,12,9), v_2''=(10,-3,31), v_3''=(-22,-53,-2)\}$, $\{\hat{v_1}=(16,30,-11), \hat{v_2}=(-27,21,29), \hat{v_3}=(38,-15,45)\}$.	147
1867	(2,110)	151	2	26	4	24	10	64	$\{v_1'=(5,18,-15), v_2'=(12,4,24), v_3'=(19,-3,-16)\}$, $\{v_1''=(2,18,-14), v_2''=(22,6,14), v_3''=(-34,38,46)\}$, $\{\hat{v_1}=(9,19,-3), \hat{v_2}=(16,6,16), \hat{v_3}=(19,-5,-6)\}$.	121
2011	(2,64)	163	2	145	4	18	9	1	$\{v_1'=(20,6,14), v_2'=(7,18,-14), v_3'=(-41,38,40)\}$, $\{v_1''=(-21,27,11), v_2''=(5,-18,35), v_3''=(-53,-25,-23)\}$, $\{\hat{v_1}=(2,21,-15), \hat{v_2}=(14,4,24), \hat{v_3}=(19,-3,-16)\}$.	157
2083	(2,49)	257	16	85	4	14	5	1	$\{v_1'=(-20,10,9), v_2'=(6,-3,35), v_3'=(-21,-53,2)\}$, $\{v_1''=(-47,19,17), v_2''=(29,3,59), v_3''=(-47,-53,10)\}$, $\{\hat{v_1}=(11,-3,10), \hat{v_2}=(-26,12,31), \hat{v_3}=(-11,-105,27)\}$.	246
2251	(2,122)	139	16	84	1	19	1	18	$\{v_1'=(11,-4,10), v_2'=(-26,13,22), v_3'=(-11,-58,-4)\}$, $\{v_1''=(-23,27,5), v_2''=(-7,-19,37), v_3''=(-39,-23,-25)\}$, $\{\hat{v_1}=(-16,9,8), \hat{v_2}=(15,13,32), \hat{v_3}=(-15,-71,29)\}$.	122
7603	(5,141)	631	128	239	257	9	245	3	$\{v_1'=(-47,18,20), v_2'=(29,3,59), v_3'=(-47,-105,27)\}$, $\{v_1''=(3,19,-3), v_2''=(14,6,16), v_3''=(21,-5,-11)\}$, $\{\hat{v_1}=(4,18,-10), \hat{v_2}=(21,6,13), \hat{v_3}=(-37,38,43)\}$.	626

$P=(x,y)$	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{23}	t_{33}	tP
(1169,3)	7	9	-2	8	6	8	3	7	4	(802,1050)
(1864,1140)	9	-5	9	9	-5	8	-10	-5	-6	(92, 1265)
(9, 1318)	1	3	1	2	2	-5	7	-10	5	(1057,597)
(13,1295)	1	16	2	3	-15	12	12	-11	8	(1539,1804)
(2,890)	-5	4	2	9	2	10	5	-2	6	(2111,1736)
(4,4221)	22	-17	-15	18	3	-9	-2	-18	-9	(2031,2010)

5.5 The Experimental Results of The 3- ISD Edwards Scalar Multiplication Method Using the Randomized Generators

Some simple computations of the Edward Scalar multiplication based on 3-ISD algorithm are presented. The experimental samples with different values of a prime p are chosen. The computational results to computed a scalar multiplication tP are shown in Tables (5.5).

5.6 The Experimental Results of The 3- ISD Twisted Edwards Scalar Multiplication Method Using the Randomized Generators

Some simple computations of the twisted Edward curve 3-ISD Randomized Generators are discussed. The experimental samples with different values of a prime p are chosen. The computational results for computing tP are shown in Tables (5.6).

