jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2021, VOL. 67, NO. 2, PP. 193–200
Manuscript received January 4, 2021; revised April, 2021. DOI: 10.24425/ijet.2021.135964

Arithmetic Using Compression on Elliptic Curves in Huff's Form and Its Applications

Robert Dryło, Tomasz Kijko and Michał Wroński

***Abstract*—In this paper for elliptic curves provided by Huff's equation $H_{a,b} : ax(y^2-1) = by(x^2-1)$ and general Huff's equation $G_{\overline{a},\overline{b}} : \overline{x}(\overline{a}\overline{y}^2-1) = \overline{y}(\overline{b}\overline{x}^2-1)$ and degree 2 compression function $f(x,y) = xy$ on these curves, herein we provide formulas for doubling and differential addition after compression, which for Huff's curves are as efficient as Montgomery's formulas for Montgomery's curves $By^2 = x^3 + Ax^2 + x$. For these curves we also provided point recovery formulas after compression, which for a point P on these curves allows to compute $[n]f(P)$ after compression using the Montgomery ladder algorithm, and then recover $[n]P$. Using formulas of Moody and Shumow for computing odd degree isogenies on general Huff's curves, we have also provide formulas for computing odd degree isogenies after compression for these curves. Moreover, it is shown herein how to apply obtained formulas using compression to the ECM algorithm.**

***Keywords*—Huff's curves, Isogeny-based cryptography, Compression functions on elliptic curves**

I. Introduction

COMPRESSION on elliptic curves is a standard approach, for example, for the reduction of key sizes and protection against side-channel attacks. The clear presentations of results on x-coordinate compression, one can find, for example, in [1] and [2]. In general, if E is an elliptic curve over a field K and $f : E \to K$ is a degree 2 rational function such that $f(P) = f(-P)$ for all $P \in E$, then f is called a degree 2 compression function and we have induced from E the multiplication of values f by integers provided by $[k]f(P) = f([k]P)$ for $k \in \mathbb{Z}$. As an example, on Weierstrass and Montgomery's curves $f(x,y) = x$ is a compression function. In general for degree 2 compression function $f : E \to K$ there exist rational functions for doubling $D(x) \in K(x)$ and differential additions $A_1, A_2 \in K(x,y)$ such that

$$f([2]P) = D(f(P)), \quad (1)$$
$$f(P+Q)f(Q-P) = A_1(f(P),f(Q)), \quad (2)$$
$$f(P+Q)+f(Q-P) = A_2(f(P),f(Q)) \quad (3)$$

for generic points $P, Q \in E$. If one determines functions D and A_1 or A_2, the Montgomery ladder algorithm allows to compute $[k]f(P)$ using values of f. There also exists a rational map $B : E \times K \times K \to E$ such that

$$Q = B(P, f(Q), f(P+Q)) \quad (4)$$

for generic points $P, Q \in E$, which we call the point recovery formula. This allows for $P \in E$ computation $[k]f(P)$ using the Montgomery ladder algorithm, which also gives $[k+1]f(P)$, and to recover point $[k]P$ on E given $P, [k]f(P), [k+1]f(P)$ substituting $Q = [k]P$ to the formula (4).

Peter Montgomery [3] provided very efficient formulas for doubling and differential addition using x-coordinates for curves of the form $By^2 = x^3 + Ax^2 + x$ called Montgomery's curves. Formulas (1) and (2) or (3) were also given for other standard models of elliptic curves: Weierstrass [4], Edwards [5], [6], Hessian [7], Jacobi quartic [8], [9], twisted Hessian and Huff's [9] curves. Formulas for point recovery (4) were given for Weierstrass [8], [10], Edwards [6], generalized and twisted Hessian, Huff's and Jacobi quartic [9] curves.

In this paper we consider Huff's curves $H_{a,b} : ax(y^2-1) = by(x^2-1)$ described by Joye, Tibouchi and Vergnaud in [11] and general Huff's curves $G_{\overline{a},\overline{b}} : \overline{x}(\overline{a}\overline{y}^2-1) = \overline{y}(\overline{b}\overline{x}^2-1)$ described by Wu and Feng [12] over a field K of $\mathrm{char}(K) \neq 2$. Formulas similar to the Montgomery formulas for differential addition were given in [13][Appendix B] for the extended Huff's model

$$EH_{a,c,d} : y(1+ax^2) = cx(1+dy^2) \quad (5)$$

with compression function $f(x,y) = x$, where differential addition is of the form

$$f(P+Q)f(P-Q) = \frac{f(P)^2 - f(Q)^2}{1 - a^2 f(P)^2 f(Q)^2}. \quad (6)$$

Moreover, formulas for doubling and differential addition after compression were also given for binary Huff's curves [14].

In this paper for Huff's curves and general Huff's curves over a field K of $\mathrm{char}(K) \neq 2$ using compression function $f(x,y) = xy$, we introduce new formulas for doubling and differential addition, which for Huff's curves are as efficient as Montgomery's formulas for the curves $By^2 = x^3 + Ax^2 + x$ (note that in [9] we used compression function y/x on Huff's curves). These formulas and formulas for point recovery are provided in Theorems 1 and 2. We provide a proof of Theorem 1, and Theorem 2 follows by carrying formulas for Huff's curves applying an isomorphism from a general Huff's curve to a suitable Huff's curve.

R. Dryło is with Institute of Mathematics and Cryptology, Faculty of Cybernetics, Military University of Technology, Warsaw, Poland (e-mail: robert.drylo@wat.edu.pl).

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

M. Wroński is with Institute of Mathematics and Cryptology, Faculty of Cybernetics, Military University of Technology, Warsaw, Poland (e-mail: michal.wronski@wat.edu.pl).

In Section III, we apply formulas of Moody and Shumow [15] and provide in Corollaries 1 and 2 formulas for compression of odd degree isogenies for general Huff's and Huff's curves.

In Section IV, we summarize the costs of computations of presented formulas using compression.

Moreover, we present application of computed formulas for obtaining efficient formulas for computation of general odd-degree isogeny and applications to the ECM method.

Additional Magma codes, where the correctness of provided formulas is checked, may be found on https://github.com/Michal-Wronski/Huff-compression.git.

II. Point compression on Huff's and general Huff's curves

In this section using compression function $f(x,y)=xy$, we provide formulas for doubling, differential addition and point recovery for Huff's and general Huff's curves. We assume that K is a field with $char(K)\neq 2$.

A. Huff's curves

Joye, Tibouchi and Vergnaud in [11] described the group law and pairing computation on Huff's elliptic curves. Huff's curve over K is provided by the equation

$$H_{a,b}\ :\ ax(y^2-1)=by(x^2-1), \tag{7}$$

where $a^2\neq b^2$ and $a,b\neq 0$. The point $O=(0,0)$ is the neutral element, and the opposite point is given by $-(x,y)=(-x,-y)$. For two points $P=(x_P,y_P)$, $Q=(x_Q,y_Q)$ on $H_{a,b}$ their sum $P+Q=(x_R,y_R)$ is provided by

$$\begin{cases} x_R=\frac{(x_P+x_Q)(1+y_Py_Q)}{(1+x_Px_Q)(1-y_Py_Q)},\\ y_R=\frac{(y_P+y_Q)(1+x_Px_Q)}{(1-x_Px_Q)(1+y_Py_Q)}.\end{cases} \tag{8}$$

Before we provide a results on compression, note that if $f:E\to K$ is a degree 2 compression function on an elliptic curve E, then the field extension $K(f)\subset K(E)$ is of degree 2 and $K(f)$ consists exactly of functions in $K(E)$ which are constant with respect to $[-1]$ (i.e., functions $g\in K(E)$, such that $g\circ[-1]=g$).

