Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 5, 1989 – 1997

Versions on 3-ISD Method for Twisted Edwards Scalar Multiplication

[1]Jolan Lazim Theyab, [2]Ruma Kareem K. Ajeena

[1]*Mathematics Department, Education College for Pure Sciences, University of Babylon, Babylon, Iraq,* *jolan.alkfaje121@gmail.com*
[2]*Mathematics Department, Education College for Pure Sciences, University of Babylon, Babylon, Iraq,* *pure.ruma.k@uobabylon.edu.iq*

Abstract

Twisted Edwards curve is a generalized of Edwards curves. These generalized curves are employed as an important tool to increase the security of encryption schemes. This work presents a new contribution of the 3-deminsion integer sub-decomposition (3-ISD) method to compute a scalar multiplication kP on the twisted Edwards curve $E_{a,d}$ defined over prime fields F_p that uses the efficiently computable endomorphisms of $E_{a,d}$ .The 3-ISD method depends on the randomization of generating the 3-ISD generators. The elements of these generators are vectors, their components are chosen from the range [1, p-1], where p is a prime number. In each vector, the elements are relatively prime to each other. Using the 3-ISD generators, a scalar t in [1, n-1] can be decomposed into t_1, t_2 and t_3 with $\max\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$, where n is a prime order of a point P that lies on $E_{a,d}$ .These scalars, namely t_1, t_2 and t_3, are sub-decomposed again into sub-scalars t_{11}, t_{12} , t_{13}, t_{21} , t_{22}, t_{23} and t_{31}, t_{32} , t_{33}The scalar multiplication tP using the 3-ISD method is computed by

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

where $\psi_1'(P) = \lambda_1' P, \psi_2'(P) = \lambda_2' P, \psi_1''(P) = \lambda_1'' P, \psi_2''(P) = \lambda_2'' P$ and $\psi_1'''(P) = \lambda_1''' P, \psi_2'''(P) = \lambda_2''' P$ are six efficiently computable endomorphisms of Edwards curve E_d defined over F_p. . On the 3-ISD method, fast computations are determined based on the randomized generating of the 3-ISD generators in comparison with the previous version that is depended on the 2-ISD generators. In comparison with the 2-ISD computation method to compute tP, the 3-ISD method considers as more secure communications using the twisted Edwards curve cryptography.

Keywords: Elliptic curves, Edwards curves, Twisted Edwards curves scalar multiplication, endomorphisms, ISD.

1. INTRODUCTION

Several mathematicians over a hundred years studied the elliptic curves [1]. They used to solve a various range of mathematical problems. Edwards curves are a family of elliptic curves which are also used for cryptographic schemes. These curves are defined on different fields, especially over finite fields. They are studied for their mathematical properties and they are used for security measures as well [2].

In 2007, Harold M. Edwards [3] presented a normal form x2 + y2 = a2 + a2x2y2 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. As well as, In 2007, Daniel J. Bernstein and Tanja Lange [4] presented the inverted Edwards coordinates (X:Y:Z) which correspond to an affine point (X/Z,Y/Z) on an Edwards curve. On the inverted Edwards coordinates, they presented the addition, doubling and tripling formulas. These formulas are strongly unified even are not complete. Also in 2007, Daniel J. Bernstein, Tanja Lange, [5] gave the fast formulas for Edwards curve group operations. The different elliptic curve forms and different coordinate systems, an extensive comparison of the operations which are doubling, mixed addition, non-mixed addition, and unified addition is discussed. As well, a higher-level operation such as multi-scalar multiplication is explained. In the same year, Daniel J. Bernstein and Tanja Lange [6], presented the answers that compared to the previous analyses that identified the faster scalar-multiplication methods. And which one is more optimized that is covered a wide range.

