Decomposition of compressions on elliptic curves and point recovery

Robert Dryło

Institute of Mathematical Economics, Warsaw School of Economics,
al. Niepodległości 162, 02-554 Warsaw, Poland
rdrylo@sgh.waw.pl
Institute of Mathematics and Cryptology, Military University of Technology,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warsaw, Poland
robert.drylo@wat.edu.pl

Abstract. Let E be an elliptic curve over a perfect field K. A function $f \in K(E)$ is a compression of degree 2 on E if $f(-P) = f(P)$ for all $P \in E$, and the field extension $K(f) \subset K(E)$ is of degree 2. For a finite subgroup $G \subset E$ over K a function $w \in K(E)$ we will call a G-compression if $w(\pm P + G) = w(P)$ for all $P \in E$, and the field extension $K(w) \subset K(E)$ is of degree $2|G|$. We will show that $w \in K(E)$ is a G-compression if and only if $w = f \circ \Phi$ for a separable isogeny $\Phi : E \to E'$ over K with $\ker \Phi = G$, an elliptic curve E'/K, and a compression $f \in K(E')$ of degree 2 on E'. This allows to obtain a doubling, a differential addition, and a method for point recovery for G-compressions using known properties of compressions of degree 2. For G-compressions w studied in the literature on an extended Jacobi quartic, a twisted Edwards curve, a twisted Jacobi intersection, and a twisted Hessian curve (for the first and third model additional conditions on coefficients are assumed) we will give the decomposition $w = f \circ \Phi$ as above, and the function induced by the dual isogeny $\widehat{\Phi}$ and compressions of degree 2, which can be used for point recovery. For the first three models this isogeny Φ is to a Montgomery curve over K, and has the first coordinate $x(\Phi) = 1/w$. We also give isomorphisms from some models of elliptic curves to a Montgomery curve.

Keywords: elliptic curve cryptography · alternative models of elliptic curves · compression · Kummer line · Montgomery ladder algorithm · isogeny

1 Introduction

Elliptic curves were introduced to cryptography by Koblitz [28] and Miller [32]. The following models of elliptic curves have properties useful for applications in cryptography: Weierstrass, Montgomery [34], twisted Edwards [2,14], extended Jacobi quartic [4,8,20], twisted Hessian [3,8,17,25,38], Huff [26,42], twisted Jacobi intersection [8,18,30], and other models.

On the Montgomery curve $M_{A,B} : By^2 = x^3 + Ax^2 + x$ the x-coordinate doubling and differential addition

$$x_{[2]P} = \frac{(x_P^2 - 1)^2}{4x_P(x_P^2 + Ax_P + 1)} \text{ and } x_{P+Q}x_{P-Q} = \left(\frac{x_P x_Q - 1}{x_P - x_Q}\right)^2 \tag{1.1}$$

for $P, Q \in M_{A,B}$ were given by Montgomery in [34]. These formulas have low cost of evaluation, and can be used in the Montgomery ladder algorithm to compute the x-coordinate of the point nP using x-coordinates only for $P \in M_{A,B}$ and $n \in \mathbb{Z}$. Therefore Montgomery curves are useful for efficient implementation of some computations in elliptic curve cryptography (see, e.g., [9]) and of the Lenstra elliptic curve factorization method [29,34].

Let E be an elliptic curve over a perfect field K with an algebraic closure $\overline{K}$. A function $f \in K(E)$ we will call a compression of degree 2 on E if $f(P) = f(-P)$ for all $P \in E$, and the field extension $K(f) \subset K(E)$ is of degree 2. The x-coordinate is a standard compression of degree 2 on elliptic curves in Weierstrass and Montgomery forms. Let $f \in K(E)$ be a compression of degree 2. We have the multiplication of values of f by integers induced from E given by $[n]f(P) = f(nP)$ for $P \in E$ and $n \in \mathbb{Z}$. The projective line with this multiplication by integers is called the Kummer line. There exist functions called an f-doubling $D(x) \in K(x)$ and an f-differential addition $A(x, y, z) \in K(x, y, z)$, which satisfy eq. (1.4) below for $w = f$, and can be used in the Montgomery ladder algorithm to compute $f(nP)$ using values of f only for $n \in \mathbb{Z}$. There exists also a rational map R_f on $E \times \overline{K}^2$ over K, which we will call a point recovery formula, such that

$$Q = \mathrm{Rec}_f(P, f(Q), f(P + Q)) \tag{1.2}$$

for generic $P, Q \in E$. If $P \in E$ and $n \in \mathbb{Z}$ are given, and $f(nP)$ is computed using the Montgomery ladder algorithm, which determines also $f((n + 1)P)$, then one can recover the point $nP = \mathrm{Rec}_f(P, f(nP), f((n + 1)P))$ on E. Formulas for doubling, differential addition and point recovery for compressions of degree 2 were given for most of the above models of elliptic curves, see [6,7,11,12,13,23,27,34,36].

Compressions of degree > 2 studied in [16,17,19,21,22] on elliptic curves are examples of G-compressions, which we will consider in this paper. Let $G \subset E$ be a finite subgroup over K (i.e. $G^\sigma = G$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$) of order $|G|$. A function $w \in K(E)$ we will call a G-compression if

$$w(\pm P + Q) = w(P) \quad \forall P \in E \; \forall Q \in G, \tag{1.3}$$

and the field extension $K(w) \subset K(E)$ is of degree $2|G|$. A function $u \in K(E)$ we will call invariant under a rational map $\sigma : E \to E$ if $u \circ \sigma = u$. Equivalently with (1.3) one can say that w is invariant under $[-1]$ and translations by all generators Q of G. Compressions of degree 2 are exactly $\{0\}$-compressions. Let $w \in K(E)$ be a G-compression. We have multiplication of values of w by integers induced from E given by $[n]w(P) = w(nP)$ for $P \in E$ and $n \in \mathbb{Z}$ (for correctness see Corollary

1). We will say that $D(x) \in K(x)$ is a w-doubling and $A(x,y,z) \in K(x,y,z)$ is a w-differential addition if

$$w(2P) = D(w(P)) \text{ and } w(P+Q) = A(w(P), w(Q), w(P-Q)) \tag{1.4}$$

for generic $P, Q \in E$. These functions can be used in the Montgomery ladder algorithm to compute $w(nP)$ using values of w only. The following formulas for w-doubling and w-differential addition

$$\begin{aligned} w(2P) &= \frac{4w(P)(w(P)^2 + Aw(P) + 1)}{(w(P)^2 - 1)^2}, \\ w(P+Q)w(P-Q) &= \left(\frac{w(P) - w(Q)}{w(P)w(Q) - 1}\right)^2, \end{aligned} \tag{1.5}$$

were given for compression $w = xy$ of degree 2 on Huff's curve $Hu_v : vx(y^2-1) = y(x^2-1)$ by Dryło et al. in [12] (see also Huang et al. [23]), and for G-compressions $w = kx^2$ on the Jacobi quartic $Jq_{k^2,a} : y^2 = k^2x^4 + 2ax^2 + 1$ by Hu et al. in [21] (see Gu et al. [19] for $k = 1$), $w = d(xy)^2$ on the twisted Edwards curve $Ed_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ by Farashahi and Hosseini in [16], and $w = acx^2$ on the twisted Jacobi intersection $Ji_{a,ac^2} : ax^2 + y^2 = 1, ac^2x^2 + z^2 = 1$ by Hu et al. in [22]. Formulas (1.5) have cost of evaluation as law as Montgomery formulas (1.1), and are also satisfied for the compression $w = 1/x$ on the Montgomery curve $M_{A,B}$, where can be easily obtained from formulas (1.1) (see Lemma 1). For compressions on binary elliptic curves in the form of Edwards, Hessian and Huff doubling and differential addition in the form of Lopez and Dahab formulas [31], and point recovery methods were given by Farashahi and Hosseini in [15].

A map $\Phi : E \to E'$ we will call a G-isogeny if Φ is a separable isogeny over K of elliptic curves over K with $\ker \Phi = G$. If $\Phi : E \to E'$ is a G-isogeny and $f \in K(E')$ is a compression of degree 2, then it is easy to see that $w = f \circ \Phi$ is a G-compression, and functions $D \in K(x)$ and $A \in K(x,y,z)$ are w-doubling and w-differential addition if and only if are f-doubling and f-differential addition (see Proposition 1). This property is implicit in the paper of Farashahi and Hosseini [15, Lem. 3.9 and Rem. 3.10], where isogenies from suitable models of binary elliptic curves to the Weierstrass curve $W : y^2 + xy = x^3 + ax^2 + b$ were used to obtain compressions with doubling and differential addition in the form of Lopez and Dahab formulas, which were given for the x-coordinate compression on W in [31].

This paper is organized as follows. Section 2 contains some basic properties of compressions. In Section 3 we recall basic formulas for standard models of elliptic curves which will be used in this paper.

The contribution of this paper is the following. In Section 4 we show the following converse property to the above. If $w \in K(E)$ is a G-compression, then for a G-isogeny $\Phi : E \to E'$ there exists a compression of degree two $f \in K(E')$ such that $w = f \circ \Phi$ (Theorem 1). We have the following applications based on this decomposition. Let $w = f \circ \Phi$ be a G-compression, where Φ and f are as in Theorem 1. The multiplication of values of w by integers induced from E is

correct, and there exist a w-doubling and a w-differential addition (see Corollary 1). We obtain the following method of point recovery for a G-compression. Let $P \in E$ be of finite order $\mathrm{ord}(P)$ with $\gcd(\mathrm{ord}(P), |G|) = 1$, and $u \in \mathbb{Z}$ be the inverse of $|G|$ modulo $\mathrm{ord}(P)$. If we are given $P \in E$, $w(unP)$ and $w((un+1)P)$ for $n \in \mathbb{Z}$, then one can recover nP on E as follows

$$\begin{aligned} nP &= \widehat{\Phi}(R_f(\Phi(P), w(unP), w((un+1)P)) \\ &= R_g(|G|P, \widehat{\Phi}_{f,g}(w(unP)), \widehat{\Phi}_{f,g}(w((un+1)P)))) \end{aligned} \tag{1.6}$$

(Theorem 2), where $\widehat{\Phi} : E' \to E$ is the dual isogeny, $g \in K(E)$ is a compression of degree 2 on E, R_f and R_g are point recovery formulas (1.2) for f and g, and $\widehat{\Phi}_{f,g} \in K(x)$ is the function induced by $\widehat{\Phi}$, f, and g (i.e. $\widehat{\Phi}_{f,g} \circ f = g \circ \widehat{\Phi}$). Thus from the Montgomery ladder algorithm one can obtain $w(unP)$ and $w((un+1)P)$, and then recover nP on E using (1.6). Note that in the lower formula in (1.6) the function $\widehat{\Phi}_{f,g}$ is used instead of the isogenies Φ and $\widehat{\Phi}$ in the upper formula, which can simplify the method and save space. Isogenies in (1.6) are applied similarly as in the method of Brier and Joye [5] to carry multiplication of a suitable point from E to E', and then recover a result on E using the dual isogeny (see Section 2). In Remark 2 we observe that this method from [5] can also be applied to multiply a point after compression using functions induced by isogenies (see also Remark 4). In Proposition 3 we show that for an isogeny $\Psi : E_1 \to E_2$ over K of elliptic curves E_i/K with G_i-compressions $w_i \in K(E_i)$, $i = 1, 2$, which satisfies $\Psi(G_1) \subset G_2$, there exists the induced function $\Psi_{w_1,w_2} \in K(x)$ such that $\Psi_{w_1,w_2} \circ w_1 = w_2 \circ \Psi$.

In Section 5 we give the following formulas. In Proposition 4 we give isomorphisms over K to a Montgomery curve over K from the generalized Huff curve $Hu_{a,ac^2} : x(ay^2 - 1) = y(ac^2x^2 - 1)$, the Huff curve Hu_v, and the twisted Jacobi intersection Ji_{a,ac^2}, where $a, c, v \in K$. In Theorems 3 and 4 for G-compressions $w \in K(E)$ studied in the literature we give a G-isogeny $\Phi : E \to E'$ and compression $f \in K(E')$ of degree 2 such that $w = f \circ \Phi$, the dual isogeny $\widehat{\Phi}$ (in the proofs), and the induced function $\widehat{\Phi}_{f,g} \in K(x)$, which can be used for point recovery in eq. (1.6), where $g \in K(E)$ is a compression of degree 2. The formulas in Theorem 3 are for the above G-compressions w on the Jacobi quartic $Jq_{k^2,a}$, the twisted Edwards curve $Ed_{a,d}$, and the twisted Jacobi intersection Ji_{a,ac^2} for which formulas in eq. (1.5) were given in [21,16,22]. For these three compressions we give an isogeny Φ is to a Montgomery curve $M_{A,B}$, which has the first coordinate $x(\Phi) = 1/w$. In Corollary 2 we use this property of isogenies Φ from Theorem 3 and of isomorphisms Φ from Proposition 4 to give an alternative proof of formulas in eq. (1.5) for compressions w from [12,16,21,22], and to give formulas (1.5) for two new compressions w obtained from Proposition 4. Corollary 2 follows from the property that the compression $w = 1/x(\Phi)$, where Φ is to a Montgomery curve, thus doubling and differential addition for w are the same as for the $1/x$ compression on a Montgomery curve, which are of the form (1.5) from Lemma 1. In Theorem 4 we give formulas for a G-compression on the twisted Hessian curve, which corresponds to the compression xy used by

Farashahi and Joye in [17] on the binary generalized Hessian curve $x^3+y^3+a=d$. Note that all formulas in Proposition 4 and Theorems 3 and 4 are over the field K. If $\mathrm{char}\, K \neq 2$, then from the result of Okeya et al. in [35] it follows that every elliptic curve over K is isomorphic to a Montgomery curve over an extension field K' of K with the degree $[K':K]$ which divides 6 (see Subsection 2.2).

