Publ. Math. Debrecen
Supplementum **100** (2022), 655–682
DOI: 10.5486/PMD.2022.Suppl.7

Arithmetic on generalized Hessian curves using compression function and its applications to the isogeny-based cryptography

By Michał Wroński and Tomasz Kijko

Abstract. In this paper, we present formulas for differential addition and doubling using the compression function $f_{GH,2}(P) = x_P + y_P$ of degree 2 on a generalized Hessian curve $E_{GH} : x^3 + y^3 + a = dxy$, where $P = (x_P, y_P)$. We use in this context elementary algebra methods. Moreover, we also present formulas for 2, 3-isogeny, and general ℓ-isogeny evaluation, using this function. It is worth noting that for the compression function $f_{GH,2}$, such formulas have not been presented before. On the other hand, we also use elementary algebra methods for obtaining differential addition and doubling formulas using the compression function $f_{GH,6}(P) = x_P y_P$ of degree 6, and we present formulas for 2 and general ℓ-isogeny evaluation using this function.

1. Introduction

Isogeny-based cryptography is one of the most promising fields in post-quantum cryptography. In the SIKE algorithm (Supersingular Isogeny Diffie–Hellman) specification, x-line arithmetic on the Montgomery curve is used. It is worth noting that it is also possible to use other alternative models of elliptic curves in this context, such as Edwards, twisted Edwards curves, Huff's curves, Hessian curves, generalized Hessian curves, and twisted Hessian curves. This paper mainly focuses on applying x-line arithmetic to the Hessian curves family. We consider the compression function on generalized Hessian curves, given by $f_{GH,2}(P) = x_P + y_P$, where $P = (x_P, y_P)$. This compression function may be easily obtained from the compression function $f_{TH,2}(P) = \frac{y_P+1}{x_P}$ on the twisted

Mathematics Subject Classification: 94A60, 14K02, 14H52.
Key words and phrases: generalized Hessian curves and compression on elliptic curves and isogeny-based cryptography.

Hessian curve E_{TH} and isomorphism between E_{GH} and E_{TH}, which is simple coordinates swapping. It is worth noting that formulas for differential addition on a twisted Hessian curve using the compression function $f_{TH,2}$ have been obtained in [5] using Gröbner basis mechanism. This paper presents algebraic methods for obtaining differential addition and doubling formulas on the curve E_{GH} using the compression function $f_{GH,2}$. The application of function $f_{GH,2}$ into the isogeny-based cryptography has not been presented before. This paper will show how to compute 2-isogeny and 3-isogeny, using formulas from [4]. Moreover, for the computation of isogeny of degree $\ell \geq 4$, we use the Vélu formula using isomorphic elliptic curves in the short Weierstrass form.

Even though the application of Vélu formula for the computation of 2-isogeny on Hessian curves using point representation in full projective coordinates was presented in [11], we apply Vélu formulas to obtain compression of isogeny evaluation formula for a point P given only by its compression $f_{GH,2}(P)$. Moreover, we use Vélu formulas only when $\ell \neq 3$.

Unfortunately, it seems that using the compression function $f_{GH,2}$ in isogeny-based cryptography is reasonable only in the context of SIDH and SIKE protocols, where consecutive computations of 2 and 3-isogenies are required. In the case, when it is necessary to compute isogenies of larger degree, like, e.g., in CRS [10] and CSIDH [3], application of the compression function $f_{GH,2}$ is challenging and inefficient because the isogeny evaluation formula for twisted Hessian curves given in [4] (and thus for generalized Hessian curves) has a multiplicative character. However, the compression function $f_{GH,2}$ has additive character.

Then next considered compression function on generalized Hessian curves presented in this paper is degree 6 function $f_{GH,6}(P) = x_P y_P$. This compression function has been considered in [7], where presented formulas for differential addition and doubling have been obtained using computational methods and Gröbner basis mechanism. In this paper, for the compression function $f_{GH,6}$, formulas for a differential addition and doubling have been derived algebraically. Moreover, we found the formulas for isogeny computations and point evaluations in the case of 2 and general ℓ-isogeny. In the paper [7] such formulas for isogenies computation have not been considered. Because of computation of such isogenies has multiplicative character, the function $f_{GH,6}$ could be used in practice in the case of ℓ-isogeny computations, for $\ell \geq 5$. In the case of $\ell = 3$ our approach of using the compression function $f_{GH,6}$ fails, because for different 3-torsion points P function $f_{GH,6}(P)$ may give the same results, which is inconvenient in our applications.

Some presented formulas in this paper are not valid if the characteristic of the field is two and/or three. For simplicity we assume in the whole paper, that the characteristic of the underlying field is larger than three.

2. Compression functions on elliptic curves

On elliptic curve E over a field $\mathbb{K}$ we call a compression function any rational function $f : E(\mathbb{K}) \to \mathbb{K}$ such that for a point $P \in E(\mathbb{K})$ holds $f(P) = f(-P)$. The degree of a compression function is the number of elements of the kernel of the map $f(P) - f(Q)$, where $P, Q \in E(\mathbb{K})$. If the function f is of degree 2, then $f(P) = f(Q)$ iff $Q = -P$. For any compression function f there is induced point multiplication of values $f(P)$ given by $[n]f(P) = f([n]P)$ for $n \in \mathbb{Z}$.

There exist rational functions for differential additions $A_1(x, y), A_2(x, y) \in K(x, y)$ such that

$$f(P + Q) + f(P - Q) = A_1(f(P), f(Q)),$$
$$f(P + Q)f(P - Q) = A_2(f(P), f(Q)).$$

Moreover, there also exists rational function for doubling $D(x) \in \mathbb{K}(x)$, such that

$$f([2]P) = D(f(P)).$$

The properties above allow to compute $[n]f(P)$ 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: $[n]f(P)$
$x_P := f(P)$; $x_Q := D(x_P)$;
for $i = k - 1, \ldots, 0$ **do**
  if $n_i = 1$ **then**
    $x_P := A(x_P, x_Q, f(P))$;
    $x_Q := D(x_Q)$;
  else
    $x_Q := A(x_P, x_Q, f(P))$;
    $x_P := D(x_P)$;
  end
end
return x_P;

It is worth noting that it is also possible to obtain a compression function of a degree greater than 2. It is possible if one considers translation $\tau_T : E \to E, \tau_T(P) = P + T$ for a particular chosen point $T \in E(\mathbb{K})$ of order n. Now one can search for the compression function f_{2n} of degree $2n$ which is invariant under involution and translation by T. It means that $f_{2n}(P) = f_{2n}(Q)$ if and only if $Q = \pm P + [k]T$, for $k = \overline{0, n-1}$. More details may be found in [7].

3. Generalized and twisted Hessian curves

Definition 1. [8] A generalized Hessian curve E_{GH} over a field $\mathbb{K}$ is given by the equation

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

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

The sum of points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on E_{GH} is given by formulas:

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

$$P + Q = \left(\frac{y_P^2 x_Q - y_Q^2 x_P}{x_Q y_Q - x_P y_P}, \frac{x_P^2 y_Q - x_Q^2 y_P}{x_Q y_Q - x_P y_P} \right);$$

(2) if $P = Q$ (point doubling)

$$[2]P = \left(\frac{y_P(a - x_P^3)}{x_P^3 - y_P^3}, \frac{x_P(y_P^3 - a)}{x_P^3 - y_P^3} \right).$$

The negation of the point $P = (x_P, y_P)$ is $-P = (y_P, x_P)$.

In projective coordinates, a generalized Hessian curve is given by the equation

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

The neutral element of the addition law is the point at infinity $(1 : -1 : 0)$. By swapping X with Z we obtain the equation of twisted Hessian curve in projective coordinates

$$E_{TH}/\mathbb{K} \ : \ aX^3 + Y^3 + Z^3 = dXYZ,$$

and affine coordinates

$$E_{TH}/\mathbb{K} \ : \ ax^3 + y^3 + 1^3 = dxy.$$

The addition law's neutral element for twisted Hessian curves is the point $(0, -1)$. The negation of the point $P = (x_P, y_P)$ is $-P = (\frac{x_P}{y_P}, \frac{1}{y_P})$.

The sum of points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on E_{TH} is given by formulas:

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

$$P + Q = \left(\frac{x_P - y_P^2 x_Q y_Q}{a x_P y_P x_Q^2 - y_Q}, \frac{y_P y_Q^2 - a x_P^2 x_Q}{a x_P y_P x_Q^2 - y_Q} \right);$$

b) if $P = Q$ (point doubling)

$$[2]P = \left(\frac{x_P - y_P^3 x_P}{a y_P x_P^3 - y_P}, \frac{y_P^3 - a x_P^3}{a y_P x_P^3 - y_P} \right).$$

Theorem 1. *Generalized Hessian curve $E_{GH}/\mathbb{K}$ is birationally equivalent to a twisted Hessian curve $E_{TH}/\mathbb{K}$. The isomorphism $\psi : E_{TH} \to E_{GH}$ for $P = (X : Y : Z) \in E_{TH}$ is given by the equation:*

$$\psi(P) = \psi(X : Y : Z) = (Z : Y : X).$$

The inverse isomorphism $\psi' : E_{GH} \to E_{TH}$ for $P' = (X' : Y' : Z') \in E_{GH}$ is given by the equation:

$$\psi'(P') = \psi'(X' : Y' : Z') = (Z' : Y' : X').$$

In the next two theorems, we denote by ω the primitive cube root of unity in the field $\mathbb{K}$.