Table 5.5: The experimental results of the Edward scalar multiplication that is created based on the randomized 3-ISD generators

p	d	n	λ_1	λ_2	3-ISD generators	t
1171	2	293	114	56	$\{v_1' = (22,11,31), v_2' = (11,14,19), v_3' = (7,8,9)\}$, $\{v_1'' = (11,13,12), v_2'' = (10,9,29), v_3'' = (7,10,47)\}$	290
1867	2	467	46	313	$\{v_1' = (101,113,85), v_2' = (12,17,29), v_3' = (27,10,117)\}$, $\{v_1'' = (10,11,17), v_2'' = (12,17,5), v_3'' = (7,10,11)\}$	459
2011	2	503	156	40	$\{v_1' = (12,11,31), v_2' = (11,24,29), v_3' = (10,11,13)\}$, $\{v_1'' = (11,13,14), v_2'' = (20,9,61), v_3'' = (7,20,107)\}$	431
2083	2	521	11	137	$\{v_1' = (37,47,31), v_2' = (15,17,42), v_3' = (27,43,29)\}$, $\{v_1'' = (27,43,11), v_2'' = (13,27,17), v_3'' = (47,75,7)\}$	296
2251	2	563	153	244	$\{v_1' = (11,25,34), v_2' = (12,11,23), v_3' = (73,23,51)\}$, $\{v_1'' = (13,11,17), v_2'' = (12,17,5), v_3'' = (7,10,11)\}$	550
7603	5	1901	1288	888	$\{v_1' = (71,25,23), v_2' = (11,12,25), v_3' = (14,17,15)\}$, $\{v_1'' = (31,11,20), v_2'' = (44,43,23), v_3'' = (42,11,103)\}$	596

$P = (x, y)$	t_{11}	t_{12}	t_{21}	t_{22}	tP
(7, 766)	7	10	5	16	(941, 136)
(3, 317)	13	16	13	5	(790, 331)
(2004, 750)	3	8	9	17	(1764, 661)
(2076, 469)	1	18	-13	-3	(201, 892)
(2244, 656)	12	-1	-3	-11	(601, 1254)
(22, 108)	4	24	-16	-17	(4324, 7547)

Table 5.6: The experimental results of the twisted Edward scalar multiplication that is created based on the randomized 3-ISD generators

p	$E_{a,d}(a,d)$	n	λ_1	λ_2	3-ISD generators	t
1171	$(2,16)$	149	105	81	$\{v_1' = (15,19,10), v_2' = (14,37,19), v_3' = (17,10,9)\}$, $\{v_1'' = (6,19,23), v_2'' = (11,37,29), v_3'' = (18,10,11)\}$	144
1867	$(2,110)$	151	138	8	$\{v_1' = (25,19,23), v_2' = (15,37,29), v_3' = (17,10,12)\}$, $\{v_1'' = (19,7,23), v_2'' = (15,37,29), v_3'' = (18,11,14)\}$	131
2011	$(2,64)$	163	113	2	$\{v_1' = (21,19,11), v_2' = (14,37,19), v_3' = (17,10,32)\}$, $\{v_1'' = (18,19,11), v_2'' = (14,37,19), v_3'' = (17,10,32)\}$	158
2083	$(2,49)$	257	166	198	$\{v_1' = (22,13.7), v_2' = (12,7,19), v_3' = (17,10,21)\}$, $\{v_1'' = (33,19,11), v_2'' = (14,37,19), v_3'' = (13,10,28)\}$	254
2251	$(2,122)$	139	20	63	$\{v_1' = (11,14,27), v_2' = (12,17,16), v_3' = (7,10,66)\}$, $\{v_1'' = (8,13,7), v_2'' = (12,7,16), v_3'' = (17,10,11)\}$	136
7603	$(5,141)$	631	67	159	$\{v_1' = (9,25,37), v_2' = (27,17,36), v_3' = (57,10,31)\}$, $\{v_1'' = (19,15,27), v_2'' = (22,17,16), v_3'' = (7,10,77)\}$	348