In the Appendix A we recall a method based on Gröbner bases for searching a solution of the following problem. Let F be a finitely generated field over K. Assume that we are given $u_1,\ldots,u_m,v \in F$ such that v belongs to the subfield $K(u_1,\ldots,u_m)$. Determine $h \in K(x_1,\ldots,x_m)$ such that $v = h(u_1,\ldots,u_m)$. A method for searching a solution h was used in [13] to obtain formulas for doubling, differential addition, and point recovery for compressions of degree 2 on some models of elliptic curves. For an isogeny of elliptic curves $\Phi : E \to E'$ this method can also be applied to determine the dual isogeny $\widehat{\Phi} : E' \to E$, and the function $\Phi_{g,f} \in K(x)$ induced by Φ and compressions $f \in K(E')$ and $g \in K(E)$ of degree 2. We implemented the method from the Appendix A in the Magma computational algebra system, and used this to determine the dual isogeny $\widehat{\Phi}$ and the induced function $\widehat{\Phi}_{f,g}$ in Theorems 3, 4, and their proofs. In the Appendix B we give programs in Magma which allow to verify correctness of formulas given in Theorems 3, 4 and their proofs.

2 Preliminaries

In this section we give mainly elementary properties of compressions on elliptic curves (see, e.g., [7,13]). For the theory of elliptic curves see the books by Silverman [37] and Washington [41]. An elliptic curve over K is a smooth projective curve over K of genus one with a specified K-rational point O. Let E/K be an elliptic curve. There exists an isomorphism $\eta : E \to W$ over K to an elliptic curve in the Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ such that $\eta(O) = (0:1:0)$, where all $a_i \in K$. If $\mathrm{char}\, K \neq 2,3$, then W can be given in the short Weierstrass form $y^2 = x^3 + a_4x + a_6$ over K. An elliptic curve over K is an algebraic group over K with the identity O. The group law on a Weierstrass model is given by the chord-and-tangent rule. By an isomorphism of elliptic curves we will mean an isomorphism of algebraic curves which preserves identities. A non-constant rational map $\Phi : E \to E'$ of elliptic curves which preserves identities is called the isogeny. Every isogeny of elliptic curves is a group homomorphism. For a finite subgroup $G \subset E$ over K there exists a G-isogeny $\Phi : E \to E'$. For an elliptic curve in a Weierstrass form W/K and a finite subgroup $G \subset W$ over K one can obtain from Vélu's formulas [40] (see also [41, Thm. 12.16]) a G-isogeny $W \to W'$ and a Weierstrass equation of W'. For an isogeny $\Phi : E \to E'$ of elliptic curves there exists the dual isogeny $\widehat{\Phi} : E' \to E$ such that $\widehat{\Phi} \circ \Phi = [\deg \Phi]$. If Φ, E and E' are over K, then $\widehat{\Phi}$ is also over K (i.e., for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have $\widehat{\Phi}^\sigma \circ \Phi = \widehat{\Phi}^\sigma \circ \Phi^\sigma = (\widehat{\Phi} \circ \Phi)^\sigma = [\deg \Phi]^\sigma = [\deg \Phi] = \widehat{\Phi} \circ \Phi$, hence $\widehat{\Phi}^\sigma = \widehat{\Phi}$).

Recall the following application of isogenies given by Brier and Joye in [5] in elliptic curve cryptography. Let $\Phi : E \to E'$ be an isogeny of degree d of elliptic

curves over a finite field. Let $P \in E$ be of the order $\mathrm{ord}(P)$ with $\gcd(\mathrm{ord}(P), d) = 1$, and $u \in \mathbb{Z}$ be the inverse of d modulo $\mathrm{ord}(P)$. To obtain nP for $n \in \mathbb{Z}$ one can compute $un\Phi(P)$ on E', and take $\widehat{\Phi}(un\Phi(P)) = un\widehat{\Phi}(\Phi(P)) = undP = nP$. This may improve efficiency of point multiplication on E if operations on E' are more efficient than on E. In Remarks 2 and 4 we note that this method can be used after compressions.

2.1 Compressions on elliptic curves

Let E/K be an elliptic curve, and $f \in K(E)$ be a compression of degree 2. If $\Phi : E \to W$ is an isomorphism over K, where W/K is in a Weierstrass form, then the first coordinate $x(\Phi)$ of Φ is a compression of degree 2 on E. The subfield of all functions in $K(E)$ invariant under $[-1]$ is equal to $K(f)$. A function $g \in K(E)$ is a compression of degree 2 if and only if $g = (a_1 f + a_2)/(a_3 f + a_4)$, where all $a_i \in K$ and $a_1 a_4 - a_2 a_3 \neq 0$. This follows from the one-to-one correspondence between automorphism of $\mathbb{P}^1$ over K and functions $(a_1 x + a_2)/(a_3 x + a_4)$, where all $a_i \in K$ and $a_1 a_4 - a_2 a_3 \neq 0$. Let E_i/K be an elliptic curve, and $f_i \in K(E_i)$ be a compression of degree 2 for $i = 1, 2, 3$. Let $\Phi : E_1 \to E_2$ be an isogeny over K. There exists the unique function, denoted by $\Phi_{f_1,f_2} \in K(x)$, such that $\Phi_{f_1,f_2} \circ f_1 = f_2 \circ \Phi$, because $f_2 \circ \Phi$ is invariant under $[-1]$ thus $f_2 \circ \Phi \in K(f_1)$. If $\Psi : E_2 \to E_3$ is an isogeny, then $(\Psi \circ \Phi)_{f_1,f_3} = \Psi_{f_2,f_3} \circ \Phi_{f_1,f_2}$. The following property is implicit in [15, Lem. 3.9 and Rem. 3.10] (see Remark 1 below).

Proposition 1 *Let E/K be an elliptic curve, $G \subset E$ be a finite subgroup over K, and $\Phi : E \to E'$ be a G-isogeny. Let $f \in K(E')$ be a compression of degree 2, and $w = f \circ \Phi$. Then*
(1) w is a G-compression on E.
(2) For $D \in K(x)$ (resp. $A \in K(x, y, z)$) we have D is an f-doubling (resp. A is an f-differential addition) if and only if D is a w-doubling (resp. A is a w-differential addition)

Proof. (1) The function w is invariant under $[-1]$ and translations by all $Q \in G$, because $w(-P) = f(\Phi(-P)) = f(-\Phi(P)) = f(\Phi(P)) = w(P)$, and $w(P + Q) = f(\Phi(P + Q)) = f(\Phi(P) + \Phi(Q)) = f(\Phi(P)) = w(P)$ for $P \in E$ and $Q \in G$. We have $[K(E) : K(w)] = [K(E) : \Phi^*(K(E'))][K(E') : K(f)] = 2|G|$. Hence w is a G-compression.
(2) We have
$D(w(P)) = w(2P)\ \forall P \in E \iff D(f(\Phi(P))) = f(2(\Phi(P)))\ \forall P \in E \iff D(f(P')) = f(2P')\ \forall P' \in E'$.
$w(P + Q) = A(w(P), w(Q), w(P - Q))\ \forall P, Q \in E \iff f(\Phi(P) + \Phi(Q)) = A(f(\Phi(P)), f(\Phi(Q)), f(\Phi(P) - \Phi(Q)))\ \forall P, Q \in E \iff f(P' + Q') = A(f(P'), f(Q'), f(P' - Q'))\ \forall P', Q' \in E'$.

In particular, if $\Phi : E \to E'$ is a G-isogeny, and E' is in a Weierstrass or Montgomery form, then $x(\Phi)$ and $1/x(\Phi)$ are G-compressions.

Remark 1 Let E be an elliptic curve over $\mathbb{F}_{2^n}$. According to [15, Sec. 3] a function $w \in \mathbb{F}_{2^n}(E)$ has doubling and differential addition in the form of Lopez and Dahab formulas if there exists $e \in \mathbb{F}_{2^n}$ such that

$$\begin{aligned} w(2P) &= w(P)^2 + e/w(P)^2, \\ w(P+Q) + w(P-Q) &= w(P)w(Q)/(w(P)+w(Q))^2 \end{aligned} \tag{2.1}$$

for generic $P, Q \in E$. Lopez and Dahab in [31] for the compression $w = x$ on the Weierstrass curve $W : y^2 + xy = x^3 + ax^2 + b$ over $\mathbb{F}_{2^n}$ gave formulas of the form (2.1), and for point recovery. Farashahi and Hosseini in [15] used isogenies $\Phi : E \to W$ over $\mathbb{F}_{2^n}$ to such a Weierstrass curve to obtain the compression $w = x(\Phi)$ on E with Lopez and Dahab formulas (2.1) for suitable models of elliptic curves E.

If we change compression of degree 2, then formulas for the new compression can be obtained as follows.

Proposition 2 *Let E/K be an elliptic curve, and $f \in K(E)$ be a compression of degree 2. Let $h(x) = (a_1x+a_2)/(a_3x+a_4)$ with $h^{-1}(x) = (-a_4x+a_2)/(a_3x-a_1)$, and $g = h(f)$, where all $a_i \in K$ and $a_1a_4 - a_2a_3 \neq 0$. Then we have the following doubling, differential addition, and point recovery formulas for g:*
(1) $D_g(x) = h(D_f(h^{-1}(x)))$.
(2) $A_g(x,y,z) = h(A_f(h^{-1}(x), h^{-1}(y), h^{-1}(z)))$.
(3) $Q = R_f(P, h^{-1}(g(Q)), h^{-1}(g(P+Q)))$ for all $P, Q \in E$.
(4) Let E_1/K be an elliptic curve, and $\Phi : E \to E_1$ be an isogeny over K. Let $f_1(x) \in K(E_1)$ be a compression of degree 2, $h_1(x) = (b_1x+b_2)/(b_3x+b_4)$ with $h_1^{-1}(x)$ as above, and $g_1 = h_1(f_1)$, where all $b_i \in K$ and $b_1b_4 - b_2b_3 \neq 0$. Then $\Phi_{g,g_1}(x) = h_1(\Phi_{f,f_1}(h^{-1}(x)))$.

Proof. (1) $g(2P) = h(f(2P)) = h(D_f(f(P))) = h(D_f(h^{-1}(g(P))))$.
(2) $g(P+Q) = h(f(P+Q)) = h(A(f(P), f(Q), f(P-Q))) =$
$h(A(h^{-1}(g(P)), h^{-1}(g(Q)), h^{-1}(g(P-Q))))$.
(3) $Q = R_f(P, f(Q), f(P+Q)) = R_f(P, h^{-1}(g(Q)), h^{-1}(g(P+Q)))$.
(4) $g_1(\Phi(P)) = h_1(f_1(\Phi(P))) = h_1(\Phi_{f,f_1}(f(P))) = h_1(\Phi_{f,f_1}(h^{-1}(g(P))))$.

2.2 Montgomery curves

Let $\operatorname{char} K \neq 2$. An elliptic curve in the Montgomery form over K is given by the equation $M_{A,B} : By^2 = x^3 + Ax^2 + x$, where $B(A^2-4) \neq 0$ and $A, B \in K$. Formulas for x-doubling and x-differential addition of the form in eq. (1.1) on $M_{A,B}$ were given by Montgomery in [34]. For the compression $1/x$ on $M_{A,B}$ we have the following formulas.

Lemma 1 *On the Montgomery curve $M_{A,B}$ with the compression $w = 1/x$ formulas for w-doubling and w-differential addition are given in eq.* (1.5).

Proof. From the Montgomery formulas in eq. (1.1) we have:

$$(x_{P+Q}x_{P-Q})^{-1} = \left(\frac{x_P - x_Q}{x_P x_P - 1}\right)^2 = \left(\frac{x_P^{-1} - x_Q^{-1}}{x_P^{-1}x_Q^{-1} - 1}\right)^2.$$

$$(x_{[2]P})^{-1} = \frac{4x_P(x_P^2 + Ax_P + 1)}{(x_P^2 - 1)^2} = \frac{4x_P^{-1}((x_P^{-1})^2 + Ax_P^{-1} + 1)}{((x_P^{-1})^2 - 1)^2}.$$

Let $W : y^2 = u(x)$ be an elliptic curve in a Weierstrass form, where $u = x^3 + a_2x^2 + a_4x + a_6 \in K[x]$. From the result of Okeya et al. in [35] W is isomorphic over K to a Montgomery curve M/K if and only if u has a root $x_0 \in K$ such that the derivative $u'(x_0)$ is a square in K. Let $u(x_0) = 0$ and $u'(x_0) = e^2$, where $x_0, e \in K$. For $v(x) = u(x + x_0)$ we have $v(0) = 0$ and $v'(0) = e^2$. Hence $v(x) = x^3 + ax^2 + e^2x$ for $a \in K$. Substituting (ex, ey) to the equation $y^2 = v(x)$ and dividing the equation by e^3 we obtain the curve in the Montgomery form $M_{a/e,1/e} : y^2/e = x^3 + (a/e)x^2 + x$. Hence we have the isomorphism

$$\Phi = ((x - x_0)/e, y/e) : W \to M_{a/e,1/e}. \tag{2.2}$$

Remark 2 The method of Brier and Joye from [5] recalled in the beginning of this section can be used after compression as follows. Let $\Phi : E_1 \to E_2$ be an isogeny of degree d of elliptic curves. Let $f_i \in K(E_i)$ be a compression of degree 2 on E_i for $i = 1, 2$, and let $[k]_{f_i}$ be the multiplication by $k \in \mathbb{Z}$ on $\mathbb{P}^1$ induced by f_i. Let $P \in E$ be of finite order relatively prime with d, and $u \in \mathbb{Z}$ be the inverse of d modulo $\mathrm{ord}(P)$. For $a = f(P)$ and $n \in \mathbb{Z}$ to obtain $[n]_{f_1}a$ one can use the multiplication on $\mathbb{P}^1$ induced by f_2, and the induced functions Φ_{f_1,f_2} and $\widehat{\Phi}_{f_2,f_1}$ on $\mathbb{P}^1$ as follows. Compute $[un]_{f_2}\Phi_{f_1,f_2}(a)$, and take

$$\widehat{\Phi}_{f_2,f_1}([un]_{f_2}\Phi_{f_1,f_2}(a)) = [un]_{f_1}\widehat{\Phi}_{f_2,f_1}(\Phi_{f_1,f_2}(a)) = [und]_{f_1}a = [n]_{f_1}a.$$

This may improve efficiency if doubling and differential addition for f_2 are more efficient than for f_1. For example, under some assumptions on E_1 we can have an isogeny over K to a Montgomery curve E_2/K, see, e.g., Theorem 3.

