2-Isogenies Between Elliptic Curves in Hesse Model

João Paulo da Silva[1], **Ricardo Dahab**[1], **Julio López**[1]

[1]Institute of Computing – University of Campinas (Unicamp)
1251 – 13083-852 – Campinas – SP – Brazil

jsilva@lasca.ic.unicamp.br, {rdahab,jlopez}@ic.unicamp.br

Abstract. *Cryptosystems based on the problem of calculating isogenies between supersingular elliptic curves were recently proposed as strong candidates in the area of Post-Quantum Cryptography. In order to evaluate isogenies applied in cryptography constructions we use the Vèlu formula. However, this formula only applies to elliptic curves in the Weierstrass model. This paper presents morphisms that can be used to construct 2-isogeny formulas for curves in the Hesse model.*

1. Introduction

Due to the fact that the most commonly used cryptosystems (e.g., RSA and ECDSA) are vulnerable to Shor's algorithm [Boneh and Lipton 1995], it is necessary to search for new options. More recently, Cryptography based on Isogenies was proposed. A construction named SIKE [Jao et al. 2017] is the representative of isogeny-based algorithms among 69 candidates of NIST's Post-Quantum Cryptography Standardization process[Chen et al. 2017]. Another construction named *Supersingular Isogeny Diffie-Hellman* was included in an experiment for a quantum-resistant version of TLS 1.3. So, there are important real applications for isogenies in cryptography. One of the main problems in isogeny-based algorithms is to compute the rational functions that make up the isogeny. Vèlu's formula [Vélu 1971] does this for curves in the Weierstrass model, but there are several other models for elliptic curves. Changing from one to another model can give us better formulas to compute and evaluate isogenies. In this paper we present the explicit morphisms that compose a 2-isogeny in the Hesse Model.

1.1. Organization of this Document

This paper is divided as follows: Section 2 presents basic definitions of elliptic curves and the Hesse model for an elliptic curve; Section 3 introduces concepts related to isogenies and how to construct them via Vèlu's formula in the Weierstrass model; in Section 4 we construct morphisms between the Hesse and Weierstrass models step by step; Section 5 presents discussions about the derived morphisms; finally, in Section 6 we put forward conclusions and directions for future works.

2. Preliminaries

2.1. Elliptic Curves

An elliptic curve E over a field K is a genus one algebraic curve that can be represented in the Weierstrass form $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, with $a_1, a_2, ..., a_6 \in K$. In addition, we need that the discriminant $\Delta = -d_2^2d_8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \neq 0$, where $d_2 = a_1^2 + 4a_2$, $d_4 = 2a_4 + a_1a_3$, $d_6 = a_3^2 + 4a_6$ and $d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. If we choose a field K with characteristic not 2 or 3, and after some admissible changes of variables, we obtain $y^2 = x^3 + Ax + B$, with $A, B \in K$. This is called the Short Weierstrass form of an elliptic

curve. As in the initial equation, we need that $\Delta = 4A^3 + 27B^2 \neq 0$. Let L be an extension field of K; then $E(L)$ is the set of L-rational points of E and is expressed by

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at infinity. In terms of the projective form of a Weierstrass equation, the point $\mathcal{O}$ is represented as $(0, 1, 0)$. Furthermore, the point at infinity is considered an L-rational point for all extensions L of the underlying field K. For practical applications, we use a finite field $K = \mathbb{F}_q$, where $q = p^m$, p prime, and $m \in \mathbb{N}$. Hasse's theorem [Washington 2008] gives a bound for the number of $\mathbb{F}_q$-rational points on E by $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$. An elliptic curve is said to be *supersingular* if, and only if, $t \equiv 0 \; mod \; p$; otherwise we call it *ordinary*.

A fundamental result (Theorem 2.1, [Washington 2008]) states that the set of elliptic points $E(K)$ together with a conveniently defined point addition forms an Abelian group.