$P = (x, y)$	t_{11}	t_{12}	t_{21}	t_{22}	tP
(1169, 3)	8	1	5	4	(948, 539)
(1864, 1140)	5	4	4	2	(1437, 32)
(9, 1318)	3	4	9	10	(76, 580)
(13, 1295)	1	6	7	4	(1758, 1646)
(2, 890)	4	6	1	9	(299, 1280)
(4, 4221)	9	12	7	1	(4859, 210)

5.7 The Experimental Results of The Edwards Scalar Multiplication Based Another Type of the randomized 3-ISD Generators

Some simple computations of the Edward Scalar multiplication based on 3-ISD algorithm are presented. The experimental samples with different values of a prime p are chosen. The computational results to computed a scalar multiplication tP are shown in Tables (5.7).

5.8 The Experimental Results of The Twisted Edwards Scalar Multiplication Based Another Type of the randomized 3-ISD Generators

Some simple computations of the twisted Edward curve 3-ISD Randomized Generators are discussed. The experimental samples with different values of a prime p are chosen. The computational results for computing tP are shown in Tables (5.8).

Table 5.7: The Experimental Results of The Edwards Multiplication Based Another Type of the randomized 3-ISD Generators

p	E_d	n	λ_1'	λ_2'	λ_1''	λ_2''	$\hat{\lambda}_1$	$\hat{\lambda}_2$	3-ISD generators	t
1171	2	293	3	65	4	56	36	292	$\{v_1'=(14,8,13),v_2'=(34,51,68),v_3'=(85,68,17)\}$, $\{v_1''=(8,29,12),v_2''=(19,12,18),v_3''=(55,21,3)\}$, $\{\hat{v_1}=(9,12,17),\hat{v_2}=(19,25,18),\hat{v_3}=(17,43,23)\}$.	142
1867	2	467	20	2	9	66	8	70	$\{v_1'=(43,57,72),v_2'=(27,65,39),v_3'=(37,55,44)\}$, $\{v_1''=(16,18,17),v_2''=(13,27,38),v_3''=(22,17,3)\}$, $\{\hat{v_1}=(22,18,17),\hat{v_2}=(13,31,38),\hat{v_3}=(24,16,5)\}$.	138
2011	2	503	3	6	3	68	4	457	$\{v_1'=(15,23,14),v_2'=(24,16,11),v_3'=(18,17,9)\}$, $\{v_1''=(24,55,19),v_2''=(13,33,32),v_3''=(28,15,6)\}$, $\{\hat{v_1}=(31,21,36),\hat{v_2}=(18,24,13),\hat{v_3}=(25,15,11)\}$.	159
2083	2	521	1	176	4	49	12	520	$\{v_1'=(51,19,45),v_2'=(20,40,11),v_3'=(23,14,12)\}$, $\{v_1''=(49,19,47),v_2''=(20,37,11),v_3''=(23,14,12)\}$, $\{\hat{v_1}=(44,17,46),\hat{v_2}=(21,49,11),\hat{v_3}=(23,18,19)\}$.	256
2251	2	563	64	178	71	33	256	269	$\{v_1'=(71,27,20),v_2'=(20,10,19),v_3'=(73,23,11)\}$, $\{v_1''=(74,29,32),v_2''=(18,7,17),v_3''=(73,22,21)\}$, $\{\hat{v_1}=(59,29,20),\hat{v_2}=(12,11,19),\hat{v_3}=(73,23,21)\}$.	132
7603	5	1901	1417	1572	1473	5	1900	797	$\{v_1'=(11,35,23),v_2'=(16,9,5),v_3'=(54,17,11)\}$, $\{v_1''=(13,34,23),v_2''=(23,9,5),v_3''=(54,18,15)\}$, $\{\hat{v_1}=(13,34,27),\hat{v_2}=(10,11,7),\hat{v_3}=(58,18,13)\}$.	1640