3 Alternative models of elliptic curves

In this section we recall basic properties of models of elliptic curves, which will be used in this paper. We also give compressions on these models, which were used in the literature.

3.1 Extended Jacobi quartic curves

Let $\mathrm{char}\, K \neq 2$. The extended Jacobi quartic is given by the equation

$$Jq_{d,a} : y^2 = dx^4 + 2ax^2 + 1,$$

where $a, d \in K$ and $d(a^2 - d) \neq 0$. This model was studied in [4,8,20]. For $d = 1$ this curve is called the Jacobi quartic. The sum (x_3, y_3) of (x_1, y_1) and (x_2, y_2) on $Jq_{d,a}$ is given by

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 - dx_1^2x_2^2}, y_3 = \frac{(y_1y_2 + 2ax_1x_2)(dx_1^2x_2^2 + 1) + 2dx_1x_2(x_1^2 + x_2^2)}{(1 - dx_1^2x_2^2)^2}.$$

The identity is $(0, 1)$, and $-(x, y) = (-x, y)$. The point $(0, -1)$ is of order 2. We have the isomorphism

$$\Phi = \left(\frac{2(y + 1)}{x^2}, \frac{4(ax^2 + y + 1)}{x^3}\right) : Jq_{d,a} \to W$$

to the Weierstrass curve $W : y^2 = x^3 + 2ax^2 - 4dx - 8ad$, which satisfies $\Phi(0, 1) = (0 : 1 : 0)$ and $\Phi(0, -1) = (-2a, 0)$ (see [41, Thm. 2.17]).

The function $f = (y+1)/x^2$ is a compression of degree 2 on $Jq_{d,a}$. Obviously f is invariant under $[-1]$, and the field extension $K(f) \subset K(Jq_{d,a}) = K(f, x)$ is of degree 2, because we have $(x^2f - 1)^2 = dx^4 + 2ax^2 + 1$ from the equation of $Jq_{d,a}$, hence x satisfies the quadratic equation $(f^2 - d)x^2 - 2(f + a) = 0$ over $K(f)$. Doubling and differential addition for f on the Jacobi quartic were given by Castryck and Vercauteren in [7].

The function $w = x^2$ is a $\langle(0, -1)\rangle$-compression. It is invariant under $[-1]$ and the translation by $(0, -1)$, i.e., we have $w((x, y)+(0, -1)) = w(-x, -y) = w(x, y)$ for $(x, y) \in Jq_{d,a}$. The field extension $K(x^2) \subset K(Jq_{d,a})$ is of degree 4, because the extensions $K(x^2) \subset K(x)$ and $K(x) \subset K(Jq_{d,a})$ are of degree 2. For the compression kx^2 on $Jq_{k^2,a}$ doubling and differential additions of the form in eq. (1.5) were given by Hu et al. in [21] and earlier for $k = 1$ by Gu et al. in [19].

3.2 Twisted Edwards curves

Let $\operatorname{char} K \neq 2$. The twisted Edwards curve over K of the form

$$Ed_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in K$ and $ad(a - d) \neq 0$, is a generalization given by Bernstein et al. in [2] of the Edwards curve introduced by Edwards in [14], which we have for $a = 1$. The sum (x_3, y_3) of points (x_1, y_1) and (x_2, y_2) on $Ed_{a,d}$ is given by

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \; y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}.$$

The identity is $(0, 1)$, and $-(x, y) = (-x, y)$. The point $(0, -1)$ is of order 2. We have the birational map

$$\Phi = \left(\frac{1 + y}{1 - y}, \frac{1 + y}{x(1 - y)}\right) : Ed_{a,d} \to M_{A,B}$$

to the Montgomery curve, where $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$, which satisfies $\varphi(0, 1) = (0 : 1 : 0)$ and $\varphi(0, -1) = (0, 0)$ (see [2]).

The y-coordinate is a compression of degree 2 on $Ed_{a,d}$. For compression $w = d(xy)^2$ on $Ed_{a,d}$ the doubling and the differential addition of the form in eq. (1.5) were given by Farashahi and Hosseini in [16]. The points $(\pm 1/\sqrt{a}, 0)$ are of order 4 on $Ed_{a,d}$, and $[2](\pm 1/\sqrt{a}, 0) = (0, -1)$. The function w is a $\langle(1/\sqrt{a}, 0)\rangle$-compression. As shown in [16] w is invariant under translation by $(1/\sqrt{a}, 0)$, i.e., we have $w((x, y) + (1/\sqrt{a}, 0)) = w(y/\sqrt{a}, -\sqrt{a}x) = w(x, y)$ for $(x, y) \in Ed_{a,d}$. Obviously, w is invariant under $[-1]$. We have $[K(Ed_{a,d}) : K(w)] = 8$, which follows for example from Theorem 3(b), where we give a $\langle(1/\sqrt{a}, 0)\rangle$-isogeny $\Phi : Ed_{a,d} \to M_{A,B}$ with $x(\Phi) = 1/w$.

3.3 Huff's curves

Let $\operatorname{char} K \neq 2$. Huff's curve can be given by the equation

$$Hu_v : vx(y^2 - 1) = y(x^2 - 1),$$

where $v \in K$ and $v \neq \pm 1$. This model introduced in the form $ax(y^2 - 1) = by(x^2 - 1)$ by Huff in [24] was studied by Joye et al. in [26]. Generalized Huff's curve of the form

$$Hu_{a,b} : x(ay^2 - 1) = y(bx^2 - 1)$$

was introduced by Wu and Feng in [42], where $a, b \in K$ and $ab(a - b) \neq 0$. The sum (x_3, y_3) of (x_1, y_1) and (x_2, y_2) on $Hu_{a,b}$ is given by

$$x_3 = \frac{(x_1 + x_2)(1 + ay_1y_2)}{(1 + bx_1x_2)(1 - ay_1y_2)},\ y_3 = \frac{(y_1 + y_2)(1 + bx_1x_2)}{(1 - bx_1x_2)(1 + ay_1y_2)}.$$

The identity is $(0, 0)$, and the negative $-(x, y) = (-x, -y)$ on $Hu_{a,b}$. The points $(1 : 0 : 0), (0 : 1 : 0)$, and $(a : b : 0)$ at infinity on $Hu_{a,b}$ are of order 2. We have the isomorphism

$$\Phi = \left(\frac{bx - ay}{y - x}, \frac{b - a}{y - x}\right) : Hu_{a,b} \to W$$

to the Weierstrass curve $W : y^2 = x^3 + (a + b)x^2 + abx$ (see [42]). If a and b are squares in K, then we have the isomorphism over K from Huff's curve over K to generalized Huff's curve $Hu_{a,b}$ given by

$$Hu_{\sqrt{a/b}} \ni (x, y) \to (x/\sqrt{b}, y/\sqrt{a}) \in Hu_{a,b}.$$

Hence Huff's curve H_v/K is isomorphic over K with generalized Huff's curve $H_{v^2,1}$.

The function xy is a compression of degree 2 on $Hu_{a,b}$ and Hu_v. The doubling and the differential addition of the form in eq. (1.5) for the compression $w = xy$ on Huff's curve were given in [12], and in slightly other form in [23].

3.4 Twisted Hessian curves

The twisted Hessian curve over K is given by the equation

$$H_{a,d} : aX^3 + Y^3 + Z^3 = dXYZ$$

in $\mathbb{P}^2$, where $a, d \in K$ and $a(27a - d^3) \neq 0$. For $a = 1$ this curve is called the Hessian curve. (Twisted) Hessian curves were studied in [3,8,17,25,38], but the model in the above form $H_{a,d}$ was introduced by Bernstein et al. in [3]. We recall some results given in [3]. From Sylvester's addition law on a Hessian curve one can obtain the so-called standard addition law on a twisted Hessian curve (see [3, Sec. 3]). The so-called rotated addition law on $H_{a,d}$ (see [3, Sec. 4]) is given by

$$X_3 = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2, Y_3 = Y_2^2 Y_1 Z_1 - a X_1^2 X_2 Z_2, Z_3 = a X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2,$$

where $(X_3 : Y_3 : Z_3)$ is the sum of points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on $H_{a,d}$ if $(X_3, Y_3, Z_3) \neq (0, 0, 0)$. The identity is $(0 : -1 : 1)$, and $-(X : Y : Z) = (X : Z : Y)$. The standard addition law and the rotated addition law form a complete set of addition laws on $H_{a,d}$ (see [3, Thm. 4.7]). If a is not a cube in K, then the rotated addition law is complete in $H_{a,b}(K)$ (see [3, Thm. 4.5]). Let $\omega \in \overline{K}$ be a third root of unity $\neq 1$. Then $(0 : -\omega : 1) \in H_{a,d}$, and $(0 : -\omega : 1) + (X : Y : Z) = (\omega^2 X : \omega Y : Z)$ for all $(X : Y : Z) \in H_{a,d}$ (see [3, Thm. 4.6]). Hence

$$G = \{(0 : -\omega^i : 1) : i = 0, 1, 2\} \subset H_{a,d} \tag{3.1}$$

is a subgroup of order 3 over K. An elliptic curve given by the equation $W : y^2 + a_1 xy + a_3 y = x^3$ is called a triangular curve. The point $(0, 0)$ on W is of order 3. From [3, Thm. 5.3] we have the isomorphism $\Phi : W \to H_{a,d}$ from the triangular curve, where

$$a = a_1^3 - 27a_3 \text{ and } d = 3a_1, \tag{3.2}$$

given by

$$\Phi = (x : \omega(y + a_1 x + a_3) - \omega^2 y - a_3 : \omega^2(y + a_1 x + a_3) - \omega y - a_3),$$

which satisfies $\Phi(0, 0) = (0 : -\omega : 1)$. $\Phi^{-1} : H_{a,d} \to W$ is given by

$$\Phi^{-1}(X : Y : Z) = \left(\frac{-3a_3 X}{a_1 X + Y + Z}, \frac{a_3(a_1 X + \omega Y + \omega^2 Z)}{a_1 X + Y + Z} \right) \tag{3.3}$$

(see the proof of [3, Thm. 5.3]).

Let $x = X/Z$, $y = Y/Z$, $t = Y/X$, and $z = Z/X$ be functions on $H_{a,d}$. We have $t = y/x$ and $z = 1/x$. In coordinates (x, y), resp. (t, z), the twisted Hessian curve has the affine equation $ax^3 + y^3 + 1 = dxy$, resp. $t^3 + z^3 + a = dtz$. The negative point on these affine models is given by $-(x, y) = (x/y, 1/y)$, resp. $-(t, z) = (z, t)$. The function $f = t + z = (y + 1)/x$ is a compression of degree 2

on $H_{a,d}$. The function $w = tz$ is a G-compression for G in (3.1). It is invariant under $[-1]$ and the translation by $(0 : -\omega : 1)$, i.e., $w((X : Y : Z) + (0 : -\omega : 1)) = w(\omega^2 X : \omega Y : Z) = \frac{\omega Y}{\omega^2 X}\frac{Z}{\omega^2 X} = \frac{Y}{X}\frac{Z}{X} = w(X : Y : Z)$. We have $[K(H_{a,d}) : K(w)] = 6$, because $K(H_{a,d}) = K(w,t)$, and $t^3 + (w/t)^3 + a = dtw/t$, hence t satisfies the equation $t^6 + (a - dw)t^3 + w^3 = 0$ over $K(w)$. For compressions $t + z$ and tz on a binary twisted Hessian curve a doubling and a differential addition were given by Farashahi and Joye in [17, Subsec. 5.4].

3.5 Twisted Jacobi intersection curves

Let $\operatorname{char} K \neq 2$. The twisted Jacobi intersection is given by the equations

$$Ji_{a,b} : \begin{cases} ax^2 + y^2 = 1 \\ bx^2 + z^2 = 1 \end{cases}$$

in $\overline{K}^3$, where $a, b \in K$ and $ab(a-b) \neq 0$. This model was studied in [8,18,30]. For $a = 1$ this curve is called the Jacobi intersection. We recall some results given by Feng et al. in [18]. The sum (x_3, y_3, z_3) of (x_1, y_1, z_1) and (x_2, y_2, z_2) on $Ji_{a,b}$ is given by

$$x_3 = \frac{x_1y_2z_2 + x_2y_1z_1}{y_2^2 + ax_2^2z_1^2}, y_3 = \frac{y_1y_2 - ax_1z_1x_2z_2}{y_2^2 + ax_2^2z_1^2}, z_3 = \frac{z_1z_2 - bx_1y_1x_2y_2}{y_2^2 + ax_2^2z_1^2}.$$

The identity is $(0, 1, 1)$, and $-(x, y, z) = (-x, y, z)$. The doubling is given by

$$[2] = \left(\frac{2xyz}{y^2 + a(xz)^2}, \frac{y^2 - a(xz)^2}{y^2 + a(xz)^2}, \frac{z^2 - b(xy)^2}{y^2 + a(xz)^2}\right).$$

We have the isomorphism $\sigma : Ji_{a,b} \to W$ given by

$$\sigma = \left(\frac{a(z+1)}{1-y}, \frac{ax}{1-y}\left(\frac{a(z+1)}{y-1} + b\right)\right),$$

where $W : y^2 = x(x-a)(x-b)$. The points $(0, 1, -1), (0, -1, 1), (0, -1, -1)$ are of order 2. For the compression $w = acx^2$ on Ji_{a,ac^2}, where $a, c \in K$, formulas of the form in eq. (1.5) were given by Hu et al. in [22, Thm 3]. The compression $w = acx^2$ is a $Ji_{a,ac^2}[2]$-compression. It is invariant under $[-1]$ and translations by points of order 2. From Theorem 3(c) it follows that $[K(Ji_{a,ac^2}) : K(w)] = 8$.

