Isogenies between (twisted) Edwards and Montgomery curves

Craig Costello and Michael Naehrig

Microsoft Research

Let $p > 3$ be a prime and let $\mathbb{F}_p$ be the finite field with p elements. For elements $a, d \in \mathbb{F}_p \setminus \{0\}$ with $a \neq d$, let $\mathrm{E}_{\mathrm{E},a,d}$ be the twisted Edwards curve over $\mathbb{F}_p$ defined by

$$\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

For elements $A \in \mathbb{F}_p \setminus \{-2, 2\}$ and $B \in \mathbb{F}_p \setminus \{0\}$, let $\mathrm{E}_{\mathrm{M},A,B}$ be the Montgomery curve over $\mathbb{F}_p$ defined by

$$\mathrm{E}_{\mathrm{M},A,B} : Bv^2 = u^3 + Au^2 + u.$$

Proposition 1. *Let $p \equiv 1 \pmod 4$. Fix a square root of -1, i.e. let $s \in \mathbb{F}_p$ such that $s^2+1 = 0$. Let $A = 4d + 2$. Then, the map*

$$\phi : \mathrm{E}_{\mathrm{E},-1,d} \to \mathrm{E}_{\mathrm{M},A,1},\ (x, y) \mapsto (u, v) = \left(-\frac{y^2}{x^2}, \frac{-ys(x^2 - y^2 + 2)}{x^3}\right)$$

is a 4-isogeny defined over $\mathbb{F}_p$ with dual isogeny

$$\hat{\phi} : \mathrm{E}_{\mathrm{M},A,1} \to \mathrm{E}_{\mathrm{E},-1,d},\ (u, v) \mapsto (x, y) = \left(\frac{4sv(u - 1)(u + 1)}{u^4 - 2u^2 + 4v^2 + 1}, \frac{(u^2 + 2v - 1)(u^2 - 2v - 1)}{-u^4 + 2uv^2 + 2Au + 4u^2 + 1}\right).$$

Proof. A direct calculation using the curve equation of $\mathrm{E}_{\mathrm{E},-1,d}$ shows that $(u, v) = \phi(x, y)$ satisfies the curve equation $v^2 = u^3 + Au^2 + u$. Similarly, using the curve equation of $\mathrm{E}_{\mathrm{M},A,1}$ shows that $(x, y) = \hat{\phi}(u, v)$ satisfies the equation $-x^2 + y^2 = 1 + dx^2y^2$. Thus, both ϕ and $\hat{\phi}$ are *rational maps* between the curves [1, Def. 5.5.1].

To show that these rational maps are both *morphisms*, it remains to show that ϕ (resp. $\hat{\phi}$) is regular at all points in $\mathrm{E}_{\mathrm{E},-1,d}(\bar{\mathbb{F}}_p)$ (resp. $\mathrm{E}_{\mathrm{M},A,1}(\bar{\mathbb{F}}_p)$) [1, Def. 5.5.12]. Following [1, Def. 5.5.1], rewrite ϕ as

$$\mathrm{E}_{\mathrm{E},-1,d} \to \mathbb{P}^2,\ (x, y) \to (U\colon V\colon W) = \left(-xy^2\colon -sy(x^2 - y^2 + 2)\colon x^3\right),$$

from which it is easy to verify that there are no points in $\mathrm{E}_{\mathrm{E},-1,d}(\bar{\mathbb{F}}_p)$ that map to $(0\colon 0\colon 0)$ under ϕ, so ϕ is a morphism. Similarly, we rewrite $\hat{\phi}$ as

$$\begin{aligned}
&\mathrm{E}_{\mathrm{M},A,1} \to \mathbb{P}^2,\quad (u, v) \to (X\colon Y\colon Z),\\
&\quad X = (4sv(u - 1)(u + 1)(-u^4 + 2uv^2 + 2Au + 4u^2 + 1),\\
&\quad Y = (u^2 + 2v - 1)(u^2 - 2v - 1)(u^4 - 2u^2 + 4v^2 + 1),\\
&\quad Z = (u^4 - 2u^2 + 4v^2 + 1)(-u^4 + 2uv^2 + 2Au + 4u^2 + 1)),
\end{aligned}$$

from which one can verify that there are no points in $\mathrm{E}_{\mathrm{M},A,1}$ that map to $(0\colon 0\colon 0)$ under $\hat{\phi}$, so $\hat{\phi}$ is a morphism as well.

