arXiv:2111.04533v2 [cs.CR] 13 Jan 2022

High-degree Compression Functions on Alternative Models of Elliptic Curves and their Applications

Michał Wroński[*]**, Tomasz Kijko, Robert Dryło**

Faculty of Cybernetics

Military University of Technology in Warsaw

Kaliskiego 2, 00-908 Warsaw, Poland

{*michal.wronski, tomasz.kijko, robert.drylo*}*@wat.edu.pl*

Abstract. This paper presents method for obtaining high-degree compression functions using natural symmetries in a given model of an elliptic curve. Such symmetries may be found using symmetry of involution $[-1]$ and symmetry of translation morphism $\tau_T = P + T$, where T is the n-torsion point which naturally belongs to the $E(\mathbb{K})$ for a given elliptic curve model. We will study alternative models of elliptic curves with points of order 2 and 4, and specifically Huff's curves and the Hessian family of elliptic curves (like Hessian, twisted Hessian and generalized Hessian curves) with a point of order 3. We bring up some known compression functions on those models and present new ones as well. For (almost) every presented compression function, differential addition and point doubling formulas are shown. As in the case of high-degree compression functions manual investigation of differential addition and doubling formulas is very difficult, we came up with a Magma program which relies on the Gröbner basis. We prove that if for a model E of an elliptic curve exists an isomorphism $\phi : E \to E_M$, where E_M is the Montgomery curve and for any $P \in E(\mathbb{K})$ holds that $\phi(P) = (\phi_x(P), \phi_y(P))$, then for a model E one may find compression function of degree 2. Moreover, one may find, defined for this compression function, differential addition and doubling formulas of the same efficiency as Montgomery's. However, it seems that for the family of elliptic curves having a natural point of order 3, compression functions of the same efficiency do not exist.

---

[*]Address for correspondence: Kaliskiego 2, 00-908 Warsaw, Poland.

1.   Introduction

Elliptic curve cryptography has been evolving over the years. Classical elliptic curve cryptography (ECC) algorithms, such as ECDH, have been replaced by the isogeny-based cryptography algorithms, such as SIDH [1], SIKE [2] and CSIDH [3]. Isogeny-based cryptography is believed to be resistant to attacks by quantum computers, unlike classical solutions. It is worth noteing, that although many current ECC notions differ from those relied upon years ago, x-line arithmetic proposed by Peter L. Montgomery in [4] is still widely used, especially in isogeny-based cryptography. For example, in SIKE reference implementation, x-line arithmetic on Montgomery curves is applied, using XZ coordinates.

Over the last 20 years, numerous alternative elliptic curves models have been proposed, e.g. Edwards [5], [6], twisted Edwards [7], Hessian [8], twisted Hessian [9], generalized Hessian [10], Huff's and generalized Huff's [11] curves, and many others. However, efficient x-line arithmetic has not been proposed for all of these alternative elliptic curves models.

The more general concept of x-line arithmetic, especially in application to elliptic curves cryptography is compression function, which is described in details in Section 2. In general, compression functions are well-known methods of obtaining shorter representation of elements used in many cryptographic applications. The basic example is representation of point on Weierstrass curve or Montgomery curve using only its x-coordinate. What is important, this concept may be extended to other, alternative models of elliptic curves, as same as for representation of finite fields elements. It is worth noting that in XTR [12] algorithm, instead of using full representation of element $h \in \mathbb{F}_{p^6}$ from subgroup of order $p^2 - p + 1$, it is enough to use the trace $Tr(h)$ which is defined over $\mathbb{F}_{p^2}$. Nowadays, the most important application of compression functions is using them in isogeny-based cryptography, especially in SIDH [13], SIKE [14], application of Velusqrt [15] method to CSIDH, CSURF and other algorithms.

The role that symmetries on elliptic curves play in the efficiency of their arithmetics has been widely discussed e.g. in [16] and [17]. Kohel noticed in [17] that symmetries obtained by an automorphism group $\{[\pm 1]\}$ and translation by the specific points of proper order have impact on the efficiency of addition law. He gave Hessian and Edwards curves as the most representative examples here.

In [17], Kohel was studying symmetric quartic models over binary fields with a rational 4-torsion point T. According to [17], a genus 1 curve admits translations by rational points and translation morphism $\tau_T = P + T$ on curve E is projectively linear (induced by a linear transformation of the ambient projective space), iff E is a degree n model determined by a complete linear system in $\mathbb{P}^{n-1}$ and T is in the n-torsion subgroup.

In this paper, we use these ideas to identify new compression functions of high degree (> 2) especially for Huff's curves, generalized Hessian and Hessian curves. The compression functions for which we are looking are invariant on the action of involution and translation by specific point T of order n, meaning that for compression function of degree $f_{2n}(P) = f_{2n}(Q)$ holds iff $Q = \pm P + [k]T$, for $k = \overline{0, n-1}$.

In the case of Huff's curves, where $E_{Hu}/\mathbb{K} : ax(y^2 - 1) = by(x^2 - 1)$, we will study their arithmetics using a high-degree point compression. Compression function f of order 4 is obtained by using symmetry given by point $(a : b : 0)$ of order 2. A compression function of order 8 is obtained

by using symmetry given by three points of order 2: $(a : b : 0), (1 : 0 : 0)$ and $(0 : 1 : 0)$. Finally, a compression function of degree 16 is obtained by using three 2-torsion points $(a : b : 0), (1 : 0 : 0)$ and $(0 : 1 : 0)$, as well as one point of order 4 of the form $(\pm 1 : \pm 1 : 1)$. Let us note that compression functions of different degrees were obtained by Farashahi and Hosseini in [18], where also translations τ_T by a proper point of order 2 and 4 were used in the case of twisted Edwards curves.

In the case of generalized Hessian curves, given by $E_{GH} : x^3 + y^3 + a = dxy$, we will study the arithmetics of these curves using a point compression of degree 6, with this compression function obtained by using symmetry given by a 3-torsion point $(1 : -\omega : 0)$.

In the case of Hessian curves, given by $E_{GH} : x^3 + y^3 + 1 = dxy$, we will study the arithmetics of these curves using a point compression of degree 18, with this compression function obtained by using symmetry given by two 3-torsion points $(1 : -\omega : 0)$ and $(-\omega : 0 : 1)$. More details about this approach will be presented in subsection 4.3.

In [19] a method for automating the process of searching for doubling and differential addition formulas for compression functions of order 2 is presented. This method uses the Gröbner basis mechanism. Because in the case of high-degree compression functions manual investigations identyfying differential and doubling formulas are very difficult, we modified the ideas from [19] and implemented a Magma program, which may be used to search for differential addition and doubling formulas also in the case of compression functions of a degree higher than 2. The method of searching for convenient formulas may be very memory-consuming. It was necessary to use a computer with 384 GB of RAM to find such a formula in some cases.

Finally, we prove that if for a model E of an elliptic curve exists an isomorphism $\phi : E \to E_M$, where E_M is the Montgomery curve and for any $P \in E(\mathbb{K})$ holds that $\phi(P) = (\phi_x(P), \phi_y(P))$, then for a model E one may find a compression function of degree 2 and, defined for this compression function, differential addition and doubling formulas, respectively, A and D of the same efficiency (in the whole paper, by the efficiency, we mean computational efficiency, which is the required number of elementary operations) as Montgomery's. However, such compression functions of degree 2 may be sometimes complicated, as same as constants appearing in differential addition and doubling formulas and therefore may be not optimal for all applications.

Basing on this theorem we also affirm, that for a family of elliptic curves having natural point of order 3, e.g. Hessian, twisted Hessian and generalized Hessian curves, obtaining formulas of the same or similar efficiency as for the Montgomery curve is impossible, because there do not exist natural isomorphisms from these curves to the Montgomery curve.

2. Compression functions

In this section we provide basic facts on doubling, differential addition and point recovery. We also describe a method based on the Gröbner bases from [19], with modifications for searching for formulas concerning high-degree compression functions. This method was used, in Magma, to search for the formulas given in the following sections (for an introduction to the Gröbner bases theory, see [20] or [21]).

Peter Montgomery [4] gave some efficient and simple formulas for point doubling and differential addition after compression on elliptic curves $By^2 = x^3 + Ax^2 + x$. These formulas may be given for

any model of an elliptic curve. Let E be an elliptic curve over a field $\mathbb{K}$. In such a case a function $f : E \to \mathbb{K}$ for which holds that $f(P) = f(Q)$ iff $Q = \pm P$ for all $P \in E$ is called a degree 2 compression function. We have induced point multiplication of values $f(P)$ given by $[n]f(P) = f([n]P)$ for $n \in \mathbb{Z}$. There exist rational functions doubling $D(x) \in \mathbb{K}(x)$ and differential additions $A_1(x,y), A_2(x,y) \in \mathbb{K}(x,y)$ after compression such that

$$f([2]P) = D(f(P)), \tag{1}$$

$$f(P+Q) + f(P-Q) = A_1(f(P), f(Q)), \tag{2}$$

$$f(P+Q)f(P-Q) = A_2(f(P), f(Q)). \tag{3}$$

These properties allow to compute, after compression, $[n]f(P)$ using the Montgomery ladder algorithm. We may adopt $A(x,y,z) = A_1(x,y)) - z$ or $A(x,y,z) = A_2(x,y)/z$ in this algorithm.

Algorithm 1: The Montgomery ladder

Input: $f(P)$ and the binary expansion of $n = (n_k, \ldots, n_0)_2$
Output: $[n]f(P)$
$x_1 := f(P); x_2 := [2]x_1;$
for $i = k - 1, \ldots, 0$ **do**
    if $n_i = 1$ **then**
        $x_1 := A(x_1, x_2, f(P));$
        $x_2 := D(x_2);$
    else
        $x_2 := A(x_1, x_2, f(P));$
        $x_1 := D(x_1);$
    end
end
return x_1;

Formulas for doubling and differential addition were given for standard models of elliptic curves: Montgomery, Weierstrass, Edwards, Hessian, Jacobi quartic, and Huff's curves.

One may also consider compressions of higher degrees. In general, the degree of compression function g is the number of different elements $Q = \pm P + [k]T$, for $k = \overline{0, n-1}$ and T being point of order n, for which equation $g(P) = g(Q)$ holds for every $P \in E(\mathbb{K}) \setminus S$. Set S contains points of order 2 and points of order n from subgroup $\langle T \rangle$. In this case the degree of compression function g is equal to $2n$. It is worth noting that the degree of compression function is always even.