In 2008, Daniel J. Bernstein et al. [7] generalized the Edwards curves Ed into twisted Edwards curves which are more defined curves over finite fields. They also presented the fast formulas for in the projective and inverted coordinates. Their study showed the computations using the s ave time in comparison with elliptic curves. Also, in the same year, Daniel J. Bernstein et al. [8] presented an addition formula that is defined for all points on the binary elliptic curves. Their work also introduced the cost of doubling the formula for these curves. In 2011, D.J. Bernstein and T. Lange [9], presented their study to cover the Edwards curves. Two addition laws for points P1 and P2 to compute the sum P1 + P2 are presented.

In 2013, Ruma Ajeena and H. Kamarulhaili [10] 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 ψ1 and ψ2 of E over prime field Fp. And also see other works in 2014 and 2015 [11,12]. Also Emilie Menard Barnard [13] in 2015 presented a comparison on the Edwards curves, twisted Edwards curves and Montgomery curves. As well, this work discussed the application of the EdDSA of

In 2016, Srinivasa R. S. Rao [14], 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 is provided with different projective coordinates.

In 2018, Zhengbing Hu et al. [17] determined an increased performance of the elliptic curve digital signature algorithms over binary fields. Their study showed that the complexity of Edwards curves group operations is less than in comparing with the elliptic curves. The digital signature computations using the Edwards curves are performed efficiently and in a more secure way.

In 2019, Maher Boudabra and Abberrahmane Nitaj [18] presented the properties of on a ring Z/nZ, where n = prqs is a prime power RSA modulus. They proposed a scheme and determined its efficiency and security. In 2020, R. Skuratovskii and V. Osadchyy [19], constructed a method to count the order of an Edwards curve Ed over a finite field. It is possible to apply this method to determine the order of elliptic curves according to the birationality equivalence between them. On the Montgomery curve and Ed, a birational isomorphism is also constructed in this work. In this work, an alternative version of the ISD method for computing a scalar multiplication is proposed. This version is applied on Edwards curves defined over a prime field and uses 3-dimension of the ISD generators that are generated randomly. The computations using the 3-ISD are fast as compare with the original one as proposed in [10,11,12] and it considers as a more secure way for Edwards curve cryptography.

The outline of this work consists of Section 2, which shows the basic facts on the Edwards curves, how to sum two points lie on it and some theorems to determine the order of this curve. In Section 3, the fuzziness of the DL encryption schemes is explained. In section 4, some small computational results are discussed. In section 5, the security considerations are determined on the fuzziness DL encryption schemes. Finally, Section 6 draws the conclusions.

II. BASIC FACTS ON THE EDWARDS CURVES

Suppose K is a non-binary finite field. An Edwards curve [7] defined over K is a curve that takes the following formula

$E_d : x^2 + y^2 = 1 + d\,x^2 y^2$, where $d \in K \setminus \{0, 1\}$.

(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

$$(x_1,y_1)+(x_2,y_2)=\left(\frac{x_1y_2+x_2y_1}{1+d\,x_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-d\,x_1x_2y_1y_2}\right) \qquad (2)$$

For addition point, the identity element is a point OE = (0,1). The inverse point –P of a point P = (x1, y1) is defined by –P = (-x1, y1). 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) 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 and twisted Edwards curves is the completeness of the addition point law when d is a non-square in K. This means that the addition point law can be computed for all points lie on Ed and .

For instance, consider the Edwards curve

E3: x2+y2 = 1+7x2y2 (mod 11). (3)

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 F11.

Equation (3) of Edwards curve can be rewritten by

E_3: $y^2 = \dfrac{1-x^2}{1-3x^2}$ (mod 11).

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

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

$$E_2 : x^2 + y^2 = 1 + 2x^2 y^2 \ (\mathrm{mod}\,13).$$

The set of points which lie on E_2 is given by

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

The point (2, 4) lies on E_d. The doubling point $2P$ can be computed as follows.