4 Decomposition of a G-compression and applications

In this section we assume that E/K is an elliptic curve, and $G \subset E$ is a finite subgroup over K. We have the following decomposition of a G-compression.

Theorem 1 *Let $\Phi : E \to E'$ be a G-isogeny. Then $w \in K(E)$ is a G-compression if and only if there exists a compression $f \in K(E')$ of degree 2 such that $w = f \circ \Phi$.*

Proof. If $f \in K(E')$ is a compression of degree 2, then $w = f \circ \Phi$ is a G-compression from Proposition 1. Let $w \in K(E)$ be a G-compression. $\Phi^*(K(E'))$ is equal to the subfield of functions in $K(E)$ invariant under translation by all $Q \in G$, and $[K(E) : \Phi^*(K(E'))] = |G|$ (see [37, Sec. 3.4]). Let $L \subset K(E)$ be the subfield of functions invariant under $[-1]$ and translations by all $Q \in G$. Obviously $w \in L \subset \Phi^*(K(E'))$. Let $L' \subset K(E')$ be the subfield of functions invariant under $[-1]$. Φ is a homomorphism hence for all $u \in K(E')$ we have $u \circ \Phi$ is invariant under $[-1]_E$ iff u is invariant under $[-1]_{E'}$. Thus $L = \Phi^*(L')$. We have $[K(E) : \Phi^*(L')] = [K(E) : \Phi^*(K(E'))][K(E') : L'] = 2|G| = [K(E) : K(w)]$, and $K(w) \subset \Phi^*(L')$. Hence $K(w) = \Phi^*(L')$. Let $w = f \circ \Phi$ for $f \in L'$. Then $K(f) = L'$. Thus f is a compression of degree 2 on E'.

Corollary 1 *Let $w \in K(E)$ be a G-compression. Then*
(1) the multiplication of values of w by integers induced from E is correct.
(2) there exist a w-doubling and a w-differential addition.

Proof. From Theorem 1 we have $w = f \circ \Phi$, where $\Phi : E \to E'$ is a G-isogeny and $f \in K(E')$ is a compression of degree 2. For $P \in E$ we have $w^{-1}(w(P)) = \Phi^{-1}(f^{-1}(f(\Phi(P)))) = \Phi^{-1}(\pm\Phi(P)) = \pm P + G$. If $w(P) = w(P')$ for $P, P' \in E$, then $P' = \pm P + Q$ for $Q \in G$. Hence $w(nP) = w(\pm nP + nQ) = w(nP')$ for $n \in \mathbb{Z}$, which gives (1). (2) follows from Proposition 1.

Remark 3 From Theorem 1 for a G-compression $w \in K(E)$ we also have the following decomposition in eq. (4.1), where we do not use an isogeny, but a function in $K(x)$ induced by an isogeny and compressions of degree 2. Let $w = f \circ \Phi$, where $\Phi : E \to E'$ is a G-isogeny and $f \in K(E')$ is a compression of degree 2. Let $g \in K(E)$ be a compression of degree 2, and $\Phi_{g,f} \in K(x)$ be the function induced by Φ, g and f. Then

$$w = \Phi_{g,f} \circ g = f \circ \Phi. \tag{4.1}$$

We have the following point recovery for a G-compression w, which is based on point recovery for compression of degree 2 and the dual isogeny. Note that in Theorem 2 for point recovery we can use the induced function $\widehat{\Phi}_{f,g} \in K(x)$ instead of isogenies Φ and $\widehat{\Phi}$, which can simplify the method and save space.

Theorem 2 *Let $w \in K(E)$ be a G-compression, $\Phi : E \to E'$ be a G-isogeny, and $f \in K(E')$ be a compression of degree 2 such that $w = f \circ \Phi$. Let $g \in K(E)$ be a compression of degree 2. Let R_f and R_g be point recovery formulas for f and g (see eq. (1.2)). For the dual isogeny $\widehat{\Phi} : E' \to E$ let $\widehat{\Phi}_{f,g} \in K(x)$ be the induced function by $\widehat{\Phi}, f$ and g.*
(1) Then

$$\begin{aligned} |G|Q &= \widehat{\Phi}(R_f(\Phi(P), w(Q), w(P+Q))) \\ &= R_g(|G|P, \widehat{\Phi}_{f,g}(w(Q)), \widehat{\Phi}_{f,g}(w(P+Q))) \end{aligned} \tag{4.2}$$

for generic $P, Q \in E$.
(2) Let $P \in E$ be of finite order with $\gcd(\mathrm{ord}(P), |G|) = 1$, *and $u \in \mathbb{Z}$ be the*

inverse of $|G|$ *modulo* $\mathrm{ord}(P)$. *If we are given* $P, w(unP)$, *and* $w((un+1)P)$ *for* $n \in \mathbb{Z}$, *then*

$$\begin{aligned} nP &= \widehat{\Phi}(R_f(\Phi(P), w(unP), w((un+1)P)) \\ &= R_g(|G|P, \widehat{\Phi}_{f,g}(w(unP)), \widehat{\Phi}_{f,g}(w((un+1)P))). \end{aligned} \tag{4.3}$$

Proof. We obtain eq. (4.2) as follows

$$\widehat{\Phi}(R_f(\Phi(P), w(Q), w(P+Q)))$$
$$= \widehat{\Phi}(R_f(\Phi(P), f(\Phi(Q)), f(\Phi(P)+\Phi(Q)))) = \widehat{\Phi}(\Phi(Q)) = |G|Q.$$
$$R_g(|G|P, \widehat{\Phi}_{f,g}(w(Q)), \widehat{\Phi}_{f,g}(w(P+Q)))$$
$$= R_g(|G|P, \widehat{\Phi}_{f,g}(f(\Phi(Q))), \widehat{\Phi}_{f,g}(f(\Phi(P+Q)))$$
$$= R_g(|G|P, \widehat{\Phi}_{f,g}(\Phi_{g,f}(g(Q))), \widehat{\Phi}_{f,g}(\Phi_{g,f}(g(P+Q))))$$
$$= R_g(|G|P, [|G|]_g(g(Q)), [|G|]_g(g(P+Q))))$$
$$= R_g(|G|P, g(|G|Q)), g(|G|P + |G|Q)) = |G|Q,$$

where $[|G|]_g$ is the multiplication by $|G|$ on $\mathbb{P}^1$ induced by g. We have $\widehat{\Phi}_{f,g} \circ \Phi_{g,f} = (\widehat{\Phi} \circ \Phi)_g = [|G|]_g$. To obtain (4.3) we apply (4.2) for $Q = unP$:

$$R_g(|G|P, \widehat{\Phi}_{f,g}(w(unP)), \widehat{\Phi}_{f,g}(w((un+1)P)))$$
$$= \widehat{\Phi}(R_f(\Phi(P), w(unP), w((un+1)P)) = |G|unP = nP.$$

We have the following function induced by a suitable isogeny Ψ and G_i-compressions.

Proposition 3 *Let* E_i/K *be an elliptic curve,* $G_i \subset E$ *be a finite subgroup over* K, *and* $w_i \in K(E_i)$ *be a* G_i*-compression for* $i = 1, 2$. *Let* $\Psi : E_1 \to E_2$ *be an isogeny over* K *such that* $\Psi(G_1) \subset G_2$. *Then there exists the unique function* $\Psi_{w_1,w_2} \in K(x)$ *such that* $\Psi_{w_1,w_2} \circ w_1 = w_2 \circ \Psi$.

Proof. Let $\Phi_i : E_i \to E_i'$ be a G_i-isogeny and $w_i = f_i \circ \Phi_i$ for the compression $f_i \in K(E_i')$ of degree 2 for $i = 1, 2$. We have $\ker \Phi_1 = G_1 \subset \Psi^{-1}(G_2) = \ker(\Phi_2 \circ \Psi)$. There exists the unique isogeny $\widetilde{\Psi} : E_1' \to E_2'$ over K such that $\widetilde{\Psi} \circ \Phi_1 = \Phi_2 \circ \Psi$ (see [37, Cor. 4.11]). Let Ψ_{w_1,w_2} be the function $\widetilde{\Psi}_{f_1,f_2} \in K(x)$ induced by $\widetilde{\Psi}$, f_1 and f_2. The upper and lower rectangles in the following diagram are commutative

$$\begin{array}{ccc} E_1 & \xrightarrow{\Psi} & E_2 \\ \downarrow{\scriptstyle \Phi_1} & & \downarrow{\scriptstyle \Phi_2} \\ E_1' & \xrightarrow{\widetilde{\Psi}} & E_2' \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ \overline{K} & \xrightarrow{\Psi_{w_1,w_2}} & \overline{K}. \end{array}$$

Thus Ψ_{w_1,w_2} has the above properties.

Remark 4 Note that similarly as in Remark 2 we can use the induced function Ψ_{w_1,w_2} in the following situation. Assume that we have the situation from Proposition 3, and additionally $\gcd(d,|G_1|)=1$ for $d=\deg\Psi$, and $|G_1|=|G_2|$. Then $\Psi(G_1)=G_2$, because of the inclusion $\subset$ and the above assumptions. We also have $\widehat{\Psi}(G_2)=G_1$, because $\widehat{\Psi}(G_2)=\widehat{\Psi}(\Psi(G_1))=dG_1=G_1$. Thus we have the induced function $\widehat{\Psi}_{w_2,w_1}$ from Proposition 3. Let $[k]_{w_i}$ be the multiplication by $k\in\mathbb{Z}$ on $\mathbb{P}^1$ induced by w_i for $i=1,2$. Let $P\in E_1$ be of finite order relatively prime with d, and $u\in\mathbb{Z}$ be the inverse of d modulo $\operatorname{ord}(P)$. For $a=w_1(P)$ and $n\in\mathbb{Z}$ one can obtain $[n]_{w_1}a$ using the multiplication induced by w_2 as follows. Compute $[un]_{w_2}\Psi_{w_1,w_2}(a)$, and take

$$\widehat{\Psi}_{w_2,w_1}([un]_{w_2}\Psi_{w_1,w_2}(a))=[un]_{w_1}\widehat{\Psi}_{w_2,w_1}(\Psi_{w_1,w_2}(a))=[und]_{w_1}a=[n]_{w_1}a.$$

5 Decomposition of G-compressions and determining functions used for point recovery for some models of elliptic curves

First we give isomorphisms from the following models to a Montgomery curve.

Proposition 4 *Let* $\operatorname{char}K\neq 2$. *We have the following isomorphisms to a Montgomery curve.*

(a) For the generalized Huff curve $Hu_{a,ac^2}: x(ay^2-1)=y(ac^2x^2-1)$, *where* $a,c\in K$, *we have the isomorphism*

$$\Phi=\left(\frac{1}{acxy},\frac{c-1/c}{y-x}\right):Hu_{a,ac^2}\to M_{A,B},$$

where $A=c+1/c$ *and* $B=1/(ac)$.

(b) For the Huff curve $Hu_v: vx(y^2-1)=y(x^2-1)$ *we have the isomorphism*

$$\Phi=\left(\frac{1}{xy},\frac{v^2-1}{vx-y}\right):Hu_v\to M_{A,B},$$

where $A=v+1/v$ *and* $B=1/v$.

(c) For the twisted Jacobi intersection $Ji_{a,ac^2}: \begin{cases} ax^2+y^2=1\\ ac^2x^2+z^2=1,\end{cases}$ *where* $a,c\in K$, *we have the isomorphism*

$$\Phi=\left(\frac{z+1}{c(1-y)},\frac{ax}{1-y}\left(\frac{z+1}{c(y-1)}+c\right)\right):Ji_{a,ac^2}\to M_{A,B},$$

where $A=-c-1/c$ *and* $B=1/(ac)$.

Proof. We will use the following result of Okeya et al. from [35] (see Subsection 2.2). If for an elliptic curve in the Weierstrass form $W: y^2=u(x)$ there exists a

root $x_0 \in K$ of u such that $u'(x_0) = e^2$ for $e \in K$, then we have the isomorphism $\varphi = ((x-x_0)/e, y/e) : W \to M$ to the Montgomery curve $M : y^2/e = e^{-3}u(ex+x_0)$.
(a) From Subsection 3.3 we have the isomorphism

$$\Phi_1 = \left(\frac{a(c^2x-y)}{y-x}, \frac{a(c^2-1)}{y-x}\right) : Hu_{a,ac^2} \to W,$$

where $W : y^2 = u(x)$ for $u(x) = x^3 + a(c^2+1)x^2 + a^2c^2x$. We have $u(0) = 0$ and $u'(0) = (ac)^2$. Hence $\Phi_2 = (x/(ac), y/(ac)) : W \to M$ is an isomorphism to the Montgomery curve $M : y^2/(ac) = x^3 + (c + 1/c)x^2 + x$. The isomorphism $\Phi = \Phi_2 \circ \Phi_1 : Hu_{a,ac^2} \to M$ is given by

$$\Phi = \left(\frac{cx - y/c}{y-x}, \frac{c - 1/c}{y-x}\right).$$

The equation of Hu_{a,ac^2} can be written $y - x = acxy(cx - y/c)$. Hence

$$\frac{cx - y/c}{y-x} = \frac{cx - y/c}{acxy(cx - y/c)} = \frac{1}{acxy}.$$

(b) We have the isomorphism $\Phi_1 = (x, y/v) : Hu_v \to Hu_{v^2,1}$ from Subsection 3.3. Let $\Phi_2 = \left(\frac{1}{vxy}, \frac{v - 1/v}{x-y}\right) : Hu_{v^2,1} \to M_{v+1/v,1/v}$ be the isomorphism from (a) for $a = v^2$ and $c = 1/v$. We have the isomorphism $\Phi = \Phi_2 \circ \Phi_1 = \left(\frac{1}{xy}, \frac{v^2-1}{vx-y}\right) : Hu_v \to M_{v+1/v,1/v}$.
(c) Let $\Phi_1 = \left(\frac{a(z+1)}{1-y}, \frac{ax}{1-y}\left(\frac{a(z+1)}{y-1} + ac^2\right)\right) : Ji_{a,ac^2} \to W$ be the isomorphism from Subsection 3.5, where $W : y^2 = u(x)$ for $u = x^3 - a(1+c^2)x^2 + a^2c^2x$. We have $u(0) = 0$ and $u'(0) = (ac)^2$. Thus we have the isomorphism to the Montgomery curve $\Phi_2 = (x/(ac), y/(ac)) : W \to M_{-c-1/c,1/(ac)}$. The isomorphism $\Phi = \Phi_2 \circ \Phi_1 : Ji_{a,ac^2} \to M_{-c-1/c,1/(ac)}$ is of the from in (c).