We provide the following formulas for Huff's curves for doubling, differential addition and point recovery after compression.

Theorem 1. *On Huff's curves $H_{a,b}$ (7) the function $f(x,y)=xy$ is a degree 2 compression function. We have the following formulas for doubling and differential addition:*

$$f([2]P)=\frac{4f(P)(f(P)^2+\left(\frac{b}{a}+\frac{a}{b}\right)f(P)+1)}{(f(P)^2-1)^2}, \tag{9}$$

$$f(P+Q)f(P-Q)=\left(\frac{f(P)-f(Q)}{f(P)f(Q)-1}\right)^2. \tag{10}$$

We also have the following formulas for point recovery. For generic points $P=(x_P,y_P),Q=(x_Q,y_Q)$ on $H_{a,b}$ if we are given $P,f(Q),f(P+Q)$, then coordinates of Q are provided by

$$\begin{cases} x_Q=f(Q)\frac{(y_Pf(P+Q)+x_P)(bf(Q)+a)+(af(Q)+b)(x_Pf(P+Q)+y_P)}{(bf(Q)+a)(f(P+Q)-f(Q)+x_Py_P(f(Q)f(P+Q)-1))},\\ y_Q=\frac{f(Q)}{x_Q}.\end{cases} \tag{11}$$

Proof. Clearly $f(P)=f(-P)$ for $P\in H_{a,b}$ and $f:E\to K$ is of degree 2, because for generic $\alpha\in\overline{K}$ (the algebraic closure of K) the system

$$\begin{cases} xy=\alpha,\\ ax(y^2-1)=by(x^2-1)\end{cases} \tag{12}$$

has two solutions, since substituting in the second equation $xy=\alpha$ and $y=\alpha/x$ we have $a\,\alpha\,\frac{\alpha}{x}-ax=b\,\alpha\,x-b\frac{\alpha}{x}$, hence x satisfies the quadratic equation $(b\,\alpha+a)x^2=a\,\alpha^2+b\,\alpha$.

Let $r=xy$. In the proof, we will use the formulas which express x^2 and y^2 as rational functions of r, which exist because x^2 and y^2 are constant with respect to $[-1]$. Substituting $y=\frac{r}{x}$ to the equation of $H_{a,b}$ we have

$$ax\left(\frac{r^2}{x^2}-1\right)=b\frac{r}{x}\left(x^2-1\right). \tag{13}$$

Hence,

$$x^2\left(br+a\right)=ar^2+br, \tag{14}$$

and

$$x^2=\frac{r(ar+b)}{br+a}. \tag{15}$$

We have

$$y^2=\frac{r^2}{x^2}=\frac{r(br+a)}{ar+b}. \tag{16}$$

We first show the formula for doubling after compression. From (8) for $P=(x,y)\in H_{a,b}$ the point $[2]P$ has the following coordinates

$$\begin{cases} x_{[2]P}=\frac{2x(y^2+1)}{(x^2+1)(1-y^2)},\\ y_{[2]P}=\frac{2y(x^2+1)}{(1-x^2)(y^2+1)}.\end{cases} \tag{17}$$

Hence,

$$f([2]P)=\frac{2x(y^2+1)}{(x^2+1)(1-y^2)}\frac{2y(x^2+1)}{(1-x^2)(y^2+1)}=\frac{4xy}{(1-x^2)(1-y^2)}. \tag{18}$$

From (15) and (16) we have

$$f([2]P)=\frac{4r}{(1-\frac{r(ar+b)}{br+a})(1-\frac{r(br+a)}{ar+b})}=\frac{4r(r^2+(\frac{a}{b}+\frac{b}{a})r+1)}{(r^2-1)^2}, \tag{19}$$

which yields formula (9).

From (8) we have

$$\begin{aligned} f(P+Q)&=\frac{(x_P+x_Q)(1+y_Py_Q)}{(1+x_Px_Q)(1-y_Py_Q)}\frac{(y_P+y_Q)(1+x_Px_Q)}{(1-x_Px_Q)(1+y_Py_Q)}\\ &=\frac{(x_P+x_Q)(y_P+y_Q)}{(1-x_Px_Q)(1-y_Py_Q)},\\ f(P-Q)&=\frac{(x_P-x_Q)(1-y_Py_Q)}{(1-x_Px_Q)(1+y_Py_Q)}\frac{(y_P-y_Q)(1-x_Px_Q)}{(1+x_Px_Q)(1-y_Py_Q)}\\ &=\frac{(x_P-x_Q)(y_P-y_Q)}{(1+x_Px_Q)(1+y_Py_Q)}.\end{aligned} \tag{20}$$

Hence

$$f(P+Q)f(P-Q)=\frac{(x_P^2-x_Q^2)(y_P^2-y_Q^2)}{(1-x_P^2x_Q^2)(1-y_P^2y_Q^2)}. \tag{21}$$

Let $r_P=f(P),r_Q=f(Q)$. From (15) and (16) we have

$$f(P+Q)f(P-Q) = \\ = \frac{\left(\frac{r_P(ar_P+b)}{br_P+a} - \frac{r_Q(ar_Q+b)}{br_Q+a}\right)\left(\frac{r_P(br_P+a)}{ar_P+b} - \frac{r_Q(br_Q+a)}{ar_Q+b}\right)}{\left(1-\frac{r_P(ar_P+b)}{br_P+a}\frac{r_Q(ar_Q+b)}{br_Q+a}\right)\left(1-\frac{r_P(br_P+a)}{ar_P+b}\frac{r_Q(br_Q+a)}{ar_Q+b}\right)}. \tag{22}$$

Simplifying and factoring the last expression (for example using Magma), we obtain $\left(\frac{r_P-r_Q}{r_Pr_Q-1}\right)^2$, which is (10).

To obtain point recovery formula (11) assume that we are given $P=(x_P,y_P)$, $f(Q)$ and $f(P+Q)$. Let $r_Q = f(Q), r_R = f(P+Q)$. Substituting $y_Q = r_Q/x_Q$ to the right hand side of (20) we have

$$r_R = \frac{(x_P+x_Q)(y_P+\frac{r_Q}{x_Q})}{(1-x_Px_Q)(1-y_P\frac{r_Q}{x_Q})}. \tag{23}$$

Multiplying by the denominator and x_Q we have

$$\begin{aligned} &r_R(x_Q - y_Pr_Q - x_Px_Q^2 + x_Px_Qy_Pr_Q) \\ &= x_Px_Qy_P + x_Pr_Q + x_Q^2y_P + r_Qx_Q. \end{aligned} \tag{24}$$

We can now compute from this equation x_Q and substitute (15) for x_Q^2, and we have

$$\begin{aligned} x_Q &= \frac{y_Pr_Qr_R + x_Pr_Q + x_Q^2(x_Pr_R+y_P)}{r_R + x_Py_Pr_Qr_R - x_Py_P - r_Q} \\ &= \frac{y_Pr_Qr_R + x_Pr_Q + \frac{r_Q(ar_Q+b)}{br_Q+a}(x_Pr_R+y_P)}{r_R - r_Q + x_Py_P(r_Qr_R-1)}. \end{aligned} \tag{25}$$

Multiplying the numerator and denominator by br_Q+a we obtain (11).