12 March 2015

Following [1, Def. 9.6.1], ϕ maps the neutral element $\mathcal{O}_{\mathrm{E}_{\mathrm{E},-1,d}} = (0,1)$ to the point at infinity $\mathcal{O}_{\mathrm{E}_{\mathrm{M},A,1}} = (0\colon 1\colon 0)$, so ϕ is an *isogeny*. For $\hat{\phi}$, we homogenize $\mathrm{E}_{\mathrm{M},A,1}$ under $u = U/W^2$ and $v = V/W^3$, so that $\mathcal{O}_{\mathrm{E}_{\mathrm{M},A,1}} = (\lambda^2\colon \lambda^3\colon 0)$ for $\lambda \in \mathbb{F}_p \setminus \{0\}$ and $\hat{\phi} : (U\colon V\colon W) \mapsto (X\colon Y\colon Z)$, where

$$\begin{aligned}
X &= ((4sVW(-W^4+U^2))(2AUW^6+W^8+4U^2W^4-U^4+2UV^2),\\
Y &= (-W^4+U^2+2VW)(-W^4+U^2-2VW)(W^8-2U^2W^4+U^4+4V^2W^2),\\
Z &= (W^8-2U^2W^4+U^4+4V^2W^2)(2AUW^6+W^8+4U^2W^4-U^4+2UV^2)),
\end{aligned}$$

takes $(\lambda^2\colon \lambda^3\colon 0)$ to $(0\colon 1\colon 1)$. Thus, $\hat{\phi}(\mathcal{O}_{\mathrm{E}_{\mathrm{M},A,1}}) = \mathcal{O}_{\mathrm{E}_{\mathrm{E},-1,d}}$, so $\hat{\phi}$ is an isogeny.

It remains to show that ϕ is a 4-isogeny and that $\hat{\phi}$ is its dual. To describe the full kernel of ϕ, we follow [1, p. 173] and use the non-singular projective variety $V_{-1,d} : \{-X^2+Y^2-Z^2-dT^2, ZT-XY\}$, as well as the corresponding homogenized version of ϕ, which is given as

$$(T:X:Y:Z) \mapsto (-XY^2 : \ -sY(X^2-Y^2+2Z^2) : \ X^3).$$

The full kernel of ϕ is the set of points $\{(0:0:1:1), (0:0:-1:1), (1:0:\sqrt{d}:0), (1:0:-\sqrt{d}:0)\}$, all points of order dividing 4, which shows that ϕ is a 4-isogeny. It is a simple exercise to verify that $\hat{\phi}\circ\phi = [4]$ on $\mathrm{E}_{\mathrm{E},-1,d}$, so $\hat{\phi}$ is indeed *the dual isogeny* [1, Thm. 9.6.21 and Def. 9.6.23]. □

Proposition 2. *Let* $p \equiv 3 \pmod 4$. *Let* $A = -(4d-2)$. *Then, the map*

$$\phi : \mathrm{E}_{\mathrm{E},1,d} \to \mathrm{E}_{\mathrm{M},A,1}, \ (x,y) \mapsto (u,v) = \left(\frac{y^2}{x^2}, \frac{-y(x^2+y^2-2)}{x^3}\right)$$

is a 4*-isogeny defined over* $\mathbb{F}_p$ *with dual isogeny*

$$\hat{\phi} : \mathrm{E}_{\mathrm{M},A,1} \to \mathrm{E}_{\mathrm{E},1,d}, (u,v) \mapsto (x,y) = \left(\frac{-4(1-u^2)v}{u^4-2u^2+4v^2+1}, \frac{(u^2+2v-1)(u^2-2v-1)}{2Au^3+u^4+2Au+6u^2+1}\right).$$

Proof. The proof proceeds in a similar way as the proof of Proposition 1. Again, it can be verified by direct calculations that $(u,v) = \phi(x,y)$ satisfies the curve equation $v^2 = u^3+Au^2+u$ and that $(x,y) = \hat{\phi}(u,v)$ satisfies $x^2+y^2 = 1+dx^2y^2$, using the respective curve equations of $\mathrm{E}_{\mathrm{E},1,d}$ and $\mathrm{E}_{\mathrm{M},A,1}$. This shows that ϕ and $\hat{\phi}$ are *rational maps* [1, Def. 5.5.1].

