www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 3, PP. 459–464
Manuscript received February 29, 2020; revised July, 2020. DOI: 10.24425/ijet.2020.131899

Simple Verification of Completeness of Two Addition Formulas on Twisted Edwards Curves

Robert Dryło, and Tomasz Kijko

***Abstract*—Daniel Bernstein and Tanja Lange [9] proved that two given addition formulas on twisted Edwards elliptic curves $ax^2 + y^2 = 1 + dxy$ are complete (i.e. the sum of any two points on a curve can be computed using one of these formulas). In this paper we give simple verification of completeness of these formulas using a program written in Magma, which is based on the fact that completeness means that some systems of polynomial equations have no solutions. This method may also be useful to verify completeness of additions formulas on other models of elliptic curves.**

***Keywords*—twisted Edwards curves, complete set of addition formulas, Gröbner bases**

I. Introduction

ELLIPTIC curves are algebraic groups with efficient group law which allows to apply them in number theory algorithms such as primality testing [3] and integer factorization [26] and in public key cryptography for Diffie-Hellman key exchange (ECDH), ElGamal encryption, and elliptic curve digital signature algorithm (ECDSA). Security of these cryptographic schemes is based on the discrete logarithm problem (DLP), which is hard on classical computer but can be broken using polynomial quantum Shor's algorithm [18], [29] if sufficiently efficient quantum computer would be constructed. On elliptic curves also exist isogeny based cryptosystems [14], [28], which are candidates on postquantum schemes, whose security is based on hardness of computing isogenies of large degrees between elliptic curves.

Basic operation in classical schemes based on the DLP is point multiplication by large integers, which has essential contribution to the cost of cryptographic protocols and was motivation to develop methods for improving its efficiency. If implemented insecurly, it may reveal bits of secret key using side channel attacks when, e.g., the double and add method is used and doubling is given by other formula that addition of two different points, which is the case for standard formulas on Weierstrass curves. To prevent this kind of attacks one can try to use suitable algorithms, multiply a point after compression applying the Mongomery ladder algorithm, or use models of elliptic curves with unified addition formula, i.e., where a formula for point addition may also be used for doubling a generic point on a curve. Unified and efficient addition formulas have been given for the following models of elliptic curves: Jacobi quartic [10], [22], Hessian curves [8], [16], [19], Huff curves [24] and Edwards curves [5], [7], [17]. An addition formula on elliptic curves may be incomplete, i.e., there may exist pairs of exceptional points whose sum cannot be computed using a given formula. D. Bernstain and T. Lange [9] proved that two addition formulas (see below (10)) on twisted Edwards curves $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ form a complete set of addition formulas. i.e., the sum of any two points on $E_{a,d}$ can be computed using one of these formulas. In this paper we will give other verification of completeness of addition formulas (10) over any field of characteristic $\neq 2$, which is based on a program written in Magma. In brief completeness means that suitable systems of polynomial equations have no solutions over any field. We first check that formulas are complete for the curve $E_{a,d}$ over the field of rational functions $\mathbb{Q}(a, d)$, where a, d are variables over $\mathbb{Q}$. This is done by checking that 1 belongs to a suitable ideal, and then we write 1 as a sum of given generators with suitable polynomial coefficients. Then we check that these coefficient polynomials can be reduced mod any prime $p \neq 2$ (i.e., there are no denominators which is zero mod p), and we check that the coefficient polynomials can be evaluated for any values $a, d \in K$, which are allowed for $E_{a,d}$ to be an elliptic curve. This shows that formulas (10) are complete over any field K with $\mathrm{char}(K) \neq 2$. We give a code in Magma for this verification. In the last section we also discuss (see also [25]) how one may use Gröbner bases to determine the space of addition formuas of given degree (if such formulas exist), which may be useful to study addtion laws on other models of elliptic curves, our method is similar to the method in [15] to determine formulas used in point compression.

II. Edwards and twisted Edwards curves

H. Edwards [17] introduced the following model of elliptic curves

$$x^2 + y^2 = c^2(1 + x^2y^2),$$

where addition is given by the formula

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{c(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)}.\right) \tag{1}$$

Edwards model was generalized by Bernstein et al. [7] to the form

$$x^2 + y^2 = 1 + dx^2y^2,$$

which covers more curves over a field K of $\mathrm{char}(K) \neq 2$, $d \neq 0, 1$. Later Bernstein et al. [5] introduced twisted Edwards curves

$$E_{a,d} \ : \ ax^2 + y^2 = 1 + dx^2y^2, \tag{2}$$

R. Dryło is with Warsaw School of Economics, Warsaw, Poland (e-mail: rdrylo@sgh.waw.pl).

T. Kijko is with Institute of Mathematics and Cryptology, Military University of Technology, Warsaw, Poland (e-mail: tomasz.kijko@wat.edu.pl).

over a field K of $\mathrm{char}(K) \neq 2$, where $a, d \in K$ are non-zero and $a \neq d$. Addition formula on the twisted curve $E_{a,d}$ extends Edwards formula and is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}. \right) \tag{3}$$

The neutral element is $\mathcal{O} = (0, 1)$ and the negation is given by $-(x, y) = (-x, y)$. If d and a/d are not squares in K, then the above addition formula is complete in the set $E(K)$ of K-rational points on E, i.e., the sum of any two points in $E(K)$ can be computed using the above adition formula.