Theorem 2. *There is given an elliptic curve E_{SW} in short Weierstrass form $E_{SW}/\mathbb{K} : y^2 = x^3 + Ax + B$ and there is point $T \in E_{SW}(\mathbb{K})$ of order 3. Then one can find isomorphic $E_{SW}/\mathbb{K}$ to the elliptic curve in triangular form $E_{TR}/\mathbb{K} : \overline{y}^2 + d\overline{x}\overline{y} + a\overline{y} = \overline{x}^3$, where*

(1) *d is any root of polynomial $W(s) = \frac{-1}{6912} s^8 - \frac{1}{24} A s^4 - B s^2 + A^2$;*
(2) *$a = (A + \frac{d^4}{48}) \frac{2}{d}$;*
(3) *$\overline{x} = x - \frac{d^2}{12}$;*
(4) *$\overline{y} = y - \frac{d\overline{x} + a}{2}$.*

Proof. The theorem is the result of allowed coordinates change for elliptic curves. □

Corollary 1. *There exists an isomorphism $\psi_1 : E_{SW} \to E_{TR}$, which transforms the point $P_{SW} \in E_{SW}(\mathbb{K})$ into the point $P_{TR} \in E_{TR}(\mathbb{K})$, where $P_{TR} = \psi_1(P_{SW}) = (\overline{x}, \overline{y}) = (x - \frac{d^2}{12}, y - \frac{d\overline{x} + a}{2})$.*

Theorem 3 (This is Theorem 5.3 in [1])**.** *There is given an elliptic curve in triangular form* $E_{TR}/\mathbb{F}_q : VW\,(V + dU + aW) = U^3$*. There exists a twisted Hessian curve* $E_{TH}/\mathbb{F}_q : (d^3 - 27a)X^3 + Y^3 + Z^3 = 3dXYZ$*, which is isomorphic to the curve* E_{TR} *by isomorphism* $\psi_2 : E_{TR} \to E_{TH}$*, where* $\psi_2(U, V, W) = (U, \omega(V + dU + aW) - \omega^2 V - aW, \omega^2\,(V + dU + aW) - \omega V - aW) = (X, Y, Z)$*. The inversion of* ψ_2 *is the isomorphism* $\psi_2^{-1} : E_{TH} \to E_{\triangle}$*, where* $\psi_2^{-1}(X, Y, Z) = \left(X, -\frac{dX+\omega Y+\omega^2 Z}{3}, -\frac{dX+Y+Z}{3a}\right)$.

Proof. The proof may be found in [1], Theorem 5.3. □

Theorem 4. *There is given an elliptic curve in triangular form* $E_{TR,a,d}/\mathbb{F}_q : VW\,(V + dU + aW) = U^3$*. There exists a generalized Hessian curve* $E_{GH}/\mathbb{F}_q : X^3 + Y^3 + (d^3 - 27a)Z^3 = 3dXYZ$*, which is isomorphic to the curve* E_{TR} *by isomorphism* $\psi_2 : E_{TR} \to E_{GH}$*, where* $\psi_2(U : V : W) = (\omega^2\,(V + dU + aW) - \omega V - aW : \omega(V + dU + aW) - \omega^2 V - aW : U) = (X : Y : Z)$*. The inversion of* ψ_2 *is the isomorphism* $\psi_2^{-1} : E_{TH} \to E_{TR}$*, where* $\psi_2^{-1}(X : Y : Z) = \left(Z : -\frac{dZ+\omega Y+\omega^2 X}{3} : -\frac{dZ+Y+X}{3a}\right)$.

Proof. The same as for Theorem 3 with replacing variables X and Z. □

The following remark is the consequence of Theorems 2 and 3.

Remark 1. For elliptic curves in short Weierstrass form E_{SW} where $3|\#E_{SW}(\mathbb{F}_q)$ and the point $P_{SW} \in E_{SW}$ given in XZ coordinates $P_{SW} = (X : Z)$, it is possible to find the point $P_{TH} = \psi_2(\psi_1(P_{SW}))$ (given in XR coordinates $(X : R)$, where $R = Y + Z$), where $P_{TH} = (12X - Zd^2 : -d(X - \frac{d^2}{12}) - 3aZ) = (X : R)$. Inverse transformation from P_{TH} (given by XR coordinates) to P_{SW} in XZ coordinates is given by $P_{SW} = \psi_1^{-1}(\psi_2^{-1}(P_{TH}) = \psi_2^{-1}(aX_{TH} : -(dX_{TH} + R_{TH})) = (12aX_{TH} - d^2(dX_{TH} + R_{TH}) : 12(dX_{TH} + R_{TH}))$.

Similarly, the remart below, is the consequence of Theorems 2 and 4.

Remark 2. For elliptic curves in short Weierstrass form E_{SW} where $3|\#E_{SW}(\mathbb{F}_q)$ and the point $P_{SW} \in E_{SW}$ given in XZ coordinates $P_{SW} = (X : Z)$, it is possible to find the point $P_{GH} = \psi_2(\psi_1(P_{SW}))$ given in RZ coordinates $(R = X + Y)$, where $P_{GH} = (-d(Z - \frac{d^2}{12}) - 3aX : 12Z - Xd^2) = (R : Z)$. Inverse transformation from P_{GH} (given by RZ coordinates) to P_{SW} (given by XZ coordinates) is given by $P_{SW} = \psi_1^{-1}(\psi_2^{-1}(P_{GH}) = \psi_2^{-1}(aZ_{GH} : -(dZ_{GH} + R_{GH})) = (12aZ_{GH} - d^2(dZ_{GH} + R_{GH}) : 12(dZ_{GH} + R_{GH}))$.

The application of compression functions in isogeny-based cryptography is presented in [9], in the context of compression functions of degree 8 on Edwards

curves. Similarly, the application of compression functions of degree 2 on Huff's curves in the isogeny-based cryptography is presented in [6]. We will focus on applying the compression function $f_{GH,6}(x,y) = xy$ on the generalized Hessian curve. The multiplicative character of formula (3) favors the compression function $f_{GH,6}$ for applications in isogeny-based cryptography. Let us note that $f_{GH,2}(x,y) = x + y$ is strictly additive and, therefore, applying this compression function to formula (3) seems to be much more challenging and inefficient.

We transformed the formulas for general ℓ-isogeny on a twisted Hessian curve from [4] into their equivalent formulas on generalized Hessian curves.

Let $E_{TH} : ax^3 + y^3 + 1 = dxy$ and $E'_{TH} : a'x^3 + y^3 + 1 = d'xy$, and let ℓ be the degree of the isogeny $\phi : E_{TH} \to E'_{TH}$, $n = \ell - 1$, and let $\overline{F} = \{(0,-1)\} \cup \sum_{i=1}^{n} \{(\overline{u_i}, \overline{v_i})\}$ be the kernel of the isogeny ϕ. Then, using the general formula for coefficients of an ℓ-isogenous twisted Hessian curve E_{TH}, the coefficients of the isogenous generalized Hessian curve E'_{TH} are equal to $a' = a^\ell, d' = \frac{(1-2n)d+6\sum_{i=1}^{n} \frac{1}{\overline{u_i v_i}}}{\prod_{i=1}^{n} \overline{u_i}}$.

Using birationally equivalence between generalized Hessian and twisted Hessian curve, coefficients of an ℓ-isogenous generalized Hessian curve may be computed as $a' = a^\ell, d' = \left((1-2n)d + 6\sum_{i=1}^{n} \frac{u_i^2}{v_i}\right) \prod_{i=1}^{n} u_i$, where the kernel of the isogeny is equal to $F = \{(1:-1:0)\} \cup \sum_{i=1}^{n} \{(u_i, v_i)\}$.

Using the fact, that if point $Q = (u_i, v_i)$ belongs to the kernel F, then $-Q = (v_i, u_i)$ also belongs to this kernel, and for odd $\ell = 2s+1$ it may be written that

$$\begin{aligned} d' &= \left((1-2n)d + 6\sum_{i=1}^{s} \left(\frac{u_i^2}{v_i} + \frac{v_i^2}{u_i}\right)\right) \prod_{i=1}^{s} u_i v_i \\ &= \left((1-2n)d + 6\sum_{i=1}^{s} \left(\frac{u_i^3 + v_i^3}{u_i v_i}\right)\right) \prod_{i=1}^{s} u_i v_i. \end{aligned} \tag{1}$$

Similarly, the equation for evaluation of degree ℓ isogeny, for $\ell \neq 3$, [4, Theorem 5] on a twisted Hessian curve may be easily transformed into the same form on a generalized Hessian curve:

$$\phi(P) = \left(\prod_{Q \neq (1:-1:0) \in F} x_{P+Q}, \prod_{Q \neq (1:-1:0) \in F} y_{P+Q}\right),$$

where $\phi : E_{GH} \to E'_{GH}$.

4. Compression function of degree 2 on generalized Hessian curves

Let us define the compression function on a generalized Hessian curve of degree 2 given by $f_{GH,2}(P) = f_{GH,2}(x_P, y_P) = x_P + y_P$. At first, it will be proved that $f_{GH,2}(P)$ has indeed degree 2.