For a function $g : E \to \mathbb{K}$, there exist rational functions $D(x) \in \mathbb{K}(x)$ and $A(x,y,z) \in \mathbb{K}(x,y,z)$ such that $g([2]P) = D(g(P))$ and $g(P+Q) = A(g(P), g(Q), g(P-Q))$ for generic points on E, then we have induced multiplication $[n]g(P) = g([n]P)$ for $n \in \mathbb{N}$ which may be computed using the Montgomery ladder algorithm (see also [10, Sec.5.4]). Note that multiplication $[n]g(P) = g([n]P)$ is independent of choosing a point P which may be checked by induction on n. Let $g(P) = g(P')$. For doubling, we have $g([2]P) = D(g(P)) = D(g(P')) = g([2]P')$. Let us assume that for each $0 \leq k \leq n$ we have $g([k]P) = g([k]P')$, then we have $g([n+1]P) = A(g([n]P), g(P), g([n-1]P)) = A(g([n]P'), g(P'), g([n-1]P')) = g([n+1]P')$.

In section 2.2, we remind, from [19], a method (with some modifications) used to search for functions D, A_1, A_2 for compressions g of degrees ≥ 2, which method was used in [19] for compressions of degree 2.

Compressions of higher degrees were given for Edwards [18] and Jacobi quartic [22] curves. Natural examples of low-order subgroups are known for Edwards, Hessian, Huff's, and Jacobi quartic elliptic curves. Given a subgroup G in the generic model of an elliptic curve, one may try to obtain compression g of degree $2|G|$ such that $g(\pm P + G) = g(P)$ for each $P \in E$.

Now will be presented approach to searching for compression functions of degree > 2.

2.1. Compression functions of high degree using symmetries on elliptic curves

In this subsection a method for obtaining compression functions of high degree using natural symmetries on a given model of an elliptic curve will be presented.

At first, let us consider translation $\tau_T : E \to E, \tau_T(P) = P + T$ for a certain chosen point $T \in E(\mathbb{K})$ of order n. We will be searching for the compression function f_{2n} of degree $2n$ which is invariant under involution and translation by T. This means that $f_{2n}(P) = f_{2n}(Q)$ iff $Q = \pm P + [k]T$, for $k = \overline{0, n-1}$.

Proposition 1. Let us note, that such a function may be easily found for a certain model E of an elliptic curve if three conditions hold:

- involution $[-1]P$ is projectively linear, which means that if $P = (X : Y : Z)$, then $[-1]P = (\alpha_1 X + \beta_1 Y + \gamma_1 Z : \alpha_2 X + \beta_2 Y + \gamma_2 Z : \alpha_3 X + \beta_3 Y + \gamma_3 Z)$ for some constant $\alpha_i, \beta_i, \gamma_i \in \mathbb{K}, i = \overline{1, 3}$,

- point T of order n naturally belongs to $E(\mathbb{K})$,

- translation $\tau_T : E \to E : \tau(P) = P + T$ is also projectively linear.

This approach, using symmetries of involution and translation, will be used for obtaining efficient compression functions on Edwards, Huff's and Hessian family of elliptic curves in section 4.

Remark 2. Using the approach presented in Proposition 1, the process of searching for a compression function of a high degree should consist of the following steps:

1. at first, use the point addition formula and find equations for $\tau_T = P + T$, where $T \in E(\mathbb{K})$ is point of order n and P is any point in $E(\mathbb{K})$,

2. check if equation for τ_T is projectively linear,

3. let us try to find a compression function of degree $2n$ using the character of τ_T.

Remark 3. Let us know that if on an elliptic curve E there is a point $T \in E(\mathbb{K})$ of order n, then one can always construct compression function of degree $2n$ [23]. It is possible by constructing an isogeny $\psi : E \to E/\langle nT \rangle$. Then a compression function of degree $2n$ may be obtained using a compression function of degree 2 and finally $f_{2n}(P) = f_2(\psi(P))$. Even though, compression functions of degree $2n$ constructed in this way may be not so efficient.

2.2.   Algorithms to determine formulas used in the compression

In the case of function $g : E \to K$, formulas (1), (2), (3) may be searched for using the method from [19], with some small modifications. Assume for simplicity that E is contained in $\mathbb{P}^2$ and is given by the equation $E : w(x, y) = 0$ in K^2 for $w(x, y) \in K[x, y]$.

Let us assume that we indent to check if there exists a formula for doubling $D \in K(x)$ satisfying

$$D(g(x, y)) = g([2](x, y)) \tag{4}$$

on E, where $D(x) = \frac{D_1(x)}{D_2(x)}$, $D_1, D_2 \in K[x]$ are polynomials of degrees d_1, d_2 at most, respectively, for fixed bounds d_i. Let $D_1 = \sum_{\alpha \leq d_1} a_\alpha x^\alpha$ and $D_2 = \sum_{\beta \leq d_2} b_\beta x^\beta$, with unknown coefficients a_α, b_β. We may write $D(g(x, y)) = \frac{v_1(x, y)}{v_2(x, y)}$, where v_1, v_2 are polynomials in x, y, whose coefficients contain a_α, b_β of degree one. Writing $g([2](x, y)) = \frac{u_1(x, y)}{u_2(x, y)}$, where $u_1, u_2 \in K[x, y]$, we intend to determine the values of a_α, b_β such that $v_1 u_2 - v_2 u_1 \in (w)$, which is equivalent to (4). Since $v_1 u_2 - v_2 u_1$ contains a_α, b_β of degree one, the normal form $N(v_1 u_2 - v_2 u_1)$ with respect to the ideal (w) contains a_α, b_β also of degree one. Hence, in order to determine a_α, b_β for which $N(v_1 u_2 - v_2 u_1) = 0$, we need to solve a system of linear equations when coefficients depending on a_α, b_β of the normal form are zero.

Let us assume that we intend to determine a function $A_2(x, y) \in K(x, y)$ such that

$$g((x_1, y_1) + (x_1, y_1))g((x_1, y_1) - (x_2, y_2)) = A_2(g(x_1, y_1), g(x_2, y_2)) \tag{5}$$

on $E \times E$. Let $w_i = w(x_i, y_i)$ for $i = 1, 2$. Let $A_2 = \frac{u_1(x, y)}{u_2(x, y)}$, where $u_1 = \sum_{|\alpha| \leq d_1} a_\alpha x^{\alpha_1} y^{\alpha_2}$, $\alpha = (\alpha_1, \alpha_2) \in \mathbb{N}^2$, $|\alpha| = \alpha_1 + \alpha_2$, and, similarly $u_2 = \sum_{|\beta| \leq d_2} b_\beta x^{\beta_1} y^{\beta_2}$ for given bounds concerning degrees $d_1, d_2 \in \mathbb{N}$.

Similarly as above, we may write $A_2(g(x_1, y_1), g(x_2, y_2)) = \frac{v_1}{v_2}$, where v_1, v_2 are polynomials in x, y, which contain unknown coefficients a_α, b_β of degree at most one. Writing $g((x_1, y_1) + (x_1, y_1))g((x_1, y_1) - (x_2, y_2)) = \frac{g_1}{g_2}$, where $g_1, g_2 \in K[x, y]$ we intend to determine the values of a_α, b_β such that $g_1 v_2 - g_2 v_1$ belongs to the ideal $I = (w_1, w_2)$, so the normal form $N(g_1 v_2 - g_2 v_1)$ with respect to I is equal to 0. Similarly as above, this leads to the system of linear equations with respect to a_α, b_β.

3.   Alternative models of elliptic curves

In this section alternative models of elliptic curves will be briefly discussed.

3.1.   Edwards curves

Definition 4. The Edwards curve E_{Ed} over a field $\mathbb{K}$ is given by the equation [6]

$$E_{Ed}/\mathbb{K} : x^2 + y^2 = 1 + dx^2 y^2, \tag{6}$$

where $d \notin \{0, 1\}$.

The sum of points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E_{Ed} is given by following formula:

$$P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right). \tag{7}$$

The neutral element is $\mathcal{O} = (0, 1)$ and the negation is given by $-(x, y) = (-x, y)$. If d is not a square in $\mathbb{K}$, then the addition formula presented above is complete in the set of $\mathbb{K}$-rational points on E.

3.2. Generalized and twisted Hessian curves

In this section, basic definitions on generalized Hessian and twisted Hessian curves will be presented.

Definition 5. The generalized Hessian curve E_{GH} over a field $\mathbb{K}$ is given by the following equation [10]

$$E_{GH}/\mathbb{K} : x^3 + y^3 + a = dxy, \tag{8}$$

for $a, d \in \mathbb{K}$ where $a \neq 0$ and $d^3 \neq 27a$.

The sum of points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E_{GH} is given by the following unified formula, which works for all inputs of $P, Q \notin T_\zeta$, where $T_\zeta = \{(-\zeta : 0 : 1) | \zeta \in \overline{\mathbb{F}}, \zeta^3 = a\}$:

$$P + Q = \left(\frac{a y_1 - x_2 y_2 x_1^2}{x_1 x_2^2 - y_2 y_1^2}, \frac{x_1 y_1 y_2^2 - a x_2}{x_1 x_2^2 - y_2 y_1^2} \right). \tag{9}$$

Alternatively, the sum of points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E_{GH} is given by the following formulas:

- if $P \neq \pm Q$ (point addition)

$$P + Q = \left(\frac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x_1 y_1}, \frac{x_1^2 y_2 - x_2^2 y_1}{x_2 y_2 - x_1 y_1} \right), \tag{10}$$

- if $P = Q$ (point doubling)

$$[2]P = \left(\frac{y_1(a - x_1^3)}{x_1^3 - y_1^3}, \frac{x_1(y_1^3 - a)}{x_1^3 - y_1^3} \right). \tag{11}$$

The neutral element is a point at infinity $(1 : -1 : 0)$. The negation of the point $P = (x_1, y_1)$ is $-P = (y_1, x_1)$.

Definition 6. The twisted Hessian curve E_{TH} over a field $\mathbb{K}$ is given by the equation [9]

$$E_{TH}/\mathbb{K} : \overline{a} x^3 + \overline{y}^3 + 1 = \overline{d}\, \overline{x}\, \overline{y} \tag{12}$$

for $\overline{a}, \overline{d} \in \mathbb{K}$ where $\overline{a} \neq 0$ and $\overline{d}^3 \neq 27\overline{a}$.

The neutral element of addition law for twisted Hessian curves is the point $(0, -1)$. The negation of the point $\overline{P} = (\overline{x}_1, \overline{y}_1)$ is $-\overline{P} = (\overline{x}_1/\overline{y}_1, 1/\overline{y}_1)$. The sum of points $\overline{P} = (\overline{x}_1, \overline{y}_1)$ and $\overline{Q} = (\overline{x}_2, \overline{y}_2)$ on E_{TH} is given by the following formulas:

- where $\overline{P} \neq \pm\overline{Q}$ (point addition)

$$\overline{P} + \overline{Q} = \left(\frac{\overline{x}_1 - \overline{y}_1^2\overline{x}_2\overline{y}_2}{a\overline{x}_1\overline{y}_1\overline{x}_2^2 - \overline{y}_2}, \frac{\overline{y}_1\overline{y}_2^2 - a\overline{x}_1^2\overline{x}_2}{a\overline{x}_1\overline{y}_1\overline{x}_2^2 - \overline{y}_2} \right) \tag{13}$$

- where $\overline{P} = \overline{Q}$ (point doubling)

$$[2]\overline{P} = \left(\frac{\overline{x}_1 - \overline{y}_1^3\overline{x}_1}{a\overline{y}_1\overline{x}_1^3 - \overline{y}_1}, \frac{\overline{y}_1^3 - a\overline{x}_1^3}{a\overline{y}_1\overline{x}_1^3 - \overline{y}_1} \right). \tag{14}$$

Although the model of twisted Hessian curves seems to be used more frequently, we chose the generalized Hessian curves model. There are two reasons behind such a decision. First of all, there is birationally equivalence between twisted Hessian and generalized Hessian models.