If P = (2, 4) then $2P$ = (x_3, y_3), where

$$x_3 = \frac{2x_1y_1}{x_1^2 + y_1^2} \quad \text{and} \quad y_3 = \frac{y_1^2 - x_1^2}{2 - x_1^2 - y_1^2}.$$

So,

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

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

The point addition of the points (2, 4) and (3, 3) is computed by

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

where

$$x_3 = \frac{2.(3)+3.(4)}{1+7.(2).(3).(4).(3)} = 4 \ \text{ and}$$

$$y_3 = \frac{4.(3)-(2).(3)}{1-7.(2).(3).(4).(3)} = 2.$$

Theorem 1. If $p \equiv 3 (\mathrm{mod}\ 4)$ is a prime and the following condition of supersingular

$$\sum_{j=0}^{\frac{p-1}{2}} (C^{\,j}_{\frac{p-1}{2}})^2 d^{\,j} \equiv 0 (\mathrm{mod}\ p), \qquad (4)$$

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

$$\#E_d(F_p) = \begin{cases} p+1, with \left(\frac{d}{p}\right) = -1, \\ p-3, with \left(\frac{d}{p}\right) = 1, \end{cases} \quad (5)$$

where $\left(\frac{d}{p}\right)$ is a Legendre symbol, where a Legendre symbol is defined by

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

with p be an odd prime [19].

Theorem 2. (Properties the order of the Edwards curves [19]).

- If $\left(\frac{d}{p}\right) = 1$, then the orders $\#E_d(F_p) = \#E_{d^{-1}}(F_p)$.
- 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

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

Now, the twisted Edwards curve over the field K, with char(K) ≠ 2 is defined

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2 \quad (6)$$

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

$$P+Q = \left(\frac{x_1y_2 + x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1-dx_1x_2y_1y_2}\right) \quad (7)$$

The sum $P + Q$ is also a point in twisted Edwards curve $E_{a,d}$ which is defined over a prime field F_p. Whereas, the law of a doubling point $2P = (x_3, y_3)$ can be derived from addition point law by

$$x_3 = \frac{2x_1y_1}{ax_1^2 + y_1^2} \quad \text{and} \quad y_3 = \frac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2}. \quad (8)$$

For example, if $E_{a,d} : 3x^2 + y^2 = 1 + 7x^2y^2$ is defined over F_{11}. The set of points which lie on $E_{a,d}$ is given by

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

The point (1, 9) lies on $E_{a,d}$. The doubling point $2P$ can be computed by

If $P = (1, 9)$ then $2P = (x_3, y_3)$, where

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

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

So, $(x_3, y_3) = (1, 2)$ belongs to $E_{3,7}(F_{11})$. The point addition of the points (7, 5) and (10, 2) is computed as

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

$$x_3 = \frac{7.(2)+10.(5)}{1+7.(7).(5).(10).(2)} = 7 \text{ and}$$

$$y_3 = \frac{2.(5)-3.(7).(10)}{1-7.(7).(5).(10).(2)} = 6.$$

III. The 3-Dimension of the ISD method for Twisted Edwards Scalar multiplication

Suppose three-dimension vectors v_1, v_2 and v_3 are chosen randomly from the range [1, p-1]. Each component on each vector is relatively prime to other components in the same vector, namely the gcd (a_i, b_j, c_i) = 1 in the vector for $i = 1,2,3$. 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 k 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 prime field F_p. Based on 3-dimensions 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

$$t \equiv t_1 + t_2\lambda_1 + t_3\lambda_2 \pmod{n} \quad \text{with max } \{|t_1|,|t_2|,|t_3|\} > \sqrt{n}, \tag{9}$$

where t_1, t_2 and t_3 are computed by

$$t_1 = t - d_1a_1 - d_2a_2 - d_3a_3,\; t_2 = t - d_1b_1 - d_2b_2 - d_3b_3 \text{ and } t_3 = d_1c_1 + d_2c_2 + d_3c_3 \;. \tag{10}$$

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, a random selection of nine 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

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

that form the ISD generators $\{v'_1,v'_2,v'_3\}$, $\{v''_1,v''_2,v''_3\}$. 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

$$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' \pmod{n},$$
$$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' \pmod{n} \text{ and}$$
$$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 (\text{mod}).$$