PROOF. For $P = (x_P, y_P) \in E_{GH}(\mathbb{K})$ set $r_P = f_{GH,2}(P) = x_P + y_P$. Then $y_P = r_P - x_P$ and then E_{GH} equation

$$x_P^3 + y_P^3 + a = dx_P y_P$$

can be transformed into:

$$x_P^3 + (r_P - x_P)^3 + a = dx_P(r_P - x_P),$$

which may be simplified to the form

$$3r_P x_P^2 + dx_P^2 - 3r_P^2 x_P - dr_P x_P + r_P^3 + a = 0.$$

If this equation is satisfied by x_P, then, because the degree of the equation is equal to 2, the second root is $r_P - x_P$, which means that the only points, for which holds $r_P = x_P + y_P$ and $3r_P x_P^2 + dx_P^2 - 3r_P^2 x_P - dr_P x_P + r_P^3 + a = 0$ are points $P = (x_P, y_P)$ and $-P = (y_P, x_P)$. □

4.1. Obtaining formulas for point doubling and points addition on generalized Hessian curves using the compression function $f_{GH,2}(x, y)$ of degree $d = 2$. Let $r = f_{GH,2}(x, y) = x + y$ be the compression function on a generalized Hessian curve. Using Sylvester formulas for points addition on a generalized Hessian curve

$$x_{P+Q} = \frac{y_P^2 x_Q - y_Q^2 x_P}{x_Q y_Q - x_P y_P}, \qquad y_{P+Q} = \frac{x_P^2 y_Q - x_Q^2 y_P}{x_Q y_Q - x_P y_P},$$

it is possible to write the sum of $f_{GH,2}(P+Q)+f_{GH,2}(P-Q)$, where $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in the following form:

$$f_{GH,2}(P+Q) + f_{GH,2}(P-Q) = \frac{L}{M} = \frac{-y_P {y_Q}^2 - x_P {y_Q}^2 + {y_P}^2 y_Q + {x_P}^2 y_Q + x_Q {y_P}^2 - {x_Q}^2 y_P - x_P {x_Q}^2 + {x_P}^2 x_Q}{x_Q y_Q - x_P y_P}.$$

Using that $r_P = x_P + y_P$ and $r_Q = x_Q + y_Q$, the nominator may be easily transformed into the form:

$$-r_P({y_Q}^2 + {x_Q}^2) + r_Q({y_P}^2 + {x_P}^2).$$

Using a generalized Hessian curve equation and putting $r = x + y$ and $t = xy$, one can obtain that if

$$x^3 + y^3 + a = dxy,$$

then

$$(x + y)((x + y)^2 - 3xy) + a = dxy. \tag{2}$$

Putting $t = xy$ the Equation (2) is equivalent to

$$r^3 - 3rt + a = dt$$

and finally:

$$t = \frac{r^3 + a}{d + 3r}. \tag{3}$$

Putting $t_P = x_P y_P$ and $t_Q = x_Q y_Q$, one can write

$$y_P{}^2 + x_P{}^2 = (x_P + y_P)^2 - 2x_P y_P = r_P^2 - \frac{2(r_P^3 + a)}{d + 3r_P} \tag{4}$$

and

$$y_Q{}^2 + x_Q{}^2 = (x_Q + y_Q)^2 - 2x_Q y_Q = r_Q^2 - \frac{2(r_Q^3 + a)}{d + 3r_Q}. \tag{5}$$

Using equations (4) and (5), one can obtain L as

$$L = -\frac{r_P(r_Q^2 - 2(r_Q^3 + a))}{d + 3r_Q} + \frac{r_Q(r_P^2 - 2(r_P^3 + a))}{d + 3r_P}.$$

M may be transformed into the following form:

$$M = \frac{(r_Q^3 + a)}{(d + 3r_Q)} - \frac{(r_P^3 + a)}{(d + 3r_P)}.$$

Finally, $\frac{L}{M}$ can be presented as:

$$\frac{L}{M} = -\frac{((3r_P^2 + dr_P)r_Q^2 + (dr_P^2 + d^2 r_P + 6a)r_Q + 6ar_P + 2ad)}{((3r_P + d)r_Q^2 + (3r_P^2 + dr_P)r_Q + dr_P^2 - 3a)}.$$

To obtain doubling formulas, it is convenient to use formulas for complete arithmetic [8]:

$$x_{[2]P} = \frac{y_P(a - x_P^3)}{x_P^3 - y_P^3}, \qquad y_{[2]P} = \frac{x_P(y_P^3 - a)}{x_P^3 - y_P^3}.$$

Then

$$r_{[2]P} = x_{[2]P} + y_{[2]P} = -\frac{(x_P y_P^2 + x_P^2 y_P + a)}{(y_P^2 + x_P y_P + x_P^2)}.$$

The nominator $-(x_P y_P^2 + x_P^2 y_P + a)$ may be transformed into the form $-(x_P y_P (x_P + y_P) + a)$ which is equivalent to $-(\frac{r_P(r_P^3+a)}{d+3r_P} + a)$. The denominator $(y_P^2 + x_P y_P + x_P^2)$ may be written as $(x_P + y_P)^2 - x_P y_P$, which is equivalent to $r_P^2 - \frac{r_P^3+a}{d+3r_P}$. Finally:

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

4.2. Computing 2-isogenies on a generalized Hessian curve using compression function of degree 2. This subsection will present how to compute 2-isogeny on a generalized Hessian curve using a point compression.

First of all, the compression of point $P = (x_P, y_P)$, where $P \in E_{GH}(\mathbb{K})$ in affine coordinates may be represented as $f(P) = x_P + y_P$, so for point $P = (X_P : Y_P : Z_P)$ in projective coordinates, its compression may be presented as $(X_P + Y_P : Z_P)$.

Several lemmas need to be proved before formulas for 2-isogeny computation on a generalized Hessian curve will be presented.

Lemma 1. *On a generalized Hessian curve, every point of order* 2 *may be presented as* (α, α) *in affine coordinates, where* α *is any root of the polynomial* $w(s) = 2s^3 - ds^2 + a$.

Proof. For every point $t_Q = (\alpha, \beta)$ of order 2 equality $P = -P$ holds. Because for every point $P = (x_P, y_P) \in E_{TH}(\mathbb{K})$ holds that $-P = (y_P, x_P)$ in affine coordinates, then for point t_Q must hold $\alpha = \beta$. Then must also hold $2\alpha^3 + a = d\alpha^2$, which is equivalent to $2\alpha^3 - d\alpha^2 + a = 0$, so α must be any root of the polynomial $2s^3 - ds^2 + a$ in the field $\mathbb{K}$. □

Lemma 2. *Coefficients of the generalized Hessian curve* $E'_{GH}/\mathbb{K}$, *which is* 2*-isogenous to the curve* $E_{GH}/\mathbb{K}$ *are equal to* $a' = a^2, d' = \frac{-d\alpha+6}{\alpha^2}$, *where the kernel of the isogeny* ϕ *is the point* $T_Q = (\alpha, \alpha)$ *of order* 2.

Proof. Let ℓ be the degree of isogeny ϕ, $n = \ell - 1$, and let $F = \{(1 : -1 : 0)\} \cup \sum_{i=1}^{n} \{(u_i, v_i)\}$ be the kernel of the isogeny ϕ. Then using the general formula for coefficients of the ℓ-isogenous generalized Hessian curve E_{GH}, where the kernel of ℓ-isogeny is $F = \{(1 : -1 : 0)\} \cup \sum_{i=1}^{n} \{(u_i, v_i)\}$,

the curve coefficients are equal to

$$a' = a^{\ell}, \tag{6}$$

$$d' = \left((1-2n)d + 6\sum_{i=1}^{n}\frac{u_i^2}{v_i}\right)\prod_{i=1}^{n}u_i. \tag{7}$$

Because in the case of 2-isogeny $F = \{(1 : -1 : 0), (\alpha, \alpha)\}$, then $a' = a^2$, $d' = -d\alpha + 6\alpha^2$. □

Lemma 3. *If T_Q is the point of order 2, then*

$$f(P + T_Q) = A(f(P), f(T_Q))/2,$$

where $A(f(P), f(T_Q))$ is a rational function.

Proof. The differential addition $f(P+T_Q) + f(P-T_Q)$ may be presented by some rational function $A(f(P), f(T_Q))$. If a point T_Q is of order 2, then $f(P + T_Q) = f(P - T_Q)$ and therefore $f(P + T_Q) = A(f(P), f(T_Q))/2$. □

Theorem 5. *Point evaluation $\phi(P)$ by the isogeny $\phi : E_{GH} \to E'_{GH}$ with the kernel $F = \{(1 : -1 : 0), T_Q\}$, using formulas from Section 3, is equal to*

$$\phi(P) = \left(x_P x_{P+T_Q}, y_P y_{P+T_Q}\right),$$

where $T_Q = (\alpha, \alpha)$, $P = (x_P, y_P)$ and $P + T_Q = (x_{P+T_Q}, y_{P+T_Q})$.

Lemma 4. *Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, where $P, Q \in E_{GH}(\mathbb{K})$. If $m = x_P x_Q + y_P y_Q$ and $n = y_P x_Q + y_Q x_P$, then $r_P r_Q = m + n$, where $r_P = f(P) = x_P + y_P$ and $r_Q = f(Q) = x_Q + y_Q$.*

Proof. Because $r_P = x_P + y_P$ and $r_Q = x_Q + y_Q$, then $r_P r_Q = y_P y_Q + x_P x_Q + y_P x_Q + y_Q x_P = m + n$. □

Lemma 5. *The number $m = x_P x_Q + y_P y_Q$ is the root of polynomial $G(s) = 3r_P r_Q s^2 - 3r_P^2 r_Q^2 s - 3t_R r_P r_Q - (dt_P - a)(dt_Q - a)$, where $t_R = t_P t_Q$.*

Proof. Let $x_P^3 + y_P^3 + a = dx_P y_P$ and $x_Q^3 + y_Q^3 + a = dx_Q y_Q$. Then $x_P^3 + y_P^3 = dx_P y_P - a$ and $x_Q^3 + y_Q^3 = dx_Q y_Q - a$. If one multiplies these formulas, then

$$\begin{aligned}\left(x_P^3 + y_P^3\right)\left(x_Q^3 + y_Q^3\right) &= x_P^3 x_Q^3 + y_P^3 y_Q^3 + x_Q^3 y_P^3 + x_P^3 y_Q^3 \\ &= (dx_P y_P - a)(dx_Q y_Q - a).\end{aligned}$$

Now one can substitute $t_P = x_P y_P$, which may be computed using formula (3) as $B(r_P)$ and $t_Q = x_Q y_Q$ as $B(r_Q)$. Then $t_R = t_P t_Q = x_P x_Q y_P y_Q$.
In the next step

$$\begin{aligned} &x_P^3 x_Q^3 + y_P^3 y_Q^3 + x_Q^3 y_P^3 + x_P^3 y_Q^3 \\ &\quad = (y_P y_Q + x_P x_Q)\left((y_P y_Q + x_P x_Q)^2 - 3 y_P y_Q x_P x_Q\right) \\ &\qquad + (y_P x_Q + y_Q x_P)\left((y_P x_Q + y_Q x_P)^2 - 3 y_P y_Q x_P x_Q\right) \\ &\quad = m(m^2 - 3t_R) + n(n^2 - 3t_R) = (d x_P y_P - a)\,(d x_Q y_Q - a)\,. \end{aligned}$$