Twisted Edwards curves are birationally equivalent to Montgomery curves, and conversely, Montgomery curves are birationally equivalent to Edwards curves. On Edwards curves also exist efficient implementations of pairing computation [2], elliptic curve factorization method [4], digital signature EdDSA [6], and isogeny computation [27].

Hisil et al. [23] gave the following addition formula on the twisted Edwards curve

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{ax_1x_2 + y_1y_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1} \right) \tag{4}$$

Note that exceptional casses of formula (3) can be determined as follows. We denote the sum $(x_1, y_1) + (x_2, y_2)$ by (x_3, y_3) and assume that the point $P = (x_1, y_1)$ is fixed.

Case 1: (x_3 does not exists).
We want to find points (x_2, y_2) for which $1 + dx_1x_2y_1y_2 = 0$. We will solve the following system of equations (two last equations mean that points (x_1, y_1) and (x_2, y_2) lay on the twisted Edwards curve):

$$\begin{cases} 1 + dx_1x_2y_1y_2 & = 0 \\ ax_1^2 + y_1^2 - 1 - dx_1^2y_1^2 & = 0 \\ ax_2^2 + y_2^2 - 1 - dx_2^2y_2^2 & = 0 \end{cases} \tag{5}$$

We get the following solutions of system (5) : $\left(\frac{1}{\sqrt{d}y_1}, \frac{-1}{\sqrt{d}x_1}\right)$, $\left(\frac{-1}{\sqrt{d}y_1}, \frac{1}{\sqrt{d}x_1}\right)$., $\left(\frac{1}{\sqrt{ad}x_1}, \frac{-\sqrt{a/d}}{y_1}\right)$ and $\left(\frac{-1}{\sqrt{ad}x_1}, \frac{\sqrt{a/d}}{y_1}\right)$.

Case 2: (y_3 does not exists).
We want to find points (x_2, y_2) for which $1 - dx_1x_2y_1y_2 = 0$. We will solve the following system of equations

$$\begin{cases} 1 - dx_1x_2y_1y_2 & = 0 \\ ax_1^2 + y_1^2 - 1 - dx_1^2y_1^2 & = 0 \\ ax_2^2 + y_2^2 - 1 - dx_2^2y_2^2 & = 0 \end{cases} \tag{6}$$

We get the following solutions of system (6) : $\left(\frac{1}{\sqrt{d}y_1}, \frac{1}{\sqrt{d}x_1}\right)$, $\left(\frac{-1}{\sqrt{d}y_1}, \frac{-1}{\sqrt{d}x_1}\right)$., $\left(\frac{1}{\sqrt{ad}x_1}, \frac{\sqrt{a/d}}{y_1}\right)$ and $\left(\frac{-1}{\sqrt{ad}x_1}, \frac{-\sqrt{a/d}}{y_1}\right)$..

Corollary II.1. *If a is a square and d is not a square in K, then the law given by (3) is complete.*

Now we examine the exceptional casses for formula (4). As above we denote the sum $(x_1, y_1) + (x_2, y_2)$ by (x_3, y_3) and assume that the point $P = (x_1, y_1)$ is fixed.

Case 1: (x_3 does not exists).
We want to find points (x_2, y_2) for which $ax_1x_2 + y_1y_2 = 0$. We will solve the following system of equations:

$$\begin{cases} ax_1x_2 + y_1y_2 & = 0 \\ ax_1^2 + y_1^2 - 1 - dx_1^2y_1^2 & = 0 \\ ax_2^2 + y_2^2 - 1 - dx_2^2y_2^2 & = 0 \end{cases} \tag{7}$$

We get the following solutions of system (7) : $\left(\frac{y_1}{\sqrt{a}}, -\sqrt{a}x_1\right)$, $\left(-\frac{y_1}{\sqrt{a}}, \sqrt{a}x_1\right)$, $\left(\frac{1}{\sqrt{ad}x_1}, -\frac{\sqrt{a/d}}{y_1}\right)$, $\left(-\frac{1}{\sqrt{ad}x_1}, \frac{\sqrt{a/d}}{y_1}\right)$.