□

In projective coordinates formulas (9) and (10) can be computed as efficiently as formulas [3] for Montgomery curves

$$By^2 = x^3 + Ax^2 + x. \tag{26}$$

Let $f(P) = (X_{f(P)} : Z_{f(P)})$ for $P \in H_{a,b}$. Then

$$\begin{cases} X_{f([2]P)} = 4X_{f(P)}Z_{f(P)}((X_{f(P)} - Z_{f(P)})^2 + AX_{f(P)}Z_{f(P)}), \\ Z_{f([2]P)} = (X_{f(P)} + Z_{f(P)})^2(X_{f(P)} - Z_{f(P)})^2, \end{cases} \tag{27}$$

where $A = \frac{a}{b} + \frac{b}{a} + 2$ and $4X_{f(P)}Z_{f(P)}$ can be computed as $4X_{f(P)}Z_{f(P)} = (X_{f(P)} + Z_{f(P)})^2 - (X_{f(P)} - Z_{f(P)})^2$. The cost of these formulas is equal to $3M + 2S + c$, where M, S, c are costs of multiplication, squaring and multiplication by a constant in K, respectively. Cost c can be made small, if coefficients a, b are chosen such that A is small. Moreover, computing $4X_{f(P)}Z_{f(P)} = (X_{f(P)} + Z_{f(P)})^2 - (X_{f(P)} - Z_{f(P)})^2$ for $B = A/4$, we obtain

$$X_{f([2]P)} = 4X_{f(P)}Z_{f(P)}((X_{f(P)} - Z_{f(P)})^2 + B(4X_{f(P)}Z_{f(P)})) \tag{28}$$

and in this way doubling requires $2M+2S+c$. Similarly, the differential addition in projective representation is provided by

$$\begin{cases} X_{f(P+Q)} = Z_{f(P-Q)}\big((X_{f(P)} - Z_{f(P)})(X_{f(Q)} + Z_{f(Q)}) \\ -(X_{f(P)} + Z_{f(P)})(X_{f(Q)} - Z_{f(Q)})\big)^2, \\ Z_{f(P+Q)} = X_{f(P-Q)}\big((X_{f(P)} - Z_{f(P)})(X_{f(Q)} + Z_{f(Q)}) \\ +(X_{f(P)} + Z_{f(P)})(X_{f(Q)} - Z_{f(Q)})\big)^2, \end{cases} \tag{29}$$

and has cost $4M + 2S$.

B. General Huff's curves

In [12] Wu and Feng introduced general Huff's curves. General Huff's curves are provided by the equation

$$G_{\overline{a},\overline{b}} \ : \ \overline{x}(\overline{a}\overline{y}^2 - 1) = \overline{y}(\overline{b}\overline{x}^2 - 1) \tag{30}$$

where $\overline{a} \neq \overline{b}$ and $\overline{a}, \overline{b} \neq 0$. Similarly as for Huff's curve the point $\overline{O} = (0,0)$ is the neutral element, and the opposite point $-(\overline{x},\overline{y}) = (-\overline{x},-\overline{y})$. For two points $P = (\overline{x}_{\overline{P}}, \overline{y}_{\overline{P}})$, $\overline{Q} = (\overline{x}_{\overline{Q}}, \overline{y}_{\overline{Q}})$ on $H_{\overline{a},\overline{b}}$ their sum $\overline{P} + \overline{Q} = (\overline{x}_{\overline{R}}, \overline{y}_{\overline{R}})$ is provided by

$$\begin{cases} \overline{x}_{\overline{R}} = \frac{(\overline{x}_{\overline{P}}+\overline{x}_{\overline{Q}})(\overline{a}\overline{y}_{\overline{P}}\overline{y}_{\overline{Q}}+1)}{(\overline{b}\overline{x}_{\overline{P}}\overline{x}_{\overline{Q}}+1)(1-\overline{a}\overline{y}_{\overline{P}}\overline{y}_{\overline{Q}})}, \\ \overline{y}_{\overline{R}} = \frac{(\overline{y}_{\overline{P}}+\overline{y}_{\overline{Q}})(\overline{b}\overline{x}_{\overline{P}}\overline{x}_{\overline{Q}}+1)}{(1-\overline{b}\overline{x}_{\overline{P}}\overline{x}_{\overline{Q}})\overline{a}\overline{y}_{\overline{P}}\overline{y}_{\overline{Q}}+1)}. \end{cases} \tag{31}$$

Lemma 1. *Every Huff's curve over a field K given by the equation (7) is also a general Huff's curve.*

Proof. By the substitutions:

$$\overline{x} = ax, \quad \overline{y} = by, \quad \overline{a} = \tfrac{1}{b^2} \text{ and } \overline{b} = \tfrac{1}{a^2} \tag{32}$$

we can transform equation (7) into the following general Huff's curve equation

$$G_{\overline{a},\overline{b}} \ : \ \overline{x}(\overline{a}\overline{y}^2 - 1) = \overline{y}(\overline{b}\overline{x}^2 - 1). \tag{33}$$

If $\overline{a}$ and $\overline{b}$ are squares in K we can transform the general Huff's curve with equation (33) into the Huff's curve (7) by substitutions

$$x = \overline{x}\sqrt{\overline{b}}, \quad y = \overline{y}\sqrt{\overline{a}}, \quad a = \frac{1}{\sqrt{\overline{b}}} \text{ and } \ b = \frac{1}{\sqrt{\overline{a}}}. \tag{34}$$

□

Theorem 2. On general Huff's curves (30) with a degree 2 compression function $f(\overline{x},\overline{y}) = \overline{x}\overline{y}$, we have the following formulas for doubling and differential addition

$$f([2]\overline{P}) = \frac{4f(\overline{P})\left(\overline{a}\overline{b}f(\overline{P})^2 + \left(\overline{a}+\overline{b}\right)f(\overline{P})+1\right)}{(\overline{a}\overline{b}f(\overline{P})^2-1)^2}, \tag{35}$$

$$f(\overline{P}+\overline{Q})f(\overline{P}-\overline{Q}) = \left(\frac{f(\overline{P})-f(\overline{Q})}{\overline{a}\overline{b}f(\overline{P})f(\overline{Q})-1}\right)^2. \tag{36}$$

We also have the following formulas for point recovery. For generic points $\overline{P} = (\overline{x}_1,\overline{y}_1), \overline{Q} = (\overline{x}_2,\overline{y}_2)$ on $G_{\overline{a},\overline{b}}$, if we are given $\overline{P}, f(\overline{Q}), f(\overline{P}+\overline{Q})$, then the coordinates of $\overline{Q}$ are provided by

$$\begin{cases} \overline{x}_2 = f(\overline{Q})\frac{(\overline{a}\overline{y}_1 f(\overline{P}+\overline{Q})+\overline{x}_1)(\overline{b}f(\overline{Q})+1)+(\overline{a}f(\overline{Q})+1)(\overline{b}\overline{x}_1 f(\overline{P}+\overline{Q})+\overline{y}_1)}{(\overline{b}f(\overline{Q})+1)(f(\overline{P}+\overline{Q})-f(\overline{Q})+\overline{x}_1\overline{y}_1(\overline{a}\overline{b}f(\overline{Q})f(\overline{P}+\overline{Q})-1)}, \\ \overline{y}_2 = \frac{f(\overline{Q})}{\overline{x}_2}. \end{cases} \tag{37}$$

Proof. Formula (35) can be mechanically obtained from (9) by substitutions (32). Similarly we can derive the doubling formula (36) from (10) and the point recovery formula (37) from (11). □

III. Applications to the isogeny-based cryptography

In general, if $\psi : E \to E_1$ is an isogeny of elliptic curves, and $f : E \to K$, $f_1 : E_1 \to K$ are degree 2 compression functions, then there exists an induced rational function $\tilde{\psi} : K \to K$, which we call compression of isogeny ψ, such that $f_1 \circ \psi = \tilde{\psi} \circ f$, because the function $f_1 \circ \psi \in K(E_1)$ is constant with respect to $[-1]$, so it is of the form $\tilde{\psi} \circ f$ for some rational function $\tilde{\psi}$. In this section we present applications of formulas obtained in the previous sections.