$P=(x,y)$	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{23}	t_{33}	tP
$(7,766)$	7	8	14	9	-8	12	-7	12	7	$(373,825)$
$(3,317)$	8	-14	8	-14	14	4	-17	16	-2	$(969,1049)$
$(2004,750)$	19	5	7	8	4	1	13	15	3	$(1756,511)$
$(2076,469)$	15	-13	1	1	1	3	-16	11	2	$(512,508)$
$(2244,656)$	5	-18	4	5	-13	4	4	10	1	$(227,379)$
$(22,108)$	5	-31	16	8	13	4	28	3	3	$(3974,2963)$

Table 5.8: The Experimental Results of The Twisted Edwards Multiplication Based Another Type of the randomized 3-ISD Generators

p	$E_{a,d}(a,d)$	n	λ_1'	λ_2'	λ_1''	λ_2''	$\hat{\lambda}_1$	$\hat{\lambda}_2$	3-ISD generators	t
1171	$(16,2)$	149	2	13	2	17	4	39	$\{v_1'=(35,18,23), v_2'=(30,44,39), v_3'=(21,64,16)\}$, $\{v_1''=(35,18,19), v_2''=(31,44,41), v_3''=(21,64,11)\}$, $\{\hat{v}_1=(59,10,23), \hat{v}_2=(21,44,51), \hat{v}_3=(41,64,12)\}$.	142
1867	$(110,2)$	151	8	131	5	66	6	5	$\{v_1'=(46,23,25), v_2'=(36,44,39), v_3'=(56,62,19)\}$, $\{v_1''=(11,17,25), v_2''=(26,11,39), v_3''=(59,60,19)\}$, $\{\hat{v}_1=(13,10,25), \hat{v}_2=(11,15,35), \hat{v}_3=(58,60,17)\}$.	138
2011	$(64,2)$	163	8	73	3	68	32	4	$\{v_1'=(19,11,22), v_2'=(13,15,29), v_3'=(10,61,12)\}$, $\{v_1''=(19,41,22), v_2''=(13,15,28), v_3''=(66,61,12)\}$, $\{\hat{v}_1=(19,40,22), \hat{v}_2=(17,15,28), \hat{v}_3=(58,56,13)\}$.	159
2083	$(49,2)$	257	10	10	32	49	4	20	$\{v_1'=(69,37,32), v_2'=(57,25,28), v_3'=(58,56,13)\}$, $\{v_1''=(22,37,32), v_2''=(23,27,17), v_3''=(20,18,13)\}$, $\{\hat{v}_1=(84,91,16), \hat{v}_2=(25,42,33), \hat{v}_3=(41,47,3)\}$.	256
2251	$(122,2)$	139	16	132	8	33	2	2	$\{v_1'=(49,65,29), v_2'=(53,46,33), v_3'=(66,7,3)\}$, $\{v_1''=(47,65,34), v_2''=(53,46,31), v_3''=(7,38,13)\}$, $\{\hat{v}_1=(17,5,43), \hat{v}_2=(13,51,31), \hat{v}_3=(16,38,13)\}$.	132
7603	$(141,5)$	631	172	20	188	8	128	517	$\{v_1'=(2,15,33), v_2'=(59,5,19), v_3'=(17,8,11)\}$, $\{v_1''=(116,15,33), v_2''=(59,5,19), v_3''=(17,8,13)\}$, $\{\hat{v}_1=(72,15,33), \hat{v}_2=(59,5,18), \hat{v}_3=(17,8,13)\}$.	599

$P=(x,y)$	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{23}	t_{33}	tP
$(1169,3)$	1	-2	10	4	-5	4	-7	6	6	$(546,163)$
$(1864,1140)$	2	6	4	3	-10	-3	-9	-3	8	$(1180,1199)$
$(9,1318)$	-6	9	5	-7	6	4	-6	-2	1	$(1066,308)$
$(13,1295)$	-3	15	-4	8	4	1	-3	1	11	$(2070,1295)$
$(2,890)$	7	3	9	3	6	2	5	6	3	$(1092,2203)$
$(4,4221)$	21	8	5	17	5	9	9	-8	8	$(2736,3320)$