Case 2: (x_3 does not exists). We want to find points (x_2, y_2) for which $x_1y_2 - x_2y_1 = 0$. We will solve the following system of equations:

$$\begin{cases} x_1y_2 - x_2y_1 & = 0 \\ ax_1^2 + y_1^2 - 1 - dx_1^2y_1^2 & = 0 \\ ax_2^2 + y_2^2 - 1 - dx_2^2y_2^2 & = 0 \end{cases} \tag{8}$$

We get the following solutions of system (8) : (x_1, y_1), $(-x_1, -y_1)$, $\left(\frac{1}{\sqrt{d}y_1}, \frac{1}{\sqrt{d}x_1}\right)$ and $\left(-\frac{1}{\sqrt{d}y_1}, -\frac{1}{\sqrt{d}x_1}\right)$.

Corollary II.2. *The formula (4) can not be used to double a point and there are exceptions for additions when a is a square and d is not a square in K.*

On the other hand if both formulas (3) and (4) produce results, the results are the same.

In the product of projective lines $\mathbb{P}^1 \times \mathbb{P}^1$ the twisted Edwards curve is by the equation

$$\overline{E}_{a,d} \ : \ aX^2T^2 + Y^2Z^2 = T^2Z^2 + dX^2Y^2. \tag{9}$$

The addition formulas (3) and (4) in homogeneous coordinates are given by

$$\begin{aligned} &((X_1 : Z_1), (Y_1 : T_1)) + ((X_2 : Z_2), (Y_2 : T_2)) = \\ &\begin{cases} ((X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2 : Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2), \\ (Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2 : Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2)) \\ \qquad \text{if in } \mathbb{P}^1(\overline{\mathbb{F}}) \times \mathbb{P}^1(\overline{\mathbb{F}}) \\ ((X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1 : aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2), \\ (X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1 : X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2)) \\ \qquad \text{if in } \mathbb{P}^1(\overline{\mathbb{F}}) \times \mathbb{P}^1(\overline{\mathbb{F}}) \end{cases} \end{aligned} \tag{10}$$

Bernstein and Lange [9] proved that these addition formulas are complete on $E_{a,d}$ over any field K of $\mathrm{char}(K) \neq 2$. We will give alternative verification of completeness of these formulas using Magma.

III. Verification of completeness of two addition formulas

We start by recalling some elementary properties of algebraic sets in the product of projective spaces. Let K be a field with algebraic closure $\overline{K}$. Let $n_1, \ldots, n_s \in \mathbb{N}_{>0}$. A polynomial $f \in K[X_{10}, \ldots, X_{1n_1}, \ldots, X_{s0}, \ldots, X_{sn_s}]$ is homogeneous of degree d_i with respect to variables $X_{i0}, \ldots, X_{in_i}$ if writing $f = \sum_{\alpha \in \mathbb{N}^{n_i+1}} g_\alpha X_{i0}^{\alpha_0} \ldots X_{in_i}^{\alpha_{n_i}}$, where $\alpha = (\alpha_0, \ldots, \alpha_{n_i})$ and g_α are polynomials which do not depend on X_{ij}, we have $g_\alpha \neq 0 \implies |\alpha| = \alpha_0 + \ldots + \alpha_{n_i} = d_i$. Algebraic sets in the product $\mathbb{P}^{n_1} \times \ldots \times \mathbb{P}^{n_s}$ are given as sets of common zeros of a system of polynomials homogeneous with

respect to each set of variables $X_{i0},\ldots,X_{in_i}$ for $i=1,\ldots,s$. We have covering of $\mathbb{P}^{n_1}\times\ldots\times\mathbb{P}^{n_s}$ by open affine sets $U_{1j_1}\times\ldots\times U_{sj_s}$ isomorphic to $K^{n_1}\times\ldots\times K^{n_s}$, where $U_{ij_i}=\{(X_{i0}:\ldots:X_{in_i})\in\mathbb{P}^{n_i}: X_{ij_i}\neq 0\}$ and $0\leq j_i\leq n_i$. In particular to show that some system of polynomial equations has no solutions in $\mathbb{P}^{n_1}\times\ldots\times\mathbb{P}^{n_s}$ over $\overline{K}$ one can equivalenty show that substituting $X_{1j_1}=\ldots X_{sj_s}=1$ to the polynomials form the system we have that 1 belongs to the ideal generated by the new polynomials for each $0\leq j_i\leq n_i$, $i=1,\ldots,s$. For an irreducible algebraic set $V\subset\mathbb{P}^{n_1}\times\ldots\times\mathbb{P}^{n_s}$ a rational map $V\to\mathbb{P}^n$ can be given in the form $F=(F_0:\ldots:F_n)$ such that for each set of variables $X_{i0},\ldots,X_{in_i}$ the polynomials $F_0,\ldots,F_n$ are homogeneous of the same degree with respect to these variables.