2.2. Points of Order 2

When working over a field K whose characteristic is different from 2, we can write E in the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$, with $e_1, e_2, e_3 \in \overline{K}$, making it possible to characterize the points of order 2 of the curve. A given point P satisfies the relation $2P = \mathcal{O}$ if, and only if, the tangent line to the curve E at P is vertical, i.e., $y = 0$. That is, $E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}$. Thus, there is a group isomorphism between $E[2]$ and $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

2.3. Isomorphisms Between Elliptic Curves in the Weierstrass Model

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$ be elliptic curves in the Weierstrass model defined over a field K. E is isomorphic to E' if there exist $u \in K^*$ and $r, s, t \in K$, such that

$$\begin{aligned}
ua'_1 &= a_1 + 2s, \\
u^2a'_2 &= a_2 - sa_1 + 3r - s^2, \\
u^3a'_3 &= a_3 + ra_1 + 2t, \\
u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\
u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1.
\end{aligned} \tag{1}$$

The transformation is given by

$$(x, y) \mapsto (x', y')$$

where

$$\begin{aligned}
x &= u^2x' + r, \\
y &= u^3y' + su^2x' + t.
\end{aligned}$$

The relation between the discriminant of the two curves is given by the expression

$$u^{12}\Delta' = \Delta.$$

2.4. Hesse's Model

Although elliptic curves are more commonly specified by the reduced and generalized Weierstrass equations, these are not the only ways to represent them. In this section we will present an alternative model of representation of elliptic curves and discuss some aspects about it and how it relates to the Weierstrass model.

Another parametrization of elliptic curves is given by curves in the Hesse model [Joye et al. 2010]. We can express such curves by an equation given as $H_d : u^3+v^3+1 = 3duv$ or, in projectives coordinates, $H_d : U^3 + V^3 + W^3 = 3dUVW$, with $d \in K$, where K is the underlying field and $d^3 \neq 1$. The identity point, in projective coordinates is $(1 : -1 : 0)$ and, for a given point $P = (u, v)$, $-P = (v, u)$ is the inverse element of P. For the addition law, let $P_1 = (u_1 : v_1)$ and $P_2 = (u_2 : v_2)$ be elliptic points on H_d with $P_1 \neq P_2$; then, the coordinates of the resulting point $P_3 = (u_3 : v_3) = P_1 + P_2$ are given by

$$u_3 = \frac{v_1^2 u_2 - v_2^2 u_1}{u_2 v_2 - u_1 v_1}, \quad v_3 = \frac{u_1^2 v_2 - u_2^2 v_1}{u_2 v_2 - u_1 v_1}.$$

For point doubling, the coordinates of $P_3 = (u_3 : v_3) = [2]P_1$ are given by

$$u_3 = \frac{v_1(1 - u_1^3)}{u_1^3 - v_1^3}, \quad v_3 = \frac{u_1(v_1^3 - 1)}{u_1^3 - v_1^3}.$$

There are some interesting properties of the addition law for a curve in Hesse form. For example, taking a point $P_1 = (U_1 : V_1 : W_1)$ in projective coordinates, we have $[2]P_1 = (W_1 : U_1 : V_1) \bigoplus (V_1 : W_1 : U_1)$. This fact enables us to use the addition formula for point doubling. In this sense, we obtain a unified formula for Hesse point operation as a tool to improve the resistance of algorithms against side-channel attacks such as timing attacks. In [Joye and Quisquater 2001] the authors present a birational map between an elliptic curve given by H_d and one E in Weierstrass form. The coordinate map is given by

$$\psi : (u, v) \mapsto (-9d^2 + \xi u, 3\xi(v - 1)), \tag{2}$$

where $\xi = \frac{12(d^3-1)}{du+v+1}$, which sends point of H_d to $E : y^2 = x^3 - 27d(d^3+8)x + 54(d^6 - 20d^3 - 8)$. The inverse map is given by

$$\psi^{-1} : (x, y) \mapsto (\eta(x + 9d^2), -1 + \eta(3d^3 - dx - 12)), \tag{3}$$

where $\eta = \frac{6(d^3-1)(y+9d^3-3dx-36)}{(x+9d^2)^3+(3d^3-dx-12)^3}$.

3. Isogenies

For our purposes, we will define and work with isogenies between elliptic curves over finite fields, but this definition is not limited to these fields. A more general and abstract approach can be found in [Silverman 1986]. Fix a prime p and a power $q = p^k$, with $k \in \mathbb{N}$, and let E_1 and E_2 be elliptic curves over $K = \mathbb{F}_q$. An *isogeny* $\phi : E_1 \to E_2$ is a non-constant algebraic morphism

$$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right),$$

with $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ and f_i, g_i polynomials for $i \in \{1, 2\}$.