Chapter Six

Conclusions and Future works

6.1 Conclusions

Depending on the contributions of this work, the following conclusions are determined by

1. From the literature review of the encryption schemes and Lattice Reduction The 3-ISD versions have been proposed in this work for computing a scalar multiplication tP on the Edwards and twisted Edwards curve defined over a prime field to give the alternative versions of the ISD method. A scalar t is sub-decomposed based on the 3-ISD generators $\{v_1,v_2,v_3\}$, $\{v'_1,v'_2,v'_3\}$ and $\{v''_1,v''_2,v''_3\}$ that are generated in the three dimension. The 3-ISD method is used to speed up the computations with the moderate and large values of the parameters. On the complicated formulas of t_{11}, t_{12}, t_{21}, and t_{22} that form a scalar t, the security considerations are determined.
2. The 3-ISD versions consider as a bright method for more secure and suitable of the Edwards and twisted Edwards curve cryptographic communications.
3. The comparison between 3-ISD versions that are depended on generators that is computed based on 3LLL lattice reduction algorithm and its extension and the 3-ISD versions which are done based on the randomized chooses of the vectors to generate the 3-ISD generators has been done based on the computational complexities of these versions.

6.2 Future works

It is possible to use another kind of elliptic curves to modify the 3-ISD algorithm. Also, it can apply the 3-ISD on the Edwards and twisted Edwards curve which are defined over extension finite fields. It can determine the computational complexity of the 3-ISD algorithm through using the computations of the bit operations.

RREFERENCES

[1] Harold Edwards. A normal form for elliptic curves. Bulletin of the American mathematical society, 44(3):393–422, 2007.

[2] Bernstein, Daniel J., and Tanja Lange. "Inverted edwards coordinates." International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. Springer, Berlin, Heidelberg, 2007.

[3] Bernstein, Daniel J., and Tanja Lange. "Faster addition and doubling on elliptic curves." international conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2007.

[4] Bernstein, Daniel J., and Tanja Lange. "Analysis and optimization of elliptic- curve single-scalar multiplication." Contemporary Mathematics 461.461 (2008).

[5] Sagheer, Ali M. "ELLIPTIC CURVES PUBLIC KEY TRAITOR TRACING SCHEME." Journal of university of Anbar for Pure science 2.1 (2008).

[6] Bernstein, Daniel J., et al. "Twisted edwards curves." International Conference on Cryptology in Africa. Springer, Berlin, Heidelberg, 2008.

[7] Morain, François. "Edwards curves and CM curves." arXiv preprint arXiv:0904.2243 (2009).

[8] Baldwin, Brian, et al. "A hardware analysis of twisted Edwards curves for an elliptic curve cryptosystem." International Workshop on Applied Reconfigurable Computing. Springer, Berlin, Heidelberg, 2009.

[9] Luk, Franklin T., Sanzheng Qiao, and Wen Zhang. "A lattice basis reduction algorithm." Institute for Computational Mathematics Technical Report 10-04. Hong Kong Baptist University (2010).

[10] Ibraheem, Samaa Fuad. "Constructing Supersingular Elliptic Curves Depending on the Coefficients of Weierstrass Equation." journal of the college of basic education 15.65 (2010).

[11] Moody, Dustin. "Mean value formulas for twisted Edwards curves " IACR Cryptol. ePrint Arch. (2010): 142. R. Feng and H.

[12] Bernstein, Daniel J., and Tanja Lange. "A complete set of addition laws for incomplete Edwards curves." Journal of Number Theory 131.5 (2011): 858-872.

[13] Sagheer, Ali M., Abdul Monem S. Rahama, and Ahmad T. Sadiq. "Design Of Public-Key Cryptosystems Based On Matrices Discrete Logarithm Problem." Journal of University of Babylon 20.4 (2012).