Now let $V\subset(\mathbb{P}^1)^4$ be an irreducible algebraic set and let $f:V\to\mathbb{P}^1\times\mathbb{P}^1$ be a rational map defined on the whole of V, which can be given by two formulas $F=((F_1:F_2),(F_3:F_4))$ and $G=((G_1:G_2),(G_3:G_4))$. Let V be given by equations $H_1=H_2=0$. We will apply this to the product $V=E\times E$, where E is an elliptic curve and F,G are two addition formulas. Assume that we want to show that values of the map f can always be obtained using F or G. Let $V_F=\{P\in V: F_1(P)=F_2(P)=0 \text{ or } F_3(P)=F_4(P)=0\}$ and $D_F=V\setminus V_F$, and similarly define the sets V_G and D_G for G. We want to show that $D_F\cup D_G=V$, or equivalently $V_F\cap V_G=\emptyset$. This means that for each $i,j\in\{1,3\}$ the system

$$H_1=H_2=F_i=F_{i+1}=G_j=G_{j+1}=0 \tag{11}$$

has no solutions in $(\mathbb{P}^1)^4$. Let $(X_i:Y_i)$ for $i=1,\ldots,4$ be homogeneous coordinates on the ith $\mathbb{P}^1$ in the product $(\mathbb{P}^1)^4$. For each $(z_1,\ldots,z_4)$, where $z_i\in\{X_i,Y_i\}$ for $i=1,\ldots,4$, let $U_{z_1,\ldots,z_4}=\prod_{i=1}^4\{z_i\neq 0\}$, which is an affine open set isomorphic to the affine space $\overline{K}^4$. Since these sets cover $(\mathbb{P}^1)^4$, we want to show that for each $(z_1,\ldots,z_4)$ as above and for each $i,j\in\{1,3\}$ the system

$$h_1=h_2=f_i=f_{i+1}=g_j=g_{j+1}=0 \tag{12}$$

has no solutions in $\overline{K}^4$, where the polynomials in (12) are obtained by substituting $z_1=\ldots=z_4=1$ in polynomials from (11). Equivalently we want to show that 1 belongs to the ideal generated by $h_1,h_2,f_i,f_{i+1},g_j,g_{j+1}$ over $\overline{K}$, but then 1 also belongs to the ideal I generated by these polynomials over K. This can be checked computing a Gröbner basis of I which will contain 1 or non-zero constant from K. If $1\in I$, for some polynomials $w_i\in K[x_1,\ldots,x_4]$ for $i=1,\ldots,6$ we can write

$$1=w_1h_1+w_2h_2+w_3g_1+w_4g_2+w_5f_1+w_6f_2. \tag{13}$$

For example, one can search for such polynomials w_i as follows. If we want to check existance of w_i of degree $\deg(w_i)\leq b$ for a given bound b, we can regard unknown coefficients of w_i as variables and equation (13) leads to the system of linear equations from which we can compute coefficients if exist.

Note also that $1\in I$ if and only if $(z_1\ldots z_4)^\alpha$ for some $\alpha\in\mathbb{N}$ belongs to the ideal generated by the polynomials $H_1,H_2,F_i,F_{i+1},G_j,G_{j+1}$, because if $1\in I$, then writing 1 as in (13) for some polynomials w_i, and multiplying this equation by suitable power $(z_1\ldots z_4)^\alpha$ we obtain that this power belong to the second ideal, and conversely.

Completeness of two addition formulas on twisted Edwards curves. We will apply the above method to check completeness of two addition formulas (10) on twisted Edwards curves over any field K of $\mathrm{char}(K)\neq 2$, and any non-zero different $a,d\in K$. First we assume that coefficients a,d are variables over $\mathbb{Q}$, so the twisted Edwards curve $E_{a,d}$ is defined over the field of rational functions $\mathbb{Q}(a,d)$ by the equation

$$H=aX^2T^2+Y^2Z^2=T^2Z^2+dX^2Y^2=0. \tag{14}$$

Let $H_i=H(X_i,Z_i,Y_i,T_i)$ for $i=1,2$. The product $V=E\times E\subset(\mathbb{P}^1)^4$ is given by the equations $H_1=H_2=0$. Let $F,G:E\times E\to E$ be the first and second addition formula (10), and let $F=((F_1:F_2),(F_3:F_4))$, $G=((G_1:G_2),(G_3:G_4))$, where

$$\begin{aligned} F_1&=X_1Y_2Z_2T_1+X_2Y_1Z_1T_2,\\ F_2&=Z_1Z_2T_1T_2+dX_1X_2Y_1Y_2,\\ F_3&=Y_1Y_2Z_1Z_2-aX_1X_2T_1T_2,\\ F_4&=Z_1Z_2T_1T_2-dX_1X_2Y_1Y_2, \end{aligned} \tag{15}$$

and

$$\begin{aligned} G_1&=X_1Y_1Z_2T_2+X_2Y_2Z_1T_1,\\ G_2&=aX_1X_2T_1T_2+Y_1Y_2Z_1Z_2,\\ G_3&=X_1Y_1Z_2T_2-X_2Y_2Z_1T_1,\\ G_4&=X_1Y_2Z_2T_1-X_2Y_1Z_1T_2. \end{aligned} \tag{16}$$