More specifically, ϕ is a group homomorphism between $E_1(\mathbb{F}_q)$ and $E_2(\mathbb{F}_q)$, i.e., given $P, Q \in E_1(\mathbb{F}_q)$ we have $\phi(P+Q) = \phi(P) + \phi(Q)$, where $+$ is the elliptic curve point addition. The degree of an isogeny is its degree as a rational map and, for separable isogenies, it is the size of its kernel. Theorem 3 from [Washington 2008, Section 12.5] gives us a necessary and sufficient condition for two elliptic curves to be isogenous. In order to explicitly compute the polynomials that make up the isogeny of the form defined above, we can use a formula due to Vèlu [Vélu 1971] which is given in Theorem 4.

Theorem 3 *(Tate) Let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_q$, where $q = p^k$ and $k \in \mathbb{N}$. E_1 is isogenous to E_2 if, and only if, $\#E_1 = \#E_2$.*

Theorem 4 *(Vèlu Formula) Consider the underlying field K such that $char(K)$ is not 2 or 3. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve in Short Weierstrass form. Let G be a subgroup of $E(K)$ with order l, l prime. Let S be the set of representatives of $G/\sim$, where $\sim$ is such that $P \sim Q \iff P = \pm Q$. Then, there exists an isogeny $\phi : E \to E'$, where $ker(\phi) = G$, given by*

$$\phi(x,y)=\left(x+\sum_{Q\in S}\left[\frac{t_Q}{x-x_Q}+\frac{\mu_Q}{(x-x_Q)^2}\right],y-\sum_{Q\in S}\left[\mu_Q\frac{2y}{(x-x_Q)^3}+t_Q\frac{y-y_Q}{(x-x_Q)^2}-\frac{g_Q^x g_Q^y}{(x-x_Q)^2}\right]\right),$$

where $Q=(x_Q,y_Q)$, $\mu_Q=(g_Q^y)^2$, with $t_Q=g_Q^x$ (if $Q=-Q$) or $t_Q=-2g_Q^x$ (if $Q\neq -Q$), $g_Q^x=3x_Q^2+A$, and $g_Q^y=-2y_Q$. Furthermore, $t=\sum_{Q\in S}t_Q$, $w=\sum_{P\in S}\mu_Q+\mu_Q t_Q$. The application of the Vèlu's formula gives us the coefficients of E':$y^2=x^3+(A-5t)x+(B-7w)$ and a normalized isogeny whose kernel is S.

A straight observation of the above formula shows that to compute an isogeny we need $\mathcal{O}(|G|)$ operations in the underlying field K.

4. 2-isogenies in the Hesse Model

From now on we will assume that we are working on a field $K = \mathbb{F}_q$ such that $q = p^n, q \equiv 2\,(mod\,3)$. Using a strategy similar to the work described in [Moody and Shumow 2011, Xiu Xu 2016] we will obtain a formula for 2-isogenies between curves in the Hesse model. These works make use of birational transformations between curves in the models of Edwards, Huff and Extended Jacobi Quartics and curves in the Weierstrass model. Once we are in Weierstrass form, Vèlu's formula is used to calculate 2-isogenies between curves in this form. After this, we return to the desired model by the inverse transformation between the models. The 2-isogeny will be given by the composition of all these morphisms. From now on, we will follow this strategy starting with curves in the Hesse model.

(Step 1) Hesse to Weierstrass: Given a curve H_d described as in 2.4, we can apply the map ψ_1 given by equation 2. The resulting curve is $E : y^2 = x^3 - 27d(d^3 + 8)x + 54(d^6 - 20d^3 - 8)$, where d is the initial coefficient of the Hesse curve.

(Step 2) 2-isogeny in Weierstrass: In order to calculate a 2-isogeny by the Vèlu's formula, it is necessary to discriminate a group of order 2 which will be the kernel of isogeny. For this, it is necessary to find points of order 2 in the curve in which we are working. As seen in Section 2.2 we need to look for roots of a cubic equation. Points of order 2 shall be of the form $(e_i, 0)$, where $e_i, i = \{1, 2, 3\}$ are the roots of the equation. The roots of $x^3 - 27d(d^3 + 8)x + 54(d^6 - 20d^3 - 8)$ are

$$e_1=\frac{3(d^4+\sigma^{2/3}+8d)}{\sqrt[3]{\sigma}},\quad e_2=\frac{3i(-d^4\theta_-+\theta_+\sigma^{2/3}-8d\theta_-)}{2\sqrt[3]{\sigma}},\quad e_3=\frac{-3i(-d^4\theta_++\theta_-\sigma^{2/3}-8d\theta_+)}{2\sqrt[3]{\sigma}},$$