Because $n = r_P r_Q - m$, then

$$\begin{aligned} &m(m^2 - 3t_R) + (r_P r_Q - m)((r_P r_Q - m)^2 - 3t_R) \\ &\quad = 3 r_P r_Q m^2 - 3 r_P^2 r_Q^2 m - 3 t_R r_P r_Q + r_P^3 r_Q^3 = (d x_P y_P - a)\,(d x_Q y_Q - a)\,. \end{aligned}$$

It means that m is a root of the polynomial

$$G(s) = 3 r_P r_Q s^2 - 3 r_P^2 r_Q^2 s - 3 t_R r_P r_Q - (d t_P - a)\,(d t_Q - a)\,. \qquad \square$$

Lemma 6. *$m = x_P x_Q + y_P y_Q$ is the root of the polynomial $H(s) = s^3 - 3t_R s - d' t_R + a'$.*

Proof. According to Lemma 2, if $P = (x_P, y_P)$, Q is 2-torsion point equal to $Q = (x_Q, y_Q)$, then point $P_3 = (x_R, y_R)$, where $r_R = x_R + y_R$ and $x_R = x_P x_Q$, $y_R = y_P y_Q$, lies on the curve $E'_{GH} : x^3 + y^3 + a' = d' xy$, where a' and d' are given by Equations (6) and (7) respectively. Moreover, it holds that $r_R = x_R + y_R = x_P x_Q + y_P y_Q = m$. Making some transformations, one can obtain

$$\begin{aligned} x_R^3 + y_R^3 &= (x_R + y_R)\left((x_R + y_R)^2 - 3 x_R y_R\right) \\ &= m(m^2 - 3t_R) = d' x_R y_R - a' = d' t_R - a'. \end{aligned}$$

So finally

$$m^3 - 3 t_R m - d' t_R + a' = 0$$

and m is a root of the polynomial $H(s) = s^3 - 3t_R s - d' t_R + a'$. $\square$

The previous lemmas lead to the following theorem.

Theorem 6. *If $m = y_P y_Q + x_P x_Q$, then m is the only root of the polynomial $J(s) = 3r_P r_Q H(s) - G(s)(s + r_P r_Q)$ and by definition $r_R = m$.*

Proof. Let us make the following transformations

$$\begin{aligned}
J(s) &= G(s) - sG(s) + 3r_P r_Q H(s) \\
&= (1-s)\left(3r_P r_Q s^2 - 3r_P^2 r_Q^2 s - 3t_R r_P r_Q - (dt_P - a)(dt_Q - a)\right) \\
&\quad + 3r_P r_Q \left(s^3 - 3t_R s - d' t_R + a'\right) \\
&= 3r_P r_Q s^2 - 3r_P^2 r_Q^2 s - 3t_R r_P r_Q - (dt_P - a)(dt_Q - a) \\
&\quad - 3r_P r_Q s^3 + 3r_P^2 r_Q^2 s^2 + 3t_R r_P r_Q s + s(dt_P - a)(dt_Q - a) \\
&\quad + 3r_P r_Q s^3 - 9r_P r_Q t_R s - 3r_P r_Q d' t_R + 3r_P r_Q a' \\
&= (a^2 - adt_P - adt_Q + d^2 t_P t_Q + 2r_P^3 r_Q^3 - 6r_P r_Q t_R)s \\
&\quad + a^2 r_P r_Q - adr_P r_Q t_P - adr_P r_Q t_Q + d^2 r_P r_Q t_P t_Q \\
&\quad + 3apr_P r_Q - 3dpr_P r_Q t_R - r_P^4 r_Q^4 + 3r_P^2 r_Q^2 t_R.
\end{aligned}$$

Finally

$$m = \quad r_R = \tfrac{L_3}{M_3},$$

where

$$\begin{aligned}
L_3 = &-a^2 r_P r_Q + adr_P r_Q t_P + adr_P r_Q t_Q - d^2 r_P r_Q t_P t_Q - 3a' r_P r_Q \\
&+ 3d' r_P r_Q t3 + r_P^4 r_Q^4 - 3r_P^2 r_Q^2 t_R
\end{aligned}$$

and

$$M_3 = a^2 - adt_P - adt_Q + d^2 t_P t_Q + 2r_P^3 r_Q^3 - 6r_P r_Q t_R. \qquad \square$$

4.3. 3-isogeny computation. Using birationally equivalence between twisted Hessian and generalized Hessian curves and formulas from [4], formulas for 3-isogeny $\phi : E_{GH} \to E'_{GH}$ computation on generalized Hessian curves, where $E_{GH} : x^3 + y^3 + a = dxy$ and $E'_{GH} : x^3 + y^3 + a' = d'xy$, are as follows:

(1) if the kernel of the isogeny is $F = \{(1 : -1 : 0), (1 : -\omega : 0), (1 : -\omega^2 : 0)\}$, then

$$P' = \left(\frac{\omega x^3 + \omega^2 y^3 + a}{x_P y_P}, \frac{\omega^2 x^3 + \omega y^3 + a}{xy}\right)$$

and $P' \in GH_{a',d'}$, where $a' = d^3 - 27a$ and $d' = 3d$;

(2) if the kernel of the isogeny is $F = \{(1 : -1 : 0), (0 : -c : 1), (-c : 0 : 1)\}$, where $c^3 = a$, then

$$P' = \left(c^2y + cx^2 + y^2x : c^2x + cy^2 + yx^2 : x_P y_P\right) \tag{8}$$

and $P' \in GH_{a',d'}$, where $a' = d^2c + 3dc^2 + 9a$ and $d' = d + 6c$;

(3) if the kernel of the isogeny is $F = \{(1 : -1 : 0), (0 : -\omega c : 1), (-\omega c : 0 : 1)\}$, where $(\omega c)^3 = a$, then

$$P' = \left(c^2\omega^2 y + c\omega x^2 + y^2x : c^2\omega^2 x + c\omega y^2 + yx^2 : xy\right)$$

and $P' \in GH_{a',d'}$, where $a' = d^2c\omega + 3dc^2\omega^2 + 9a$ and $d' = d + 6c\omega$;

(4) if the kernel of the isogeny is $F = \{(1 : -1 : 0), (0 : -\omega^2 c : 1), (-\omega^2 c : 0 : 1)\}$, where $(\omega^2 c)^3 = a$, then

$$P' = \left(c^2\omega y + c\omega^2 x^2 + y^2x : c^2\omega x + c\omega^2 y^2 + yx^2 : xy\right)$$

and $P' \in GH_{a',d'}$, where $a' = d^2c\omega + 3dc^2\omega^2 + 9a$ and $d' = d + 6c\omega$.

Proof. Points (1) and (2) follow simply from [4]. Moreover, let us note that if $a = c^3$, then $a = c_2^3 = (\omega c)^3$ and $a = c_3^3 = (\omega^2 c)^3$. It means that if one substitute c in Equation (8) by c_2, c_3 respectively, then one obtains formulas from points (2), (3) and (4). □

Theorem 7. *Using the compression function $r_P = f_{GH,2}(P) = (x_P + y_P)$ one can write as follows.*

If the kernel of the isogeny $\phi : E_{GH} \to E'_{GH}$ is point $(1 : -\omega : 0)$ or $(1 : -\omega^2 : 0)$, and $P' = \phi(P), r_P = f_{GH,2}(P)$ then

$$r_{P'} = f_{GH,2}(P') = \frac{3a(d + 3r_P)}{r_P^3 + a} - d.$$

Proof. Let $K = (1 : -\omega : 0)$ or $K = (1 : -\omega^2 : 0)$ be the point generating the kernel of the 3-isogeny. The only rational points having Z-coordinate equal to 0 are $(1 : -1 : 0)$, which is the neutral element, and $(1 : -\omega : 0), (1 : -\omega^2 : 0)$ which are points of order 3. If one checks that $Z \neq 0$, one can compute the 3-isogeny with such kernel.

At first, $r_P = x_P + y_P$, so it means that

$$r_{P'} = \frac{\omega x_P^3 + \omega^2 y_P^3 + a + \omega^2 x_P^3 + \omega y_P^3 + a}{x_P y_P}.$$

Using that

$$\omega + \omega^2 = -1,$$

one obtains

$$r_{P'} = \frac{-(x_P^3 + y_P^3) + 2a}{x_P y_P} = \frac{3a}{x_P y_P} - d = \frac{3a(d + 3r_P)}{r_P^3 + a} - d. \qquad \square$$

Theorem 8. *Using the compression function $r_P = f_{GH,2}(P) = (x_P + y_P)$ one can write as follows: if the kernel of the isogeny ϕ is point $Q = (0 : -c : 1)$ or $Q = (-c : 0 : 1)$, where $c^3 = a$, and $r = f_{GH,2}(P)$ then*

$$r_{P'} = f_{GH,2}(P') = \frac{(d + 3r_P)(c^2 r_P + c r_P^2)}{r_P^3 + a} - 2c + r_P.$$

Proof. Let $K = (0 : -c : 1)$ or $K = (-c : 0 : 1)$ be the generator of the kernel of the 3-isogeny. One can compute c as $c = -\frac{K_X + K_Y}{K_z}$. Then one can compute the 3-isogeny with such kernel as follows.

At first, $r_P = x_P + y_P$, so it means that

$$\begin{aligned} r_{P'} &= \frac{c^2 y_P + c x_P^2 + y_P^2 x_P + c^2 x_P + c y_P^2 + y_P x_P^2}{x_P y_P} \\ &= \frac{c^2(x_P + y_P) + c(x_P^2 + y_P^2) + x_P y_P (x_P + y_P)}{x_P y_P} \\ &= \frac{c^2 r_P + c(r_P^2 - 2x_P y_P) + x_P y_P r_P}{x_P y_P} \\ &= \frac{c^2 r_P + c r_P^2}{x_P y_P} - 2c + r_P = \frac{(d + 3r_P)(c^2 r_P + c r_P^2)}{r_P^3 + a} - 2c + r_P. \end{aligned} \qquad \square$$

4.4. Computation of general odd degree isogenies on twisted Hessian curves. Using formulas presented in [4] for computations using a point compression function $f_{GH,2}(P)$ of isogenies of degree $\ell > 3$ seems to be, however possible, very hard and inefficient.

