

# Fast tripling on Hessian Kummer lines

Thomas Decru & Sabrina Kunzweiler

June 19th, 2025

# Elliptic curve cryptography

- With ECC in mind, people were looking at finding the most efficient ways to compute on elliptic curves
- Montgomery ladder with double-and-add is very efficient!

# Elliptic curve cryptography

- With ECC in mind, people were looking at finding the most efficient ways to compute on elliptic curves
- Montgomery ladder with double-and-add is very efficient!
- Montgomery forms/curves/standard use, e.g. Curve25519:

$$E/\mathbb{F}_{2^{255}-19} : y^2 = x^3 + 486662x^2 + x$$

- Typically projectively to avoid inversions

- General Weierstraß equation:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

- Assuming  $\text{char}(k) \neq 2, 3$ , this simplifies to:

$$E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

- General Weierstraß equation:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

- Assuming  $\text{char}(k) \neq 2, 3$ , this simplifies to:

$$E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

- (Twisted) Montgomery curve:

$$bY^2Z = X^3 + aX^2Z + XZ^2$$

- Edwards curves, Huff curves, etc

## Definition

A twisted Hessian curve  $\mathcal{H}_{a,d}/k$  (with  $\text{char}(k) \neq 2, 3$ ) is a projective elliptic curve defined by the polynomial

$$aX^3 + Y^3 + Z^3 = 3dXYZ,$$

where  $a(d^3 - a) \neq 0$  and  $(0 : -1 : 1)$  is the neutral element.

## Definition

A twisted Hessian curve  $\mathcal{H}_{a,d}/k$  (with  $\text{char}(k) \neq 2, 3$ ) is a projective elliptic curve defined by the polynomial

$$aX^3 + Y^3 + Z^3 = 3dXYZ,$$

where  $a(d^3 - a) \neq 0$  and  $(0 : -1 : 1)$  is the neutral element.

- Factor  $3d$  vs  $d$ ?

## Definition

A twisted Hessian curve  $\mathcal{H}_{a,d}/k$  (with  $\text{char}(k) \neq 2, 3$ ) is a projective elliptic curve defined by the polynomial

$$aX^3 + Y^3 + Z^3 = 3dXYZ,$$

where  $a(d^3 - a) \neq 0$  and  $(0 : -1 : 1)$  is the neutral element.

- Factor  $3d$  vs  $d$ ?
- Untwisted Hessian curve:  $a = 1$
- Twisted Hessian normal form:  $d = 1$

## Definition

A twisted Hessian curve  $\mathcal{H}_{a,d}/k$  (with  $\text{char}(k) \neq 2, 3$ ) is a projective elliptic curve defined by the polynomial

$$aX^3 + Y^3 + Z^3 = 3dXYZ,$$

where  $a(d^3 - a) \neq 0$  and  $(0 : -1 : 1)$  is the neutral element.

- Factor  $3d$  vs  $d$ ?
- Untwisted Hessian curve:  $a = 1$
- Twisted Hessian normal form:  $d = 1$
- $d = 0$  is not excluded

# Hessian group law

Let  $P_1, P_2 \in \mathcal{H}_{a,d}$ , with  $P_i = (X_i : Y_i : Z_i)$ , then

- $P_1 + P_2$  is given by

$$(X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1 : Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1 : Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1),$$

# Hessian group law

Let  $P_1, P_2 \in \mathcal{H}_{a,d}$ , with  $P_i = (X_i : Y_i : Z_i)$ , then

- $P_1 + P_2$  is given by

$$(X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1 : Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1 : Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1),$$

- unless this fails, then it's

$$(Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2 : Y_2^2 Y_1 Z_1 - X_1^2 X_2 Z_2 : X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2),$$

# Hessian group law

Let  $P_1, P_2 \in \mathcal{H}_{a,d}$ , with  $P_i = (X_i : Y_i : Z_i)$ , then

- $P_1 + P_2$  is given by

$$(X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1 : Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1 : Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1),$$

- unless this fails, then it's

$$(Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2 : Y_2^2 Y_1 Z_1 - X_1^2 X_2 Z_2 : X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2),$$

- and  $-P_1$  is given by

$$(X_1 : Z_1 : Y_1)$$

Consider

$$\begin{aligned}\pi : \mathcal{H}_{a,d} &\rightarrow \mathcal{H}_{a,d}/\langle \pm 1 \rangle \\ (X : Y : Z) &\mapsto (X : U) := (X : Y + Z)\end{aligned}$$

We will call  $\mathcal{H}_{a,d}/\langle \pm 1 \rangle$  the twisted Hessian Kummer line and denote it by  $\mathcal{HK}_{a,d}$ .