As above let z_i for $i=1,\ldots,4$ be one of the coordinates on the ith copy of $\mathbb{P}^1$ in the product $(\mathbb{P}^1)^4$. Choosing all combinations of z_i for $i=1,\ldots,4$ and substituting $z_i=1$ for $i=1,\ldots,4$ to polynomials in (11) with above F_i,G_i, we want to show that $1\in I$ for ideal I generated by polynomials in (12). The program below in Magma checks that $1\in I$ and determines polynomials $w_i\in\mathbb{Q}(a,b)[x_1,x_2,x_3,x_4]$ such that (13) is satisfied.

Assume that we want to reduce this equation mod p for prime $p\neq 2$. It turns out that polynomials w_i can be reduced mod p, i.e., reducing coefficients of w_i we never get zero in denominator. The program below checks this. First taking all denominators of coefficients of polynomials w_i, the program below computes the least common multiplicity of these denominators, and it turns out that lcm always divides $a^2d^3(a-d)$, this is the lcm over $\mathbb{Q}[a,b]$. It turns also that all coefficients in the denominator of coefficients of w_i are equal ±1. All coefficients in the numerator of coefficients of w_i have denominators at most 2. Thus all coefficients can be reduced mod $p\neq 2$. Thus if $a',d'\in K^*$ are different and $\mathrm{char}(K)\neq 2$, then substituting a',d' to $E_{a,d}$, formulas F,G and coefficients of w_i we obtain that denominators of coefficients of w_i are non-zero and (13) holds for the curve $E_{a',d'}$ over K.

Below we give a Magma code to check completeness of addition formulas on twisted Edwards curves in the above way (which can be performed in Magma calculator `http://magma.maths.usyd.edu.au/calc/`).

During computation 64 systems of equations (13) were considered. Below we give one example of a system obtained during computations.

```
Q:=Rationals();
Z:=Integers();
R<a,d>:=FunctionField(Q,2);
pF<X1,Z1,Y1,T1,X2,Z2,Y2,T2>:=
PolynomialRing(R,8);
pF4<x1,x2,x3,x4>:=PolynomialRing(R,4);

x:=[x1,x2,x3,x4];

// Twisted Edwards curve equations
H1:=a*X1^2*T1^2+Y1^2*Z1^2
-Z1^2*T1^2-d*X1^2*Y1^2;
H2:=a*X2^2*T2^2+Y2^2*Z2^2
-Z2^2*T2^2-d*X2^2*Y2^2;

// Addition formula F = (F12 , F34)
// F12 = (F1 : F2)
F12:=[X1*Y2*Z2*T1+X2*Y1*Z1*T2,
Z1*Z2*T1*T2+d*X1*X2*Y1*Y2];
// F34 = (F3 : F4)
F34:=[Y1*Y2*Z1*Z2-a*X1*X2*T1*T2,
Z1*Z2*T1*T2-d*X1*X2*Y1*Y2];

// Addition formula G = (G12 , G34)
// G12 = (G1 : G2)
G12:=[X1*Y1*Z2*T2+X2*Y2*Z1*T1,
a*X1*X2*T1*T2+Y1*Y2*Z1*Z2];
// G34 = (G3 : G4)
G34:= [X1*Y1*Z2*T2-X2*Y2*Z1*T1,
X1*Y2*Z2*T1-X2*Y1*Z1*T2];

F:=[F12,F34]; G:=[G12,G34];

for A in F do
   for B in G do
       S:= A cat B cat [H1,H2];
    for s in  CartesianPower({0,1},4) do
         sq:=[];
       for i in [1..4] do
          if s[i] eq 0 then
             sq:=sq cat [1,x[i]];
          else
             sq:= sq cat [x[i],1];
          end if;
        end for;
      U:=[];
      for f in S do
        U:=U cat [pF4!Evaluate(f,sq)];
      end for;
      I:=IdealWithFixedBasis(U);
      1 in I; cg:=[];
      C:=Coordinates(I,pF4!1);
      for g in C do
        cg:=cg cat Coefficients(g);
      end for;

   D:=[]; N:=[]; cD:=[];  cN:=[];

    for u in cg do
      D:=D cat [Denominator(u)];
      N:=N cat [Numerator(u)];
      cD:= cD cat Coefficients(Denominator(u));
      cN:= cN cat Coefficients(Numerator(u));
    end for;
    dcN:=[];
    for i in cN do dcN:= dcN cat [Denominator(i)]
    end for;
    dcD:=[]; ncD:=[];
    for i in cD do dcD:= dcD cat [Denominator(i)]
                   ncD:= ncD cat [Numerator(i)];
    end for;
  Factorization(Lcm(D)); Lcm(dcD); Lcm(ncD);
  Lcm(dcN);
 end for;
end for;
end for;
```

The following example gives polynomial computed by the above algorithm in one of the 64 cases.