In this case, instead of using formulas presented in [4] alone, in this paper, we proposed a method of adaptation Velú's formulas on the short Weierstrass curve, together with formulas presented in [4].

The main idea may be presented as follows. Because the compression function $f_{GH,2}(x, y) = x + y$ is additive, at first, the point P, for which one wants to compute an isogeny $\phi : E_{GH} \to E'_{GH}$ and all points belonging to the kernel F of the isogeny, have to be transformed into the short Weierstrass curve E_{SW}. At the same time, using formulas from [4], it is possible to compute the coefficients of

the isogenous generalized Hessian curve E'_{GH}. In the next step, one computes isogenous short Weierstrass curve E'_{SW}, and the point P'_{SW}, using isogeny ψ. It should be noted that curves E'_{GH} and E'_{SW} will be isomorphic. At the next step, it is easy to find the isomorphism between E'_{GH} and E'_{SW} and therefore, it is easy to transform the point P'_{SW} into the point $P'_{GH} \in E'_{GH}$.

In the Figure 1 we present all transformations necessary to obtain an isogenous generalized Hessian curve E'_{GH} using the compression function $f_{GH,2}$, where the degree ℓ of isogeny is odd and $\ell \geq 5$.

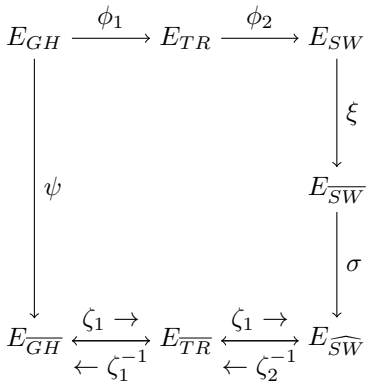

Figure 1. Transformations necessary for obtaining ℓ-isogenous generalized Hessian curve using the compression function $f_{GH,2}$.

Now we define particular isomorphisms and isogenies, which appear in Figure 1.

(1) Isomorphism ϕ_1: $E_{GH} \rightarrow E_{TR}$, where $E_{GH}/\mathbb{K} : x^3 + y^3 + a = dxy$, $E_{TR}/\mathbb{K} : t^2 + a_\triangle st + d_\triangle t = s^3$ and:

$$a_\triangle = \frac{d^3}{27^2} - \frac{a}{27}, \quad d_\triangle = \frac{d}{3}.$$

For $P_{GH} = (x_P, y_P) \in E_{GH}$ with the compression function $f_{GH,2}(P_{GH}) = x_p + y_p = r_P$ we have:

$$f_{TR,2}\left(\phi_1(P_{GH})\right) = \frac{-3a}{f_{GH,2}(P_{GH}) + d} = \frac{-3a}{r_P + d},$$

where the compression function of degree 2 on a triangular curve is equal to $f_{TR,2}(s_P, t_P) = s_P$ for $P_{TR} = (s_P, t_P) \in E_{TR}(\mathbb{K})$.

(2) Isomorphism ϕ_2: $E_{TR} \to E_{SW}$, where $E_{TR}/\mathbb{K} \ : \ t^2 + a_\triangle st + d_\triangle t = s^3$, $E_{SW}/\mathbb{K} \ : \ v^2 = u^3 + Au + B$ and

$$A = \frac{a_\triangle d_\triangle}{2} - \frac{d_\triangle^4}{48}, \quad B = \frac{-d_\triangle^2}{12}A + \frac{a_\triangle^2}{4} - \frac{d_\triangle^6}{2^6}.$$

For $P_{TR} = (s_P, t_p) \in E_{TR}$ with the compression function $f_{TR,2}(P_{TR}) = s_P$ we have:

$$f_{SW,2}\left(\phi_2(P_{TR})\right) = f_{TR,2}(P_{TR}) + \frac{d_\triangle^2}{12} = s_P + \frac{d_\triangle^2}{12},$$

where the compression function of degree 2 on a short Weierstrass curve is equal to $u_P = f_{SW,2}(u_P, v_P)$ and $P_{SW} = (u_P, v_P) \in E_{SW}(\mathbb{K})$.

(3) Isogeny ξ with a kernel $F = \{(0:1:0)\} \cup \sum_{i=1}^{n} \{Q_i = (u_i, v_i)\}$ from $E_{SW} \to E_{\overline{SW}}$, where $E_{SW} \ : \ v^2 = u^3 + Au + B$ and $E_{\overline{SW}} \ : \ \overline{v}^2 = \overline{u}^3 + \overline{A}\overline{u} + \overline{B}$, and:

$$\xi(u_p, v_p) = \left(u_p + \sum_{Q \in F - \{(0:1:0)\}} (u_{P+Q} - u_Q), v_p + \sum_{Q \in F - \{(0:1:0)\}} (v_{P+Q} - v_Q) \right),$$

where

$$\overline{A} = (A - 5\alpha), \quad \overline{B} = B - 7\beta,$$

$$\alpha = 2\sum_{Q \in F^+}(3 \quad u_P^2 + A), \qquad \beta = 2\sum_{Q \in F^+}(2v_P^2 + v_p(3v_P^2 + A)).$$

For the compression function $f_{\overline{SW},2}(\overline{u}, \overline{v}) = \overline{u}$ we have

$$\begin{aligned} f_{\overline{SW},2}(\xi(u_P, v_P)) &= f_{\overline{SW},2}\big(u_P + \sum_{Q \in F - \{(0:1:0)\}} (u_{P+Q} - u_Q), v_p + \sum_{Q \in F - \{(0:1:0)\}} (v_{P+Q} - v_Q)\big) \\ &= u_p + \sum_{Q \in F - \{(0:1:0)\}} (u_{P+Q} - u_Q). \end{aligned}$$

where

$$\overline{A} = A - 5\alpha, \quad \overline{B} = B - 7\beta,$$

$$\alpha = 2\sum_{Q \in F^+}(3 \quad u_Q^2 + A), \qquad \beta = 2\sum_{Q \in F^+}(5u_Q^3 + 3Au_P + 2B).$$

(4) Isomorphism σ: $E_{\overline{SW}} \to E_{\widehat{SW}}$, $E_{\overline{SW}} \ : \ \overline{v}^2 = \overline{u}^3 + \overline{A}\overline{u} + \overline{B}$ and $E_{\widehat{SW}} \ : \ \widehat{v}^2 = \widehat{u}^3 + \widehat{A}\widehat{u} + \widehat{B}$. Let $\gamma \in \mathbb{K}^*$ be a solution of the following system of equations:

$$\begin{cases} \gamma^4 \widehat{A} = \overline{A}, \\ \gamma^6 \widehat{B} = \overline{B}. \end{cases}$$

For $P_{\overline{SW}} = (\overline{u}_P, \overline{v}_P) \in E_{\overline{SW}}$ with the compression function $f_{\overline{SW},2}(P_{\overline{SW}}) = \overline{u}_P$ we have:

$$f_{\widehat{SW},2}\left(\sigma(P_{\overline{SW}})\right) = f_{\widehat{SW},2}(\gamma^2\overline{u}_P, \gamma^3\overline{v}_P) = \gamma^2\overline{u}_P,$$

where the compression function of degree 2 on $E_{\widehat{SW}}$ is equal to $f_{\widehat{SW},2}(\hat{u}_P, \hat{v}_P) = \hat{u}$ for $P_{\widehat{SW}} = (\hat{u}_P, \hat{v}_P) \in \overline{E}_{\widehat{SW}}(\mathbb{K})$.

(5) Isogeny ψ with a kernel $F = \{(1 : -1 : 0)\} \cup \sum_{i=1}^{s}\{Q_i = (x_i, y_i), -Q_i = (y_i, x_i)\}$ from E_{GH} to $E_{\overline{GH}}$, where $E_{GH} : x^3 + y^3 + a = dxy$ and $E_{\overline{GH}}/\mathbb{K} : \overline{x}^3 + \overline{y}^3 + \overline{a} = \overline{d}\overline{x}\overline{y}$, and:

$$\begin{aligned}\overline{a} &= a^{\ell},\\ \overline{d} &= \left((1-2n)d + 6\sum_{i=1}^{s}\left(d - a\tfrac{d+3r_i}{r_i^3+a}\right)\right)\prod_{i=1}^{s}\tfrac{r_i^3+a}{d+3r_i}.\end{aligned}$$

and $r_i = x_i + y_i$.