In the following theorem for G-compressions w used on the Jacobi quartic $Jq_{k^2,a}$ by Hu et al. in [21] and by Gu et al. in [19] for $k = 1$, on the twisted Edwards curve $Ed_{a,d}$ by Farashahi and Hosseini in [16], and on the twisted Jacobi intersection $Ji_{a,ac^2} : ax^2 + y^2 = 1, ac^2x^2 + z^2 = 1$ by Hu et al. in [22] we give a G-isogeny Φ to a Montgomery curve with the first coordinate $x(\Phi) = 1/w$. We also give formulas on the dual isogeny $\widehat{\Phi}$ in the proof, and the induced function $\widehat{\Phi}_{1/x,g}$, which can be used for point recovery from Theorem 2, where g is a compression of degree 2.

Theorem 3 *For models of elliptic curves E/K below, where* $\operatorname{char} K \neq 2$*, and G-compression $w \in K(E)$ we have the following G-isogeny $\Phi : E \to M_{A,B}$ to the Montgomery curve with the first coordinate $x(\Phi) = 1/w$, and the function $\widehat{\Phi}_{1/x,g} \in K(x)$ induced by the dual isogeny $\widehat{\Phi}$ and compressions of degree two $1/x$ on $M_{A,B}$ and $g \in K(E)$.*

(a) *For the extended Jacobi quartic* $Jq_{k^2,a} : y^2 = k^2x^4+2ax^2+1$, *where* $a, k \in K$, *with the* G*-compression* $w = kx^2$ *for* $G = \langle(0,-1)\rangle$ *of order 2 we have the* G*-isogeny*

$$\Phi = \left(\frac{1}{w}, \frac{2y}{kx^3}\right) : Jq_{k^2,a} \to M_{A,B},$$

where $A = 2a/k$ *and* $B = 1/(4k)$, *with* $\widehat{\Phi}_{1/x,g} = \dfrac{k(x^2+1)}{2x}$ *for* $g = (y+1)/x^2$.

(b) *For the twisted Edwards curve* $Ed_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ *with the* G*-compression* $w = d(xy)^2$ *for* $G = \langle(1/\sqrt{a}, 0)\rangle$ *of order 4 we have the* G*-isogeny*

$$\Phi = \left(\frac{1}{w}, \frac{y^2 - ax^2}{d(xy)^3}\right) : Ed_{a,d} \to M_{A,B},$$

where $A = -4a/d + 2$ *and* $B = 1/d$, *with*

$$\widehat{\Phi}_{1/x,y} = \frac{x^4 + (-8a/d+4)x^3 + 6x^2 + (-8a/d+4)x + 1}{x^4 - 4x^3 + (16a/d-10)x^2 - 4x + 1}.$$

(c) *For the twisted Jacobi intersection* Ji_{a,ac^2}, *where* $a, c \in K$, *with the* G*-compression* $w = acx^2$ *for the 2-torsion subgroup* $G = Ji_{a,ac^2}[2]$ *we have the* G*-isogeny*

$$\Phi = \left(\frac{1}{w}, -\frac{yz}{acx^3}\right) : Ji_{a,ac^2} \to M_{A,B},$$

where $A = -c - 1/c$ *and* $B = 1/(ac)$, *with* $\widehat{\Phi}_{1/x,g} = \dfrac{4x(x^2+Ax+1)}{(x^2-1)^2}$ *for the compression* $g = \dfrac{c(1-y)}{z+1}$ *on* Ji_{a,ac^2} *obtained from Proposition 4(c).*

Proof. We prove (a) and (b) as follows. First we use an isomorphism $\Phi_1 : E \to W$ from Section 3 to a Weierstrass curve. Then for the subgroup $H = \Phi_1(G) \subset W$ from Velu's formulas we obtain an H-isogeny $\Phi_2 : W \to W'$. Recall the formula on isogeny of degree 2, which follows from Vélu's formulas ([41, Thm. 12.16]). Let $W : F = 0$ for $F = x^3 + a_2x^2 + a_4x + a_6 - y^2$ be an elliptic curve in a Weierstrass form, and $P = (x_0, 0) \in W$. Let $v = F'_x(P) = 3x_0^2 + 2a_2x_0 + a_4$, $t = x_0v$, $A_2 = a_2$, $A_4 = a_4 - 5v$, and $A_6 = a_6 - 4a_2v - 7t$. Then

$$\Phi = (x + v/(x - x_0), y - vy/(x - x_0)^2) : W \to W_1$$

is a $\langle P\rangle$-isogeny, where $W_1 : y^2 = x^3 + A_2x^2 + A_4x + A_6$. In (b) we will obtain an isogeny of degree 4 as the composition of two isogenies of degree 2. From [35] we will obtain an isomorphism $\Phi_3 : W' \to M$ to a Montgomery curve. Then $\Phi = \Phi_3 \circ \Phi_2 \circ \Phi_1 : E \to M$ is a G-isogeny. The composition Φ was computed with the help of Magma, and using the equation of E the coordinates $x(\Phi)$ and $y(\Phi)$ were simplified to the form in Theorem 3. The dual isogeny $\widehat{\Phi}$ and the induced function $\widehat{\Phi}_{1/x,g}$ were obtained using the implementation in Magma of the method in the Appendix A. One can also determine $\widehat{\Phi}$ using that $\widehat{\Phi} = \Phi_1^{-1} \circ \widehat{\Phi}_2 \circ \Phi_3^{-1}$.

In the proof of (c) we use that G is the 2-torsion subgroup. In the Appendix B we give programs in Magma, which allow to verify correctness of formulas in Theorem 3 and its proof.

(a) Let $\Phi_1 = \left(\frac{2(y+1)}{x^2}, \frac{4(ax^2+y+1)}{x^3}\right) : Jq_{k^2,a} \to W$ be the birational map from Subsection 3.1, where $W : y^2 = x^3 + 2ax^2 - 4k^2x - 8ak^2$. We have $\Phi_1(0,-1) = (-2a, 0)$. For the group $H = \langle \Phi_1(G)\rangle = \langle(-2a,0)\rangle$ of order 2 we have the H-isogeny from Vélu's formulas

$$\Phi_2 = \left(x + \frac{4(a^2-k^2)}{x+2a}, y - \frac{4(a^2-k^2)y}{(x+2a)^2}\right) : W \to W',$$

where $W' : y^2 = u(x)$ for $u(x) = x^3 + 2ax^2 + (16k^2 - 20a^2)x + 24a^3 - 32ak^2$. We have the root $x_0 = 2a$ of u such that $u'(x_0) = 16k^2$ is a square in K. From Subsection 2.2 we have the isomorphism $\Phi_3 = \left(\frac{x-2a}{4k}, \frac{y}{4k}\right) : W' \to M$ to the Montgomery curve $M : y^2/(4k) = x^3 + (2a/k)x^2 + x$. Hence $\Phi = \Phi_3 \circ \Phi_2 \circ \Phi_1 : Jq_{k^2,a} \to M$ is a G-isogeny given by

$$\Phi = (\varphi_1, \varphi_2) = \left(\frac{-k^2x^4 + y^2 + 2y + 1}{2kx^2(ax^2+y+1)}, \frac{k^2x^4 + 2ax^2y + 2ax^2 + y^2 + 2y + 1}{kx^3(ax^2+y+1)}\right).$$

Substituting $k^2x^4 = y^2 - 2ax^2 - 1$ we can simplify φ_1 and φ_2 as follows

$$\varphi_1 = \frac{2(ax^2+y+1)}{2kx^2(ax^2+y+1)} = \frac{1}{kx^2} \text{ and } \varphi_2 = \frac{2y(ax^2+y+1)}{kx^3(ax^2+y+1)} = \frac{2y}{kx^3}.$$

We have

$$\widehat{\Phi} = \left(\frac{y}{k(x^2-1)}, \frac{(20k^2-16a^2)x^2 + kxy^2 + 8akx + 2ay^2 + 4k^2}{(16a^2-12k^2)x^2 + kxy^2 + 8akx - 2ay^2 + 4k^2}\right).$$

(b) Let $\Psi_0 = \left(\frac{1+y}{1-y}, \frac{1+y}{x(1-y)}\right) : Ed_{a,d} \to M_{\alpha,\beta}$ be the birational map to the Montgomery curve from Subsection 3.2, where $\alpha = 2(a+d)/(a-d)$ and $\beta = 4/(a-d)$. Substituting $(\beta x, \beta y)$ to the equation of $M_{\alpha,\beta}$, and dividing this equation by β^3 we obtain the Weierstrass curve $W : y^2 = x^3 + \frac{1}{2}(a+d)x^2 + \frac{1}{16}(a-d)^2x$, and the isomorphism $\Psi_1 = (x/\beta, y/\beta) : M_{\alpha,\beta} \to W$. Thus

$$\Phi_1 = \Psi_1 \circ \Psi_0 = \left(\frac{(d-a)(y+1)}{4(y-1)}, \frac{(d-a)(y+1)}{4x(y-1)}\right) : Ed_{a,d} \to W$$

is a birational map. We have $\Phi_1(1/\sqrt{a}, 0) = ((a-d)/4, \sqrt{a}(a-d)/4)$. From Subsection 3.2, $[2](1/\sqrt{a}, 0) = (0,-1)$ and $\Phi_1(0,-1) = (0,0)$. The group $H = \Phi_1(G) = \langle((a-d)/4, \sqrt{a}(a-d)/4)\rangle \subset W$ has the subgroup $H_1 = \langle(0,0)\rangle \subset H$

of order 2. We will obtain an H-isogeny as the composition of two isogenies of degree 2 determined from Vélu's formulas. The H_1-isogeny is given by

$$\Psi_2 = \left(x + \frac{(a-d)^2}{16x}, y - \frac{(a-d)^2 y}{16x^2}\right) : W \to W_1,$$

where $W_1 : y^2 = x^3 + \frac{1}{2}(a+d)x^2 - \frac{1}{4}(a-d)^2 x - \frac{1}{8}(a+d)(a-d)^2$. We have $\Psi_2((a-d)/4, \sqrt{a}(a-d)/4) = ((a-d)/2, 0)$. For the subgroup $H_2 = \Psi_2(H) = \langle((a-d)/2, 0)\rangle \subset W_1$ of order 2 we have the H_2-isogeny

$$\Psi_3 = \left(x + \frac{a(a-d)}{x-(a-d)/2}, y - \frac{a(a-d)y}{(x-(a-d)/2)^2}\right) : W_1 \to W',$$

where $W' : y^2 = u(x)$ and $u(x) = x^3 + \frac{1}{2}(a+d)x^2 - \frac{1}{4}(a-d)(21a-d)x + \frac{1}{8}(a-d)(-45a^2+d^2+12ad)$. Thus $\Phi_2 = \Psi_3 \circ \Psi_2 : W \to W'$ is an H-isogeny. We have a root $x_0 = (-3a+d)/2$ of $u(x)$ such that $u'(x_0) = d^2$ is a square. From Subsection 2.2 we have the isomorphism

$$\Phi_3 = ((2x + 3a - d)/(2d), y/d) : W' \to M$$

to the Montgomery curve $M : y^2/d = u(dx + x_0)/d^3$. Hence $M : y^2/d = x^3 + (-4a/d + 2)x^2 + x$. The G-isogeny $\Phi = \Phi_3 \circ \Phi_2 \circ \Phi_1 : Ed_{a,d} \to M$ is given by

$$\Phi = (\varphi_1, \varphi_2) = \left(\frac{y^2 - a/d}{y^2(y^2-1)}, \frac{y^4 - 2ay^2/d + a/d}{xy^3(y^2-1)}\right).$$

We have $y^2 - 1 = dx^2(y^2 - a/d)$ on $Ed_{a,d}$. Hence $\varphi_1 = \dfrac{y^2 - a/d}{y^2 dx^2(y^2 - a/d)} = \dfrac{1}{d(xy)^2}$. We have $\varphi_2 = \dfrac{y^2(y^2 - a/d) - (a/d)(y^2-1)}{xy^3(y^2-1)}$
$= \dfrac{y^2(y^2 - a/d) - (a/d)dx^2(y^2 - a/d)}{xy^3 dx^2(y^2 - a/d)} = \dfrac{y^2 - ax^2}{d(xy)^3}$.
$\widehat{\Phi} = (\widehat{\varphi}_1, \widehat{\varphi}_2)$ is given by

$$\widehat{\varphi}_1 = \frac{4y(-x^2+1)}{(-16a^2/d + 16a - d)x^2 - xy^2 + 2(2a-d)x - 2(2a/d+1)y^2 - d},$$

$$\widehat{\varphi}_2 = \frac{(-16a^2 + 16ad + d^2)x^2 + dxy^2 + 2d(-2a+d)x + 2(-2a+d)y^2 + d^2}{(16a^2 - 16ad + d^2)x^2 + dxy^2 + 2d(-2a+d)x + 2(2a-3d)y^2 + d^2}.$$