Remark 7. In projective coordinates the generalized Hessian curve is given by the equation

$$E_{GH}/\mathbb{K} \ : \ X^3 + Y^3 + aZ^3 = dXYZ. \tag{15}$$

By swapping X with Z, we get the equation of a twisted Hessian curve in projective coordinates

$$E_{TH} : \overline{a}\overline{X}^3 + \overline{Y}^3 + \overline{Z}^3 = \overline{d}\,\overline{X}\,\overline{Y}\,\overline{Z}, \tag{16}$$

The isomorphism ϕ between E_{GH} and E_{TH}, is given by $\phi : E_{GH} \to E_{TH}, \phi(X : Y : Z) = (Z : Y : X), \overline{a} = a, \overline{d} = d$.

The other reason is that the generalized Hessian curve (in affine model) is symmetrical and the twisted Hessian curve is not. Relying on this fact, it was easier to construct a compression function acting on 3-torsion points in this case.

3.3. Huff's curves

Definition 8. The Huff's curve E_{Hu} over a field $\mathbb{K}$ is given by the equation [11]

$$E_{Hu}/\mathbb{K} \ : \ ax(y^2 - 1) = by(x^2 - 1), \tag{17}$$

where $a^2 \neq b^2$ and $a, b \neq 0$.

The sum of points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E_{Hu} is given by the following complete formula:

$$P + Q = \left(\frac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)}, \frac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \right), \tag{18}$$

Alternatively, to compute $P + Q$, one may use following formulas:

- if $P \neq \pm Q$ (point addition)

$$P + Q = \left(\frac{(x_1 - x_2)(y_1 + y_2)}{(1 - x_1 x_2)(y_1 - y_2)}, \frac{(y_1 - y_2)(x_1 + x_2)}{(1 - y_1 y_2)(x_1 - x_2)} \right), \tag{19}$$

- if $P = Q$ (point doubling)

$$[2]P = \left(\frac{(2y_1^2 + 2)x_1}{(x_1^2 + 1)y_1^2 - x_1^2 - 1}, \frac{(2x_1^2 + 2)y_1}{(x_1^2 - 1)y_1^2 + x_1^2 - 1} \right). \tag{20}$$

Point $O = (0,0)$ is the neutral element, and the opposite point $-(x, y) = (-x, -y)$. In projective coordinates the equation, (17) has a form:

$$E_{Hu}/\mathbb{K} \; : \; aX(Y^2 - Z^2) = bY(X^2 - Z). \tag{21}$$

There are three points at infinity on E_{Hu}: $T_1 = (1 : 0 : 0)$, $T_2 = (0 : 1 : 0)$ and $T_3 = (a : b : 0)$. Points T_1, T_2 and T_3 are of order 2. Additionally there are four points of order 4: $(1 : 1 : 1)$, $(-1 : 1 : 1)$, $(1 : -1 : 1)$ and $(-1 : -1 : 1)$ (e.g. $(1, 1)$, $(-1, 1)$, $(1, -1)$ and $(-1, -1)$ in the affine space).

4. High-degree compression function on alternative models of elliptic curves

In this section we will present compression functions of degree ≥ 2 for Edwards, Huff's and Hessian family of elliptic curves. However, it is worth noting that a compression function of order 4 for Jacobi quartics has been also proposed in [22]. We will mainly focus on compression functions that are new for these models and have not been presented before.

4.1. Edwards curves

4.1.1. Compression function of degree 2

Edwards curves were widely analyzed in the context of their arithmetics using compression functions. The obvious compression function of degree 2 is $f_2(x, y) = y$. The arithmetic using this compresison function may be found, for example, in [24], but we recall this arithmetic below. If $f_2(P) = r_P$ and $f_2(Q) = r_Q$, then the differential addition $f_2(P + Q)f_2(P - Q)$ is given by the following formula:

$$f_2(P + Q)f_2(P - Q) = -\frac{(dr_P^2 - 1)r_Q^2 - r_P^2 + 1}{(dr_P^2 - d)r_Q^2 - dr_P^2 + 1}. \tag{22}$$

The formula for doubling has the following form:

$$f_2([2]P) = -\frac{dr_P^4 - 2r_P^2 + 1}{dr_P^4 - 2dr_P^2 + 1}. \tag{23}$$

Explanation: Formula (22) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.E. Accordingly, formula (23) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.D. □

4.1.2. Compression function of degree 4

We will give an example of a compression function of degree 4 for the Edwards curve $E_{Ed} : x^2 + y^2 = 1 + dx^2y^2$. A compression function of degree 4 may be given by $f_4(x, y) = y^2$. It is easy to show, that f_4 has the degree of 4. At first, let us note, that

- involution $[-1]P$ is projectively linear, because $[-1]P = (-X : Y : Z)$ for $P = (X : Y : Z)$,

- point $T = (0 : -1 : 1)$ of order 2 naturally belongs to $E_{Ed}(\mathbb{K})$,

- translation $\tau_T : E_{Ed} \to E_{Ed} : \tau(P) = P + T$ is also projectively linear, because if $P = (X : Y : Z) \in E_{Ed}(\mathbb{K})$, then $P + (0 : -1 : 1) = (-X : -Y : Z)$.

Let us note that $f_4(P) = f_4(Q)$, iff $Q = \pm P + [k](0 : -1 : 1)$, for $k = \overline{0,1}$ is in set $S = \{(x, y), (-x, y), (x, -y), (-x, -y)\}$, for $P = (x, y)$.

Let us assume that $r = y^2$ for $y \neq 0$. Using this identity in the Edwards curve equation, one may obtain that

$$x^2 + r = 1 + dx^2 r. \tag{24}$$

This means that

$$x^2(rd - 1) - r = 0. \tag{25}$$

Because equation (25) is a polynomial of order 2, it means that one may find two roots of such a polynomial at most. This means, that for every r one has at most 2 distinct values of x. Because on an Edwards curve there are always exactly two points having the same x-coordinate, it means that equation (25) may be satisfied by 4 points at most. All of these points belong to set S, which may be easily checked manually.

Theorem 4.1. A differential addition formula for $f_4(P + Q)f_4(P - Q)$ on an Edwards curve and a compression function $f_4(x, y) = y^2$, where $f_4(P) = r_P$ and $f_4(Q) = r_Q$, is given by:

$$f_4(P + Q)f_4(P - Q) = \tfrac{L}{M}, \tag{26}$$

where

$$
\begin{aligned}
L &= (d^2 r_P{}^2 - 2adr_P + a^2)r_Q{}^2 + (-2adr_P{}^2 + (2ad + 2a^2)r_P - 2a^2)r_Q + a^2 r_P{}^2 - 2a^2 r_P + a^2, \\
M &= (d^2 r_P{}^2 - 2d^2 r_P + d^2)r_Q{}^2 + (-2d^2 r_P{}^2 + (2d^2 + 2ad)r_P - 2ad)r_Q + d^2 r_P{}^2 - 2adr_P + a^2.
\end{aligned} \tag{27}
$$

for every $P \in E_{Ed}(\mathbb{K})$ holds $f(P) = r_P$.

Similarly, doubling is given by

$$f_4([2]P) = \frac{d^2 r_P{}^4 - 4adr_P{}^3 + (2ad + 4a^2)r_P{}^2 - 4a^2 r_P + a^2}{d^2 r_P{}^4 - 4d^2 r_P{}^3 + (4d^2 + 2ad)r_P{}^2 - 4adr_P + a^2}. \tag{28}$$

Explanation: Formula (26) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.F. Accordingly, formula (28) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.E. □

4.1.3. Compression function of degree 8

A compression function of degree 8 on an Edwards curve, was presented by Farashahi and Hosseini in [18]. They gave the example of a compression function dx^2y^2 of degree 8 for the Edwards curve $E_{Ed} : x^2 + y^2 = 1 + dx^2y^2$. Below, we present results for a similar compression function of degree 8 on curve E_{Ed} given by $f_8(x, y) = x^2y^2$. It is easy to show, that f_8 has the degree of 8. At first, let us note, that

- involution $[-1]P$ is projectively linear, because $[-1]P = (-X : Y : Z)$ for $P = (X : Y : Z)$,

- point $T = (1 : 0 : 1)$ of order 4 naturally belongs to $E_{Ed}(\mathbb{K})$,

- translation $\tau_T : E_{Ed} \to E_{Ed} : \tau(P) = P + T$ is also projectively linear, because if $P = (X : Y : Z) \in E_{Ed}(\mathbb{K})$, then $P + (1 : 0 : 1) = (Y : -X : Z)$.

Let us note that $f_8(P) = f_8(Q)$, iff $Q = \pm P + [k](1 : 0 : 1)$, for $k = \overline{0,3}$ is in set $S = \{(x, y), (-x, y), (x, -y), (-x, -y), (y, x), (-y, x), (y, -x), (-y, -x)\}$, for $P = (x, y)$.

Let us assume that $r = x^2y^2$ for $x, y \neq 0$. Using this identity in the Edwards curve equation, one may obtain that

$$x^2 + \frac{r}{x^2} = 1 + dr. \tag{29}$$

This means that

$$x^4 - (dr + 1)x^2 + r = 0. \tag{30}$$

Because equation (30) is a polynomial of order 4, it means that one may find four roots of such a polynomial at most. This means, that for every r one has at most 4 distinct values of x. Because on an Edwards curve there are always at most two points having the same x-coordinate, it means that equation (25) may be satisfied by 4 points at most. All of these points belong to set S, which may be easily checked manually.