where $\sigma=-d^6+20d^3+8\sqrt{-(d^3-1)^3}+8$, $\theta_+=\sqrt{3}+i$, $\theta_-=\sqrt{3}-i$. Let take the point $P=(e_1,0)\in K$ (the others points of order 2 are defined over $\overline{K}$) as the generator of the 2-isogeny kernel in Weierstrass form. The kernel representatives S will be $S=\{\mathcal{O},(e_1,0)\}$. Applying the formula of Theorem 4 with the respective set S we will obtain ψ_2 such that

$$\psi_2(x,y)=\left(x+\frac{(3e_1^2+A)}{x-e_1},y\frac{(x-e_1)^2-(3e_1^2+A)}{(x-e_1)^2}\right)$$

is a 2-isogeny between the two curves in the Weierstrass model. The equation of the resulting curve is $E':y^2=x^3+(A-5(3e_1^2+A))x+B-7e_1(3e_1^2+A)$, with $A=-27d(d^3+8)$ and $B=54(d^6-20d^3-8)$.

(Step 3) Triangular Curve: In order to return to a curve in Hesse form, we can take an intermediate step in which we transform a curve in the form $y^2=x^3+A_4x+A_6$ into one of the form $y^2+A_1xy+A_3y=x^3$. For this, we generate the system of equations 1 for the given curves and solve it. The resulting system is

$$\begin{aligned}&uA_1=2s,\\&0=3r-s^2,\\&u^3A_3=2t,\\&0=A_4+3r^2-2st,\\&0=A_6+rA_4+r^3-t^2.\end{aligned}\tag{4}$$

The system solution assuming $u\equiv 1\ (mod\ q)$ (for $A_4=(A-5(3e_1^2+A)),A=-27d(d^3+8)$ and $A_6=B-7e_1(3e_1^2+A),B=54(d^6-20d^3-8)$) is

$$\gamma=\sqrt[3]{2}\sqrt[3]{4A_4^3+27A_6^2},\quad \alpha=\sqrt{\gamma-2A_4},\quad r=\frac{\alpha-\sqrt{-\gamma-\frac{6\sqrt{6}A_6}{\alpha}-4A_4}}{\sqrt{6}},\quad s=-\sqrt{3}\sqrt{r},$$

$$t=-\frac{1}{2A_6}\sqrt{3}\sqrt{r}(r^3+3A_4r+4A_6),\quad A_1=-2\sqrt{3}\sqrt{r},\quad A_3=2t.$$

The coordinates of the morphism will be

$$\psi_3(x,y)=(u^2x'+r,u^3y'+su^2x'+t),$$

and the resulting curve will be $E'':y^2+A_1x'y'+A_3y'=x^3$.

(Step 4) Triangular to Hesse: At this point we are able to return to curves in the Hesse model. From the coefficients of the curve E'' obtained previously we define the following

$$\mu=\frac{1}{3}((-27A_3\delta^2-\delta^3)^{1/3}+\delta)\in\mathbb{F}_q,\qquad \delta=A_1^3-27A_3.$$

In order to simplify the writing, we will describe the transformation in projective coordinates

$$\psi_4(x',y')=(U',V',W')$$

$$U'=\frac{A_1(2\mu-\delta)}{3\mu-\delta}x'+y'+A_3, \qquad V'=\frac{-A_1\mu}{3\mu-\delta}x'-y', \qquad W'=\frac{-A_1\mu}{3\mu-\delta}x'-A_3.$$

The transformation above maps E'' to $H_{d'}$:$U'^3+V'^3+W'^3=3d'U'V'W'$, where $d'=\frac{\mu-\delta}{\mu}$.

Finally, to obtain the 2-isogeny between curves in the Hesse model, it comes down to composing the morphisms described in each step above.

$$\psi:H_d\rightarrow H_{d'}$$

$$\psi=\psi_4\circ\psi_3\circ\psi_2\circ\psi_1.$$

Despite the path we took in the above construction, we can turn directly and, more simply, to the Hesse curve after the 2-isogeny computation in Weierstrass form. For that, we derive from the curve E':$y^2=x^3+(A-5(3e_1^2+A))x+B-7e_1(3e_1^2+A)$, as stated in Step 2, the curve H'_d:$u^3+v^3+1=3d'uv$, via the map

$$\psi'_3=(-9d'^2+\xi u,3\xi(v-1)),$$

where $d'=\frac{A'(-4A'^3-27B'(B'-65664)+62990638848)}{3456(2A'^3+321489(B'-11664)}$ and $A'=A-5(3e_1^2+A)$, $B'=B-7e_1(3e_1^2+A)$. In this case, we have