Example 1. Let $z_1 = x_1$, $z_2 = x_2$, $z_3 = x_3$ and $z_4 = y_4$. Substituting $z_i = 1$ for $i = 1, \ldots, 4$ leads to the following formulas for the twisted Edwards curves

$$\begin{aligned} H_1((1:Z_1),(1:T_1)) &= -Z_1^2T_1^2 + aT_1^2 + Z_1^2 - d = 0 \\ H_2(((1:Z_2),(Y_2:1))) &= Z_2^2Y_2^2 - dY_2^2 - Z_2^2 + a = 0 \end{aligned} \tag{17}$$

and addition formulas

$$\begin{aligned} F_1(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= T_1Z_2Y_2 + Z_1 \\ F_2(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= Z_1T_1Z_2 + dY_2 \\ F_3(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= Z_1Z_2Y_2 - aT_1 \\ F_4(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= Z_1T_1Z_2 - dY_2 \\ G_1(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= TZ_1T_1Y_2 + Z_2 \\ G_2(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= Z_1Z_2Y_2 + aT_1 \\ G_3(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= -Z_1T_1Y_2 + Z_2 \\ G_4(((1:Z_1),(1:T_1)),((1:Z_2),(Y_2:1))) &= -Z_1T_1Y_2 + Z_2 \end{aligned} \tag{18}$$

The system of equations (13) for $i = 1$ and $j = 1$ in affine space $\overline{K}^4$ has a form

$$\begin{cases} h_1 &= -y_1^2y_2^2 + ay_2^2 + y_1^2 - d = 0 \\ h_2 &= y_3^2x_4^2 - dx_4^2 - y_3^2 + a = 0 \\ f_1 &= y_2y_3x_4 + y_1 = 0 \\ f_2 &= y_1y_2y_3 + dx_4 = 0 \\ g_1 &= y_1y_2x_4 + y_3 = 0 \\ g_2 &= y_1y_3x_4 + ay_2 = 0 \end{cases} \tag{19}$$

The ideal I generated by polynomials $h_1, h_2, f_1, f_2, g_1, g_2$ contains 1 (the system has no solutions). Now we can write

$$1 = w_1h_1 + w_2h_2 + w_3f_1 + w_4f_2 + w_5g_1 + w_6g_2$$

where

$$w_i = \frac{v_i}{2(a^2d^2 - ad^3)}, \quad i \in \{1, \ldots, 6\}$$

and

$$\begin{aligned}
v_1 &= -dy_2^2y_3^4 + 2ady_2^2y_3^2 - 2ady_3^2 + 2d^2y_3^2\\
v_2 &= -ady_2^4y_3^2 + ady_2^2y_3^2 + d^2y_2^2y_3^2 + 2ad^2 - 2d^3\\
v_3 &= -ay_1y_2^4y_3^4 + ady_1y_2^4y_3^2 + ay_1y_2^2y_3^4 + dy_1y_2^2y_3^4 -\\
&\quad - 2ady_1y_2^2y_3^2 + 2ady_1y_3^2 - 2d^2y_1y_3^2\\
v_4 &= ay_2^4y_3^4x_4 - ady_2^4y_3^2x_4 + ay_1y_2^3y_3^3 - dy_1y_2^3y_3^3 -\\
&\quad - ay_2^2y_3^4x_4 - dy_2^2y_3^4x_4 + ady_1y_2^3y_3 + ady_2^2y_3^2x_4 +\\
&\quad + d^2y_2^2y_3^2x_4 - ay_1y_2y_3^3 - 2ady_1y_2y_3 + 2d^2y_1y_2y_3 -\\
&\quad - 2ady_3^2x_4 + 2d^2y_3^2x_4 + 2ad^2x_4 - 2d^3x_4\\
v_5 &= ady_2^2y_3^3 - ad^2y_2^2y_3\\
v_6 &= -ady_2^3y_3^2 + ady_2y_3^2
\end{aligned}$$

Denominator of w_i is zero if $a = 0$ or $b = 0$ or $a = b$ or $\mathrm{char}(K) = 2$.