(6) Isomorphism ζ_1: $E_{\overline{GH}} \to E_{\overline{TR}}$, where $E_{\overline{GH}}/\mathbb{K} : \overline{x}^3+\overline{y}^3+\overline{a} = \overline{d}\overline{x}\overline{y}$, $E_{\overline{TR}}/\mathbb{K} : \overline{t}^2 + \overline{a}_{\triangle}\overline{s}\overline{t} + \overline{d}_{\triangle}\overline{t} = \overline{s}^3$ and:

$$\overline{a}_{\triangle} = \frac{\overline{d}^3}{27^2} - \frac{\overline{a}}{27}, \quad \overline{d}_{\triangle} = \frac{\overline{d}}{3}.$$

(7) Isomorphism ζ_2: $E_{\overline{TR}} \to E_{\widehat{SW}}$, where $E_{\overline{TR}}/\mathbb{K} : \overline{t}^2 + \overline{a}_{\triangle}\overline{s}\overline{t} + \overline{d}_{\triangle}\overline{t} = \overline{s}^3$, $E_{\widehat{SW}} : \hat{v}^2 = \hat{u}^3 + \widehat{A}\hat{u} + \widehat{B}$ and

$$\widehat{A} = \frac{\overline{a}_{\triangle}\overline{d}_{\triangle}}{2} - \frac{\overline{d}_{\triangle}^4}{48}, \quad \widehat{B} = \frac{-\overline{d}_{\triangle}^2}{12}\hat{A} + \frac{\overline{a}_{\triangle}^2}{4} - \frac{\overline{d}_{\triangle}^6}{2^6}.$$

(8) Isomorphism ζ_1^{-1}: $E_{\overline{TR}} \to E_{\overline{GH}}$, where $E_{\overline{TR}}/\mathbb{K} : \overline{t}^2 + \overline{a}_{\triangle}\overline{s}\overline{t} + \overline{d}_{\triangle}\overline{t} = \overline{s}^3$, $E_{\overline{GH}}/\mathbb{K} : \overline{x}^3+\overline{y}^3+\overline{a} = \overline{d}\overline{x}\overline{y}$. For $P_{\overline{TR}} = (\overline{s}_P, \overline{t}_P) \in E_{\overline{TR}}$ with the compression function $f_{\overline{TR},2}(P_{\overline{TR}}) = \overline{s}_P$ we have:

$$f_{\overline{GH},2}(\zeta_1^{-1}(P_{\overline{TR}})) = \frac{-\overline{d}_{\triangle}\overline{s}_P - 3\overline{a}_{\triangle}}{\overline{s}_P},$$

where the compression function of degree 2 on a generalized Hessian curve is equal to $f_{\overline{GH},2}(\overline{x}_P, \overline{y}_P) = \overline{x}_P + \overline{y}_P$ for $P_{\overline{GH}} = (\overline{x}_P, \overline{y}_P) \in E_{\overline{GH}}(\mathbb{K})$.

(9) Isomorphism ζ_2^{-1}: $E_{\widehat{SW}} \to E_{\overline{TR}}$, where $E_{\widehat{SW}} : \hat{v}^2 = \hat{u}^3 + \widehat{A}\hat{u} + \widehat{B}$ and $E_{\overline{TR}}/\mathbb{K} : \overline{t}^2 + \overline{a}_{\triangle}\overline{s}\overline{t} + \overline{d}_{\triangle}\overline{t} = \overline{s}^3$ For $P_{\widehat{SW}} = (\widehat{x}_P, \widehat{y}_P) \in E_{\widehat{SW}}$ with the compression function $f_{\widehat{SW},2}(P_{\widehat{SW}}) = \widehat{x}_P = \widehat{r}_P$ we have:

$$f_{\overline{TR},2}(\kappa_2(P_{\widehat{SW}})) = \widehat{r}_P - \frac{\overline{d}^2}{12},$$

where the compression function of degree 2 on a triangular curve is equal to $f_{\overline{TR},2}(\overline{s}_P, \overline{t}_P) = \overline{s}_P$ for $P_{\overline{TR}} = (\overline{s}_P, \overline{t}_P) \in E_{\overline{TR}}(\mathbb{K})$.

5. Compression function of degree 6 on generalized Hessian curves using 3-torsion point

This section will present how to obtain a compression function f of degree 6 using natural symmetries on generalized Hessian curves and action on a 3-torsion point.

Theorem 9 ([7]). *If $T_3 \in E_{GH}(\mathbb{K})$ is a point of order 3 of the form $(1 : -\omega : 0)$ on a generalized Hessian curve E_{GH}, where ω is a root of the polynomial $\omega^2 + \omega + 1$, then the compression function $f_{GH,6} : E_{GH}(\mathbb{K}) \to \mathbb{K}$, $f_{GH,6}(x, y) = xy$ has degree 6, more exactly $f_{GH,6}(P) = f_{GH,6}(Q)$, where $Q = \pm P + [k]T_3$ and $k = \overline{0, 2}$.*

Proof. At first, we will show that $f_{GH,6}(P) = f_{GH,6}(Q)$ if and only if $P = \pm Q + [k]T_3$, where $k = \overline{0, 2}$ and $T_3 = (1 : -\omega : 0)$.

Let us denote $f_{GH,6}(P) = r_P = xy$. Let us assume that $x, y \neq 0$. Then $y = \frac{r_P}{x}$ and because $x^3 + y^3 + a = dxy$, then

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

and

$$g(x) = x^6 + (a - dr_P)x^3 + {r_P}^3 = 0.$$

The equation (5) has at most 6 different roots in $\mathbb{K}$. It is easy to show that if x is one of the roots of this equation, then the other roots are equal to $\omega x, \omega^2 x, \frac{r_P}{x}, \frac{r_P}{\omega x}, \frac{r_P}{\omega^2 x}$. It means that

$$\begin{aligned} rp &= f_{GH,6}(x, y) = f_{GH,6}(y, x) = f_{GH,6}(\omega x, \omega^2 y) \\ &= f_{GH,6}(\omega^2 y, \omega x) = f_{GH,6}(\omega^2 x, \omega y) = f_{GH,6}(\omega y, \omega^2 x) \end{aligned}$$

and finally $f_{GH,6}(P) = f_{GH,6}(Q)$ if and only if $Q = \pm P + [k]T_3$, for $k = \overline{0, 2}$. □

Remark 3. Let us note that Joye in [8] obtained the compression function $g_6(x, y) = x^3 + y^3$ for binary generalized Hessian curves. Indeed, the same compression function works also on generalized Hessian curves over fields of the characteristic greater than 3. Let us see, that $g_6(x, y) = x^3 + y^3 = dxy - a = d \cdot f_{GH,6}(x, y) - a$.

On a generalized Hessian curve, the opposite point to point $P = (x, y)$ equals to $-P = (y, x)$. Let ω be a nontrivial cube root from 1, which means that $\omega^2 + \omega + 1 = 0$. Then $T_3 = (1 : -\omega : 0)$ is a point of order 3 and for every point $P \in E_{GH}$ holds $P + T_3 = (\omega X : \omega^{-1} Y : Z)$.

5.1. Compression function $f_{GH,6}(P) = xy$. Now we present formulas for differential addition and doubling for the compression function $f_{GH,6}$. Let us consider points $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $P - Q = (x_{P-Q}, y_{P-Q})$ and $P + Q = (x_{P+Q}, y_{P+Q})$ on the generalized Hessian curve E_{GH}, and set $r_P = f_{GH,6}(P)$, $r_Q = f_{GH,6}(Q)$, $r_{P-Q} = f_{GH,6}(P - Q)$, and $r_{P+Q} = f_{GH,6}(P + Q)$.

5.1.1. *Differential addition.* It will be showed that for points P and Q the formula for a differential addition is as follows:

$$r_{P+Q}r_{P-Q} = \frac{{r_P}^2{r_Q}^2 - adr_Pr_Q + a^2r_Q + a^2r_P}{(r_Q - r_P)^2}. \tag{9}$$

Using Sylvester formulas, one obtains

$$x_{P+Q} = \frac{y_P^2x_Q - y_Q^2x_P}{x_Qy_Q - x_Py_P}, \qquad y_{P+Q} = \frac{x_P^2y_Q - x_Q^2y_P}{x_Qy_Q - x_Py_P},$$
$$x_{P-Q} = \frac{x_Px_Q^2 - y_P^2y_Q}{x_Py_P - x_Qy_Q}, \qquad y_{P-Q} = \frac{-x_P^2x_Q + y_Py_Q^2}{x_Py_P - x_Qy_Q}.$$

After multiplication $r_{P+Q}r_{P-Q} = x_{P+Q}y_{P+Q}x_{P_Q}y_{P-Q}$ one obtains $x_{P+Q}y_{P+Q}x_{P_Q}y_{P-Q} = \frac{L}{M}$, where

$$\begin{aligned}
L = {} & (x_Py_P)^3y_Q^6 - (x_Py_P)(x_Qy_Q)^2y_P^3y_Q^3 - x_P^3(x_Qy_Q)^2(x_Py_P)y_Q^3 \\
& - (x_Py_P)^2(x_Qy_Q)y_P^3y_Q^3 + (x_Py_P)^2(x_Qy_Q)^4 - x_P^3(x_Qy_Q)(x_Py_P)^2y_Q^3 \\
& + (x_Qy_Q)^3y_P^6 + 2(x_Py_P)^3(x_Qy_Q)^3 + x_P^6(x_Qy_Q)^3 - (x_Py_P)x_Q^3y_P^3(x_Qy_Q)^2 \\
& + (x_Py_P)^4(x_Qy_Q)^2 - x_P^3x_Q^3(x_Py_P)(x_Qy_Q)^2 - (x_Py_P)^2x_Q^3y_P^3(x_Qy_Q) \\
& - x_P^3x_Q^3(x_Py_P)^2(x_Qy_Q) + (x_Py_P)^3x_Q^6, \\
M = {} & ((x_Py_P) - (x_Qy_Q))^4.
\end{aligned}$$

Substituting $r_P = x_Py_P$ and $r_Q = x_Qy_Q$, one obtains

$$\begin{aligned}
L = {} & {r_P}^3(x_Q^6 + y_Q^6) - r_P{r_Q}^2(y_P^3y_Q^3 + x_P^3y_Q^3 + x_Q^3y_P^3 + x_P^3x_Q^3) \\
& - {r_P}^2r_Q(y_P^3y_Q^3 + x_P^3y_Q^3 + x_P^3x_Q^3 + x_Q^3y_P^3) + {r_P}^2{r_Q}^4 \\
& + {r_Q}^3y_P^6 + 2{r_P}^3{r_Q}^3 + x_P^6{r_Q}^3 + {r_P}^4{r_Q}^2.
\end{aligned}$$

Since points $P, Q \in E_{GH}$, that is

$$x_P^3 + y_P^3 = dr_P - a \tag{10}$$

and

$$x_Q^3 + y_Q^3 = dr_Q - a,$$

and after the multiplication of these formulas one obtains

$$y_P^3 y_Q^3 + x_P^3 y_Q^3 + x_Q^3 y_P^3 + x_P^3 x_Q^3 = (dr_P - a)(dr_Q - a).$$