(c) Let $\Phi_1 : Ji_{a,ac^2} \to M_{A,B}$ be the isomorphism from Proposition 4(c). Using the formula on doubling on Ji_{a,ac^2} from Subsection 3.5 we obtain the G-isogeny $\Phi = \Phi_1 \circ [2] = (\varphi_1, \varphi_2) : Ji_{a,ac^2} \to M_{A,B}$, where

$$\varphi_1 = \frac{-ac^2x^2y^2 + ax^2z^2 + y^2 + z^2}{2acx^2z^2}, \varphi_2 = \frac{ac^2x^2y^3 + (2ac^2 - a)x^2yz^2 - y^3 - yz^2}{2acx^3z^3}.$$

Using the equations $ax^2+y^2=1$ and $ac^2x^2+z^2=1$ of Ji_{a,ac^2} we have

$$\varphi_1 = \frac{y^2(1-ac^2x^2)+z^2(ax^2+1)}{2acx^2z^2} = \frac{y^2z^2+z^2(ax^2+1)}{2acx^2z^2}$$

$$= \frac{y^2+ax^2+1}{2acx^2} = \frac{2}{2acx^2} = \frac{1}{acx^2},$$

$$\varphi_2 = \frac{y^3(ac^2x^2-1)+(2ac^2-a)x^2yz^2-yz^2}{2acx^3z^3} = \frac{-y^3z^2+(2ac^2-a)x^2yz^2-yz^2}{2acx^3z^3}$$

$$= \frac{-y^3+(2ac^2-a)x^2y-y}{2acx^3z} = \frac{y(-y^2-ax^2-1+2ac^2x^2)}{2acx^3z}$$

$$= \frac{y(-1+ac^2x^2)}{acx^3z} = \frac{-yz^2}{acx^3z} = \frac{-yz}{acx^3}.$$

We have $\widehat{\Phi} = \widehat{\Phi_1 \circ [2]}_J = [2]_J \circ \Phi_1^{-1} = \Phi_1^{-1} \circ [2]_M$, where $[2]_J$ on Ji_{a,ac^2} and $[2]_M$ on $M_{A,B}$ are doublings. From Proposition 4(c) $x(\Phi_1) = 1/g$. Thus $(\Phi_1)_{g,1/x} = x$, which gives $(\Phi_1^{-1})_{1/x,g} = x$. We have $\widehat{\Phi}_{1/x,g} = (\Phi_1^{-1})_{1/x,g} \circ [2]_{M\,1/x} = [2]_{M\,1/x} = 4x(x^2+Ax+1)/(x^2-1)^2$, where the $1/x$-doubling on $M_{A,B}$ is in Lemma 1.

In Corollary 2 we obtain formulas in eq. (1.5) for the following compressions in an alternative way to [12,16,21,22], and for two new compressions, which come from Proposition 4.

Corollary 2 *Let E/K be the model of an elliptic curve with the compression w obtained either from Proposition 4 with $w = acxy$ in (a), $w = xy$ in (b), and $w = c(1-y)/(z+1)$ in (c) or from Theorem 3. Then the w-doubling and the w-differential addition are given by eq.* (1.5)*, where A is from the Montgomery curve $M_{A,B}$ in Proposition 4 or Theorem 3, respectively.*

Proof. For $\Phi : E \to M_{A,B}$ from Proposition 4 or Theorem 3 we have $x(\Phi) = 1/w$. From Proposition 1 a w-doubling and a w-differential addition are the same as for the $1/x$ compression on the Montgomery curve $M_{A,B}$. Thus can be given by eq. (1.5) from Lemma 1.

We have the following formulas for a G-compression on a twisted Hessian curve.

Theorem 4 *Let $H_{a,d} : aX^3+Y^3+Z^3 = dXYZ$ be the twisted Hessian curve over K with* $\operatorname{char} K \neq 2,3$. *Let $\omega \in \overline{K}$ be a third root of unity $\neq 1$. For the subgroup $G = \{(0 : -\omega^i : 1) : i = 0,1,2\} \subset H_{a,d}$ of order 3, and the G-compression $w = tz$ on $H_{a,d}$, where $t = Y/X$ and $z = Z/X$, we have the following G-isogeny*

$$\Phi = (-w, \frac{1}{2}(dtz - 2z^3 - a)) : H_{a,d} \to W$$

to the Weierstrass curve $W : y^2 = x^3 + \frac{1}{4}d^2x^2 + \frac{1}{2}adx + \frac{1}{4}a^2$. *The function induced by the dual isogeny* $\widehat{\Phi}$ *and compressions of degree two* $-x$ *on* W *and* $t + z$ *on* $H_{a,d}$ *is given by*

$$\widehat{\Phi}_{-x,t+z} = \frac{-dx^3 + 9ax^2 - ad^2x + a^2d}{3x^3 - d^2x^2 + 3adx - 3a^2}.$$

Proof. Let $x = X/Z$ and $y = Y/Z$. Computing from eq. (3.2) coefficients a_1 and a_3 we let $a_1 = d/3$ and $a_3 = (d^3/27 - a)/27$. From eq. (3.3) we have the isomorphism

$$\Phi_0 = \left(\frac{-3a_3x}{a_1x + y + 1}, \frac{a_3(a_1x + \omega\, y + \omega^2)}{a_1x + y + 1}\right) : H_{a,d} \to W_1$$

to the Weierstrass curve $W_1 : y^2 + a_1xy + a_3y = x^3$ such that $\Phi_0(0 : -\omega : 1) = (0, 0)$. For the subgroup $H = \Phi_0(G) = \langle(0, 0)\rangle \subset W_1$ from Vélu's formulas ([41, Thm. 12.16]) we obtain the H-isogeny $\Phi_1 : W_1 \to W_2$ given by

$$\Phi_1 = (x + v/x + u/x^2, y - u(2y + a_1x + a_3)/x^3 - v(a_1x + y)/x^2 - a_1u/x^2),$$

where $u = a_3^2, v = a_1a_3, W_2 : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, A_1 = a_1, A_2 = 0, A_3 = a_3, A_4 = -5v, A_6 = -a_1^2v - 7u$. Completing the square we have $W_2 : (y + (A_1x + A_3)/2)^2 - A_1^2x^2/4 - A_1A_3x/2 - A_3^2/4 = x^3 + A_2x^2 + A_4x + A_6$. Let $\Phi_2 = (x, y + (A_1x + A_3)/2) : W_2 \to W_3$ be an isomorphism to $W_3 : y^2 = x^3 + b_2x^2 + b_4x + b_6$, where $b_2 = A_2 + A_1^2/4$, $b_4 = A_4 + A_1A_3/2$, $b_6 = A_6 + A_3^2/4$. The composition $\Psi = (\psi_1, \psi_2) = \Phi_2 \circ \Phi_1 \circ \Phi_0 : H_{a,d} \to W$ is of the form

$$\psi_1 = \frac{(9a - d^3)x^3 - 3d^2x^2y - 3d^2x^2 + 9y^3 + 27y^2 + 27y + 9}{27x^2(dx + 3y + 3)},$$

$$\psi_2 = (2\,\omega + 1)\frac{-ax^3y + ax^3 + dxy^3 + dxy^2 - dxy - dx + 2y^4 + 4y^3 - 4y - 2}{18x^3(dx + 3y + 3)}.$$

We have $(2\,\omega + 1)^2 = -3$. Let $\lambda = 2\,\omega + 1$. To obtain an isogeny over K we use the isomorphism $\Phi_3 = (\lambda^2\, x, \lambda^3\, y) = (-3x, -3(2\,\omega + 1)y) : W_3 \to W_4$, where $W_4 : y^2 = x^3 + \lambda^2\, b_2x^2 + \lambda^4\, b_4x + \lambda^6\, b_6$. Then $\Phi_3 \circ \Psi : H_{a,d} \to W_4$ is over K. We have $x = 1/z$ and $y = t/z$. The formula on $\Phi_3 \circ \Psi(x, y)$ is given in the coordinates (t, z) by $\Gamma(t, z) = (\gamma_1, \gamma_2) = \Phi_3 \circ \Psi(1/z, t/z)$, where

$$\gamma_1 = \frac{-9t^3 - 27t^2z - 27tz^2 + 3d^2t - 9z^3 + 3d^2z - 9a + d^3}{27t + 27z + 9d},$$

$$\gamma_2 = \frac{2t^4 + 4t^3z + dt^3 + dt^2z - 4tz^3 - dtz^2 - at - 2z^4 - dz^3 + az}{6t + 6z + 2d}.$$

The affine equation of $H_{a,d}$ in the (t, z) coordinates is of the form $t^3 + z^3 + a = dtz$. We can simplify γ_1 as follows:

$$\gamma_1 = \frac{-9(t^3 + z^3) - 27tz(t + z) + d^2(3t + 3z + d) - 9a}{9(3t + 3z + d)}$$

$$= \frac{-9(dtz-a)-27tz(t+z)-9a}{9(3t+3z+d)} + \frac{d^2}{9}$$

$$= \frac{-9dtz-27tz(t+z)}{9(3t+3z+d)} + \frac{d^2}{9} = \frac{-9tz(3t+3z+d)}{9(3t+3z+d)} + \frac{d^2}{9}$$

$$= -tz + \frac{d^2}{9}.$$

Using the method from the Appendix A we simplified γ_2 to the form $\gamma_2 = \frac{1}{2}(dtz - 2z^3 - a)$. For the isomorphism $\Phi_4 = (x - d^2/9, y)$ we obtain the G-isogeny

$$\Phi = \Phi_4 \circ \Gamma = (-tz, \frac{1}{2}(dtz - 2z^3 - a)) : H_{a,d} \to W,$$

where W is of the form $W : y^2 = (x+d^2/9)^3 + \lambda^2\, b_2(x+d^2/9)^2 + \lambda^4\, b_4(x+d^2/9) + \lambda^6\, b_6$. Substituting the above values we have $W : y^2 = x^3 + \frac{1}{4}d^2x^2 + \frac{1}{2}adx + \frac{1}{4}a^2$.

Applying the method from the Appendix A we obtain the dual isogeny $\widehat{\Phi} = (\widehat{\varphi}_1 : \widehat{\varphi}_2 : \widehat{\varphi}_3) : W \to H_{a,d}$, and the induced function $\widehat{\Phi}_{-x,t+z}$, where
$\widehat{\varphi}_1 = -(2d^2x^3 + 12adx^2 + 24xy^2 + 18a^2x)$,
$\widehat{\varphi}_2 = (36a - d^3)x^3 + 2d^2x^2y + 2ad^2x^2 + 4dxy^2 + 12adxy + 3a^2dx - 8y^3 + 18a^2y$,
$\widehat{\varphi}_3 = (36a - d^3)x^3 - 2d^2x^2y + 2ad^2x^2 + 4dxy^2 - 12adxy + 3a^2dx + 8y^3 - 18a^2y$.

Remark 5 Formulas on the dual isogeny $\widehat{\Phi}$ and the induced function $\widehat{\Phi}_{f,g}$ in Theorems 3 and 4, and their proofs were obtained over the field of rational functions $\mathbb{Q}(a,b)$ using Magma, where a and b are variables over $\mathbb{Q}$, and b is equal to the variable k, d, and c, resp., in these theorems. One can show as follows that these formulas are correct over a field K for generic coefficients from $\overline{K}$. Let p be a prime number $\neq 2$ and $\neq 2, 3$ in Theorems 3 and 4, resp. Now let $\mathbb{F}$ be $\mathbb{Q}$ or $\mathbb{F}_p$, and $\mathbb{F}(a,b)$ be the field of rational functions, where b is the same as above for $\mathbb{Q}$. The isogeny Φ is over K, because it is the composition of maps over K. By the subscript p we will denote the reduction modulo p of a curve or a map on a curve over $\mathbb{Q}(a,b)$ if this is possible. We have $\widehat{\Phi} \circ \Phi = [\deg \Phi]$ over $\mathbb{Q}(a,b)$. All these maps can be reduced modulo p, and we have $\widehat{\Phi}_p \circ \Phi_p = [\deg \Phi]_p$. It follows that $\widehat{\Phi}_p : E'_p \to E_p$ is the dual isogeny to Φ_p. Similarly $(\widehat{\Phi}_{f,g})_p$ is equal to $(\widehat{\Phi}_p)_{f_p,g_p}$. Therefore we can assume that for $\Phi : E \to E'$ over $\mathbb{F}(a,b)$ we have $\widehat{\Phi}$ and $\widehat{\Phi}_{f,g}$. Let $\mathbb{F} \subset K$ be a field extension, and $a', b' \in K$. By subscripts a', b' we denote evaluation of variables a, b at a', b' of a curve or a map on a curve over $\mathbb{F}(a,b)$ if this is possible. Assume that $E_{a',b'}$ and $E'_{a',b'}$ are elliptic curves (i.e. are non-singular), and the evaluation $\widehat{\Phi}_{a',b'}$ at a', b' is possible. From the equation $\widehat{\Phi} \circ \Phi = [\deg \Phi]$ we have $\widehat{\Phi}_{a',b'} \circ \Phi_{a',b'} = [\deg \Phi]_{a',b'}$. Hence $\widehat{\Phi}_{a',b'} : E'_{a',b'} \to E_{a',b'}$ is the dual isogeny to $\Phi_{a',b'}$. Similarly we can obtain the induced function $(\widehat{\Phi}_{f,g})_{a',b'}$.

Acknowledgements. The author would like to thank Tomasz Kijko and Michał Wroński for valuable discussions.