[14] Farashahi, Reza Rezaeian, Dustin Moody, and Hongfeng Wu. "Isomorphism classes of Edwards curves over finite fields." Finite Fields and Their Applications 18.3 (2012): 597-612.

[15] Ahmadi, Omran, and Robert Granger. "On isogeny classes of Edwards curves over finite fields." Journal of Number Theory 132.6 (2012): 1337-1358.

[16] Hamburg, Mike. "Fast and compact elliptic-curve cryptography." IACR Cryptol. ePrint Arch. (2012): 309.

[17] Hamburg, Mike. "Twisting Edwards curves with isogenies." IACR Cryptol. ePrint Arch. (2014): 27.

[18] Abd ulkareem, EFFICIENT HYBIRD (OFKM-ECC) CRYPTOGRAPH SYSTEM USING IN COLOR IMAGEAL-Qadisiyha Journal For Science Vol.19 No. 3 Year 2014.

[19] R.K.K. Ajeena and H. Kamarulhaili, " Point Multiplication using Integer Sub-Decomposition for Elliptic Curve Cryptography," Applied Mathematics & Information Sciences 8(2), pp: 517-525, 2014.

[20] Barnard, Emilie Menard. "Tutorial of Twisted Edwards Curves in Elliptic Curve Cryptography." UC SANTA BARBARA, CS 290 G, FALL (2015).

[21] Liu, Zhe, et al. "VLSI implementation of double-base scalar multiplication on a twisted edwards curve with an efficiently computable endomorphism." (2015).

[22] Rao, Srinivasa Rao Subramanya. "Differential Addition in Edwards Coordinates Revisited and a Short Note on Doubling in Twisted Edwards Form." SECRYPT. 2016.

[23] Farashahi, Reza Rezaeian, and Seyed Gholamhossein Hosseini. "Differential addition on twisted edwards curves." Australasian Conference on Information Security and Privacy. Springer, Cham, 2017.

[24] Skuratovskii, Ruslan. "Edwards curve point counting method and supersingular Edwards and Montgomery curves." arXiv preprint arXiv:1811.12544 (2018).

[25] Vo, L. T, Parameterization of Edwards curves on the rational field Q with given torsion subgroups, IACR Cryptol. ePrint Arch., 2018.

[26] Ajeena, Ruma KK, and Sanaa K. Kamal. "Connecting on the Lattice Based Reductions for Computing the Generators in the ISD Method." Journal of Physics: Conference Series. Vol. 1003. No. 1. IOP Publishing, 2018.

[27] Boudabra, M., & Nitaj, A, A new public key cryptosystem based on Edwards curves. Journal of Applied Mathematics and Computing, 61.1(2019), 431-450.

[28] Skuratovskii, R., and V. Osadchyy. "The order of edwards and Montgomery curves." WSEAS Transactions on Mathematics 19 (2020).

[29] Atnashev, Pavel, and George Woltman. "Edwards curves and FFT-based multiplication." (2021).

[30] Bessalov, Anatoly, et al. "Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves." Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021): 1-11.

[31] Ajeena, Ruma Kareem K. "The soft graphic integer sub-decomposition method for elliptic scalar multiplication." Journal of Discrete Mathematical Sciences and Cryptography 24.6 (2021): 1751-1765.

[32] Hankerson, Darrel, Alfred J Menezes, and Scott Vanstone, Guide to elliptic curve cryptography. Springer-Verlag Professional Computing Series, 2004.

[33] Judson, T.W. Abstract Algebra: Theory and Applications. Boston: MA: pws publishing company, 2013.

[34] Lidl, Rudolf, Introduction to finite fields and their applications. University of Tasmania, Launceston, Australia, 2000.

[35] Ling, San and Xing, Chaoping, *Coding Theory*. A First Course, Cambridge University Press. New York, 2004.

[36] Jeffery, Hoffstein, Jill, Pipher and Joseph, silverman H, An Introduction to Mathematical cryptography. Volume. 1. New York: springer, 2000.

[37] Yan, Song Y. Number theory for computing. Springer Science & Business Media, 2002.