It means that

$$\begin{aligned} L = {r_P}^2 {r_Q}^4 + 2{r_P}^3 {r_Q}^3 + {r_P}^4 {r_Q}^2 + {r_P}^3 (x_Q^6 + y_Q^6) + {r_Q}^3 (x_P^6 + y_P^6) \\ - r_P {r_Q}^2 (dr_P - a)(dr_Q - a) - {r_P}^2 r_Q (dr_P - a)(dr_Q - a). \end{aligned}$$

Using the following equalities

$$\begin{aligned} (x_P^3 + y_P^3)^2 = x_P^6 + y_P^6 + 2x_P^3 y_P^3 = x_P^6 + y_P^6 + 2{r_P}^3, \\ (x_Q^3 + y_Q^3)^2 = x_Q^6 + y_Q^6 + 2x_Q^3 y_Q^3 = x_Q^6 + y_Q^6 + 2{r_Q}^3, \end{aligned}$$

one obtains that

$$\begin{aligned} x_P^6 + y_P^6 = (dr_P - a)^2 - 2{r_P}^3, \\ x_Q^6 + y_Q^6 = (dr_Q - a)^2 - 2{r_Q}^3. \end{aligned} \tag{11}$$

Using equalities from (11) one obtains that

$$\begin{aligned} L = {r_P}^2 {r_Q}^4 + 2{r_P}^3 {r_Q}^3 + {r_P}^4 {r_Q}^2 {r_P}^3 ((dr_Q - a)^2 - 2{r_Q}^3) {r_Q}^3 ((dr_P - a)^2 - 2{r_P}^3) \\ - r_P {r_Q}^2 (dr_P - a)(dr_Q - a) - {r_P}^2 r_Q (dr_P - a)(dr_Q - a) \end{aligned}$$

It is worth noting that L may be factorized into form

$$L = (r_Q - r_P)^2 ({r_P}^2 {r_Q}^2 - a d r_P r_Q + a^2 r_Q + a^2 r_P).$$

Finally:

$$r_{P+Q} r_{P-Q} = \frac{(r_Q - r_P)^2 ({r_P}^2 {r_Q}^2 - a d r_P r_Q + a^2 r_Q + a^2 r_P)}{(r_Q - r_P)^4}$$

and

$$r_{P+Q} r_{P-Q} = \frac{{r_P}^2 {r_Q}^2 - a d r_P r_Q + a^2 r_Q + a^2 r_P}{(r_Q - r_P)^2}.$$

Remark 4. For the compression function $f_{GH,6}(P) = r_P = x_P y_P$ represented as $(R_P : S_P)$ in RZ coordinates we have

$$\frac{R_{P+Q} R_{P-Q}}{S_{P+Q} S_{P-Q}} = \frac{R_P^2 R_Q^2 - a d R_P R_Q S_P S_Q + a^2 S_P S_Q (R_P S_Q + R_Q S_P)}{(R_P S_Q - R_Q S_P)^2}. \tag{12}$$

5.1.2. *Doubling.* Using doubling formulas on the generalized Hessian curve

$$x_{[2]P} = \frac{y_P(a - x_P^3)}{x_P^3 - y_P^3}, \qquad y_{[2]P} = \frac{x_P(y_P^3 - a)}{x_P^3 - y_P^3},$$

it is possible to present $x_{[2]P}y_{[2]P} = r_{[2]P}$ as a rational function depending on r_P, a, d.

After multiplication of $x_{[2]P}y_{[2]P}$ one obtains

$$x_{[2]P}y_{[2]P} = \frac{x_P(a - x_P^3)y_P(y_P^3 - a)}{(x_P^3 - y_P^3)^2} = \frac{x_P y_P(a(y_P^3 + x_P^3) - y_P^3 x_P^3 - a^2)}{(x_P^6 - 2x_P^3 y_P^3 + y_P^6)}.$$

Using equalities (10) and (11), one gets

$$\begin{aligned} r_{[2]P} &= \frac{r_P(a(dr_P - a) - {r_P}^3 - a^2)}{(dr_P - a)^2 - 4{r_P}^3} \\ &= \frac{r_P(adr_P - 2a^2 - {r_P}^3)}{(dr_P - a)^2 - 4{r_P}^3} = \frac{ad{r_P}^2 - 2a^2 r_P - {r_P}^4}{(dr_P - a)^2 - 4{r_P}^3}. \end{aligned}$$

Remark 5. For the compression function $f_{GH,6}(P) = r_P = x_P y_P$ represented as $(R_P : S_P)$ in RZ coordinates we have

$$\frac{R_{[2]P}}{S_{[2]P}} = \frac{adR_P^2 S_P^2 - 2a^2 R_P S_P^3 - R_P^4}{S_P\,(S_P(dR_P - aS_P)^2 - 4R_P^3)}. \tag{13}$$

6. Applications of high-degree compression functions in isogeny-based cryptography

A method for computing an odd general ℓ-isogeny on a generalized Hessian curve using the compression function $f_{GH,6}(x, y) = xy$ will be described below.

Using identity

$$x^3 + y^3 = dxy - a,$$

where $r = xy$, and Equation (1), one may finally obtain that

$$a' = a^\ell, \qquad d' = \left((1 - 2n)d + 6\sum_{i=1}^{s}\left(\frac{dr_i - a}{r_i}\right)\right)\prod_{i=1}^{s} r_i. \tag{14}$$

Finally, using formula (3), one obtains that

$$\begin{aligned} f_{GH,6}(\phi(P)) &= \prod_{Q \neq (1:-1:0) \in F} x_{P+Q}y_{P+Q} = \prod_{Q \neq (1:-1:0) \in F} f_{GH,6}(P + Q) \\ &= \prod_{i=1}^{s} f_{GH,6}(P + Q) f_{GH,6}(P - Q), \end{aligned}$$

which may be easily computed using formula (9).

Remark 6. In the case of 2-isogenies, the computations have to be a little different. Point of order 2 on a generalized Hessian curve is always of the form $Q = (x_Q, y_Q)$. where $x_Q = y_Q$. Setting $r_Q = x_Q y_Q = x_Q^2$ and using generalized Hessian curve equation, one obtains that

$$2x_Q^3 + a = dx_Q^2$$

is equivalent to

$$2r_Q x_Q + a = dr_Q.$$

From the above equation, one obtains that

$$x_Q = \frac{dr_Q - a}{2r_Q}.$$

For Q being a point of order 2, the formula $x_{P+Q}y_{P+Q} + x_{P-Q}y_{P-Q}$ is equal to $2x_{P+Q}y_{P+Q} = 2r_{P+Q}$. Using Sylvester formula [8] for point addition and evaluating $x_{P+Q}y_{P+Q} + x_{P-Q}y_{P-Q}$, one obtains that

$$r_{P+Q} = \frac{r_Q(r_Q r_P + {r_P}^2 - x_Q(dr_P - a))}{(r_Q - r_P)^2}.$$

Finally, for the 2-isogeny $\phi_2(P)$ with the kernel $F = \{(1 : -1 : 0), (x_Q : x_Q : 1)\}$ it holds that

$$\begin{aligned} f_{GH,6}(\phi_2(P)) = r_{P+Q} &= \frac{r_Q(r_Q r_P + {r_P}^2 - x_Q(dr_P - a))}{(r_Q - r_P)^2} \\ &= \frac{2r_P r_Q^2 + (2r_P^2 - d^2 r_P + ad)r_Q + adr_P - a^2}{2(r_Q - r_P)^2}. \end{aligned}$$

Remark 7. Let us note that the compression function $f_{GH,6}(x, y) = xy$ on a Hessian curve (and, thus, on a generalized and twisted Hessian curve) cannot be used for the computation of all possible 3-isogenies. Therefore, it is useless to the isogeny-based cryptography if the computation of 3-isogenies is necessary. It is worth noting that each 3-isogeny on Hessian curve [2] is generated by $\langle T_1 \rangle = \langle (-1 : 0 : 1) \rangle$ or $\langle T_2 \rangle = \langle (-\omega : 0 : 1) \rangle$ or $\langle T_3 \rangle = \langle (-\omega^2 : 0 : 1) \rangle$ or $\langle T_4 \rangle = \langle (1 : -\omega : 0) \rangle$. At the same time, $f_{GH,6}(T_1) = f_{GH,6}(T_2) = f_{GH,6}(T_3) = (0 : 1)$. Therefore, it is impossible to distinguish a point that should be the kernel of a given 3-isogeny. However, $f_{GH,6}(T_4) = (-\omega : 0)$.

6.1. Computational cost for operations using the compression function $f_{GH,6}(x,y)=xy$ on a generalized Hessian curve.

6.1.1. *Differential addition and doubling in projective coordinates.* Let $a=(a_1:a_2)$ and $d=(d_1:d_2)$. We can write $a=(a_1d_2:a_2d_2)=(a_L:M)$ and $d=(d_1a_2:a_2d_2)=(d_L:M)$. By (12) for the compression function $f_{GH,6}(P)=r_P=x_Py_P$ in the projective representation $(R_P:S_P)$ the formulae for differential addition is

$$\frac{R_{P+Q}R_{P+Q}}{S_{P+Q}S_{P-Q}}=\frac{M^2R_P^2R_Q^2-a_Ld_LR_PR_QS_PS_Q+a_L^2S_PS_Q(R_PS_Q+R_QS_P)}{M^2\left(R_PS_Q-R_QS_P\right)^2}.$$

If $a=1$ then for $d=(d_1:d_2)$ one obtains

$$\frac{R_{P+Q}R_{P+Q}}{S_{P+Q}S_{P-Q}}=\frac{d_2\left(R_P^2R_Q^2+S_PS_Q(R_PS_Q+R_QS_P)\right)-d_1R_PR_QS_PS_Q}{d_2\left(R_PS_Q-R_QS_P\right)^2}.$$

Using (13) we obtain the formula for doubling

$$\frac{R_{[2]P}}{S_{[2]P}}=\frac{a_Ld_LR_P^2S_P^2-2a_L^2R_PS_P^3-M^2R_P^4}{S_P\left(S_P(d_LR_P-a_LS_P)^2-4M^2R_P^3\right)}.$$