References

1. W. W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, American Mathematical Society, Providence, RI, 1994.
2. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves, in: Progress in Cryptology, AFRICACRYPT 2008, in: LNCS, vol. 5023, 2008, pp. 389–405.
3. D. J. Bernstein, C. Chuengsatiansup, D. Kohel, T. Lange, Twisted Hessian curves, in: Progress in Cryptology, LATINCRYPT 2015, in: LNCS, vol. 9230, 2015, pp. 269–294.
4. O. Billet, M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC 2003, in: LNCS, vol. 2643, 2003, pp. 34–42.
5. E. Brier, M. Joye, Fast point multiplication on elliptic curves through isogenies, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC 2003, in: LNCS, vol. 2643, 2003, pp. 43–50.
6. E. Brier, M. Joye, Weierstraß elliptic curves and side-channel attacks, in: Public Key Cryptography, PKC 2002, in: LNCS, vol. 2274, 2002, pp. 335–345.
7. W. Castryck, F. Vercauteren, Toric forms of elliptic curves and their arithmetic, J. Symb. Comput., 46 (2011) 943-966.
8. D. V. Chudnovsky, G. V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Adv. Appl. Math., 7 (1986) 385-434.
9. C. Costello, B. Smith, Montgomery curves and their arithmetic: The case of large characteristic fields, J. Cryptogr. Eng., 8 (2018), 227-240.
10. C. Doche, T. Icart, D. R. Kohel, Efficient scalar multiplication by isogeny decompositions, in: Public Key Cryptography, PKC 2006, in: LNCS, vol. 3958, 2006, pp. 191–206.
11. R. Dryło, Compression on the Twisted Jacobi Intersection, Fundam. Inform., 181 (2021), 303-312.
12. R. Dryło, T. Kijko, M. Wroński, Arithmetic using compression on elliptic curves in Huff's form and its applications, Int. J. Electron. Telecommun., 67 (2021), 193–200.
13. R. Dryło, T. Kijko, M. Wroński, Determining formulas related to point compression on alternative models of elliptic curves, Fundam. Inform., 169 (2019), 285-294.
14. H. Edwards, A normal form for elliptic curves, Bull. Am. Math. Soc., 44 (2007) 393-422.
15. R. R. Farashahi, S. G. Hosseini, Differential addition on binary elliptic curves, Finite Fields Appl., 87 (2023) 102141.
16. R. R. Farashahi, S. G. Hosseini, Differential addition on twisted Edwards curves, in: Information Security and Privacy, ACISP 2017, Part II, in: LNCS, vol. 10343, 2017, pp. 366–378.
17. R. R. Farashahi, M. Joye, Efficient arithmetic on Hessian curves, in: Public Key Cryptography, PKC 2010, in: LNCS, vol. 6056, 2010, pp. 243–260.
18. R. Feng, M. Nie, H. Wu, Twisted Jacobi intersections curves, Theor. Comput. Sci., 494 (2013) 24-35.
19. H. Gu, D. Gu, W. Xie, Differential addition on Jacobi quartic curves, in: Symposium on ICT and Energy Efficiency and Workshop on Information Theory and Security (CIICT 2012), in: IET Conference Publications, vol. 606, pp. 192-195.
20. H. Hisil, K. K. H. Wong, G. Carter, E. Dawson, Jacobi quartic curves revisited, in: Information Security and Privacy, ACISP 2009, LNCS, vol. 5594, 2009, pp. 452–468.

21. Z. Hu, Z. Liu, L. Wang, and Z. Zhou, Simplified isogeny formulas on twisted Jacobi quartic curves, Finite Fields Appl., 78 (2022) 101981.
22. Z. Hu, L. Wang, Z. Zhou, Isogeny computation on twisted Jacobi intersections, in: Information Security Practice and Experience, ISPEC 2021, in: LNCS 13107, 2021, pp. 46–56.
23. Y. Huang, F. Zhang, Z. Hu, Z. Liu, Optimized arithmetic operations for isogeny-based cryptography on Huff curves, in: Information Security and Privacy, ACISP 2020, in: LNCS, vol. 12248, 2020, pp. 23-40.
24. G. B. Huff, Diophantine problems in geometry and elliptic ternary forms, Duke Math. J., 15 (1948) 443–453.
25. M. Joye, J. J. Quisquater, Hessian elliptic curves and side-channel attacks, in: Cryptographic Hardware and Embedded Systems, CHES 2001, in: LNCS, vol. 2162, 2001, pp. 402–410.
26. M. Joye, M. Tibouchi, D. Vergnaud, Huff's model for elliptic curves, in: Algorithmic Number Theory, ANTS-IX 2010, in: LNCS, vol. 6197, 2010, pp. 234–250.
27. B. Justus, D. Loebenberger, Differential addition in generalized Edwards coordinates, in: Advances in Information and Computer Security, IWSEC 2010, in: LNCS, vol. 6434, 2010, pp. 316–325.
28. N. Koblitz, Elliptic curves cryptosystem, Math. Comput., 48 (1987) 203–209.
29. H. W. Lenstra Jr, Factoring integers with elliptic curves, Ann. Math., 126 (1987) 649-673.
30. P. Y. Liardet, N. P. Smart, Preventing SPA/DPA in ECC systems using the Jacobi form, in: Cryptographic Hardware and Embedded Systems, CHES 2001, in: LNCS, vol. 2162, 2001, pp. 391–401.
31. J. López, R. Dahab, Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation, in: Cryptographic Hardware and Embedded Systems, CHES 99, in: LNCS, vol. 1717, 1999, pp. 316–327.
32. V. Miler, Use of elliptic curves in cryptography, in: Advances in Cryptology, CRYPT0 85, in: LNCS, vol. 218, 1986, pp. 417-426.
33. M. Monagan, R. Pearce, Rational simplification modulo a polynomial ideal, in: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, 2006, pp. 239-245.
34. P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, Math. Comput., 48 (1987) 243-264.
35. K. Okeya, H. Kurumatani, K. Sakurai, Elliptic curves with the Montgomery-form and their cryptographic applications, in: Public Key Cryptography, PKC 2000, in: LNCS, vol. 1751, 2000, pp. 238–257.
36. K. Okeya, K. Sakurai, Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve, in: Cryptographic Hardware and Embedded Systems, CHES 2001, in: LNCS, vol. 2162, 2001, pp. 126–141.
37. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, 2009.
38. N. P. Smart, The Hessian form of an elliptic curve, in: Cryptographic Hardware and Embedded Systems, CHES 2001, in: LNCS, vol. 2162, 2001, pp. 118-125.
39. M. Sweedler, Using Groebner bases to determine the algebraic and transcendental nature of field extensions: Return of the killer tag variables, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-10, in: LNCS, vol. 673, 1993, pp. 66–75.
40. J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci., 273 (1971) 238-241.
41. L. C. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman & Hall/CRC, 2008.

42. H. Wu, R. Feng, Elliptic curves in Huff's model, Wuhan Univ. J. Nat. Sci., 17 (2012) 473-480.

6 Appendix

A Presenting a function on generators of a subfield

We recall a method based on Gröbner bases for searching a solution of the following problem. Let F be a finitely generated field over K. Assume we are given $u_1, \ldots, u_m, v \in F$ such that v belongs to the subfield $K(u_1, \ldots, u_m)$.

$$\text{Determine } h \in K(x_1, \ldots, x_m) \text{ such that } v = h(u), \tag{6.1}$$

where $u = (u_1, \ldots, u_m)$. We assume that F is the field of fractions of the quotient ring $K[X]/P$, where P is a prime ideal in the polynomial ring $K[X] = K[x_1, \ldots, x_n]$.

The method of Sweedler [39] based on Gröbner bases can be used to determine a solution of (6.1). We recall an alternative method based on the approach used by Monagan and Pearce in [33, Sec. 4] for rational simplification modulo a polynomial ideal, which can return a solution with degrees of numerator and denominator not greater than given upper bounds if it exists. This method was used to obtain formulas for doubling, differential addition, and point recovery for compressions of degree 2 in [13], and dual isogenies and functions induced by isogenies and compressions in this paper (see the example below).

Let $d_1, d_2 \in \mathbb{N}$ be upper bounds on degrees, which can be increased if necessary. If there exists a solution $h = h_1/h_2$ of (6.1) with $h_2(u) \neq 0$, where $h_1, h_2 \in K[x_1, \ldots, x_m]$ are polynomials with $\deg h_i \leq d_i$ for $i = 1, 2$, then coefficients of h_1 and h_2 are given by non-trivial solutions of the system of linear equations over K (see below of (6.4)), which is obtained as follows.

For $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$ let $|\,\alpha\,| = \alpha_1 + \ldots + \alpha_m$. Let $T_i = \{t_{i,\alpha} : \alpha \in \mathbb{N}^m, |\,\alpha\,| \leq d_i\}$ be the set of variables over K corresponding to coefficients of h_i for $i = 1, 2$, and let $T = T_1 \cup T_2$. Variables in T are ordered in some way and will be regarded as coordinates in $K^{|T|}$ according to that order. Let $x_1, \ldots, x_\ell$ be variables over the field $K(T)$ for any $\ell \in \mathbb{Z}_{\geq 1}$. If for $H \in K(T)[x_1, \ldots, x_\ell]$ and $c \in K^{|T|}$ all coefficients of H from $K(T)$ are defined at c, then $H_c \in K[x_1, \ldots, x_\ell]$ is obtained by evaluating at c all these coefficients. A polynomial in $K(T)[x_1, \ldots, x_\ell]$ we will call T-linear if it is a linear form of variables from T with coefficients from $K[x_1, \ldots, x_\ell]$. Let $H_i = \sum_{\alpha \in \mathbb{N}^m : |\,\alpha\,| \leq d_i} t_{i,\alpha} x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ for $i = 1, 2$. We want to determine $c \in K^{|T|}$ such that

$$h = (H_1)_c/(H_2)_c \text{ is a solution of (6.1) and } (H_2)_c(u) \neq 0. \tag{6.2}$$

One can omit monomials in H_i which are divisible by the leading term of some polynomial from a suitable Gröbner basis (see Remark 6). Let $K(T)[X] = K(T)[x_1, \ldots, x_n]$. Let $\bar{f}$ denote the image in $K[X]/P$ for $f \in K[X]$. Let $u_i = \overline{N}_i/\overline{D}_i$, where $N_i, D_i \in K[X]$ and $D_i \notin P$ for $i = 1, \ldots, m$, and $U = (N_1/D_1, \ldots, N_m/D_m)$.

Let $M \in K[X] \setminus P$ be such that $MH_i(U) \in K(T)[X]$ for $i = 1, 2$, and let $W_i = MH_i(U)$. Let $v = \overline{V}_1/\overline{V}_2$, where $V_1, V_2 \in K[X]$ and $V_2 \notin P$. Let $A = V_1 MH_2(U) - V_2 MH_1(U)$. The polynomials H_i, W_i and A are T-linear for $i = 1, 2$. $(H_i)_c$ for $c \in K^{|T|}$ and $i = 1, 2$ satisfy (6.2) iff

$$A_c \in P \text{ and } (W_2)_c \notin P. \tag{6.3}$$

Let $I \subset P$ be an ideal in $K[X]$. In practice F can be the field of rational functions over K of an affine variety Z over K, which is the set of zeros in $\overline{K}^n$ of an ideal $I \subset K[X]$, and $P = \{f \in K[X] : f(x) = 0 \ \forall x \in Z\}$ is the ideal of Z over K. Then instead to determine P and $c \in K^{|T|}$ which satisfies (6.3) it may be easier in practice to determine $c \in K^{|T|}$ satisfying the condition

$$A_c \in I \text{ and } (W_2)_c(x) \neq 0 \text{ for some } x \in Z,$$

which implies (6.3).

Let G be a Gröbner basis of I. For basic properties of Gröbner bases see, e.g., the book by Adams and Loustaunau [1]. Let $I_{K(T)} = IK(T)[X]$ be the extension of I to the ideal in $K(T)[X]$. G is also a Gröbner basis of $I_{K(T)}$ (see Remark 7). Let $N_G(f)$ be the normal form of $f \in K(T)[X]$ with respect to G. For $c \in K^{|T|}$ we have $A_c \in I$ iff $N_G(A_c) = 0$. Assume that $f \in K(T)[X]$ is T-linear. Using the division algorithm of f by G one can obtain T-linear polynomials $q_g \in K(T)[X]$ for $g \in G$ and $r \in K(T)[X]$, where r is reduced with respect to G, such that $f = \sum_{g \in G} q_g g + r$. Then $N_G(f) = r$. We have $f_c = \sum_{g \in G} (q_g)_c g + r_c$ for $c \in K^{|T|}$. Hence $N_G(f_c) = r_c$, because r is reduced with respect to G, so is r_c. From the above

$$N_G(A) \text{ is } T\text{-linear and } N_G(A)_c = N_G(A_c) \text{ for } c \in K^{|T|}.$$

Let $N_G(A) = \sum_{\alpha \in \mathbb{N}^n : |\alpha| \leq e} L_\alpha(T) x_1^{\alpha_1} \dots x_n^{\alpha_n}$, where all $L_\alpha(T)$ are linear forms of variables from T over K, and e is the degree of $N_G(A)$ with respect to $x_1, \dots, x_n$. For $c \in K^{|T|}$ we have $A_c \in I$ iff

$$L_\alpha(c) = 0 \ \text{ for all } \ \alpha \in \mathbb{N}^n \text{ with } |\alpha| \leq e. \tag{6.4}$$

A solution $c \in K^{|T|}$ of the system of linear equations (6.4) we will call non-trivial if $(W_2)_c \notin P$. If $c \in K^{|T|}$ is a non-trivial solution of system (6.4), then $(H_i)_c$ for $i = 1, 2$ satisfy (6.2). If $I = P$, then $c \in K^{|T|}$ is a non-trivial solution of system (6.4) if and only if $(H_i)_c$ for $i = 1, 2$ satisfy (6.2).

For an upper bound d_i on the degree of H_i we have $\binom{d_i+n-1}{n-1}$ variables in the above system given by coefficients of H_i for $i = 1, 2$. Therefore efficiency of this method may be low when d_1 or d_2 are not sufficiently small.