(11)

where

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

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

(12)

and

$$t_{31} \equiv t_3 - \hat{d}_1\hat{a}_1 - \hat{d}_2\hat{a}_2 - \hat{d}_3\hat{a}_3 \pmod{n},$$
$$t_{32} \equiv t_{31} - \hat{d}_1\hat{b}_1 - \hat{d}_2\hat{b}_2 - \hat{d}_3\hat{b}_3 \pmod{n}, \tag{13}$$
$$t_{33} \equiv \hat{d}_1\hat{c}_1 + \hat{d}_2\hat{c}_2 + \hat{d}_3\hat{c}_3 \pmod{n}$$

with max $\{|t_{11}|,|t_{12}|,|t_{13}|\} \le \sqrt{n}, \{|t_{21}|,|t_{22}|,|t_{23}|\} \le \sqrt{n}$ and max$\{|t_{31}|,|t_{32}|,|t_{33}|\} \le \sqrt{n}$. So, the scalar t can be written by

$$t \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' + t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' + t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2 \pmod{n}. \tag{14}$$

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

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

where

$$\psi_1'(P) = \lambda_1'P, \psi_2'(P) = \lambda_2'P, \psi_1''(P) = \lambda_1''P, \psi_2''(P) = \lambda_2''P$$

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

IV. COMPUTATIONAL results of the 3-ISD method

With a prime number p = 1171, suppose v_1= (71, 97, 31), v_2= (79, 28, 91) and v_3= (91, 71, 55) 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 $t=142\in[1,148]$

$$d_1=\lfloor -b_3t/n \rceil = \lfloor -(71)142/149 \rceil = -68,$$
$$d_2=\lfloor b_2t/n \rceil = \lfloor (28)142/149 \rceil = 27 \quad \text{and}$$
$$d_3=\lfloor b_1t/n \rceil = \lfloor (97)142/149 \rceil = 92.$$

can be decomposed into scalars t_1 , t_2 and t_3 such that

$$t_1\equiv t-a_1d_1-a_2d_2-a_3d_3 \pmod n \equiv 127 \pmod{149},$$
$$t_2\equiv t_1-b_1d_1-b_2d_2-b_3d_3 \pmod n \equiv 62 \pmod{149},$$

and $t_3\equiv d_1c_1+d_2c_2+d_3c_3 \pmod n \equiv 102 \pmod{149}$,

where $\max\{127,62,102\}>\sqrt{n}=\sqrt{149}=12.20.$

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 $\{\hat{v}_1,\hat{v}_2,\hat{v}_3\}$, where

$$v_1'=(35,18,23), v_2'=(30,44,39), v_3'=(21,64,16),$$
$$v_1''=(35,18,19), v_2''=(31,44,41), v_3''=(21,64,11).$$

and
$$\hat{v}_1=(59,10,23), \hat{v}_2=(21,44,41), \hat{v}_3=(41,64,12)$$

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

$$t_1\equiv t_{11}+t_{12}\lambda_1'+t_{13}\lambda_2' \pmod n \equiv 1+(-2)(2)+10(13) \pmod{149},$$
$$t_2\equiv t_{21}+t_{22}\lambda_1''+t_{23}\lambda_2'' \pmod n \equiv 4+(-5)(2)+4(17) \pmod{149},$$
and
$$t_3\equiv t_{31}+t_{32}\hat{\lambda}_1+t_{33}\hat{\lambda}_2 \pmod n \equiv (-7)+6(4)+6(39) \pmod{149}.$$

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

where

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

$\psi_1'(P)=\lambda_1'P, \psi_2'(P)=\lambda_2'P, \psi_1''(P)=\lambda_1''P, \psi_2''(P)=\lambda_2''P$ and $\hat{\psi}_1(P)=\hat{\lambda}_1P, \hat{\psi}_2(P)=\hat{\lambda}_2P$ are six efficiently computable endomorphisms that are pre-computed by

$$\psi_1'(P)=\lambda_1'P=2(1169,3)=(64,644),$$
$$\psi_2'(P)=\lambda_2'P=13(1169,3)=(907,469),$$
$$\psi_1''(P)=\lambda_1''P=2(1169,3)=(64,644),$$
$$\psi_2''(P)=\lambda_2''P=17(1169,3)=(231,84)$$
$$\hat{\psi}_1(P)=\hat{\lambda}_1P=4(1169,3)=(957,745),$$
$$\hat{\psi}_2(P)=\hat{\lambda}_2P=39(1169,3)=(1103,423).$$