$$\psi:H_d\rightarrow H_{d'}$$
$$\psi=\psi'_3\circ\psi_2\circ\psi_1.$$

5. Results and Discussion

The first construction presented in Section 4 is quite expensive due to the computation of the solutions for points of order 2 in the Weierstrass curve and the solutions for equations in (4) for the isomorphism to triangular curves. In Step 2 we need to compute one square root and one cubic root that are costly. In step 3, we need to compute four square roots. Moreover, when we turn to Hesse curves, one more cubic root is needed. In addition to the fact that these operations are costly, we need to assume that square roots can only be defined over a extension field. So, the basic operations like point addition and doubling become more expensive in this scenario. The second approach presented return to Hesse form after the 2-isogeny computation in the Weierstrass form. Despite being simpler, we cannot avoid computing the square and cubic roots when computing points of order 2. Even when we use intermediate isomorphisms between Weiertrass curves, the expressions for points of order 2 do not seem simpler. There are analogous formulas for elliptic curves in the Edwards and Huff Models in [Moody and Shumow 2011] and for Extended Jacobi Quartic model [Xiu Xu 2016]. In the work of [Moody and Shumow 2011] the 2-isogenies between curves in Edwards model also need to work in the extension field due to the appearance of square roots. The simplest expression for 2-isogenies among these works appears in [Xiu Xu 2016]. The costs of performing 2-isogeny computations in these models are summarized in Table 1.

Table 1. Operation cost of 2-isogeny computation in different models. The cost is expressed in the usual way: M=Multiplication; S=Squaring; A=Addition; I=Inversion; SR=Square Root. We are not taking into account operations involving constants.

Model	Function	Cost
Twist Edwards	Iso. Comp.	1**S**+1**I**
	Iso. Eval.	4**M**+1**S**+1**I**+1**SR**
Extended Jacobi Quartic	Iso. Comp.	1**S**+1**A**
	Iso. Eval.	6**M**+4**S**+4**A**+1**I**
Huff	Iso. Comp	1**M**+2**A**+1**SR**
	Iso. Eval.	7**M**+5**S**+6**A**+1**SR**+1**I**

6. Conclusion

The interest in the use of isogenies for post-quantum cryptographic constructions has increased enormously in recent years. Suitable and efficient formulas for isogeny computation is a key area of research for improving the performance of such systems. This work seeks to contribute to this area by presenting new constructions for 2-isogenies in the Hesse model. There is a lot of work still to be done. For future works we intend to simplify such formulas. Another research direction is to derive formulas for isogenies of higher degree.

7. Acknowledgment

This work is supported in part by the Intel/FAPESP grant 14/50704-7 under project "Secure Execution of Cryptographic Algorithms".

References

Boneh, D. and Lipton, R. J. (1995). Quantum cryptanalysis of hidden linear functions (extended abstract). In *CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 424–437. Springer.

Chen, L., Moody, D., and Liu, Y.-K. (2017). National institute of standards and technology's post-quantum cryptography standardization.

Jao, D., Azarderakhs, R., Campagna, M., Costello, C., Feo, L. D., Hess, B., Jalali, A., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Renes, J., Soukharev, V., and Urbanik, D. (2017). Supersingular isogeny key encapsulation. *NIST Post-Quantum Cryptography Standardization,*, Round 1 Submission.

Joye, M. and Quisquater, J.-J. (2001). Hessian elliptic curves and side-channel attacks. In Koç, Ç. K., Naccache, D., and Paar, C., editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, pages 402–410, Berlin, Heidelberg. Springer Berlin Heidelberg.

Joye, M., Tibouchi, M., and Vergnaud, D. (2010). Huff's model for elliptic curves.

Moody, D. and Shumow, D. (2011). Analogues of velu's formulas for isogenies on alternate models of elliptic curves. Cryptology ePrint Archive, Report 2011/430.

Silverman, J. (1986). *The arithmetic of elliptic curves*. Graduate Texts in Mathematics. Springer-Verlag, first edition.

Vélu, J. (1971). Isogénies entre courbes elliptiques. *C.R. Acad. Sc. Paris*, Série A(273):238–241.

Washington, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, second edition.

Xiu Xu, Wei Yu, K. W. X. H. (2016). Constructing isogenies on extended jacobi quartic curves. In *International Conference on Information Security and Cryptology*, Lecture Notes in Computer Science, pages 416–427. Chen K., Lin D., Yung M. (eds) Information Security and Cryptology, Springer, Cham.