IV. Determining space of addition laws of a given degree

Given an elliptic curve E together with an addition formula we want to describe the space of addition formulas of given degree if is non-zero (see also [25]). For simplicity we assume that E is contained in $\mathbb{P}^2$ and we are given an addition formula $A : E \times E \to E$, but a similar method can be used for elliptic curves in $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2}$. Let (X, Y), where $X = (X_0 : X_1 : X_2), Y = (Y_0 : Y_1 : Y_2)$, be homogeneous coordinates on $\mathbb{P}^2 \times \mathbb{P}^2$. Let $A = (a_1/a_0, a_2/a_0)$ be given on the affine open subsets $X_0 \neq 0, Y_0 \neq 0$ in $\mathbb{P}^2 \times \mathbb{P}^2$ and $X_0 \neq 0$ in $\mathbb{P}^2$, where $a_0, a_1, a_2 \in K[x_1, x_2, y_1, y_2]$ and $x_i = X_i/X_0, y_i = Y_i/Y_0$ for $i = 1, 2$. For a given bidegree (n, m) let $\mathcal{F}$ be the set of addition laws $(F_0 : F_1 : F_2) : E \times E \to E$ such that each F_i is homogeneous in variables X and Y of degrees $\deg_X F_i = n$ and $\deg_Y F_i = m$, respectively. Then $\mathcal{F} \cup \{0\}$ is a vector space over K in the usual way

$$\begin{aligned}
&\lambda(F_0 : F_1 : F_2) + \mu(G_0 : G_1 : G_2)\\
&= (\lambda F_0 + \mu G_0 : \lambda F_1 + \mu G_1 : \lambda F_2 + \mu G_2)
\end{aligned}$$

for $\lambda, \mu \in K$. Assuming the $\mathcal{F}$ is non-empty our goal is to determine all coefficients $\lambda_{k\,\alpha\,\beta} \in K$ such that $(F_0 : F_1 : F_2)$ belongs to $\mathcal{F}$ for $F_k = \sum_{|\,\alpha\,|=n, |\,\beta\,|=m} \lambda_{k\,\alpha\,\beta} X^\alpha Y^\beta$ and $k = 0, 1, 2$, where $\alpha = (\alpha_0, \alpha_1, \alpha_2)$, $X^\alpha = X_0^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2}$, $|\,\alpha\,| = \alpha_0 + \alpha_1 + \alpha_2$ similarly for β. Substituting $X_0 = Y_0 = 1$ and x_i, y_i to F_k for $i = 1, 2$ we have $f_k = F_k(1, x_1, x_2, 1, y_1, y_2)$, where $\deg_{(x_1,x_2)} f_k \leq n$ and $\deg_{(y_1,y_2)} f_k \leq m$. We want to determine coefficients $\lambda_{k\,\alpha\,\beta}$ such that we get addition formula on E, so $\frac{a_i}{a_0} = \frac{f_i}{f_0}$ for $i = 1, 2$, thus $v_i = a_i f_0 - f_i a_0$ belongs to the ideal $I = (h_1, h_2)$ of $E \times E$, where $h = 0$ is an equation of E in the affine part $X_0 \neq 0$, and $h_1 = h(x_1, x_2)$, $h_2 = h(y_1, y_2)$. So we want to determine $\lambda_{k\,\alpha\,\beta} \in K$ such that $v_i \in I$ for $i = 1, 2$. This the ideal membership problem $v_i \in I \iff N(v_i, Gr) = 0$ for $i = 1, 2$, where $N(w_i, Gr)$ is the normal form of w_i with respect to a Gröbner basis Gr of I (see [1], [13]). Since the coefficients $\lambda_{k\,\alpha\,\beta}$ are in the first power in v_i and a Gröbner basis Gr of I do not depend on $\lambda_{k\,\alpha\,\beta}$, computing the normal form $N(v_i, Gr)$, which is the remainder of division of v_i by Gr, the coefficients $\lambda_{k\,\alpha\,\beta}$ in $N(v_i, Gr)$ also appear in degree 1. Thus the coefficients of $N(v_i, Gr)$ are linear in $\lambda_{k\,\alpha\,\beta}$, and to determine when $N(v_i, Gr) = 0$, we can solve a system of linear equations with $\lambda_{k\,\alpha\,\beta}$. Note that a similar method was applied in [15] to determine formulas used in point compression.

V. Conclusion

In this paper we gave a simple method of verification of completeness of a system of two addition formulas on twisted Edwards curves over any field K of $\mathrm{char}(K) \neq 2$ using program written in Magma, which checks that some systems of polynomial equations over algebraic closure of rational function field $\mathbb{Q}(a, d)$ do not have solutions and that some obtained formulas may reduced mod any prime $p \neq 2$ and evaluated at any values $a, d \in K$ allowed in the equation of twisted Edwards curve $E_{a,d}$. This approach may also be useful to study completeness of addition formulas on other models of elliptic curves. We also described method based on Gröbner bases, which may be useful to obtain space of addition formulas of given degree.