The computation of
$t_{11}P, t_{12}\psi_1'(P), t_{13}\psi_2'(P), t_{21}P, t_{22}\psi_1''(P), t_{23}\psi_2''(P)$

and $t_{31}P, t_{32}\hat{\psi}_1(P), t_{33}\hat{\psi}_2(P)$ are

$$t_{11}p=1(1169,3)=(1169,3),$$
$$t_{12}\psi_1'(p)=(-2)(64,644)=(214,745),$$
$$t_{13}\psi_2'(p)=10(907,469)=(596,282)$$
$$t_{21}P=4(1169,3)=(957,745),$$
$$t_{22}\psi_1''(P)=-5(589,896)=(582,896),$$
$$t_{23}\psi_2''(P)=4(316,255)=(231,84)$$

$$t_{31}P=-7(1169,3)=(546,163),$$
and $t_{32}\hat{\psi}_1(P)=6(957,745)=(386,71)$,
$$t_{33}\hat{\psi}_2(P)=6(1103,423)=(119,1051)$$

Then, the ISD scalar multiplication can be computed by

$$\begin{aligned} tP &=(1169,\ 3)+(214,\ 745)+(596,\ 282)+(957,\ 745)+(582,\ 896)+ \\ &\quad (231,\ 84)+(546,\ 163)+(386,\ 71)+(119,\ 1051) \\ &= (546,\ 163) \end{aligned}$$

Some computational results are seen in Table (1).

TABLE 1. *Small experimental results of the Twisted Edwards of the 3-ISD method for computing*

p	$E_{a,d}\,(a,d)$	n	$\lambda_1^{'}$	$\lambda_2^{'}$	$\lambda_1^{''}$	$\lambda_2^{''}$	$\hat{\lambda}_1$	$\hat{\lambda}_2$	3-ISD generators	t
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
$(1864,1140)$	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	$(2736,3320)$

The original 2-ISD expression to compute in comparison with the proposed version is derived based on two dimension of the ISD generators {v3, v4} and {v5, v6}, where v3, v4, v5 and v6 are vectors. These vectors are computed using the extended Euclidean algorithm. It can see more experimental results of 2-ISD method in [12,20].

V. THE EFFICIENCY AND SECURITY CONSIDERATIONS OF THE 3-ISD METHOD

In comparison with the original two-dimension integer sub-decomposition (2-ISD) method [10,11,12] for computing tP on Ed over Fp, the 3-ISD version considers as a fast computation method, especially with the moderate and large values rather than to the previous version that is applied faster with the small values. On the other hand, the sub-decomposition of a scalar t into the form that is given in Equation (15), where the sub-scalars t11, t12, t21 and t22 which are taken the expressions in Equations (13) and (14) are more complicated to recover the value of t from their sub-decomposition. This sub-decomposition needs more and more computations to get the correct possibility to determine the correct choices of ai, bi and ci, for i =1,2,3, to determine the elements of the 3-ISD method that help us to recover the values of t11, t12, t13, t21, t22, t23 and t31, t32, t33.

For instance, the probability to find the correct value of the element a1 is determined by

$$P_{a_1}=\frac{\#\ the\ correct\ value}{\#\ the\ \ possible\ outcomes}=\frac{1}{p-1}.$$

In the similar way, one needs the probability 1/p-1 to find a2 as well as the probabilities of a3, b1, b2, b3, c1, c2 and c3. So, it is more difficult to recover a scalar k from it is sub-decomposition.

CONCLUSIONS

This work proposes new version of three dimensions of integer sub-decomposition (3-ISD) method to compute a scalar multiplication on twisted Edwards curves defined over the prime field that can be employed by any cryptographer to improve the twisted Edwards curve cryptosystems.

