Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 4, 3467 – 3474

Versions on 3-Dimension Integer Sub-Decomposition Method Using the Edwards Curves

[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

cIn this work, another version of the integer sub-decomposition (ISD) method is presented to compute a scalar multiplication on Edwards curves Eds which are defined over prime fields Fp. This version depended on applying a 3-dimension of the ISD generators. The elements of these generators are chosen randomly from the range [1, p-1], where p is a prime number. In each vector, the elements are relatively prime to each other. Using these generators, a scalar k can be decomposed into k1 , k2 and k3 with max $\{|t_1|,|t_2|,|t_3|\} > \sqrt{n}$. These scalars are sub-decomposed again into sub-scalars and t31, t32, t33. The scalar multiplication tP using the 3-ISD method is computed using the sub-scalars and the efficiently computable endomorphisms of Edwards curve Ed defined over Fp. On the 3-ISD method, fast computations are determined based on the randomization choices of the elements that form 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 the 3-ISD method considers as more secure communications using the Edwards curve cryptography.

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

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 [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 TEds 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

Let be a prime field with Suppose is an Edward curve[7] defined over in the following equation:

$E_d : x^2 + y^2 = 1 + d x^2 y^2$, where d ∈ F \ {0, 1}. (1)

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

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

For addition point, the identity point addition is a point OE = (0,1). In other words, P + OE = P. The inverse point –P of a point P = (x1,y1) is defined by –P = (-x1,y1). Also, there are points with some special orders such (0, −1) which has order 2 and (1, 0), (−1, 0) possess order 4. The point addition formula that is defined in Equation (2) is known as strongly unified. The reason for that is because of the possibility to use it also for computing the double a point. There is another attractive point that increases the motivation to work with the Edwards curves is the completeness of the point addition law when d is a non-square in F. This means that the point addition law can be computed for all points lie on Ed.

Theorem 1. If p ≡ 3(mod 4) is a prime and the following condition of supersingular

$$\sum_{j=0}^{\frac{p-1}{2}}\left(C^{j}_{\frac{p-1}{2}}\right)^2 d^{j} \equiv 0(\bmod p), \quad (3)$$

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

$$\#E_d(F_p)=\begin{cases} p+1, \text{ with } \left(\frac{d}{p}\right)=-1, \\ p-3, \text{ with } \left(\frac{d}{p}\right)=1, \end{cases} \quad (4)$$

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

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

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

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

III. THE 3-DIMENSION OF THE ISD METHOD FOR EDWARDS SCALAR MULTIPLICATION

Suppose v1, v2 and v3 are vectors that have three dimensions that are chosen randomly from the range [1, p-1]. The elements that form the coordinates on each vector are chosen randomly from the range [1, n-1]. Each component on each vector is relatively prime to other components in the same vector, namely the gcd (a i, b i, ci) = 1 in the vector.

Based on 3-dimensions of the coordinates of the vectors that form the first generator, the scalar can be decomposed into three scalars k1, k2and k3 such that

$$t \equiv t_1 + t_2\lambda_1 + t_3\lambda_2 \pmod n \quad \text{with max } \{|t_1|,|t_2|,|t_3|\} > \sqrt{n}, \quad (6)$$

where k_1, k_2 and k_3 are computed by

$$t_1 = t - d_1a_1 - d_2a_2 - d_3a_3,\; t_2 = t - d_1b_1 - d_2b_2 - d_3b_3 \text{ and } t_3 = d_1c_1 + d_2c_2 + d_3c_3 \;. \quad (7)$$

so, the parameters $d_1 = \lfloor -b_3k/n \rceil$, $d_2 = \lfloor b_2k/n \rceil$ and $d_3 = \lfloor b_1k/n \rceil$.

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

$$t_1 \equiv t_{11} + t_{12}\lambda_1^{'} + t_{13}\lambda_2^{'} (\bmod\ n),$$

$$t_2 \equiv t_{21} + t_{22}\lambda_1^{''} + t_{23}\lambda_2^{''} (\bmod\ n) \text{ and}$$

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

(8)

where

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

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

(9)

and

$$t_{31} \equiv t_3 - \hat{d}_1\hat{a}_1 - \hat{d}_2\hat{a}_2 - \hat{d}_3\hat{a}_3 (\bmod\ n),$$
$$t_{32} \equiv t_{31} - \hat{d}_1\hat{b}_1 - \hat{d}_2\hat{b}_2 - \hat{d}_3\hat{b}_3 \quad (\bmod\ n), \qquad (10)$$
$$t_{33} \equiv \hat{d}_1\hat{c}_1 + \hat{d}_2\hat{c}_2 + \hat{d}_3\hat{c}_3 \quad (\bmod\ n)$$

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

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

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, **s**uppose v_1= (17, 12, 23), v_2= (34, 51, 68) and v_3= (85, 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 $\{v_1, v_2, v_3\}$. Suppose $k = 250 \in [1, 292]$

$$d_1 = \lfloor -b_3k\ /\ n \rceil = \lfloor -(68)250/293 \rceil = -58,$$
$$d_2 = \lfloor b_2k\ /\ n \rceil = \lfloor (51)250/293 \rceil = 44 \qquad \text{and}$$
$$d_3 = \lfloor b_1k\ /\ n \rceil = \lfloor (12)250/293 \rceil = 10.$$