Theorem 4.2. A differential addition formula for $f_8(P + Q)f_8(P - Q)$ on an Edwards curve and a compression function $f_8(x, y) = x^2y^2$, where $f_8(P) = r_P$ and $f_8(Q) = r_Q$, is given by:

$$f_8(P + Q)f_8(P - Q) = \frac{(r_P - r_Q)^2}{(d^2 r_P r_Q - 1)^2}. \tag{31}$$

Similarly, doubling is given by

$$f_4([2]P) = \frac{4d^2 r_P^3 + (8d - 16a)r_P^2 + 4x}{d^4 r_P^4 - 2d^2 r_P^2 + 1}. \tag{32}$$

Explanation: Formula (31) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.G. Accordingly, formula (32) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.F.   □

4.2.   Hessian, generalized Hessian and twisted Hessian curves

4.2.1.   Compression function of degree 2

Let us define a compression function on a generalized Hessian curve of degree 2 given by $f_2(P) = x + y$. This function may be obtained from the function $\overline{f}_2(\overline{P}) = \frac{\overline{y}+1}{\overline{x}}$ from [19], using isomorphism between E_{GH} and E_{TH}. Using the same isomorphism between $f_2(P)$ and $\overline{f}_2(\overline{P})$, one may use differential addition and doubling formulas from [19] and obtain that if $r_P = f_2(P)$ and $r_Q = f_2(Q)$ then $f(P + Q)f(P - Q)$ may be presented in the following form:

$$f_2(P+Q)f_2(P-Q) = \frac{(dr_P{}^2 - 3a)r_Q{}^2 + (6ar_P + 2ad)r_Q - 3ar_P{}^2 + 2adr_P + ad^2}{(3r_P + d)r_Q{}^2 + (3r_P{}^2 + dr_P)r_Q + dr_P{}^2 - 3a}. \qquad (33)$$

In the same manner, $f(P + Q) + f(P - Q)$ may be presented as

$$f_2(P+Q) + f_2(P-Q) = -\frac{((3r_P{}^2 + dr_P)r_Q{}^2 + (dr_P{}^2 + d^2r_P + 6a)r_Q + 6ar_P + 2ad}{(3r_P + d)r_Q{}^2 + (3r_P{}^2 + dr_P)r_Q + dr_P{}^2 - 3a}. \qquad (34)$$

Similarly, doubling may be presented as:

$$f_2([2]P) = \frac{-(r_P^4 + 4ar_P + ad)}{(2r_P^3 + dr_P^2 - a)}. \qquad (35)$$

Explanation: Formula (33) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.B. Formula (34) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.C Accordingly, formula (35) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.B.   □

4.2.2.   Compression function of degree 6

We will give an example of a compression function of degree 6 for the generalized Hessian curve $E_{GH} : x^3 + y^3 + a = dxy$. A compression function of degree 6 may be given by $f_6(x, y) = xy$.

It is easy to show, that f_6 has the degree of 6. At first, let us note, that compression function f_6 fulfills all the criteria from Proposition 1:

- involution $[-1]P$ is projectively linear, because $[-1]P = (Y : X : Z)$ for $P = (X : Y : Z)$,

- for every generalized Hessian curve over field $\mathbb{K}$, there exists root ω of polynomial $\omega^2 + \omega + 1 = 0$ in field $\overline{\mathbb{K}}$ and point $T \in E_{GH}\left(\overline{\mathbb{K}}\right)$ of order 3 $T = (1 : -\omega : 0)$ in projective coordinates,

- translation $\tau_T : E_{GH} \to E_{GH} : \tau(P) = P + T$ is projectively linear, because if $P = (X : Y : Z) \in E(\mathbb{K})$, then $P + (1 : -\omega : 0) = (\omega X : \omega^{-1}Y : Z)$.

Let us note that $f_6(P) = f_6(Q)$, iff $Q = \pm P + [k](1 : -\omega : 0)$ for $k = \overline{0, 2}$ is in set $S = \{(x, y), (y, x), (\omega x, \omega^2 y), (\omega^2 x, \omega y), (\omega y, \omega^2 x), (\omega^2 y, \omega x)\}$, for $P = (x, y)$.

Let us assume that $r = xy$ for $x, y \neq 0$. Then $y = \frac{r}{x}$ and because $x^3 + y^3 + a = dxy$, then

$$x^3 + \left(\frac{r}{x}\right)^3 + a = dx\frac{r}{x} \tag{36}$$

and

$$g(x) = x^6 + (a - dr)x^3 + r^3 = 0. \tag{37}$$

Equation (37) has 6 roots at most. It is easy to show, that all points for which equation (37) is satisfied belong to the set S which is easy to check manually.

Theorem 4.3. The differential addition formula for $f_6(P + Q)f_6(P - Q)$ on a generalized Hessian curve and compression function $f_6(x, y) = xy$, where $f_6(P) = r_P$ and $f_6(Q) = r_Q$, is given by:

$$f_6(P + Q)f_6(P - Q) = \frac{r_P{}^2 r_Q{}^2 - adr_P r_Q + a^2 r_Q + a^2 r_P}{(r_Q - r_P)^2}. \tag{38}$$

Similarly, doubling is given by

$$f_6([2]P) = \frac{r_P(a(dr_P - a) - r_P{}^3 - a^2)}{(dr_P - a)^2 - 4r_P{}^3}. \tag{39}$$

Explanation: Formula (38) may be obtained using the algorithm from Appendix G.A, without any modifications. Correspondingly, formula (39) may be obtained using the algorithm from Appendix H.A, without any modifications. □

Remark 9. By comparing the formulas for $f_2(P+Q)f_2(P-Q)$ and $f_6(P+Q)f_6(P-Q)$, it is easy to notice that in the case of the differential addition function, $f_6(P)$ is more efficient. However, in the case of doubling, it seems that $f_2(P)$ has a lower computational cost than $f_6(P)$.

Remark 10. Let us note, that Farashahi and Joye in [10] obtained compression functions $f_6(x, y) = xy$ and $g_6(x, y) = x^3 + y^3$ for binary generalized Hessian curves. Indeed, the same compression functions work also on generalized Hessian curves over fields with large characteristics. Let us see, that $g_6(x, y) = x^3 + y^3 = dxy - a = d \cdot f_6(x, y) - a$.

4.3. Compression function of degree 18

In the previous subsections, we defined a compression function of degree 6 on a generalized Hessian curve of degree 6. In this subsection, we will be investigating a compression function of degree 18 on a Hessian curve, using additional symmetries. Let us begin by noteing that for a Hessian curve given in projective coordinates

$$E_H : X^3 + Y^3 + Z^3 = dXYZ \tag{40}$$

if $P_1 = (X : Y : Z) \in E_H(\mathbb{K})$, then also $P_2 = (X : Z : Y), P_3 = (Y : X : Z), P_4 = (Y : Z : X), P_5 = (Z : X : Y), P_6 = (Z : Y : X) \in E_H(\mathbb{K})$. Furthermore, let us also note, that if

$T_1 = (1 : -\omega : 0)$ and $T_2 = (-\omega : 0 : 1)$, then:

1. translation $\tau_{T_1} : E_{GH} \to E_{GH} : \tau(P) = P + T$ is projectively linear, because $P + T_1 = (\omega X : \omega^2 Y : Z) \in E_H(\mathbb{K})$;

2. translation $\tau_{T_2} : E_{GH} \to E_{GH} : \tau(P) = P + T$ is projectively linear, because $P + T_2 = (\omega Y : \omega^2 Z : X) \in E_H(\mathbb{K})$.

The above means that we will be searching for the compression function f_{18} for which $f_{18}(P) = f_{18}(Q)$, iff $Q = \pm P + [k](1 : -\omega : 0) + [l](-\omega : 0 : 1)$.

Now, we will give the following theorem.

Theorem 4.4. Let us state that $f_6(P) = xy = \frac{XY}{Z^2}$ is a compression function on a generalized Hessian curve and, therefore, on a Hessian curve. Because the Hessian curve equation is invariant under permutation of its coordinates $E(X : Y : Z) = E(Y : X : Z) = E(Z : Y : X) = E(Y : Z : X) = E(X : Z : Y) = E(Z : X : Y)$, then, using these symmetries, the compression function of degree 18 may be given by $f_{18}(P) = \frac{XY}{Z^2} + \frac{YZ}{X^2} + \frac{ZX}{Y^2} = \frac{x^3 y^3 + x^3 + y^3}{x^2 y^2}$.

Proof:
At first, let us assume that $f_{18}(P) = R$, then

$$x^3 + y^3 = Rx^2 y^2 - x^3 y^3 \tag{41}$$

and substituting $x^3 + y^3$ in the equation of the Hessian curve, one obtains that

$$Rx^2 y^2 - x^3 y^3 + 1 = dxy. \tag{42}$$

Let us note, that $xy = f_6(P)$. Let $r = f_6(P)$. Then

$$g(r) = -r^3 + Rr^2 - dr + 1 = 0. \tag{43}$$

For any R there are at most three distinct roots of the polynomial g. Let us note that we showed that there are at most six distinct points in $E_H(\mathbb{K})$ for which $f_6(P) = r$.

This means, that $f_{18}(P)$ has at most 18 distinct solutions. We will list all of those solutions in the set S, for $P = (x, y)$. It is easy to check that for every $Q \in S$ holds that $f_{18}(Q) = R$.

The set S is given by

$$\begin{aligned}
S = \Big\{ &(X : Y : Z), (X : Z : Y), (Y : X : Z), (Y : Z : X), (Z : X : Y), (Z : Y : X), \\
&(\omega X : \omega^2 Y : Z), (\omega X : \omega^2 Z : Y), (\omega Y : \omega^2 X : Z), (\omega Y : \omega^2 Z : X), (\omega Z : \omega^2 X : Y), \\
&(\omega Z : \omega^2 Y : X), (\omega^2 X : \omega Y : Z), (\omega^2 X : \omega Z : Y), (\omega^2 Y : \omega X : Z), (\omega^2 Y : \omega Z : X), \\
&(\omega^2 Z : \omega X : Y), (\omega^2 Z : \omega Y : X) \Big\}
\end{aligned} \tag{44}$$

in projective coordinates, which is equivalent to

$$
\begin{aligned}
S = \Big\{ & (x,y), \left(\tfrac{x}{y}, \tfrac{1}{y}\right), (y,x), \left(\tfrac{y}{x}, \tfrac{1}{x}\right), \left(\tfrac{1}{y}, \tfrac{x}{y}\right), \left(\tfrac{1}{x}, \tfrac{y}{x}\right), \\
& (\omega x, \omega^2 y), \left(\omega \tfrac{x}{y}, \omega^2 \tfrac{1}{y}\right), (\omega y, \omega^2 x), \left(\omega \tfrac{y}{x}, \omega^2 \tfrac{1}{x}\right), \left(\omega \tfrac{1}{y}, \omega^2 \tfrac{x}{y}\right), \left(\omega \tfrac{1}{x}, \omega^2 \tfrac{y}{x}\right), (\omega^2 x, \omega y), \\
& \left(\omega^2 \tfrac{x}{y}, \omega \tfrac{1}{y}\right), (\omega^2 y, \omega x), \left(\omega^2 \tfrac{y}{x}, \omega \tfrac{1}{x}\right), \left(\omega^2 \tfrac{1}{y}, \omega \tfrac{x}{y}\right), \left(\omega^2 \tfrac{1}{x}, \omega \tfrac{y}{x}\right) \Big\}.
\end{aligned}
\tag{45}
$$

in affine coordinates. □

Theorem 4.5. The differential addition formula for $f_{18}(P+Q)f_{18}(P-Q)$ on a Hessian curve and a compression function $f_{18}(x,y) = \frac{x^3 y^3 + x^3 + y^3}{x^2 y^2}$, where $f_{18}(P) = r_P$ and $f_{18}(Q) = r_Q$, is given by:

$$
f_{18}(P+Q)f_{18}(P-Q) = \frac{r_P{}^2 r_Q{}^2 + 9 d r_P r_Q + (-4d^3 - 27) r_P + (-4d^3 - 27) r_Q + d^5 + 27 d^2}{(r_P - r_Q)^2}.
\tag{46}
$$