This version depended on creating the three dimension of the ISD generators {v'1,v'2,v'3},{v"1,v"2,v"3} and to sub-decompose a scalar t. The 3-ISD method is used to speed up the computations with the moderate and large values of the parameters. The security is determined based on the complicated formulas of t11, t12, t13, t21, t22, t23 and t31, t32, t33 that form a scalar t. This scalar is a secret key in the Edwards curve cryptosystem that is difficult to get t from the sub-decomposition of it. Eve here needs to compute many cases to determine the elements of the 3-ISD generators reach up to p-1, where p is a (large) moderate prime number, and to get the correct probabilities. So, the 3-ISD method is more secure and suitable for Edwards curve cryptographic communications.

References

[1] D. Hankerson, A. J. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.

[2] Dam, M. R. Edwards Elliptic Curves. Diss. Faculty of Science and Engineering, 2012.

[3] H. Edwards. A normal form for elliptic curves. Bulletin of the American mathematical society, 44(3):393– 422, 2007.

[4] Bernstein, D. J., & Lange, T. (2007, December). Faster addition and doubling on elliptic curves. In international conference on the theory and application of cryptology and information security (pp. 29-50). Springer, Berlin, Heidelberg.

[5] Bernstein, D. J., & Lange, T. (2007, December). Inverted Edwards Coordinates. In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (pp. 20-27). Springer, Berlin, Heidelberg.

[6] D. J. Bernstein & T. Lange. Analysis and optimization of elliptic-curve single-scalar multiplication. Contemporary Mathematics, 461(461), 1(2008).

[7] D. J. Bernstein, P. Birkner, M. Joye, T. Lange & C. Peters. Twisted Edwards Curves. In International Conference on Cryptology in Africa, Springer, Berlin, Heidelberg, pp. 389-405, (2008).

[8] Bernstein, Daniel J., Tanja Lange, and Reza Rezaeian Farashahi. "Binary Edwards Curves." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2008.

[9] 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.

[10] R. K. K. Ajeena, and H. Kamarulhaili. "Point multiplication using integer sub-decomposition for elliptic curve cryptography." Applied Mathematics & Information Sciences 8.2 (2014): 517.

[11] R. K. K. Ajeena, and H. Kamarulhaili. "Analysis on the Elliptic Scalar Multiplication Using Integer Sub-Decomposition Method." International Journal of Pure and Applied Mathematics 87.1 (2013): 95-114.

[12] R. K. K. Ajeena. Integer sub-decomposition (ISD) method for elliptic curve scalar multiplication. Diss. Universiti Sains Malaysia, 2015.

[13] E. M. Barnard . Tutorial of Twisted Edwards Curves in Elliptic Curve Cryptography. UC SANTA BARBARA, CS 290 G, FALL 2015.

[14] Rao, Srinivasa Rao Subramanya. "Three dimensional Montgomery ladder, differential point tripling on Montgomery curves and point quintupling on Weierstrass' and Edwards curves." International Conference on Cryptology in Africa. Springer, Cham, 2016.

[15] Justus, Benjamin, and Daniel Loebenberger. "Differential addition in generalized Edwards coordinates."

International Workshop on Security. Springer, Berlin, Heidelberg, 2010.
[16] Nandi, Steven Galbraith Mridul. "Progress in Cryptology- INDOCRYPT 2012.
[17] Hu, Zhengbing, et al. "Method of searching birationally equivalent Edwards curves over binary fields." International Conference on Computer Science, Engineering and Education Applications. Springer, Cham, 2018.
[18] M. Boudabra& A .Nitaj . A new public key cryptosystem based on Edwards curves. Journal of Applied Mathematics and Computing, 61(1), 431-450(2019).
[19] R. Skuratovskii & V.Osadchyy. The order of Edwards and Montgomery curves. WSEAS Transactions on Mathematics, 19, 253-264 (2020).
[20] R. K. K. Ajeena, and H. Kamarulhaili. "Comparison Studies on Integer Decomposition Method for Elliptic Scalar Multiplication." Advanced Science Letters 20 (2), 526-530 (2014).