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

$$t_1 \equiv t - a_1d_1 - a_2d_2 - a_3d_3 (\bmod\ n) \equiv 62 (\bmod\ 293),$$
$$t_2 \equiv t_1 - b_1d_1 - b_2d_2 - b_3d_3 (\bmod\ n) \equiv 178 (\bmod\ 293),$$

and $t_3 \equiv d_1c_1 + d_2c_2 + d_3c_3 (\bmod\ n) \equiv 70 (\bmod\ 293)$,

where $\max\{178, 62, 70\} > \sqrt{n} = \sqrt{293} = 17.11$.
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

$$v_1^{'} = (14, 8, 13), v_2^{'} = (34, 51, 68), v_3^{'} = (85, 68, 17),$$
$$v_1^{''} = (8, 29, 12), v_2^{''} = (19, 12, 18), v_3^{''} = (55, 21, 3).$$

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

$t_1 \equiv t_{11} + t_{12}\lambda_1' + t_{13}\lambda_2' (\bmod\ n) \equiv 7 + 8(265) + 14(292) (\bmod 293)$,
$t_2 \equiv t_{21} + t_{22}\lambda_1'' + t_{23}\lambda_2'' (\bmod\ n) \equiv 9 + (-11)(287) + 12(292) (\bmod 293)$.

and

$t_3 \equiv t_{31} + t_{32}\hat{\lambda}_1 + t_{33}\hat{\lambda}_2\ (\bmod\ n) \equiv (-7) + 12(36) + 7(292)(\bmod 293)$.

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

where

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

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

$$\begin{aligned} \psi_1'(P) &= \lambda_1'P = 3(7,766) = (230,136), \\ \psi_2'(P) &= \lambda_2'P = 65(7,766) = (51,1125), \\ \psi_1''(P) &= \lambda_1''P = 9(7,766) = (391,944), \\ \psi_2''(P) &= \lambda_2''P = 65(7,766) = (127,296) \\ \hat{\psi}_1(P) &= \hat{\lambda}_1P = 36(7,766) = (912,581), \\ \hat{\psi}_2(P) &= \hat{\lambda}_2P = 292(7,766) = (1164,766). \end{aligned}$$

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

$$\begin{aligned} t_{11}P &= 7(7,766) = (443,548), \\ t_{12}\psi_1'(p) &= 8(230,136) = (1065,148), \\ t_{13}\psi_2'(p) &= 14(51,1125) = (12,186) \\ t_{21}P &= 9(7,766) = (391,944), \\ t_{22}\psi_1''(P) &= -8(51,1125) = (68,238), \\ t_{23}\psi_2''(P) &= 12(1164,766) = (724,1027) \end{aligned}$$

and
$$\begin{aligned} t_{31}P &= -7(7,766) = (728,548), \\ t_{32}\hat{\psi}_1(P) &= 12(912,581) = (234,248), \\ t_{33}\hat{\psi}_2(P) &= 7(1164,766) = (728,548) \end{aligned}$$

Then, the ISD scalar multiplication can be computed by

$$\begin{aligned} tP &= (443,\ 548) + (1065,\ 148) + (12,\ 186) + (391,\ 944) + (188,\ 384) + \\ &\quad (573,\ 576) + (728,\ 548) + (234,\ 248) + (728,\ 548) \\ &= (373,\ 825) \end{aligned}$$

Some computational results are seen in Table (1).

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

p	d	n	λ_1'	λ_2'	λ_1''	λ_2''	$\hat{\lambda}_1$	$\hat{\lambda}_2$	3-ISD generators	t
1867	2	467	85	466	21	466	8	70	$\{v_4' = (43,57,72), v_5' = (27,65,39), v_6' = (37,55,44)\}$, $\{v_4'' = (16,18,17), v_5'' = (13,27,38), v_6'' = (22,17,3)\}$, $\{\hat{v}_4 = (22,18,17), \hat{v}_5 = (13,31,38), \hat{v}_6 = (24,16,5)\}$.	458
2011	2	503	3	6	3	432	4	457	$\{v_4' = (15,23,14), v_5' = (24,16,11), v_6' = (18,17,9)\}$, $\{v_4'' = (24,55,19), v_5'' = (13,33,32), v_6'' = (28,15,6)\}$, $\{\hat{v}_4 = (31,21,36), \hat{v}_5 = (18,24,13), \hat{v}_6 = (25,15,11)\}$.	463
2083	2	521	1	176	4	64	12	520	$\{v_4' = (51,19,45), v_5' = (20,40,11), v_6' = (23,14,12)\}$, $\{v_4'' = (49,19,47), v_5'' = (20,37,11), v_6'' = (23,14,12)\}$, $\{\hat{v}_4 = (44,17,46), \hat{v}_5 = (21,49,11), \hat{v}_6 = (23,18,19)\}$.	485

2251	2	563	64	178	71	41	256	269	$\{v_4' = (71,27,20), v_5' = (20,10,19), v_6' = (73,23,11)\}$, $\{v_4'' = (74,29,32), v_5'' = (18,7,17), v_6'' = (73,22,21)\}$, $\{\hat{v_4} = (59,29,20), \hat{v_5} = (12,11,19), \hat{v_6} = (73,23,21)\}$.	518
7603	5	1901	1417	1572	1473	5	1900	797	$\{v_4' = (11,35,23), v_5' = (16,9,5), v_6' = (54,17,11)\}$, $\{v_4'' = (13,34,23), v_5'' = (23,9,5), v_6'' = (54,18,15)\}$, $\{\hat{v_4} = (13,34,27), \hat{v_5} = (10,11,7), \hat{v_6} = (58,18,13)\}$.	1640

$P = (x, y)$	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{23}	t_{33}	tP
(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)

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 (13), where the sub-scalars t11, t12, t21 and t22 which are taken the expressions in Equations (11) and (12) 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.

VI. CONCLUSIONS

This work proposed an alternative version of the ISD method, which is the 3-ISD version, for computing a scalar multiplication on the Edwards curve defined over a prime field. 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 k 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.

Reference

[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).