A. General Huff's isogenies computation using compression techniques

Moody and Shumow in [15] gave formulas on isogenies for general Huff's curves. Because to compute values of $f(x, y)$ at points of order 2 at infinity requires to take another representation of compression function $f : G_{\overline{a},\overline{b}} \to K$, we consider isogenies of odd degrees.

Let $\overline{F} = \{(0,0), (\overline{\alpha}_i, \overline{\beta}_i), (-\overline{\alpha}_i, -\overline{\beta}_i) : i = 1 \dots s\}$, where $-(\overline{\alpha}_i, \overline{\beta}_i) = (-\overline{\alpha}_i, -\overline{\beta}_i)$, is the kernel of an isogeny $\overline{\psi}$ of degree ℓ, where $\ell = 2s + 1$. Let $\overline{A} = \prod_{i=1}^{s} \overline{\alpha}_i$ and $\overline{B} = \prod_{i=1}^{s} \overline{\beta}_i$.

Theorem 3. *([15], Theorem 5.) Define*

$$\overline{\psi}(\overline{P}) = \left(\overline{x}_P \prod_{\overline{Q} \neq (0,0) \in \overline{F}} \frac{-\overline{x}_{\overline{P}+\overline{Q}}}{\overline{x}_{\overline{Q}}}, \overline{y}_{\overline{P}} \prod_{\overline{Q} \neq (0,0) \in \overline{F}} \frac{-\overline{y}_{\overline{P}+\overline{Q}}}{\overline{y}_{\overline{Q}}} \right). \tag{38}$$

Then $\overline{\psi}$ is an ℓ-isogeny with kernel $\overline{F}$ from the curve $G_{\overline{a},\overline{b}}$ to the curve $G_{\overline{a}',\overline{b}'}$, where $\overline{a}' = \overline{a}^{\ell}\overline{B}^4$ and $\overline{b}' = \overline{b}^{\ell}\overline{A}^4$.

Now we present how to compute isogeny $f(\overline{\psi})$ using point compression.

Corollary 1. *Let $\overline{R} \in G_{\overline{a},\overline{b}}$ and let $(X_{f(\overline{R})} : Z_{f(\overline{R})})$ be projective representation of $f(\overline{R})$, where $\overline{R}$ is the point defining kernel $\overline{F}$ of the isogeny $\overline{\psi}$. Let $Ord(\overline{R})$ be the odd number. Let's note that $f(\overline{\psi}(\overline{P}))$ is provided by*

$$\begin{aligned} &f(\overline{\psi}(\overline{P})) \\ &= \left(\overline{x}_{\overline{P}} \textstyle\prod_{\overline{Q} \neq (0,0) \in \overline{F}} \frac{-\overline{x}_{\overline{P}+\overline{Q}}}{\overline{x}_{\overline{Q}}} \cdot \overline{y}_{\overline{P}} \prod_{\overline{Q} \neq (0,0) \in \overline{F}} \frac{-\overline{y}_{\overline{P}+\overline{Q}}}{\overline{y}_{\overline{Q}}} \right), \end{aligned} \tag{39}$$

which is equal to

$$\begin{aligned} f(\overline{\psi}(\overline{P})) &= \left(\overline{x}_{\overline{P}} \overline{y}_{\overline{P}} \textstyle\prod_{\overline{Q} \neq (0,0) \in \overline{F}} \frac{\overline{x}_{\overline{P}+\overline{Q}} \overline{y}_{\overline{P}+\overline{Q}}}{\overline{x}_{\overline{Q}} \overline{y}_{\overline{Q}}} \right) \\ &= \left(f(\overline{P}) \textstyle\prod_{\overline{Q} \in \overline{F}^+} \frac{f(\overline{P}+\overline{Q}) f(\overline{P}-\overline{Q})}{f(\overline{Q})^2} \right), \end{aligned} \tag{40}$$

where $\overline{F}^+$ is the set $\{(\overline{\alpha}_i, \overline{\beta}_i) : i = 1 \dots s\}$. Having generator $\overline{R}$ of the kernel of the isogeny $\overline{\psi}$, provided by projective compression $(\overline{X}_{f(\overline{R})} : \overline{Z}_{f(\overline{R})})$, it is easy to obtain other elements of the $\overline{F}^+$, using for example a ladder method. Let $\overline{J}$ be the set of compressions in projective representation of $\overline{F}^+$, so $\overline{J} = \{(\overline{X}_{f(\overline{P}_i)} : \overline{Z}_{f(\overline{P}_i)}) : i = 1 \dots s\}$. The value of $f(\overline{\psi})$ using point compression may be provided by

$$f(\overline{\psi}(\overline{P})) = \left(\frac{\overline{X}_{f(\overline{P})}}{\overline{Z}_{f(\overline{P})}} \prod_{i=1}^{s} \frac{\overline{X}_{f(\overline{P}+\overline{Q}_i)} \overline{X}_{f(\overline{P}-\overline{Q}_i)} \overline{Z}^2_{f(\overline{Q}_i)}}{\overline{Z}_{f(\overline{P}+\overline{Q}_i)} \overline{Z}_{f(\overline{P}-\overline{Q}_i)} \overline{X}^2_{f(\overline{Q}_i)}} \right). \tag{41}$$

Having compression $f(\overline{P})$ of point $\overline{P}$, provided in projective compression representation by $(\overline{X}_{f(\overline{P})} : \overline{Z}_{f(\overline{P})})$ and the set $\overline{J}$, one can compute $\frac{\overline{X}_{f(\overline{P}+\overline{Q})} \overline{X}_{f(\overline{P}-\overline{Q})}}{\overline{Z}_{f(\overline{P}+\overline{Q})} \overline{Z}_{f(\overline{P}-\overline{Q})}}$ using identities

$$\begin{cases} \overline{X}_{f(\overline{P}+\overline{Q})} \overline{X}_{f(\overline{P}-\overline{Q})} = \left(\overline{X}_{f(\overline{P})} \overline{Z}_{f(\overline{Q})} - \overline{X}_{f(\overline{Q})} \overline{Z}_{f(\overline{P})} \right)^2, \\ \overline{Z}_{f(\overline{P}+\overline{Q})} \overline{Z}_{f(\overline{P}-\overline{Q})} = \left(\overline{a}\overline{b} \overline{X}_{f(\overline{P})} \overline{X}_{f(\overline{Q})} - \overline{Z}_{f(\overline{P})} \overline{Z}_{f(\overline{Q})} \right)^2, \end{cases} \tag{42}$$

and therefore one can obtain $f(\overline{\psi}(\overline{P}))$.