Similarly, doubling is given by

$$
f_{18}([2]P) = \frac{\tfrac{1}{4} r_P{}^4 + \tfrac{9}{4} d r_P{}^2 + (-2d^3 - \tfrac{27}{2}) r_P + \tfrac{1}{4} d^5 + \tfrac{27}{4} d^2}{r_P{}^3 - \tfrac{1}{4} d^2 r_P{}^2 - \tfrac{9}{2} d r_P + d^3 + \tfrac{27}{4}}.
\tag{47}
$$

Explanation: Formula (46) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.D. Correspondingly, formula (47) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.C. □

4.4. Huff's curves

4.4.1. Compression function of degree 2

Let us define the compression function on a Huff's curve of degree 2 given by $f_2(P) = xy$. This function was presented in [25]. If $r_P = f_2(P)$ and $r_Q = f_2(Q)$, then the differential addition $f_2(P+Q)f_2(P-Q)$ is given by the following formula:

$$
f_2(P+Q)f_2(P-Q) = \left(\frac{r_P - r_Q}{r_P r_Q - 1} \right)^2.
\tag{48}
$$

The formula for doubling has the following form:

$$
f_2([2]P) = \frac{4 r_P (r_P^2 + \left(\frac{a^2 + b^2}{ab} \right) r_P + 1}{(r_P^2 - 1)^2}.
\tag{49}
$$

Explanation: Formula (48) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.H. Correspondingly, formula (49) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.G. □

4.4.2.   Compression function of degree 4

In this subsection, a method for obtaining a compression function f_4 of degree 4 using natural symmetries on Huff's curves and action on 2-torsion point is presented.

Let $T_3 = (a : b : 0) \in E_{Hu}(\mathbb{K})$ be a point of order 2 on Huff's curve E_{Hu} given by the equation (21). For a finite point $P = (X : Y : Z) = (x, y) \neq (0, 0)$ the following translation:

$$\tau_{T_3} \ : \ P + T_3 = \left(\frac{1}{x}, \frac{1}{y} \right) \tag{50}$$

is projectively linear.

Proof:
In order to verify, if the translation τ_{T_3} is linear in a projective space $\mathbb{P}^3$, we start by embedding the Huff's curve equation E_{Hu} and the point P into a $\mathbb{P}^1 \times \mathbb{P}^1$. We get the following Huff's curve equation:

$$E_{Hu} \ : \ aXZ_1(Y^2 - Z_2^2) = aYZ_2(X^2 - Z_2^1). \tag{51}$$

In the space $(\mathbb{P}^1)^2$ for $P = ((X : Z_1), (Y : Z_2))$ the translation τ_3 has a form

$$\tau_{T_3} \ : \ P + T_3 = ((Z_1 : X), (Z_2 : Y)). \tag{52}$$

By embedding the above solution into a projective space via Segre embedding $\rho : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ given by

$$((X_1 : X_2), (Y_1 : Y_2)) \to (X_1Y_1 : X_1Y_2 : X_2Y_1 : X_2Y_2), \tag{53}$$

we finally get

$$\begin{aligned} P &= (XY : XZ_2 : YZ_1 : Z_1Z_2) = (U_1 : U_2 : U_3 : U_4), \\ \tau_{T_3} \ : \ P + T_3 &= (Z_1Z_2 : YZ_1 : XZ_2 : XY) = (U_4 : U_3 : U_2 : U_1). \end{aligned} \tag{54}$$

Additionally we have

$$- P = (XY : -XZ_2 : -YZ_1 : Z_1Z_2) = (U_1 : -U_2 : -U_3 : U_4). \tag{55}$$

In consequence, we see that the translation τ_3 and the involution $[-1]P$ are projectively linear in $\mathbb{P}^3$. $\qquad \square$

We will give an example of a compression function of degree 4 for a Huff's curve $E_{Hu} : ax(y^2 - 1) = by(x^2 - 1)$. A compression function of degree 4 may be given by $f_4(x, y) = xy + \frac{1}{xy}$. It is easy to show, that f_4 has the degree of 4. At first, let us note, that

- involution $[-1]P$ is projectively linear in $\mathbb{P}^3$ (see Remark 4.4.2),

- point $T_3 = (a : b : 0)$ of order 2 naturally belongs to $E_{Hu}(\mathbb{K})$,

- translation $\tau_{T_3} : E_{Hu} \to E_{Hu} : \tau_{T_3}(P) = P + T_3$ is also projectively linear (see Remark 4.4.2).

Let us note that $f_4(P) = f_4(Q)$, iff $Q = \pm P + [k](a : b : 0)$, for $k = \overline{0,1}$ and $P = (x, y)$ is in set $S = \{(x, y), (-x, -y), (\frac{1}{x}, \frac{1}{y}), (-\frac{1}{x}, \frac{1}{y})\}$.

Let us assume that $xy = t$ and $t \neq 0$. Then $f_4(x, y) = xy + \frac{1}{xy} = t + \frac{1}{t}$. One can denote $f_4(x, y) = r$. After short calculations we get

$$h(t) = t^2 - rt + 1 = 0. \tag{56}$$

Polynomial $h(t)$ has at most 2 distinct roots. Let t_1 be a root of $h(t)$. If we substitute $y = \frac{t_1}{x}$ in the Huff's curve equation (17), we get

$$g(x) = (bt_1 + a)x^2 - bt_1 - at_1^2 = 0. \tag{57}$$

Equation (57) is quadratic and has at most two distinct roots. In consequence, the degree of the compression function f_4 is 4 at most.

Theorem 4.6. A differential addition formula for $f_4(P + Q)f_4(P - Q)$ on a Huff's curve and compression function $f_4(x, y) = xy + \frac{1}{xy}$, where $f_4(P) = r_P$ and $f_4(Q) = r_Q$, is given by:

$$f_4(P + Q)f_4(P - Q) = \frac{(ab)^2(r_P r_Q + 4)^2 + 16(a^2 + b^2)(ab)(r_P + r_Q) + 16(a^2 + b^2)^2}{(ab)^2(r_P - r_Q)^2}. \tag{58}$$

Denoting $(a^2 + b^2)/(ab) = A$, we get

$$f_4(P + Q)f_4(P - Q) = \frac{(r_P r_Q + 4)^2 + 16A(r_P + r_Q) + 16A^2}{(r_P - r_Q)^2}. \tag{59}$$

Similarly, doubling is given by

$$f_4([2]P) = \frac{(ab)^2(r_P^2 + 4)^2 + 32(a^2 + b^2)(ab)r_P + 16(a^2 + b^2)^2}{4ab((ab)(r_P^3 - 4r_P) + (a^2 + b^2)r_P^2 - 4(a^2 + b^2))}. \tag{60}$$

Denoting $(a^2 + b^2)/(ab) = A$ we get

$$f_4([2]P) = \frac{((r_P^2 + 4) + 4A)^2 + 8A(r_P^2 + 4)}{4(r_P + A)(r_P^2 - 4)}. \tag{61}$$

Explanation: Formula (58) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.I. Correspondingly, formula (60) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.H. □

4.4.3. Compression function of degree 8

In this subsection a method for obtaining a compression function f_8 of degree 8 using natural symmetries on Huff's curves and action on three 2-torsion points will be presented.

Let $T_1, T_2, T_3 \in E_{Hu}(\mathbb{K})$ be points of order 2 of the form $T_1 = (1 : 0 : 0)$, $T_2 = (0 : 1 : 0)$ and $T_3 = (a : b : 0) = T_1 + T_2$ on a Huff's curve E_{Hu} given by the equation (21). For a finite point $P = (X : Y : Z) = (x, y) \neq (0, 0)$ we consider the following translations:

$$\begin{aligned}
\tau_{T_1} &: P + T_1 &= \left(\frac{1}{x}, -y\right), \\
\tau_{T_2} &: P + T_2 &= \left(-x, \frac{1}{y}\right).
\end{aligned} \tag{62}$$

Remark 11. Now we intend to check if the above translations are projectively linear. As in Remark 4.4.2, we consider the Huff's curve equation E_{Hu} in the space $(\mathbb{P}^1)^2$ given by the equation (51). In the space $(\mathbb{P}^1)^2$ for point $P = ((X : Z_1) : (Y : Z_2))$ the translations τ_1 and τ_2 have the following form

$$
\begin{aligned}
\tau_{T_1} &: P + T_1 &= ((Z_1 : X), (-Y : Z_2)), \\
\tau_{T_2} &: P + T_2 &= ((-X : Z_1), (Z_2 : Y)).
\end{aligned}
\tag{63}
$$

By embedding the above formulas into a projective space via Segre embedding $\rho : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ given by (53), we get

$$
\begin{aligned}
P &= (XY : XZ_2 : YZ_1 : Z_1Z_2) = (U_1 : U_2 : U_3 : U_4), \\
\tau_{T_1} : P + T_1 &= (-YZ_1 : Z_1Z_2 : -XY : XZ_2) = (-U_3 : U_4 : -U_1 : U_2), \\
\tau_{T_2} : P + T_2 &= (-XZ_2 : -XY : Z_1Z_2 : YZ_1) = (-U_2 : -U_1 : U_4 : U_3).
\end{aligned}
\tag{64}
$$

Additionally, we have

$$
- P = (XY : -XZ_2 : -YZ_1 : Z_1Z_2) = (U_1 : -U_2 : -U_3 : U_4).
\tag{65}
$$

In consequence, we see that the translations τ_1, τ_2 and the involution $[-1]P$ are projectively linear in $\mathbb{P}^3$.

We will give an example of a compression function of degree 8 for a Huff's curve $E_{Hu} : ax(y^2 - 1) = by(x^2 - 1)$. A compression function of degree 8 may be given by $f_8(x, y) = xy + \frac{1}{xy} - \frac{x}{y} - \frac{y}{x}$. It is easy to show, that f_8 has the degree of 8. At first, let us note, that

- involution $[-1]P$ is projectively linear in $\mathbb{P}^3$ (see Remark 11),

- points $T_1 = (1 : 0 : 0)$ and $T_2 = (0 : 1 : 0)$ of order 2 naturally belong to $E_{Hu}(\mathbb{K})$,

- translations $\tau_{T_1} : E_E \to E_E : \tau_{T_1}(P) = P + T_1$ and $\tau_{T_2} : E_E \to E_E : \tau_{T_2}(P) = P + T_2$ are also projectively linear (see Remark 11).