To show that ϕ is regular everywhere, we rewrite it as

$$\mathrm{E}_{\mathrm{E},1,d} \to \mathbb{P}^2 \,,\ (x,y) \to (U\colon V\colon W) = \left(xy^2\colon \ -y(x^2+y^2-2)\colon x^3\right),$$

from which it is straightforward to deduce that there are no points in $\mathrm{E}_{\mathrm{E},1,d}(\bar{\mathbb{F}}_p)$ that map to $(0\colon 0\colon 0)$ under ϕ. Similarly, to show that $\hat{\phi}$ is regular everywhere we rewrite it as

$$\begin{aligned}
&\mathrm{E}_{\mathrm{M},A,1} \to \mathbb{P}^2, \quad (u,v) \to (X\colon Y\colon Z),\\
&\quad X = -(4(-u^2+1))v(2Au^3+u^4+2Au+6u^2+1),\\
&\quad Y = (u^2+2v-1)(u^2-2v-1)(u^4-2u^2+4v^2+1),\\
&\quad Z = (2Au^3+u^4+2Au+6u^2+1)(u^4-2u^2+4v^2+1),
\end{aligned}$$

from which it is again straightforward to deduce that no points in $\mathrm{E}_{\mathrm{M},A,1}(\bar{\mathbb{F}}_p)$ map to $(0\colon 0\colon 0)$ under $\hat{\phi}$. Thus, ϕ and $\hat{\phi}$ are both regular everywhere, so they are both morphisms [1, Def. 5.5.12].

Following [1, Def. 9.6.1], ϕ maps the neutral element $\mathcal{O}_{\mathrm{E}_{\mathrm{E},1,d}} = (0,1)$ to the point at infinity $\mathcal{O}_{\mathrm{E}_{\mathrm{M},A,1}} = (0\colon 1\colon 0)$, so ϕ is an *isogeny*. For $\hat{\phi}$, we again homogenize $\mathrm{E}_{\mathrm{M},A,1}$ under $u = U/W^2$ and $v = V/W^3$, so that $\mathcal{O}_{\mathrm{E}_{\mathrm{M},A,1}} = (\lambda^2\colon \lambda^3\colon 0)$ for $\lambda \in \mathbb{F}_p \setminus \{0\}$ and $\hat{\phi} : (U\colon V\colon W) \mapsto (X\colon Y\colon Z)$, where

$$\begin{aligned}
X &= 4W(-W^2+U)(W^2+U)V(2AUW^6+W^8+2AU^3W^2+6U^2W^4+U^4),\\
Y &= (-W^4+U^2+2VW)(-W^4+U^2-2VW)(W^8-2U^2W^4+U^4+4V^2W^2),\\
Z &= (2AUW^6+W^8+2AU^3W^2+6U^2W^4+U^4)(W^8-2U^2W^4+U^4+4V^2W^2),
\end{aligned}$$

takes $(\lambda^2\colon \lambda^3\colon 0)$ to $(0\colon 1\colon 1)$. Thus, $\hat{\phi}(\mathcal{O}_{\mathrm{E}_{\mathrm{M},A,1}}) = \mathcal{O}_{\mathrm{E}_{\mathrm{E},1,d}}$, so $\hat{\phi}$ is an isogeny.

It remains to show that ϕ is a 4-isogeny and that $\hat{\phi}$ is its dual. As in the proof of Proposition 1, we again follow [1, p. 173] and use the non-singular projective variety $V_{1,d}$: $\{X^2+Y^2-Z^2-dT^2, ZT-XY\}$, as well as the corresponding homogenized version of ϕ, which is given as

$$(T : X : Y : Z) \mapsto (XY^2 :\ -Y(X^2+Y^2-2Z^2) :\ X^3).$$

The kernel of ϕ is $\{(0:0:1:1), (0:0:-1:1), (1:0:\sqrt{d}:0), (1:0:-\sqrt{d}:0)\}$, all points of order dividing 4, which shows that ϕ is a 4-isogeny. Again, one can verify that $\hat{\phi} \circ \phi = [4]$ on $\mathrm{E}_{\mathrm{E},1,d}$, so $\hat{\phi}$ is indeed *the dual isogeny* [1, Thm. 9.6.21 and Def. 9.6.23]. □

References

1. Steven D Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, 2012.