To find the coefficients $\overline{a}'$ and $\overline{b}'$ of general Huff's curve $G_{\overline{a}',\overline{b}'}$, one can use similar transformations as for formulas (15) and (16) and obtain

$$\begin{aligned} \overline{x}^2_{\overline{P}} &= \frac{\overline{X}_{f(\overline{P})} \left(a \overline{X}_{f(\overline{P})} + \overline{Z}_{f(\overline{P})} \right)}{\overline{Z}_{f(\overline{P})} \left(b \overline{X}_{f(\overline{P})} + \overline{Z}_{f(\overline{P})} \right)}, \\ \overline{y}^2_{\overline{P}} &= \frac{\overline{X}_{f(\overline{P})} \left(b \overline{X}_{f(\overline{P})} + \overline{Z}_{f(\overline{P})} \right)}{\overline{Z}_{f(\overline{P})} \left(a \overline{X}_{f(\overline{P})} + \overline{Z}_{f(\overline{P})} \right)}. \end{aligned} \tag{43}$$

Finally,

$$\begin{aligned} \overline{a}' &= \overline{a}^{\ell} \overline{B}^4 = \overline{a}^{\ell} \prod_{i=1}^{s} {y_{\overline{P}_i}}^4 = \overline{a}^{\ell} \prod_{i=1}^{s} \left(\frac{\overline{X}_{f(\overline{P}_i)} \left(\overline{b} \overline{X}_{f(\overline{P}_i)} + \overline{Z}_{f(\overline{P}_i)} \right)}{\overline{Z}_{f(\overline{P}_i)} \left(\overline{a} \overline{X}_{f(\overline{P}_i)} + \overline{Z}_{f(\overline{P}_i)} \right)} \right)^2, \\ \overline{b}' &= \overline{b}^{\ell} \overline{A}^4 = \overline{b}^{\ell} \prod_{i=1}^{s} {x_{\overline{P}_i}}^4 = \overline{b}^{\ell} \prod_{i=1}^{s} \left(\frac{\overline{X}_{f(\overline{P}_i)} \left(\overline{a} \overline{X}_{f(\overline{P}_i)} + \overline{Z}_{f(\overline{P}_i)} \right)}{\overline{Z}_{f(\overline{P}_i)} \left(\overline{b} \overline{X}_{f(\overline{P}_i)} + \overline{Z}_{f(\overline{P}_i)} \right)} \right)^2. \end{aligned} \tag{44}$$

B. Huff's isogenies computation using compression techniques

In this subsection, it will be shown how to obtain formulas for computation of isogeny on Huff's curves using Theorem 3 and sequence of isomorphisms and isogenies between Huff's and general Huff's curves.

Theorem 4. *Let $F = \{(0,0), (\alpha_i, \beta_i), (-\alpha_i, -\beta_i) : i = 1 \dots s\}$, where $-(\alpha_i, \beta_i) = (-\alpha_i, -\beta_i)$, be the kernel of an isogeny ψ. Let $A = \prod_{i=1}^{s} \alpha_i$ and $B = \prod_{i=1}^{s} \beta_i$. Let's define*

$$\begin{aligned} \psi(P) = \; &\Big(x_P (-1)^s \textstyle\prod_{Q \neq (0,0) \in F} x_{P+Q}, \\ &y_P (-1)^s \textstyle\prod_{Q \neq (0,0) \in F} y_{P+Q} \Big). \end{aligned} \tag{45}$$

Then ψ is a ℓ-isogeny with kernel F, from the curve $H_{a,b}$, to the curve $H_{a',b'}$, where $a' = \frac{a}{A^2} = \frac{a}{\prod_{i=1}^{s} x^2_{Q_i}}$ and $b' = \frac{b}{B^2} = \frac{b}{\prod_{i=1}^{s} y^2_{Q_i}}$

Proof. To prove the Theorem 4 we will use the following composition $\tau \circ \overline{\psi} \circ \xi$, where:

- ξ is an isomorphism from Huff's curve $H_{a,b}$ to general Huff's curve $G_{\overline{a},\overline{b}}$, where $\overline{a} = \frac{1}{b^2}, \overline{b} = \frac{1}{a^2}$ and where for $P = (x, y)$ the isomorphism ξ using Lemma 1 has the form $\overline{P} = \xi(P) = (ax, by) = (\overline{x}, \overline{y})$,
- $\overline{\psi}$ is an isogeny from general Huff's curve $G_{\overline{a},\overline{b}}$ to general Huff's curve $G_{\overline{a}',\overline{b}'}$, where the kernel $\overline{F} = \{(0,0), \xi(\alpha_i, \beta_i), \xi(-\alpha_i, -\beta_i)\} = \{(0,0), (\overline{\alpha}_i, \overline{\beta}_i), (-\overline{\alpha}_i, -\overline{\beta}_i)\}$ and for $\overline{P} = (\overline{x}, \overline{y})$ the isogeny $\overline{\psi}$ has the form

$$\begin{aligned}\overline{P}' &= \overline{\psi}(\overline{P})\\ &= \left(\overline{x}_{\overline{P}}\prod_{\overline{Q}\neq(0,0)\in\overline{F}}\frac{-\overline{x}_{\overline{P}+\overline{Q}}}{\overline{x}_{\overline{Q}}}, \overline{y}_{\overline{P}}\prod_{\overline{Q}\neq(0,0)\in\overline{F}}\frac{-\overline{y}_{\overline{P}+\overline{Q}}}{\overline{y}_{\overline{Q}}}\right)\\ &= \left(ax_P\prod_{Q\neq(0,0)\in F}\frac{-x_{P+Q}}{x_Q}, by_P\prod_{Q\neq(0,0)\in F}\frac{-y_{P+Q}}{y_Q}\right)\end{aligned} \tag{46}$$

where

$$\begin{aligned}\overline{a}' &= \overline{a}^{\ell}\overline{B}^4 = \overline{a}^{\ell}\left(\prod_{i=1}^{s}\overline{\beta}_i\right)^4,\\ \overline{b}' &= \overline{b}^{\ell}\overline{A}^4 = \overline{b}^{\ell}\left(\prod_{i=1}^{s}\overline{\alpha}_i\right)^4.\end{aligned} \tag{47}$$

- τ is an isomorphism from general Huff's curve $G_{\overline{a}',\overline{b}'}$ to the Huff's curve $H_{a',b'}$, where

$$\begin{aligned}a' &= \frac{1}{\sqrt{\overline{b}'}} = \frac{1}{\sqrt{\frac{1}{a^{2\ell}}\left(\prod_{i=1}^{s}ax_{Q_i}\right)^2}} = \frac{1}{\frac{a^{2s}}{a^{\ell}}\left(\prod_{i=1}^{s}x_{Q_i}\right)^2} = \frac{a}{\left(\prod_{i=1}^{s}x_{Q_i}\right)^2},\\ b' &= \frac{1}{\sqrt{\overline{a}'}} = \frac{1}{\sqrt{\frac{1}{b^{2\ell}}\left(\prod_{i=1}^{s}by_{Q_i}\right)^2}} = \frac{1}{\frac{b^{2s}}{b^{\ell}}\left(\prod_{i=1}^{s}y_{Q_i}\right)^2} = \frac{b}{\left(\prod_{i=1}^{s}y_{Q_i}\right)^2}\end{aligned} \tag{48}$$

and

$$\begin{aligned}P' &= \tau(\overline{P}')\\ &= \left(\frac{a}{a'}x_P\prod_{Q\neq(0,0)\in F}\frac{-x_{P+Q}}{x_Q}, \frac{b}{b'}y_P\prod_{Q\neq(0,0)\in F}\frac{-y_{P+Q}}{y_Q}\right)\\ &= \left(x_P\left(\prod_{i=1}^{s}x_{Q_i}\right)^2\prod_{Q\neq(0,0)\in F}\frac{-x_{P+Q}}{x_Q},\right.\\ &\left. y_P\left(\prod_{i=1}^{s}y_{Q_i}\right)^2\prod_{Q\neq(0,0)\in F}\frac{-y_{P+Q}}{y_Q}\right)\\ &= \left(x_P(-1)^s\prod_{Q\neq(0,0)\in F}x_{P+Q}, y_P(-1)^s\prod_{Q\neq(0,0)\in F}y_{P+Q}\right).\end{aligned} \tag{49}$$