Let us note that $f_8(P) = f_8(Q)$, iff $Q = \pm P + [l](1 : 0 : 0) + [k](0 : 1 : 0)$, for $l, k = \overline{0, 1}$ and $P = (x, y)$ is in set
$S = \{(x, y), (-x, -y), (\frac{1}{x}, -y), (-\frac{1}{x}, y), (-x, \frac{1}{y}), (x, -\frac{1}{y}), (\frac{1}{x}, \frac{1}{y}), (-\frac{1}{x}, -\frac{1}{y})\}$.

Let us assume that $xy = t$ and $t \neq 0$. From the Huff's curve equation (17), one may derive:

$$
x^2 = \frac{xy(axy + b)}{bxy + a} = \frac{t(at + b)}{bt + a}, \quad y^2 = \frac{xy(bxy + a)}{axy + b} = \frac{t(bt + a)}{at + b}.
\tag{66}
$$

Then, one may write

$$
f_8(x, y) = xy + \frac{1}{xy} - \frac{x}{y} - \frac{y}{x} = t + \frac{1}{t} - \frac{at + b}{bt + a} - \frac{bt + a}{at + b}.
\tag{67}
$$

Let us denote $f_8(x, y) = r$. By simple calculations, we get

$$
h(t) = abt^4 - abrt^3 - (a^2r + b^2r + 2ab)t^2 - abrt + ab = 0.
\tag{68}
$$

Polynomial $h(t)$ has at most 4 distinct roots. Let t_1 be a root of $h(t)$. If we substitute $y = \frac{t_1}{x}$ in the Huff's curve equation (17), we get the quadratic equation (57). In consequence, a degree of the compression function f_8 is 8 at most.

Theorem 4.7. A differential addition formula for $f_8(P + Q)f_8(P - Q)$ on a Huff's curve and a compression function $f_8(x, y) = xy + \frac{1}{xy} - \frac{x}{y} - \frac{y}{x}$ is given by:

$$f_8(P + Q)f_8(P - Q) = \frac{(r_P r_Q - 16)^2}{(r_P - r_Q)^2}. \tag{69}$$

Similarly, doubling is given by

$$f_8([2]P) = \frac{(r_P^2 - 16)^2}{4r_P(r_P^2 + 4\frac{a^2+b^2}{ab}r_P + 16)}. \tag{70}$$

Explanation: Formula (69) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.J. Correspondingly, formula (70) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.I. □

Remark 12. Let us note that formulas (69) and (70) that we obtained for compression function f_8 are as efficient as formulas for the Montgomery curve.

4.4.4. Compression function of degree 16

One may check, in a similar manner as in the preceding sections, that a compression function of degree 16 is given by

$$f_{16}(x, y) = xy + \frac{1}{xy} - \frac{y}{x} - \frac{x}{y} + \frac{y+1}{1-y} \cdot \frac{x+1}{1-x} + \frac{y+1}{y-1} \cdot \frac{1-x}{1+x} + \frac{y-1}{1+y} \cdot \frac{x-1}{x+1} + \frac{1-y}{1+y} \cdot \frac{x+1}{x-1}. \tag{71}$$

This compression function may be obtained using natural symmetries on Huff's curves and action on three 2-torsion points and points of order of 4, given by $(\pm 1 : \pm 1 : 1)$.

Let us note that $f_{16}(P) = f_{16}(Q)$, iff $Q = \pm P + [l](1 : 0 : 0) + [m](1 : 1 : 1)$, for $l = \overline{0, 1}, m = \overline{0, 3}$ and $P = (x, y)$ is in set

$$S = \left\{ (x, y), (-x, -y), \left(\frac{1}{x}, -y\right), \left(-\frac{1}{x}, y\right), \left(x, -\frac{1}{y}\right), \left(-x, \frac{1}{y}\right), \left(\frac{1}{x}, \frac{1}{y}\right), \left(-\frac{1}{x}, -\frac{1}{y}\right), \right.$$
$$\left(\frac{y+1}{1-y}, \frac{x+1}{1-x}\right), \left(\frac{y+1}{y-1}, \frac{1-x}{1+x}\right), \left(\frac{y-1}{y-1}, \frac{x-1}{1+x}\right), \left(\frac{1-y}{1+y}, \frac{x+1}{x-1}\right), \left(-\frac{y+1}{1-y}, -\frac{x+1}{1-x}\right), \left(-\frac{y+1}{y-1}, -\frac{1-x}{1+x}\right),$$
$$\left. \left(-\frac{y-1}{1+y}, -\frac{x-1}{x+1}\right), \left(-\frac{1-y}{1+y}, -\frac{x+1}{x-1}\right) \right\}.$$

Theorem 4.8. The differential addition formula for $f_{16}(P + Q)f_{16}(P - Q)$ on a Huff's curve and a compression function $f_{16}(x, y)$ given by the formulae (71), where $f_{16}(P) = r_P$ and $f_{16}(Q) = r_Q$, is given by:

$$f_{16}(P + Q)f_{16}(P - Q) = \frac{(r_P r_Q + 64)^2 + 1024\frac{a^2+b^2}{ab}(r_P + r_Q + \frac{a^2+b^2}{ab})}{(r_P - r_Q)^2}. \tag{72}$$

Similarly, doubling is given by

$$f([2]P) = \frac{L}{M},$$ (73)

where

$$L = \frac{1}{4}x^4 + 32x^2 + \frac{512a^2 + 512b^2}{ab}x + \frac{1024a^4 + 3072a^2 * b^2 + 1024b^4}{a^2b^2},$$
$$M = x^3 + \frac{4a^2 + 4b^2}{ab}x^2 - 64x + \frac{-256a^2 - 256b^2}{ab}.$$ (74)

Explanation: Formula (72) may be obtained using the algorithm from Appendix G.A, with modifications from Appendix G.K. Correspondingly, formula (74) may be obtained using the algorithm from Appendix H.A, with modifications from Appendix H.J.   □

5.   Formulas as fast as Montgomery's

A short analysis of the cost of applying a compression functions f_2, f_6 and f_{18} on a generalized Hessian curve shows that the applications of these functions are not as efficient as Montgomery-like formulas for Montgomery, Huff's and Edwards curves. Now, we will present the following theorem.

Theorem 13. Let E be a model of an elliptic curve, for which isomorphism ϕ from E to the Montgomery curve $E_M : B\overline{y}^2 = \overline{x}^3 + A\overline{x}^2 + \overline{x}$ is given by a function $\phi(x, y) = (W_x(x, y), W_y(x, y))$, where $W_x(x, y), W_y(x, y)$ are rational functions. Let us $f_2(\overline{P}) = \overline{x}$ be compression function of degree 2 on the Montgomery curve, where $\overline{P} = (\overline{x}, \overline{y}) \in E_M(\mathbb{K})$. Then $g_2(x, y) = f_2(W_x(x, y))$ is compression function of degree 2. Let $A(f_2(\overline{P}), f_2(\overline{Q}), f_2(\overline{P} - \overline{Q}))$ be differential addition and $D(f_2(\overline{P}))$ be the doubling formulas on the Montgomery curve. In such a case, on an elliptic curve E we may define differential addition $A(g_2(P), g_2(Q), g_2(P - Q))$ and doubling $D(g_2(P))$ formulas of the same efficiency as Montgomery's, up to constants which depends on the coefficients of E.

Proof:
Let us ϕ be an isomorphism from a curve E to the Montgomery curve $E_M : B\overline{y}^2 = \overline{x}^3 + A\overline{x}^2 + \overline{x}$, given by $\phi(P) = (W_x(P), W_y(P))$, where $W_x(P)$ and $W_y(P)$ are rational functions. Then, for $P \in E(\mathbb{K})$ holds that $g_2(P) = f_2(W_x(P), W_y(P)) = W_x(P)$ is indeed a compression function of degree 2 on a curve E. Let us note, that $f_2(\overline{P}) = \overline{x} = \overline{r}_P$ gives the same value $\overline{r}_P$ only for two points $\overline{P}, -\overline{P} \in E_M(\mathbb{K})$. Because ϕ is an isomorphism from E to E_M, it means that $f_2(W_x(P), W_y(P)) = W_x(P) = r_P$ also gives the same value r_P for only two points $P, -P \in E(\mathbb{K})$. It follows that $g_2(P) = f_2(W_x(P), W_y(P)) = W_x(P)$ is a compression function of degree 2 on a curve E.
     Now, let us denote $\overline{r}_{\overline{P}} = f_2(\overline{P}), \overline{r}_{\overline{Q}} = f_2(\overline{Q}), \overline{r}_{\overline{P}+\overline{Q}} = f_2(\overline{P} + \overline{Q}), \overline{r}_{\overline{P}-\overline{Q}} = f_2(\overline{P} - \overline{Q}), \overline{r}_{[2]\overline{P}} = f_2([2]\overline{P})$. Let us note that hold $r_P = g_2(P), r_Q = g_2(Q), r_{P+Q} = g_2(P + Q), r_{P-Q} = g_2(P - Q), r_{[2]P} = g_2([2]P)$. If $A(f_2(\overline{P}), f_2(\overline{Q}), f_2(\overline{P} - \overline{Q}))$ is a differential addition and $D(f_2(\overline{P}))$ is a doubling formula on the Montgomery curve, then $A(f_2(W_x(P), W_y(P)), f_2(W_x(Q), W_y(Q)), f_2(W_x(P - Q), W_y(P - Q))) = A(g_2(P), g_2(Q), g_2(P - Q))$ is a differential addition formula on a curve E. Correspondingly, if $D(f_2(\overline{P}))$ is a doubling formula on the Montgomery curve, then $D(f_2(\overline{P})) = D(f_2(W_x(P), W_y(P))) = D(g_2(P))$ is a doubling formula on a curve E. Because for every $\overline{P} \in E_M(\mathbb{K})$ holds that $r_{\overline{P}} = f_2(\overline{P}) = W_x(P) = g_2(P) = r_P$, it follows that $A(r_P, r_Q, r_{P-Q})$

and $D(r_P)$ on E are of the same efficiency as $A(\overline{r}_{\overline{P}}, \overline{r}_{\overline{Q}}, \overline{r}_{\overline{P}-\overline{Q}})$ and $D(\overline{r}_{\overline{P}})$ on the Montgomery curve, up to constants which depends on the coefficients of a curve E.   □

Let us note that an isomorphism ϕ for which conditions presented in Theorem 13 hold, may be defined, for example, from a twisted Edwards curve to the Montgomery [7], from the Huff's curves to the Montgomery [10] and also other models of elliptic curves. Using these isomorphisms, one may obtain for these compression functions of degree 2 Montgomery-like formulas of the same efficiency. However, compression functions of degree 2 obtained by Theorem 13 may be sometimes complicated, as same as constants appearing in differential addition and doubling formulas and therefore may be not optimal for all applications.