[38] Kerl, John, Computation in finite fields. Arizona State University and Lockheed Martin Corporation, 2004.

[39] Burton, David M., Elementary number theory. University of New Hampshire, seventh edition, 2006.

[40] Gallant, Robert, Robert Lambert, and Scott Vanstone, Faster point multiplication on elliptic curves with efficient endomorphisms. Advances in Cryptology—CRYPTO 2001. Springer Berlin/Heidelberg, 2001.

[41] Khan, Koffka, The Security of Elliptic Curve Cryptosystems - A Survey. Global Journal of Computer Science and Technology: E Network,Web & Security. Volume 15, Issue 5, Version 1.0, 2015.

[42] Washington, L. C., Elliptic curves: number theory and cryptography, CRC press, USA, 2008.

[43] Ajeena, Ruma Kareem K., and Kamarulhaili, Hailiza, Analysis on the elliptic scalar multiplication using integer sub decomposition method. International Journal of Pure and Applied Mathematics. Volume 87. No. 1, pp: 95-114, 2013.

[44] Ajeena, Ruma Kareem K., and Kamarulhaili, Hailiza, The computational complexity of elliptic curve integer sub-decomposition (ISD) method. AIP Conference Proceedings. Volume 1605. No. 1. AIP, 2014.

[45] Ajeena, Ruma Kareem K., and Kamarulhaili, Hailiza, Two dimensional Sub-decomposition method for point multiplication on elliptic curves. Journal of Mathematical Sciences: Advances and Applications. Volume 25, pp: 43-56, 2014.

[46] Ajeena, Ruma Kareem K., and Kamarulhaili, Hailiza, Accelerating Integer Generalizad wj−NAF Expansions Method. Malaysian Journal of Mathematical Sciences 9(S) June, pp: 115-137, 2015.

[47] Ajeena, Ruma Kareem K., and Kamarulhaili, Hailiza, Mathematical analysis of the computational complexity of integer sub-decomposition algorithm. Journal of Physics: Conference Series. Volume 622. No. 1. IOP Publishing, 2015.

[48] Ajeena, Ruma Kareem K., Integer Sub-Decomposition (ISD) Method For Elliptic Curve Scalar Multiplication. Diss. Universiti Sains Malaysia, 2015.

الملخص

في وقتنا الحالي يستخدم نظام التشفير باستخدام المنحني الاهليجي اكثر من اي وقت سابق كاحد انظمة تشفير المفتاح المعلن. العملية الاهم في هذا النظام هي ضرب النقطة في عدد ثابت. هيكلية هذه العملية تتضمن ثلاث مستويات رياضياتية: الحسابات الخاصة بالحقل المنتهي والحسابات الخاصة بالنقطة على المنحني الاهليجي والحسابات المتعلقة بالعدد الثابت. الغرض من هذه الدراسة هي تحسين هذه العملية من خلال تحسين المستوي الثاني منها. حيث قدمنا ثلاثة ابعاد لطريقة التحليل الجزئي للاعداد الصحيحة لحساب ضرب النقطة في عدد ثابت على منحنيات ادوردز ومنحنيات ادوردز الملتوية المعرفة على الحقل الاولي اثبتنا ان هذه الطريقة حققت كفاءة عالية من خلال حساب التحليل الجزئي للعدد عن طريقة تقليل الشبكة والطريقة العشوائية لانشاء المولدات.

جمهورية العراق
جامعة بابل
كلية التربية للعلوم الصرفة
قسم الرياضيات

منحنيات ادوردس الملتوية لطريقة ضرب المنحنيات الاهليجية

مقدمة إلى مجلس كلية التربية للعلوم الصرفة في جامعة بابل
كجزء من متطلبات نيل درجة الدكتوراه فلسفة في التربية/الرياضيات

من قبل
جولان لازم ذياب عبد

بإشراف
أ.م.د. رومى كريم خضر عجينة

1443هـ 2021