□

Corollary 2. *Let $R \in H_{a,b}$ and let $(X_{f(R)} : Z_{f(R)})$ be projective representation of $f(R)$, where R is the point defining the kernel F of the isogeny ψ. Let $Ord(R)$ be the odd number. Let's note that $f(\psi(P))$ is given by*

$$f(\psi(P)) = \left(x_P(-1)^s\prod_{Q\neq(0,0)\in F}x_{P+Q}\cdot y_P(-1)^s\prod_{Q\neq(0,0)\in F}y_{P+Q}\right), \tag{50}$$

which is equal to

$$\begin{aligned}f(\psi(P)) &= \left(x_Py_P\prod_{Q\neq(0,0)\in F}x_{P+Q}y_{P+Q}\right)\\ &= \left(f(P)\prod_{Q\in F^+}f(P+Q)f(P-Q)\right),\end{aligned} \tag{51}$$

where F^+ is the set $\{(\alpha_i,\beta_i) : i = 1,\ldots,s\}$. Having generator R of the kernel of the isogeny $\overline{\psi}$, given by projective compression representation $(X_{f(R)} : Z_{f(R)})$, it is easy to obtain other elements of the F^+, using for example a ladder method. Let J be the set of projective representations of F^+, so $J = \{(X_{f(Q_i)} : Z_{f(Q_i)}) : i = 1,\ldots,s\}$. In a projective representation $f(\overline{\psi})$ using point compression may be provided by

$$f(\psi(P)) = \left(\frac{X_{f(P)}}{Z_{f(P)}}\prod_{i=1}^{s}\frac{X_{f(P+Q_i)}X_{f(P-Q_i)}}{Z_{f(P+Q_i)}Z_{f(P-Q_i)}}\right). \tag{52}$$

To find the coefficients a' and b' of Huff's curve $H_{a',b'}$, if $f(P) = \frac{X_{f(P)}}{Z_{f(P)}}$, one can use formula (53)

$$\begin{aligned}x_P^2 &= \frac{X_{f(P)}\left(aX_{f(P)}+bZ_{f(P)}\right)}{Z_{f(P)}\left(bX_{f(P)}+aZ_{f(P)}\right)},\\ y_P^2 &= \frac{X_{f(P)}\left(bX_{f(P)}+aZ_{f(P)}\right)}{Z_{f(P)}\left(aX_{f(P)}+bZ_{f(P)}\right)},\end{aligned} \tag{53}$$

and finally gets

$$\begin{aligned}a' &= \frac{a}{\left(\prod_{i=1}^{s}x_{Q_i}\right)^2} = \frac{a\prod_{i=1}^{s}Z_{f(Q_i)}\left(bX_{f(Q_i)}+aZ_{f(Q_i)}\right)}{\prod_{i=1}^{s}X_{f(Q_i)}\left(aX_{f(Q_i)}+bZ_{f(Q_i)}\right)},\\ b' &= \frac{b}{\left(\prod_{i=1}^{s}x_{Q_i}\right)^2} = \frac{b\prod_{i=1}^{s}Z_{f(Q_i)}\left(aX_{f(Q_i)}+bZ_{f(Q_i)}\right)}{\prod_{i=1}^{s}X_{f(Q_i)}\left(bX_{f(Q_i)}+aZ_{f(Q_i)}\right)}.\end{aligned} \tag{54}$$

IV. Efficiency of obtained formulas

Formulas obtained in the previous sections may be used, for example, in the isogeny-based cryptography, like in the SIDH algorithm, and may be the alternative for Montgomery curves' arithmetic.

Efficient algorithms for isogeny-based cryptography using compression on Montgomery curves have been presented in [16] and [17].

As follows from (27) and (29), the computation of $f(P+Q)f(P-Q)$, addition and doubling in all cases of (Huff's and Montgomery curves) costs $4M+2S$, $2M+2S$ and $2M+2S+c$ respectively. For general Huff's curves computational costs are $4M+2S+c$, $6M+2S+c$ and $2M+3S+2c$.

It is worth noting that, e.g., in the SIKE algorithm, only coefficient A of the Montgomery curve $M_{A,B}$ provided by equation (26) is required, and this coefficient may be obtained having x-coordinates of three distinct points on $M_{A,B}$. It costs $8M+3S$. It is an open issue to use a similar approach to (general) Huff's curves.

A. Huff's curves

1) Cost of ℓ-isogenous curve computation: At first, one needs to compute the projective representation of elements Q_i, for $i = \overline{1,s}$ of the kernel of the isogeny. This may be computed having the first element of the kernel (generator of the subgroup) in projective representation $\left(X_{f(Q_1)} : Z_{f(Q_1)}\right)$ and making doubling to obtain $\left(X_{f(Q_2)} : Z_{f(Q_2)}\right)$ and $s-2$ times differential addition to obtain other elements of the kernel $\left(X_{f(Q_3)} : Z_{f(Q_3)}\right)$, $\left(X_{f(Q_4)} : Z_{f(Q_4)}\right)$, $\ldots$, $\left(X_{f(Q_s)} : Z_{f(Q_s)}\right)$. Moreover, let's note, that in both formulas for a' and b' (54), there appears $aX_{f(Q_i)}$, $bX_{f(Q_i)}$, $aZ_{f(Q_i)}$, $bZ_{f(Q_i)}$ for every $i = \overline{1,s}$. The computation of these elements requires 4 multiplications by constants. Additionally, in both nominators and denominators, there are required multiplications by $Z_{f(Q_i)}$ and $X_{f(Q_i)}$ respectively, which results in 4 additional multiplications. Product multiplications require additional $4(s-1)$ multiplications. Finally, there are required other multiplications by a and b. So finally, to compute a' and b' one requires

$$\begin{aligned}&Doub + (s-2)DiffAdd + 4s(c+M) + 4(s-1)M + 2M\\ &\quad = (s-1)(4M+2S) + 4s(c+M) + 4(s-1)M + 2M\\ &\quad = 2sS + 4sc + 12sM - 2S - 6M,\end{aligned} \tag{55}$$

where $Doub$ and $DiffAdd$ are the costs of doubling and differential addition respectively. In the most interesting cases for us, computation of the 3-isogenous and 5-isogenous curve, one obtains that computing the isogenous curve $H_{a',b'}$ costs $6M+4c$ and $2S+8c+18M$ respectively.

2) Cost of odd ℓ-isogeny evaluation, where $\ell = 2s+1$: Let's note, that every computation of $X_{f(P+Q_i)}X_{f(P-Q_i)}$ and $Z_{f(P+Q_i)}Z_{f(P-Q_i)}$ for $i = \overline{1,s}$ requires $2M+2S$ every. Additionally, there are required $2(s-1)$ product multiplications (in the nominator and denominator). Moreover, there are required 2 additional multiplications by $X_{f(P)}$ and $Z_{f(P)}$. So finally, for $\ell = 2s+1$ isogeny evaluation cost is

$$\begin{aligned} &s(2M+2S)+2(s-1)M+2M \\ &= 2sS+4sM. \end{aligned} \tag{56}$$

In the most interesting cases, evaluation of 3-isogeny and 5-isogeny, one obtains that such evaluation costs $4M+2S$ and $8M+4S$ respectively.