If $a=1$ then for $d=(d_1:d_2)$ one obtains

$$\frac{R_{[2]P}}{S_{[2]P}}=\frac{d_1d_2R_P^2S_P^2-2d_2^2R_PS_P^3-d_2^2R_P^4}{S_P\left(S_P(d_1R_P-d_2S_P)^2-4d_2^2R_P^3\right)}.$$

6.1.2. *Isogeny computations.* Let us consider the isogeny $\phi : E_{GH}\to E'_{GH}$ of odd degree $\ell=1+2s$ with the kernel $F=\{(1:-1:0)\}\cup\sum_{i=1}^{s}\{Q_i,-Q_i\}$. Let $f_{GH,6}(Q_i)=r_i=(R_i:S_i)$ for $i=\overline{1,s}$. For the application of projective representation of the compression function $f_{GH,6}(P)=(R_P:S_P)$ to the isogeny-based cryptography, according to equation (14) one obtains

$$d'=\left((1-4s)d+6\sum_{i=1}^{s}\left(\frac{dR_i-aS_i}{R_i}\right)\right)\prod_{i=1}^{s}\frac{R_i}{S_i}.$$

For $l=5$ $(s=2)$, we have got

$$\begin{aligned}d'&=\left(-7d+6\left(\frac{dR_1-aS_1}{R_1}+\frac{dR_2-aS_2}{R_2}\right)\right)\frac{R_1R_2}{S_1S_2}\\&=\frac{-7dR_1R_2+6\left(R_2(dR_1-aS_1)+R_1(dR_2-aS_2)\right)}{S_1S_2}.\end{aligned}$$

Let $a = (a_1 : a_2)$ and $d = (d_1 : d_2)$. Writing $a = (a_1 d_2 : a_2 d_2) = (a_L : M)$ and $d = (d_1 a_2 : a_2 d_2) = (d_L : M)$ one gets

$$(d_1' : d_2') = \left(\frac{(1-4s)d_L}{M} + 6 \sum_{i=1}^{s} \left(\frac{d_L R_i - a_L S_i}{M R_i} \right) \right) \prod_{i=1}^{s} \frac{R_i}{S_i}.$$

In case of $\ell = 5$ one gets

$$(d_1' : d_2') = \frac{-7dR_1R_2 + 6\left(R_2(dR_1 - aS_1) + R_1(dR_2 - aS_2)\right)}{MS_1S_2}.$$

If $a = 1$ then for $d = (d_1 : d_2)$ one obtains

$$(d_1' : d_2') = \left(\frac{(1-4s)d_1}{d_2} + 6 \sum_{i=1}^{s} \left(\frac{d_1 R_i - d_2 S_i}{d_2 R_i} \right) \right) \prod_{i=1}^{s} \frac{R_i}{S_i}.$$

For $\ell = 5$ we get

$$(d_1' : d_2') = \frac{-7dR_1R_2 + 6\left(R_2(d_1R_1 - d_2S_1) + R_1(d_1R_2 - d_2S_2)\right)}{d_2S_1S_2}.$$

For $P = (X_P : Y_P : Z_P)$ the image of P in isogeny ϕ is given by

$$\phi(P) = \left(\prod_{Q \in F - \{(1:-1:0)\}} X_{P+Q} : \prod_{Q \in F - \{(1:-1:0)\}} Y_{P+Q} : \prod_{Q \in F - \{(1:-1:0)\}} Z_{P+Q} \right).$$

For the compression function $f_{GH,6}(P) = r_P = x_P y_P$ represented as $(R_P : S_P)$, one gets

$$\begin{aligned} f_{GH,6}(\phi(P)) &= \left(\prod_{i=1}^{s} R_{P+Q_i} R_{P-Q_i} : \prod_{i=1}^{s} S_{P+Q_i} S_{P-Q_i} \right) \\ &= \Big(\prod_{i=1}^{s} \left(R_P^2 R_{Q_i}^2 - adR_P R_{Q_i} S_P S_{Q_i} + a^2 S_P S_{Q_i} (R_P S_{Q_i} + R_{Q_i} S_P) \right) : \\ &\quad \prod_{i=1}^{s} \left(R_P S_{Q_i} - R_{Q_i} S_P \right)^2 \Big). \end{aligned}$$

Let $a = (a_1 : a_2)$ and $d = (d_1 : d_2)$. We can write $a = (a_1 d_2 : a_2 d_2) = (a_L : M)$ and $d = (d_1 a_2 : a_2 d_2) = (d_L : M)$. Then one gets

$$\begin{aligned} f_{GH,6}(\phi(P)) = \Big(\prod_{i=1}^{s} \big(& M^2 R_P^2 R_{Q_i}^2 - a_L d_L R_P R_{Q_i} S_P S_{Q_i} \\ & + a_L^2 S_P S_{Q_i} (R_P S_{Q_i} + R_{Q_i} S_P) \big) : \prod_{i=1}^{s} M^2 \left(R_P S_{Q_i} - R_{Q_i} S_P \right)^2 \Big). \end{aligned}$$

If $a = 1$ then for $d = (d_1 : d_2)$ one obtains

$$f_{GH,6}(\phi(P)) = \Big(\prod_{i=1}^{s} \big(d_2 \left(R_P^2 R_{Q_i}^2 + S_P S_{Q_i} (R_P S_{Q_i} + R_{Q_i} S_P) \right) \\ -d_1 R_P R_{Q_i} S_P S_{Q_i} \big) : \prod_{i=1}^{s} d_2 \left(R_P S_{Q_i} - R_{Q_i} S_P \right)^2 \Big).$$

Computational costs for differential addition and doubling operations on a generalized Hessian curve with the compression function $f_{GH,6}$ are presented in Table 1, where M, S and c mean multiplication, squaring and multiplication by a constant respectively.

Operation	Computational cost
Differential addition (eq. (12))	19M+3S
Differential addition (eq. (6.1.1))	11M+4S
Differential addition (eq. (6.1.1))	7M+3S
Doubling (eq. (13))	11M+4S+2c
Doubling (eq. (6.1.1))	14M+4S+2c
Doubling (eq. (6.1.1))	14M+4S+2c

Table 1. Computational costs for differential addition and doubling

Computational costs for 5-isogeny computations and evaluation on a generalized Hessian curve with the compression function $f_{GH,6}$ are presented in Table 2.

Operation	Computational cost
5-isogenous E_{HG} curve (eq. (6.1.2))	8M+2c
5-isogenous E_{HG} curve (eq. (6.1.2))	9M+2c
5-isogenous E_{HG} curve (eq. (6.1.2))	9M+2c
Point evaluation at 5-isogeny (eq. (6.1.2))	11M+3S
Point evaluation at 5-isogeny (eq. (6.1.2))	13M+3S
Point evaluation at 5-isogeny (eq. (6.1.2))	11M+3S

Table 2. Computational costs for 5-isogeny computations

7. Conclusion

This paper has presented how to obtain differential addition and doubling formula for the compression function of degrees 2 and 6 on generalized Hessian

curves. However, such formulas have been previously presented in [5] and [7]. This time these formulas have been obtained using elementary algebra methods, not the Gröbner basis mechanism. The most important part of this paper is presenting formulas for computing 2,3, and ℓ-isogenies on generalized Hessian curves using the compression function of degree 2 and formulas for general computing ℓ-isogenies, for $\ell \neq 3$. In the case of the compression function of degree 6, it is worth noting that computing 3-isogenies, in this case, is impossible because it is impossible to distinguish a compression of different points of order 3.

As we presented in the paper, it is clear that the compression function of degree 6 is much more convenient for using the isogeny-based cryptography because computation and evaluation of ℓ-isogeny are, in this case, much more efficient than similar computations for the compression function of degree 2. This situation is because the compression function of degree 6 has a multiplicative character, and the compression function of degree 2 has an additive character.

References

[1] D. J. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange, Twisted Hessian curves, In: International Conference on Cryptology and Information Security in Latin America, 2015, 269–194.

[2] F. L. P. Broon and E. Fouotsa, Analogue of Vélu's formulas for computing isogenies over hessian model of elliptic curves, *IACR Cryptol. ePrint Arch.* (2019), https://eprint.iacr.org/2019/1480.

[3] W. Castryck, T. Lange, C. Martindale, L. Panny and J. Renes, CSIDH: An efficient post-quantum commutative group action, In: International Conference on the Theory and Application of Cryptology and Information Security, 2018, 395–427.

[4] T. Dang and D. Moody, Twisted hessian isogenies, *IACR Cryptol. ePrint Arch.* (2019), https://eprint.iacr.org/2019/1003.

[5] R. Drylo, T. Kijko and M. Wroński, Determining formulas related to point compression on alternative models of elliptic curves, *Fundamenta Informaticae* **169** (2019), 285–294.

[6] R. Drylo, T. Kijko and M. Wroński, Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography, *IACR Cryptol. ePrint Arch.* (2020), https://eprint.iacr.org/2020/526.pdf.

[7] R. Drylo, T. Kijko and M. Wroński, High-degree compression functions on alternative models of elliptic curves and their applications, *Fundamenta Informaticae* **184** (2021), 107–139.

[8] R. R. Farashahi and M. Joye, Efficient arithmetic on Hessian curves, In: International Workshop on Public Key Cryptography, 2010, 243–260.

[9] S. Kim, K. Yoon, Y.-H. Park and S. Hong, Optimized method for computing odd-degree isogenies on Edwards curves, In: International Conference on the Theory and Application of Cryptology and Information Security, 2019, 273–292.

[10] A. Rostovtsev and A. Stolbunov, Public-key cryptosystem based on isogenies, *IACR Cryptol. ePrint Arch.* (2006), https://eprint.iacr.org/2006/145.pdf.

[11] J. P. da Silva, R. Dahab and J. López, 2-isogenies between elliptic curves in Hesse model, In: Anais do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2018, 57–64.

michał wroński, tomasz kijko
faculty of cybernetics
military university of technology
kaliskiego str. 2, warsaw
poland

E-mail: {michal.wronski,tomasz.kijko}@wat.edu.pl