Remark 6 One can omit some monomials in H_i as follows. Let J be an ideal in $K[x_1, \dots, x_m]$ such that $f(u) = 0$ for all $f \in J$. Let $\preceq$ be a monomial order in $K[x_1, \dots, x_m]$ such that for all monomials M_1 and M_2 in $K[x_1, \dots, x_m]$ we have if $\deg M_1 < \deg M_2$, then $M_1 \preceq M_2$. Let G_J be a Gröbner basis of J with respect to this order. For $d \in \mathbb{N}$ let $\mathcal{M}_d$ be the set of monomials $M \in K[x_1, \dots, x_m]$ with $\deg M \leq d$, which are not divisible by the leading term of some $g \in G_J$.

For given upper bounds d_i on degrees of h_i let $T_i = \{t_{i,M} : M \in \mathcal{M}_{d_i}\}$ be the set of variables corresponding to coefficients of h_i at monomials $M \in \mathcal{M}_{d_i}$ for $i = 1, 2$. Then one can assume that $H_i = \sum_{M \in \mathcal{M}_{d_i}} t_{i,M} M$ for $i = 1, 2$, because if $h_1, h_2 \in K[x_1, \ldots, x_m]$ satisfy $\deg h_i \leq d_i$ for $i = 1, 2$, $h_2(u) \neq 0$, and $h = h_1/h_2$ is a solution of (6.1), then for the normal forms we have $\deg N_{G_J}(h_i) \leq \deg h_i$, $N_{G_J}(h_i)$ is a linear combination over K of monomials from $\mathcal{M}_{d_i}$ for $i = 1, 2$, $N_{G_J}(h_2)(u) \neq 0$, and $N_{G_J}(h_1)/N_{G_J}(h_2)$ is a solution of (6.1).

Remark 7 Let $K \subset L$ a field extension, and $I_L = IL[X]$ be the extension of an ideal I in $K[X]$ to the ideal in the polynomial ring $L[X] = L[x_1, \ldots, x_n]$. Then a Gröbner basis G of I is also a Gröbner basis of I_L. To show this let $\{b_i\}_{i \in \Lambda}$ be a linear basis of L over K. This is also a basis of the free module $L[X]$ over $K[X]$. For $0 \neq f \in L[X]$ let $\mathrm{lm}(f)$ be the leading monomial of f (for the same order as for G). Let $0 \neq f \in I_L$. We have $f = f_{i_1} b_{i_1} + \ldots + f_{i_\ell} b_{i_\ell}$, where all $0 \neq f_{i_j} \in I$ and $i_1, \ldots, i_\ell$ are different. Hence $\mathrm{lm}(f) = \max\{\mathrm{lm}(f_{i_j}) : j = 1, \ldots, \ell\}$. Thus $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g)$ for some $g \in G$.

Example. Let $\Phi : E \to E'$ be an isogeny of elliptic curves over K. Let $f \in K(E')$ and $g \in K(E)$ be compressions of degree 2. To determine the dual isogeny $\widehat{\Phi} : E' \to E$ and the induced function $\Phi_{g,f} \in K(x)$ we have the situation of problem (6.1). For $\Phi_{g,f}$ this is obvious. To obtain $\widehat{\Phi}$ using the addition on E one can determine the formula on $[\deg \Phi]$. Assume for example that E and E' are on the plane. Let $\Phi = (\varphi_1, \varphi_2)$ and $[\deg \Phi] = (\alpha_1, \alpha_2)$, where $\varphi_i, \alpha_i \in K(E)$ for $i = 1, 2$. If $\psi_i \in K(x_1, x_2)$ satisfies $\alpha_i = \psi_i(\varphi_1, \varphi_2)$ for $i = 1, 2$, then $\widehat{\Phi} = (\psi_1, \psi_2)$. Note that if $w \in K(E)$ is a G-compression and Φ is a G-isogeny, then to determine the compression $f \in K(E)$ of degree 2 such that $w = f \circ \Phi$ from Theorem 1 we also have the case of problem (6.1).

B Verification of formulas from Section 5

The following programs in Magma can be used to verify correctness of formulas from Theorems 3 and 4. One can execute these programs in Magma calculator at `https://magma.maths.usyd.edu.au/calc/`

Theorem 3 (a)

```
Q:=Rationals(); F<a,k>:=FunctionField(Q,2); pF2<x,y>:=PolynomialRing(F,2);
J:=k^2*x^4+2*a*x^2 +1-y^2; w:=k*x^2;
Phi1:=[ 2*(y+1)/x^2, 4*(a*x^2+y+1)/x^3];
Phi2:=[x+ 4*(a^2 - k^2)/(x+2*a), y-4*(a^2 - k^2)*y/(x+2*a)^2];
Phi3:=[(x-2*a)/(4*k), y/(4*k)];
A:=2*a/k; B:= 1/(4*k); M:=x^3+A*x^2+x-B*y^2;
Psi:=Phi1;
for Eta in [Phi2,Phi3] do Psi:=[Evaluate(Eta[1],Psi), Evaluate(Eta[2],Psi)];
end for;
Phi:=[1/w, 2*y/(k*x^3)];
for i:=1 to 2 do IsDivisibleBy(Numerator(Phi[i]-Psi[i]), J); end for;
```

```
IsDivisibleBy(Numerator(Evaluate(M,Phi)), J);
Doubl:=[2*x*y/(1 - k^2*x^4),
((y^2 + 2*a*x^2)*(k^2*x^4+1)+4*k^2*x^4)/(1-k^2*x^4)^2];
DPhi1:=y/(k*(x^2 - 1));
DPhi2:=((20*k^2-16*a^2)*x^2 + k*x*y^2 + 8*a*k*x + 2*a*y^2 + 4*k^2)/
((16*a^2 - 12*k^2)*x^2 + k*x*y^2 + 8*a*k*x - 2*a*y^2 + 4*k^2);
DualPhi:=[DPhi1,DPhi2];
for i:=1 to 2 do IsDivisibleBy(Numerator(Evaluate(DualPhi[i],Phi)-Doubl[i]), J);
end for;
h:=k*(x^2 + 1)/(2*x);
IsDivisibleBy(Numerator(Evaluate(h,[1/x,0])-Evaluate((y+1)/x^2,DualPhi)), M);
```

(b)

```
Q:=Rationals(); F<a,d>:=FunctionField(Q,2); pF2<x,y>:=PolynomialRing(F,2);
E:=a*x^2+y^2-1-d*(x*y)^2; w:=d*(x*y)^2;
al:=2*(a+d)/(a-d);  be:=4/(a-d);
Phi1:= [(d-a)*(y+1)/(4*(y-1)), (d-a)*(y+1)/(4*x*(y-1))];
Psi2:= [ x +  (a-d)^2/(16*x), y - (a-d)^2*y/(16*x^2)];
Psi3:=[x + a*(a - d)/(x-(a -d)/2),  y- a*(a - d)*y/( x-(a -d)/2)^2 ];
x0:=(-3*a+d)/2; Phi3:= [(2*x + 3*a - d )/(2*d),  y/d ];
A:=-4*a/d + 2;  B:= 1/d;  M:=x^3 + A*x^2 + x - B*y^2;
Psi:=Phi1;
for Eta in [Psi2,Psi3,Phi3] do
Psi:=[Evaluate(Eta[1],Psi),Evaluate(Eta[2],Psi)]; end for;
Phi:=[1/w, (y^2-a*x^2)/(d*(x*y)^3)];
IsDivisibleBy(Numerator(Evaluate(M,Phi)), E);
for i:=1 to 2 do IsDivisibleBy(Numerator(Phi[i]-Psi[i]), E); end for;
Dub:=[2*x*y/(1 + d*(x*y)^2), (y^2 - a*x^2)/(1 - d*(x*y)^2)];
M4:=[Evaluate(Dub[1],Dub),Evaluate(Dub[2],Dub)];
DPhi1:=(4*y*(-x^2 + 1))/((-16*a^2/d + 16*a -d)*x^2 - x*y^2 + 2*(2*a - d)*x
- 2*(2*a/d + 1)*y^2 - d);
DPhi2:=
((-16*a^2+16*a*d + d^2)*x^2 + d*x*y^2+2*d*(-2*a + d)*x + 2*(-2*a +d)*y^2+d^2)/
((16*a^2 - 16*a*d + d^2)*x^2+d*x*y^2 + 2*d*(-2*a + d)*x + 2*(2*a-3*d)*y^2+d^2);
DualPhi:=[DPhi1,DPhi2];
for i:=1 to 2 do IsDivisibleBy(Numerator(Evaluate(DualPhi[i],Phi)-M4[i]),E);
end for;
h:=(x^4 + (-8*a/d + 4)*x^3 + 6*x^2 + (-8*a/d + 4)*x + 1)/
(x^4 - 4*x^3 + (16*a/d - 10)*x^2 - 4*x + 1);
IsDivisibleBy(Numerator(Evaluate(h,[1/x,0])-Evaluate(y,DualPhi)), M);
```

(c)

```
Q:=Rationals(); F<a,c>:=FunctionField(Q,2); pF3<x,y,z>:=PolynomialRing(F,3);
```

```
b:=a*c^2;  I:=ideal<pF3| [a*x^2+y^2-1, b*x^2+z^2-1]>; w:=a*c*x^2;
Phi1:=[(z+1)/(c*(1-y)), (a*x/(1-y))*( (z+1)/(c*(y-1)) + c),0];
Doubl:=[2*x*y*z/(y^2+a*(x*z)^2), (y^2 - a*(x*z)^2)/(y^2+a*(x*z)^2),
(z^2 - b*(x*y)^2)/(y^2+a*(x*z)^2)];
Psi:=[Evaluate(Phi1[1],Doubl), Evaluate(Phi1[2],Doubl),0];
Phi:=[1/w, -y*z/(a*c*x^3),0];
A:=-c-1/c; B:=1/(a*c); M:=x^3+A*x^2+x-B*y^2;
for i:=1 to 2 do NormalForm(Numerator(Phi[i]-Psi[i]),I); end for;
NormalForm(Numerator(Evaluate(M,Phi)), I);
```

Theorem 4

```
Q:=Rationals(); pQ<U>:=PolynomialRing(Q);
R<om>:=quo<pQ | U^2 + U + 1>;
F<a,d>:=FunctionField(R,2); pF2<x,y>:=PolynomialRing(F,2);
a1:=d/3; a3:=(d^3/27 - a)/27;
Phi0:=[-3*a3*x/(a1*x + y + 1), a3*(a1*x + om*y + om^2)/(a1*x+y+1)];
u:=a3^2; v:=a1*a3; A1:=a1; A2:=0; A3:=a3; A4:=-5*v; A6:=-a1^2*v-7*u;
Phi1:=[x + v/x + u/x^2, y- u*(2*y+a1*x+a3)/x^3 - v*(a1*x+y)/x^2 - a1*u/x^2];
b2:=A2+A1^2/4; b4:=A4+A1*A3/2; b6:=A6+A3^2/4; Phi2:=[x,y+(A1*x+A3)/2];
la:=2*om+1; Phi3:=[-3*x,-3*(2*om+1)*y];
pF2tz<t,z>:=PolynomialRing(F,2); Htz:=t^3+z^3+a-d*t*z;
Ga:=[1/z,t/z];
for Eta in [Phi0,Phi1,Phi2,Phi3] do
Ga:=[Evaluate(Eta[1],Ga), Evaluate(Eta[2],Ga)]; end for;
Ga:=[Ga[1]-d^2/9,Ga[2]];
Phi:=[-t*z, (d*t*z - 2*z^3 - a)/2];
W:=x^3 + 1/4*d^2*x^2 + 1/2*a*d*x  + 1/4*a^2 - y^2;
for i:=1 to 2 do  IsDivisibleBy(Numerator(Ga[i]-Phi[i]), Htz); end for;
IsDivisibleBy(Numerator(Evaluate(W,Phi)), Htz);
pF4<x1,y1,x2,y2>:=PolynomialRing(F,4);
x3:=(x1-y1^2*x2*y2)/(a*x1*y1*x2^2-y2);
y3:=(y1*y2^2-a*x1^2*x2)/(a*x1*y1*x2^2-y2);
Dubl:=[Evaluate(x3,[x,y,x,y]), Evaluate(y3,[x,y,x,y])];
Tripl:=[Evaluate(x3, [x,y] cat Dubl), Evaluate(y3, [x,y] cat Dubl)];
DPhi1:=-(2*d^2*x^3 + 12*a*d*x^2 + 24*x*y^2 + 18*a^2*x);
DPhi2:=(36*a - d^3)*x^3 + 2*d^2*x^2*y + 2*a*d^2*x^2 + 4*d*x*y^2 + 12*a*d*x*y +
3*a^2*d*x - 8*y^3 + 18*a^2*y;
DPhi3:= (36*a - d^3)*x^3 - 2*d^2*x^2*y + 2*a*d^2*x^2 + 4*d*x*y^2 - 12*a*d*x*y +
3*a^2*d*x + 8*y^3 - 18*a^2*y;
DualPhi:=[DPhi1, DPhi2, DPhi3]; Tr:=[];
for i:=1 to 3 do Tr:=Tr cat [Evaluate(DualPhi[i], Phi)]; end for;
Tripltz:=[Evaluate(Tripl[1], [1/z,t/z]), Evaluate(Tripl[2], [1/z,t/z])];
for i:=1 to 2 do IsDivisibleBy(Numerator(Tripltz[i]-Tr[i]/Tr[3]), Htz); end for;
h:=(-d*x^3 + 9*a*x^2 - a*d^2*x + a^2*d)/(3*x^3 - d^2*x^2 + 3*a*d*x - 3*a^2);
```

```
t0:=DualPhi[2]/DualPhi[1]; z0:=DualPhi[3]/DualPhi[1];
IsDivisibleBy( Numerator(t0+z0 - Evaluate(h,[-x,y])), W);
```