Remark 14. Let us note that for Hessian, twisted Hessian and generalized Hessian curve models there do not exist natural isomorphisms from these curves to the Montgomery curve. We therefore state the conjecture that for Hessian, twisted Hessian and generalized Hessian curves arithmetics using compression of the same or similar efficiency as for Montgomery do not exist.

6. Conclusion

This paper presents new compression functions of degree > 2 on Edwards, Huff's and the Hessian family of elliptic curves. As it was presented in section 2, compression functions of high degree may be obtained using natural symmetries on elliptic curves obtained by the action on the n-torsion point T.

Additionally, it is worth noteing that models of elliptic curves for which a birationally equivalent Montgomery curve exists, have some compression functions of degree 2 for which differential addition and doubling is of the same efficiency as the Montgomery curves. Unfortunately, it seems that compression functions of the same efficiency as the Montgomery curve do not exist for models of elliptic curves with a natural point of order 3. Such representatives of elliptic curves are Hessian, twisted Hessian, and generalized Hessian curves. This is because, for these models, natural isomorphisms do not exist from these curves to the Montgomery curve.

References

[1] Jao D, De Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang BY (ed.), Post-Quantum Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-642-25405-5, 2011 pp. 19–34.

[2] Azarderakhsh R, Campagna M, Costello C, Feo L, Hess B, Jalali A, Jao D, Koziel B, LaMacchia B, Longa P, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2020.

[3] Castryck W, Lange T, Martindale C, Panny L, Renes J. CSIDH: an efficient post-quantum commutative group action. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2018 pp. 395–427. doi:10.1007 / 978-3-030-03332-3_15.

[4] Montgomery PL. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 1987. **48**(177):243–264. doi:10.1090/S0025-5718-1987-0866113-7.

[5] Edwards H. A normal form for elliptic curves. *Bulletin of the American mathematical society*, 2007. **44**(3):393–422. doi:10.1090/S0273-0979-07-01153-6.

[6] Bernstein DJ, Lange T. Inverted Edwards Coordinates. In: Boztaş S, Lu HFF (eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Springer Berlin Heidelberg, Berlin, Heidelberg. 2007 pp. 20–27. ISBN: 978-3-540-77224-8.

[7] Bernstein DJ, Birkner P, Joye M, Lange T, Peters C. Twisted Edwards curves. In: International Conference on Cryptology in Africa. Springer, 2008 pp. 389–405. doi:c798703ae3ecfdc375112f19dd0787e4.

[8] Joye M, Quisquater JJ. Hessian Elliptic Curves and Side-Channel Attacks. In: Koç ÇK, Naccache D, Paar C (eds.), Cryptographic Hardware and Embedded Systems — CHES 2001. Springer Berlin Heidelberg, Berlin, Heidelberg. 2001 pp. 402–410. ISBN:978-3-540-44709-2.

[9] Bernstein DJ, Chuengsatiansup C, Kohel D, Lange T. Twisted hessian curves. In: International Conference on Cryptology and Information Security in Latin America. Springer, 2015 pp. 269–294. doi:10.1007/978-3-319-22174-8_15.

[10] Farashahi RR, Joye M. Efficient arithmetic on Hessian curves. In: International Workshop on Public Key Cryptography. Springer, 2010 pp. 243–260. doi:10.1007/978-3-642-13013-7_15.

[11] Joye M, Tibouchi M, Vergnaud D. Huff's model for elliptic curves. In: International Algorithmic Number Theory Symposium. Springer, 2010 pp. 234–250. doi:10.1007/978-3-642-14518-6_20.

[12] Lenstra AK, Verheul ER. The XTR public key system. In: Annual International Cryptology Conference. Springer, 2000 pp. 1–19. doi:10.1007/3-540-44598-6_1.

[13] De Feo L, Jao D, Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 2014. **8**(3):209–247. doi:10.1515/jmc-2012-0015.

[14] Jao D, Azarderakhsh R, Campagna M, Costello C. Supersingular Isogeny Key Encapsulation (version from April 17, 2019. NIST PQC, 2019. `https://sike.org/files/SIDH-spec.pdf`.

[15] Bernstein D, De Feo L, Leroux A, Smith B. Faster computation of isogenies of large prime degree. *arXiv preprint arXiv:2003.10118*, 2020.

[16] Kohel D. Addition law structure of elliptic curves. *Journal of Number Theory*, 2011. **131**(5):894–919. doi:10.1016/j.jnt.2010.12.001.

[17] Kohel D. Efficient arithmetic on elliptic curves in characteristic 2. In: International Conference on Cryptology in India. Springer, 2012 pp. 378–398. ISBN:978-3-642-34930-0, doi:10.1007/978-3-642-34931-7_22.

[18] Farashahi RR, Hosseini SG. Differential Addition on Twisted Edwards Curves. In: Pieprzyk J, Suriadi S (eds.), Information Security and Privacy. Springer International Publishing, Cham. 2017 pp. 366–378. ISBN:978-3-319-59870-3.

[19] Dryło R, Kijko T, Wroński M. Determining Formulas Related to Point Compression on Alternative Models of Elliptic Curves. *Fundamenta Informaticae*, 2019. **169**(4):285–294. doi:10.3233/FI-2019-1848.

[20] Adams WW, Loustaunau P. An introduction to Grobner bases. 3. American Mathematical Soc., 1994. ISBN:978-1-4704-6981-8.

[21] Cox D, Little J, O'Shea D, Sweedler M. Ideals, varieties, and algorithms. *American Mathematical Monthly*, 1994. **101**(6):582–586.

[22] Haihua Gu, Dawu Gu, WenLu Xie. Differential addition on Jacobi quartic curves. In: Symposium on ICT and Energy Efficiency and Workshop on Information Theory and Security (CIICT 2012). 2012 pp. 194–197. doi:10.1049/cp.2012.1890.

[23] Faugère JC, Huot L, Joux A, Renault G, Vitse V. Symmetrized Summation Polynomials: Using Small Order Torsion Points to Speed Up Elliptic Curve Index Calculus. In: Nguyen PQ, Oswald E (eds.), Advances in Cryptology – EUROCRYPT 2014. Springer Berlin Heidelberg, Berlin, Heidelberg. 2014 pp. 40–57. ISBN:978-3-642-55220-5.

[24] Castryck W, Galbraith SD, Farashahi RR. Efficient arithmetic on elliptic curves using a mixed Edwards-Montgomery representation. *IACR Cryptology ePrint Archive*, 2008. **2008**:218. http://eprint.iacr.org/2008/218.

[25] Dryło R, Kijko T, Wroński M. Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography. Cryptology ePrint Archive, Report 2020/526, 2020. https://eprint.iacr.org/2020/526.

G   Computer program for generation differential addition formula

Appendix G.A   Main program

```
Q:=Rationals();
Z:=Integers();
rQ<a,b>:=FunctionField(Q,2);
/* maximal degree d of nominator and denominator in rational function
   for f(P+Q)*f(P-Q) or for f(P+Q)+f(P-Q) */
d:=4;
n:=(d+1)*(d+2);    /* Number of unknown parameters   */
R:=PolynomialRing(rQ,n);
F:= FieldOfFractions(R);
pF2<x,y>:=PolynomialRing(F,2);
pF4<x1,y1,x2,y2>:=PolynomialRing(F,4);
rF4:=FieldOfFractions(pF4);


//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +a-b*x*y;
/*definition of compression function f*/
f:=x*y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(y1^2*x2-y2^2*x1)/(x2*y2-x1*y1);
y3:=(x1^2*y2-x2^2*y1)/(x2*y2-x1*y1);
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
```

```
x4:=Evaluate(x3, [x1,y1,y2,x2]);
y4:=Evaluate(y3, [x1,y1,y2,x2]);
//End of exchangeable parameters

I:=ideal<pF4|[ Evaluate(E,[x1,y1]), Evaluate(E, [x2,y2]) ] >;
f1:=Evaluate(f,[x1,y1]);  f2:=Evaluate(f,[x2,y2]);
f3:=Evaluate(f,[x3,y3]);  f4:=Evaluate(f,[x4,y4]);

/* In here we search for rational function f(P+Q)*f(P-Q).
   If one intends to search for rational function f(P+Q)+f(P-Q),
                                                then H:=f3+f4; */
H:=f3*f4;
G:=[pF2!0,pF2!0];
k:=0;
for u:=1 to 2 do
  for  j:=1 to d+1 do
    for i:=1 to j do  k:=k+1;
      G[u]:=G[u]+ R.k*x^(i-1)*y^(j-i);
end for; end for; end for;
Nor:=NormalForm(Numerator( H - Evaluate(G[1]/G[2],[f1,f2])), I);
cf:=Coefficients(Nor);
sd:=[];
for i in cf do sd:= sd cat [Denominator(i)]; end for;
ld:=Lcm(sd);
cf0:=[];
/* multiplication by common denominator Coefficients(Nor) */
for  i:=1 to #cf do  cf0:=cf0 cat [R!(ld*cf[i])]; end for;
Proj:=ProjectiveSpace(R);
Sch:=Scheme(Proj,cf0);
dim:=Dimension(Sch);
if dim eq 0 then Rp:=RationalPoints(Sch);
  for i in Rp do sq:=Eltseq(i); end for;
  G:=[pF2!0,pF2!0];
  k:=0;
  for u:=1 to 2 do
    for  j:=1 to d+1 do
      for i:=1 to j do  k:=k+1;
        G[u]:=G[u]+ sq[k]*x^(i-1)*y^(j-i);
  end for; end for; end for;
  [G[1], G[2]];
end if;
```

Appendix G.B   Modifications for compression function $f_{18}(x, y) = xy$ on generalized Hessian curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +1-b*x*y;
/*definition of compression function f*/
f:=x+y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(y1^2*x2-y2^2*x1)/(x2*y2-x1*y1);
y3:=(x1^2*y2-x2^2*y1)/(x2*y2-x1*y1);
x4:=Evaluate(x3, [x1,y1,y2,x2]);
y4:=Evaluate(y3, [x1,y1,y2,x2]);
//End of exchangeable parameters
```

Appendix G.C   Modifications for compression function $f_{18}(x, y) = xy$ on generalized Hessian curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +1-b*x*y;
/*definition of compression function f*/
f:=x+y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(y1^2*x2-y2^2*x1)/(x2*y2-x1*y1);
y3:=(x1^2*y2-x2^2*y1)/(x2*y2-x1*y1);
x4:=Evaluate(x3, [x1,y1,y2,x2]);
y4:=Evaluate(y3, [x1,y1,y2,x2]);
//End of exchangeable parameters
```

Additionally, $H = f3 + f4$.