B. General Huff's curves

1) Cost of ℓ-isogenous curve computation: Similarly to Huff's curves at the beginning, one needs to compute projective representation of the isogeny elements $\overline{Q}_i$, for $i = \overline{1,s}$ of the kernel of the isogeny. This may be computed having the first element of the kernel (generator of the subgroup) in projective representation $\left(\overline{X}_{f(\overline{Q}_1)} : \overline{Z}_{f(\overline{Q}_1)}\right)$ and making doubling to obtain $\left(\overline{X}_{f(\overline{Q}_2)} : \overline{Z}_{f(\overline{Q}_2)}\right)$ and $s-2$ times differential addition to obtain other elements of the kernel $\left(\overline{X}_{f(\overline{Q}_3)} : \overline{Z}_{f(\overline{Q}_3)}\right)$, $\left(\overline{X}_{f(\overline{Q}_4)} : \overline{Z}_{f(\overline{Q}_4)}\right)$, $\ldots$, $\left(\overline{X}_{f(\overline{Q}_s)} : \overline{Z}_{f(\overline{Q}_s)}\right)$. Moreover, let's note, that in both formulas for $\overline{a}'$ and $\overline{b}'$ (44), there appears $\overline{a}\overline{X}_{f(\overline{Q}_i)}$, $\overline{bX}_{f(\overline{Q}_i)}$, $\overline{a}\overline{Z}_{f(\overline{Q}_i)}$, $\overline{bZ}_{f(\overline{Q}_i)}$ for every $i = \overline{1,s}$. The computation of these elements requires 4 multiplications by constants. Additionally, in both nominators and denominators, there are required multiplications by $\overline{Z}_{f(\overline{Q}_i)}$ and $\overline{X}_{f(\overline{Q}_i)}$ respectively and squarings, which results in 4 additional multiplications and 4 squarings. Product multiplications require additional $4(s-1)$ multiplications. Finally, there are required other multiplications by $\overline{a}^\ell$ and $\overline{b}^\ell$. Computing both $\overline{a}^\ell$ and $\overline{b}^\ell$ requires $len(\ell)-1$ constant doubling and $hwt(\ell)-1$ constant squaring respectively, where $len(\ell)$ denotes binary length of ℓ and $hwt(\ell)$ the Hamming weight of ℓ. So finally, to compute $\overline{a}'$ and $\overline{b}'$ one requires

$$\begin{aligned} &Doub+(s-2)DiffAdd+s(4c+6M+2S) \\ &\quad+4(s-1)M+2M+2((len(\ell)-1)d+(hwt(\ell)-1)c) \\ &\quad= 4M(4s-3)+S(4s-1)+c(5s+2hwt(\ell)-3) \\ &\quad+2d(len(\ell)-1), \end{aligned} \tag{57}$$

where, $Doub$ and $DiffAdd$ are the costs of doubling and differential addition respectively and d is a cost of constant squaring. In the most interesting cases for us, computation of 3-isogeny and 5-isogeny, one obtains that computing isogenous curve $G_{\overline{a}',\overline{b}'}$ costs $4M+3S+6c+2d$ and $20M+7S+11c+4d$ respectively. Performing a constant squaring simply as a multiplication we obtain for the ℓ-isogeny

$$4M(4s-3)+S(4s-1)+c(5s+2hwt(\ell)+2len(\ell)-5). \tag{58}$$

For the computation of 3-isogenous and 5-isogenous curves, one obtains $4M+3S+8c$ and $20M+7S+15c$ respectively.

2) Cost of odd ℓ-isogeny evaluation, where $\ell = 2s+1$: Let's note, that every computation of $\overline{X}_{f(\overline{P}+\overline{Q}_i)}\overline{X}_{f(\overline{P}-\overline{Q}_i)}\overline{Z}^2_{f(\overline{Q}_i)}$ and $\overline{Z}_{f(\overline{P}+\overline{Q}_i)}\overline{Z}_{f(\overline{P}-\overline{Q}_i)}\overline{X}^2_{f(\overline{Q}_i)}$ for $i = \overline{1,s}$ requires $4M+4S$ every. Additionally, there are required $2(s-1)$ product multiplications (in the nominator and denominator). Moreover, there are required 2 additional multiplications by $X_{f(P)}$ and $Z_{f(P)}$ and 4 squarings. So finally, for the $\ell = 2s+1$ isogeny evaluation cost is

$$\begin{aligned} &s(4M+4S)+2(s-1)M+2M \\ &= 4sS+6sM. \end{aligned} \tag{59}$$

In the most interesting cases, evaluation of 3-isogeny and 5-isogeny, one obtains that such evaluation costs $6M+4S$ and $12M+8S$, respectively.

V. ECM ALGORITHM USING HUFF'S AND GENERAL HUFF'S CURVES

In this subsection we will show how to generate Huff's and general Huff's curves convenient for the use in ECM algorithm, where compression techniques presented in this paper may be used.

In [18] the Theorem 5 was proven.

Theorem 5. *([18], Theorem 4.10.) Let $K = \mathbb{Q}\left(\sqrt{-1}, \sqrt{t^4-6t^2+1}\right)$ with $t \in \mathbb{Q}$ and $t \neq 0, \pm 1$ and let E be an elliptic curve defined by the equation*

$$E : \breve{y}^2 + \breve{x}\breve{y} - \left(v^2 - \frac{1}{16}\right)\breve{y} = \breve{x}^3 - \left(v^2 - \frac{1}{16}\right)\breve{x}^2, \tag{60}$$

where $v = \frac{t^4-6t^2+1}{4(t^2+1)^2}$. Then, the torsion subgroup of E over K is equal to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ for almost all t.

We will show how to find Huff's curve $H_{a,b}$ isomorphic to the curve E.

At first, the isomorphic short Weierstrass curve E_1 to the curve E is equal to

$$\begin{aligned} E_1 : \dot{y}^2 &= \dot{x}^3 + (-432s^2 - 432s - 27)\dot{x} \\ &+(-3456s^3 + 6480s^2 + 1296s + 54), \end{aligned} \tag{61}$$

where $s = \left(v^2 - \frac{1}{16}\right)$. Now it is necessary to find the x-coordinate of three points of order 2, which are the roots of $f(u) = u^3 + (-432s^2 - 432s - 27)u + (-3456s^3 + 6480s^2 + 1296s + 54)$. They are equal to

$$\begin{cases} r_0 = \frac{3t^8-12t^6+66t^4-12t^2+3}{t^8+4t^6+6t^4+4t^2+1}, \\ r_1 = -\frac{6t^8-24t^6-12t^4-24t^2+6}{t^8+4t^6+6t^4+4t^2+1}, \\ r_2 = \frac{3t^8-12t^6-78t^4-12t^2+3}{t^8+4t^6+6t^4+4t^2+1}. \end{cases} \tag{62}$$

Substituting,

$$R_0 = 0, \;\; R_1 = r_1 - r_0, \;\; R_2 = r_2 - r_0,$$

one obtains isomorphic elliptic curve

$$E_2 : \hat{y}^2 = \hat{x}^3 - (R_1 + R_2)\hat{x}^2 + R_1R_2\hat{x}. \tag{63}$$

The roots R_0, R_1, R_2 are equal to:

$$\begin{cases} R_0 = 0, \\ R_1 = -\frac{9(t-1)^4(t+1)^4}{(t^2+1)^4} = -\left(\frac{3(t-1)^2(t+1)^2}{(t^2+1)^2}\right)^2, \\ R_2 = -\frac{144t^4}{(t^2+1)^4} = -\left(\frac{12t^2}{(t^2+1)^2}\right)^2. \end{cases} \tag{64}$$