References

[1] W. W. Adams, P. Loustaunau, An introduction to Gröbner bases (No. 3). American Mathematical Soc. (1994)

[2] Arene, C., Lange, T., Naehrig, M., & Ritzenthaler, C. Faster computation of the Tate pairing. Journal of number theory, 131(5), 842-857 (2011).

[3] Atkin, A. O. L., Morain, F. Elliptic curves and primality proving. Mathematics of computation, 61(203), 29-68 (1993).

[4] Bernstein, D., Birkner, P., Lange, T., & Peters, C. ECM using Edwards curves. Mathematics of Computation, 82(282), 1139-1179 (2013).

[5] D. Bernstein, P. Birkner, M. Joye, T. Lange and Ch. Peters, "Twisted Edwards curves", In: Progress in Cryptology-AFRICACRYPT 2008, Springer, 2008, pp. 389-405.

[6] Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., & Yang, B. Y. High-speed high-security signatures. Journal of cryptographic engineering, 2(2), 77-89 (2012).

[7] D. Bernstein and T. Lange, "Faster addition and doubling on elliptic curves", In: Advances in cryptology-ASIACRYPT 2007, Springer, 2007, pp. 29-50.

[8] Bernstein, D. J., Chuengsatiansup, C., Kohel, D., & Lange, T. Twisted hessian curves. In International Conference on Cryptology and Information Security in Latin America (pp. 269-294). Springer, Cham (2015).

[9] D. Bernstein and T. Lange, "A complete set of addition laws for incomplete Edwards curves". Journal of Number Theory, 131(5), pp. 858-872 (2011).

[10] O. Billet and M. Joye, "The Jacobi model of an elliptic curve and side-channel analysis", In: AAECC-15 Conference Proceedings, Lecture Notes in Computer Science, vol. 2643, Springer, 2003, pp. 34-42.

[11] Bosma, W., & Lenstra, H. W. Complete systems of two addition laws for elliptic curves. Journal of Number theory, 53(2), 229-240 (1995).

[12] W. Castryck anf F. Vercauteren, "Toric forms of elliptic curves and their arithmetic", Journal of Symbolic Computation, vol. 46, issue 8, (2011), Elsevier, 2011, pp. 943-966.

[13] D. Cox, J. Little, D. O'shea, Ideals, varieties, and algorithms (Vol. 3). New York: Springer (1992)

[14] De Feo, L., Jao, D., & Plût, J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, 8(3), 209-247 (2014).

[15] Dryło, R., Kijko, T., & Wroński, M. Determining Formulas Related to Point Compression on Alternative Models of Elliptic Curves. Fundamenta Informaticae, 169(4), 285-294 (2019).

[16] Farashahi, R. R., & Joye, M. Efficient arithmetic on Hessian curves. In International Workshop on Public Key Cryptography (pp. 243-260). Springer, Berlin, Heidelberg (2010).

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

[18] Eicher, J., & Opoku, Y. Using the Quantum Computer to Break Elliptic Curve Cryptosystems (1997).
[19] R. Farashahi and M. Joye, "Efficient Arithmetic on Hessian Curves", Lecture Notes in Computer Science, vol. 6056, Springer, 2010, pp. 243-260.
[20] R. Farashahi and S. Hosseini, "Differential Addition on Twisted Edwards Curves", In: ACISP 2017: Information Security and Privacy, Lecture Notes in Computer Science, vol. 10343, Springer, 2017, pp. 366-378.
[21] Hisil, H., Wong, K. K. H., Carter, G., & Dawson, E. Faster group operations on elliptic curves. In Information Security 2009: proceedings of the 7th Australasian Information Security Conference (Vol. 98, pp. 11-19). CRPIT/Springer (2009).
[22] Hisil, H., Wong, K. K. H., Carter, G., & Dawson, E. Jacobi quartic curves revisited. In Australasian Conference on Information Security and Privacy (pp. 452-468). Springer, Berlin, Heidelberg (2009).
[23] Hisil, H., Wong, K. K. H., Carter, G., & Dawson, E. Twisted Edwards curves revisited. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 326-343). Springer, Berlin, Heidelberg (2008).
[24] Joye, M., Tibouchi, M., & Vergnaud, D. Huff's model for elliptic curves. In International Algorithmic Number Theory Symposium (pp. 234-250). Springer, Berlin, Heidelberg (2010).
[25] Kohel, D. Addition law structure of elliptic curves. Journal of Number Theory, 131(5), 894-919 (2011).
[26] Lenstra Jr, H. W. Factoring integers with elliptic curves. Annals of mathematics, 649-673 (1987).
[27] Moody, D., & Shumow, D. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, 85(300), 1929-1951 (2016).
[28] Rostovtsev, A., & Stolbunov, A. Public-Key Cryptosystem Based on Isogenies. IACR Cryptology ePrint Archive, 145 (2006).
[29] Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee (1994, November).