Appendix G.D   Modifications for compression function $f_{18}(x, y) = xy$ on generalized Hessian curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +1-b*x*y;
/*definition of compression function f*/
f:=(x^3*y^3+x^3+y^3)/(x^2*y^2);
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(y1^2*x2-y2^2*x1)/(x2*y2-x1*y1);
y3:=(x1^2*y2-x2^2*y1)/(x2*y2-x1*y1);
```

```
x4:=Evaluate(x3, [x1,y1,y2,x2]);
y4:=Evaluate(y3, [x1,y1,y2,x2]);
//End of exchangeable parameters
```

Appendix G.E   Modifications for compression function $f_2(x,y) = y$ on Edwards curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
a:=1;
E:=a*x^2 + y^2 -1 - b*x^2*y^2;
/*definition of compression function f*/
f:=y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1*y2+y1*x2)/(1+b*x1*x2*y1*y2);
y3:=(y1*y2-a*x1*x2)/(1-b*x1*x2*y1*y2);
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,y2]);
y4:=Evaluate(y3, [x1,y1,-x2,y2]);
//End of exchangeable parameters
```

Appendix G.F   Modifications for compression function $f_4(x,y) = y^2$ on Edwards curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
a:=1;
E:=a*x^2 + y^2 -1 - b*x^2*y^2;
/*definition of compression function f*/
f:=y^2;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1*y2+y1*x2)/(1+b*x1*x2*y1*y2);
y3:=(y1*y2-a*x1*x2)/(1-b*x1*x2*y1*y2);
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,y2]);
y4:=Evaluate(y3, [x1,y1,-x2,y2]);
//End of exchangeable parameters
```

Appendix G.G   Modifications for compression function $f_8(x,y) = x^2y^2$ on Edwards curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
a:=1;
E:=a*x^2 + y^2 -1 - b*x^2*y^2;
```

```
/*definition of compression function f*/
f:=x^2*y^2;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1*y2+y1*x2)/(1+b*x1*x2*y1*y2);
y3:=(y1*y2-a*x1*x2)/(1-b*x1*x2*y1*y2);
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,y2]);
y4:=Evaluate(y3, [x1,y1,-x2,y2]);
//End of exchangeable parameters
```

Appendix G.H   Modifications for compression function $f_2(x, y) = xy$ on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1+x2)*(y1*y2+1)/((x1*x2+1)*(1-y1*y2));
y3:=(y1+y2)*(x1*x2+1)/((1-x1*x2)*(y1*y2+1));
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,-y2]);
y4:=Evaluate(y3, [x1,y1,-x2,-y2]);
//End of exchangeable parameters
```

Appendix G.I   Modifications for compression function $f_4(x, y) = xy + \frac{1}{xy}$ on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y+1/(x*y);
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1+x2)*(y1*y2+1)/((x1*x2+1)*(1-y1*y2));
y3:=(y1+y2)*(x1*x2+1)/((1-x1*x2)*(y1*y2+1));
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,-y2]);
y4:=Evaluate(y3, [x1,y1,-x2,-y2]);
//End of exchangeable parameters
```

Appendix G.J   Modifications for compression function $f_8(x,y) = xy + \frac{1}{xy} - \frac{x}{y} - \frac{y}{x}$ on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y+1/(x*y)-x/y-y/x;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1-x2)*(y1+y2)/((y1-y2)*(1-x1*x2));
y3:=(y1-y2)*(x1+x2)/((x1-x2)*(1-y1*y2));
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,-y2]);
y4:=Evaluate(y3, [x1,y1,-x2,-y2]);
//End of exchangeable parameters
```

Appendix G.K   Modifications for compression function $f_{16}(x,y) =$ given by equation (71) on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y+1/(x*y)-y/x-x/y+(y+1)/(1-y)*(x+1)/(1-x)+(y+1)/(y-1)*(1-x)/(1+x)+
(y-1)/(1+y)*(x-1)/(x+1)+(1-y)/(1+y)*(x+1)/(x-1);
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1-x2)*(y1+y2)/((y1-y2)*(1-x1*x2));
y3:=(y1-y2)*(x1+x2)/((x1-x2)*(1-y1*y2));
/* subtraction of points (x1,y1)-(x2,y2), depends on the curve equation */
x4:=Evaluate(x3, [x1,y1,-x2,-y2]);
y4:=Evaluate(y3, [x1,y1,-x2,-y2]);
//End of exchangeable parameters
```

H   Doubling

Appendix H.A   Main program

```
Q:= Rationals();
Z:=Integers();
rQ<a,b>:=FunctionField(Q,2);
for d  in [1..10] do
n:=2*d+2;
```

```
R:=PolynomialRing(rQ,n);
F:= FieldOfFractions(R);
pF2<x,y>:=PolynomialRing(F,2);
rF2:=FieldOfFractions(pF2);
pF4<x1,y1,x2,y2>:=PolynomialRing(F,4);
rF4:=FieldOfFractions(pF4);


//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +a-b*x*y;
/*definition of compression function f*/
f:=x*y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3 := (a*y1-x2*y2*x1^2)/(x1*x2^2-y2*y1^2);
y3 := (x1*y1*y2^2 - a*x2)/(x1*x2^2-y2*y1^2);
//End of exchangeable parameters


I:=ideal<pF2|E>;
D1:=Evaluate(x3,[x,y,x,y]);   /*doubling */
D2:=Evaluate(y3,[x,y,x,y]);
H1:=D1; H2:=D2;
F1:=0; F2:=0;
for  j:=1 to n do
  if j le  d+1 then
    F1:=F1+R.j*x^(j-1);
  else
    F2:=F2+R.j*x^(j-d-2);
  end if;
end for;


Nor:=NormalForm(Numerator(Evaluate(f,[H1,H2]) - Evaluate(F1/F2,[f,1])), I);
cf:=Coefficients(Nor);    sd:=[];
for i in cf do sd:= sd cat [Denominator(i)]; end for;
ld:=Lcm(sd);
cf0:=[];
for  i:=1 to #cf do  cf0:=cf0 cat [R!(ld*cf[i])];
end for;
Proj:=ProjectiveSpace(R);
Sch:=Scheme(Proj,cf0);
```

```
dim:=Dimension(Sch);
if dim eq 0 then Rp:=RationalPoints(Sch);
for i in Rp do sq:=Eltseq(i); end for;
F1:=0; F2:=0;
for  j:=1 to n do
  if j le  d+1 then
    F1:=F1+sq[j]*x^(j-1);
  else
    F2:=F2+sq[j]*x^(j-d-2);
  end if;
end for;
[F1, F2];
break d;
end if;
end for;
```

Appendix H.B   Modifications for compression function $f_2(x, y) = xy$ on generalized Hessian curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +1-b*x*y;
/*definition of compression function f*/
f:=x+y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3 := (y1-x2*y2*x1^2)/(x1*x2^2-y2*y1^2);
y3 := (x1*y1*y2^2 - x2)/(x1*x2^2-y2*y1^2)
//End of exchangeable parameters
```

Appendix H.C   Modifications for compression function $f_{18}(x, y) = xy$ on generalized Hessian curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=x^3 + y^3 +1-b*x*y;
/*definition of compression function f*/
f:=(x^3*y^3+x^3+y^3)/(x^2*y^2);
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3 := (y1-x2*y2*x1^2)/(x1*x2^2-y2*y1^2);
y3 := (x1*y1*y2^2 - x2)/(x1*x2^2-y2*y1^2)
//End of exchangeable parameters
```

Appendix H.D   Modifications for compression function $f_2(x, y) = y$ on Edwards curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
a:=1;
E:=a*x^2 + y^2 -1 - b*x^2*y^2;
/*definition of compression function f*/
f:=y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1*y2+y1*x2)/(1+b*x1*x2*y1*y2);
y3:=(y1*y2-a*x1*x2)/(1-b*x1*x2*y1*y2);
//End of exchangeable parameters
```

Appendix H.E   Modifications for compression function $f_4(x, y) = y^2$ on Edwards curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
a:=1;
E:=a*x^2 + y^2 -1 - b*x^2*y^2;
/*definition of compression function f*/
f:=y^2;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1*y2+y1*x2)/(1+b*x1*x2*y1*y2);
y3:=(y1*y2-a*x1*x2)/(1-b*x1*x2*y1*y2);
//End of exchangeable parameters
```

Appendix H.F   Modifications for compression function $f_8(x, y) = x^2 y^2$ on Edwards curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
a:=1;
E:=a*x^2 + y^2 -1 - b*x^2*y^2;
/*definition of compression function f*/
f:=x^2*y^2;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1*y2+y1*x2)/(1+b*x1*x2*y1*y2);
y3:=(y1*y2-a*x1*x2)/(1-b*x1*x2*y1*y2);
//End of exchangeable parameters
```

Appendix H.G Modifications for compression function $f_2(x, y) = xy$ on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y;
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1+x2)*(y1*y2+1)/((x1*x2+1)*(1-y1*y2));
y3:=(y1+y2)*(x1*x2+1)/((1-x1*x2)*(y1*y2+1));
//End of exchangeable parameters
```

Appendix H.H Modifications for compression function $f_4(x, y) = xy + \frac{1}{xy}$ on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y+1/(x*y);
/* addition of points (x1,y1)+(x2,y2), depends on the curve equation */
x3:=(x1+x2)*(y1*y2+1)/((x1*x2+1)*(1-y1*y2));
y3:=(y1+y2)*(x1*x2+1)/((1-x1*x2)*(y1*y2+1));
//End of exchangeable parameters
```

Appendix H.I Modifications for compression function $f_8(x, y) = xy + \frac{1}{xy} - \frac{x}{y} - \frac{y}{x}$ on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y+1/(x*y)-x/y-y/x;
/* doubling of point (x1,y1), depends on the curve equation */
x3:=(2*y1^2+2)*x1/((x1^2+1)*y1^2-x1^2-1);
y3:=(2*x1^2+2)*y1/((x1^2-1)*y1^2+x1^2-1);
//End of exchangeable parameters
```

Appendix H.J Modifications for compression function $f_{16}(x, y)$ given by equation (71) on Huff's curve

```
//Beginning of exchangeable parameters
/*definition of an elliptic curve E*/
```

```
E:=a*x*(y^2-1)-b*y*(x^2-1);
/*definition of compression function f*/
f:=x*y+1/(x*y)-y/x-x/y+(y+1)/(1-y)*(x+1)/(1-x)+(y+1)/(y-1)*(1-x)/(1+x)+
(y-1)/(1+y)*(x-1)/(x+1)+(1-y)/(1+y)*(x+1)/(x-1);
/* doubling of point (x1,y1), depends on the curve equation */
x3:=(2*y1^2+2)*x1/((x1^2+1)*y1^2-x1^2-1);
y3:=(2*x1^2+2)*y1/((x1^2-1)*y1^2+x1^2-1);
//End of exchangeable parameters
```