Using isomorphism between Weierstrass and Huff's curve given in [11]

$$H_{a,b} : ax(y^2-1) = by(x^2-1) \cong E_2 : \hat{y}^2 = \hat{x}(\hat{x}+a^2)(\hat{x}+b^2) \tag{65}$$

and isomorphism between general Huff's and Weierstrass curve [12]

$$G_{\overline{a},\overline{b}} : \overline{x}(\overline{a}\overline{y}^2 - 1) = \overline{y}(\overline{b}\overline{x}^2 - 1) \cong E_2 : \hat{y}^2 = \hat{x}(\hat{x}+\overline{a})(\hat{x}+\overline{b}), \tag{66}$$

one can find the coefficients of the isomorphic Huff's curve whose are therefore equal to

$$a = \frac{3(t-1)^2(t+1)^2}{(t^2+1)^2}, \ b = \frac{12t^2}{(t^2+1)^2}. \tag{67}$$

and the coefficients of the isomorphic general Huff's curve whose are therefore equal to

$$\overline{a} = \frac{9(t-1)^4(t+1)^4}{(t^2+1)^4}, \ \overline{b} = \frac{144t^4}{(t^2+1)^4}. \tag{68}$$

VI. Conclusion

This paper presents formulas for doubling and differential addition on Huff's and general Huff's curves of odd characteristic and the degree 2 compression function. For Huff's curves, the efficiency of those formulas is similar as for the Montgomery curve and formulas for general Huff's curves are not so efficient. Moreover, these formulas seem to be new for these models of elliptic curves. Additionally, formulas for point recovery after compression were presented.

Recently formulas as efficient as Montgomery's were given by Farashahi [5] for twisted Edwards curves, who used a compression function $E \to K$ of degree 8.

The important part of the paper is the presentation of formulas for general odd-isogeny computation on Huff's curves, which seem to be new for this model. Additionally, it is shown how to apply these formulas to the isogeny-based cryptography using a proposed compression function.

The applications of obtained formulas for Huff's and general Huff's curves to the isogeny-based cryptography and ECM method have been shown.

It is an open issue, if for the presented formulas for Huff's curves it is possible to use a similar scheme as in [16] and [17] for Montgomery curves to obtain better efficiency.

References

[1] D. J. Bernstein and T. Lange, "Montgomery curves and the montgomery ladder." *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 293, 2017.

[2] C. Costello and B. Smith, "Montgomery curves and their arithmetic," *Journal of Cryptographic Engineering*, vol. 8, no. 3, pp. 227–240, 2018.

[3] P. L. Montgomery, "Speeding the pollard and elliptic curve methods of factorization," *Mathematics of Computation*, vol. 48, pp. 243–264, 1987.

[4] E. Brier and M. Joye, "Weierstraß elliptic curves and side-channel attacks," in *International workshop on public key cryptography*. Springer, 2002, pp. 335–345.

[5] R. R. Farashahi and S. G. Hosseini, "Differential addition on twisted edwards curves," in *Australasian Conference on Information Security and Privacy*. Springer, 2017, pp. 366–378.

[6] B. Justus and D. Loebenberger, "Differential addition in generalized edwards coordinates," in *International Workshop on Security*. Springer, 2010, pp. 316–325.

[7] R. R. Farashahi and M. Joye, "Efficient arithmetic on hessian curves," in *International Workshop on Public Key Cryptography*. Springer, 2010, pp. 243–260.

[8] W. Castryck and F. Vercauteren, "Toric forms of elliptic curves and their arithmetic," *Journal of Symbolic Computation*, vol. 46, no. 8, pp. 943–966, 2011.

[9] R. Dryło, T. Kijko, and M. Wroński, "Determining formulas related to point compression on alternative models of elliptic curves," *Fundamenta Informaticae*, vol. 169, no. 4, pp. 285–294, 2019.

[10] K. Okeya and K. Sakurai, "Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a montgomery-form elliptic curve," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2001, pp. 126–141.

[11] M. Joye, M. Tibouchi, and D. Vergnaud, "Huff's model for elliptic curves," in *International Algorithmic Number Theory Symposium*. Springer, 2010, pp. 234–250.

[12] H. Wu and R. Feng, "Elliptic curves in huff's model," *Wuhan University Journal of Natural Sciences*, vol. 17, no. 6, pp. 473–480, 2012.

[13] T. Oliveira, J. López, H. Hışıl, A. Faz-Hernández, and F. Rodríguez-Henríquez, "How to (pre-) compute a ladder," in *International Conference on Selected Areas in Cryptography*. Springer, 2017, pp. 172–191.

[14] R. R. Farashahi and S. G. Hosseini, "Differential addition on binary elliptic curves," in *International Workshop on the Arithmetic of Finite Fields*. Springer, 2016, pp. 21–35.

[15] D. Moody and D. Shumow, "Analogues of vélu's formulas for isogenies on alternate models of elliptic curves," *Mathematics of Computation*, vol. 85, no. 300, pp. 1929–1951, 2016.

[16] C. Costello and H. Hisil, "A simple and compact algorithm for sidh with arbitrary degree isogenies," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2017, pp. 303–329.

[17] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik, "Supersingular isogeny key encapsulation," 04 2019.

[18] D. Jeon, C. H. Kim, and Y. Lee, "Families of elliptic curves over quartic number fields with prescribed torsion subgroups," *Mathematics of computation*, vol. 80, no. 276, pp. 2395–2410, 2011.

VII. Appendices

A. Comparison of computational costs

In the Table I computational costs of operations on Huff's curve using compression function $f(x,y) = xy$, general Huff's curve operations using compression function $f(x,y) = xy$ and Montgomery curve operations using compression function $f(x,y) = x$ are presented.

TABLE I

COMPUTATIONAL COSTS OF OPERATIONS ON HUFF'S CURVE USING COMPRESSION FUNCTION $f(x,y) = xy$, GENERAL HUFF'S CURVE OPERATIONS USING COMPRESSION FUNCTION $f(x,y) = xy$ AND MONTGOMERY CURVE OPERATIONS USING COMPRESSION FUNCTION $f(x,y) = x$, WHERE COSTS OF OPERATIONS IN FIELD K ARE DENOTED AS: M FOR MULTIPLICATION, S FOR SQUARING, c FOR MULTIPLICATION BY CONSTANT.

Operation	$H_{a,b}$	$G_{\overline{a},\overline{b}}$	$M_{A,B}$
$f(P+Q)f(P-Q)$	$2M+2S$	$4M+2S+c$	$2M+2S$ [3]
Differential addition $f(P+Q)$	$4M+2S$	$6M+2S+c$	$4M+2S$ [3]
Doubling $f([2]P)$	$3M+2S+c$	$2M+3S+3c$	$3M+2S+c$ [3]
Doubling ($\frac{(a+b)^2}{4ab}$, $\overline{a}\overline{b}$ and $\frac{A-2}{4}$ are constant)	$2M+2S+c$	$2M+3S+2c$	$2M+2S+c$ [3]
2-isogenous curve	-	-	$2S$ [17]
2-isogenous curve	-	-	w [17]
3-isogenous curve	$6M+4c$	$6M+2S+8c$	$2M+3S$
5-isogenous curve the full kernel is not given	$18M+2S+8c$	$20M+7S+15c$	$8M+3S$ [16][Eq. 16]
ℓ-isogenous curve the full kernel is not given	$6M(2s-1)+$ $S(2s-1)+4sc$	$4M(4s-3)+$ $S(4s-1)+$ $c(5s+2hwt(\ell)+$ $2len(\ell)-5)$	$8M+3S$ [16][Eq. 16]
2-isogeny evaluation	-	-	$4M$ [17]
3-isogeny evaluation	$4M+2S$	$6M+4S$	$2M+3S$ [17]
5-isogeny evaluation	$8M+4S$	$12M+8S$	$8M+2S$ [16][Alg. 3]
ℓ-isogeny evaluation	$4sM+2sS$	$6sM+4sS$	$4sM+2S$