## Proposition

Let  $E$  be an elliptic curve in Weierstraß form defined over some field  $k$  and  $E[3] = \langle P_1, P_2 \rangle$ . Let  $x_1, x_2, x_3$  be the  $x$ -coordinates of  $P_1, P_2$  and  $P_1 + P_2$ , respectively. Then

$$T = \begin{pmatrix} -(x_1 - x_3) & x_2(x_1 - x_3) \\ (x_1 + (\omega - 1)x_2 - \omega x_3) & -(\omega x_1 x_2 + (-\omega + 1)x_1 x_3 - x_2 x_3) \end{pmatrix}$$

describes the coordinate transformation

$$\begin{aligned} \theta : E / \langle \pm 1 \rangle &\rightarrow \mathcal{HK}_{1,d} \\ P &\mapsto T \cdot P, \end{aligned}$$

where  $\omega$  is a cubic root of unity.

## Proposition

*We have that*

$$\mathcal{H}_{a,d}[3] = \langle (0 : -\omega : 1), (1 : -\alpha : 0) \rangle,$$

*with  $\alpha^3 = a$ , and consequently  $(X : Y : Z) \in \mathcal{H}_{a,d}[3]$  iff  $XYZ = 0$ .*

# Hessian 3-isogenies part 1

## Proposition

The isogeny  $\phi_1 : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_1,d_1}$  with  $\ker \phi_1 = \langle (0 : -\omega : 1) \rangle$  is given by  $(X : Y : Z) \mapsto$

$$(XYZ : aX^3 + \omega^2 Y^3 + \omega Z^3 : aX^3 + \omega Y^3 + \omega^2 Z^3),$$

where  $a_1 = 27(d^3 - a)$  and  $d_1 = 3d$ .

# Hessian 3-isogenies part 1

## Proposition

The isogeny  $\phi_1 : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_1,d_1}$  with  $\ker \phi_1 = \langle (0 : -\omega : 1) \rangle$  is given by  $(X : Y : Z) \mapsto$

$$(XYZ : aX^3 + \omega^2 Y^3 + \omega Z^3 : aX^3 + \omega Y^3 + \omega^2 Z^3),$$

where  $a_1 = 27(d^3 - a)$  and  $d_1 = 3d$ .

The isogeny  $\phi_2 : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_2,d_2}$  with  $\ker \phi_2 = \langle (1 : -\alpha : 0) \rangle$  is given by  $(X : Y : Z) \mapsto$

$$(XYZ : \alpha^2 X^2 Z + \alpha XY^2 + YZ^2 : \alpha^2 X^2 Y + \alpha XZ^2 + Y^2 Z),$$

where  $\alpha^3 = a$ ,  $a_2 = 9(\alpha d^2 + \alpha^2 d + a)$  and  $d_2 = d + 2\alpha$ .

# Hessian 3-isogenies part 2

## Proposition

The isogeny  $\phi_3 : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_3,d_3}$  with  $\ker \phi_3 = \langle (-\omega : 1 : 0) \rangle$  is given by  $(X : Y : Z) \mapsto$

$$(XYZ : \omega\alpha^2 X^2 Z + \omega^2 \alpha XY^2 + YZ^2 : \omega\alpha^2 X^2 Y + \omega^2 \alpha XZ^2 + Y^2 Z),$$

where  $\alpha^3 = a$ ,  $a_3 = 9(\omega^2 \alpha d^2 + \omega \alpha^2 d + a)$  and  $d_3 = \omega^2 d + 2\omega \alpha$ .

The isogeny  $\phi_4 : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_4,d_4}$  with  $\ker \phi_4 = \langle (1 : -\omega : 0) \rangle$  is given by  $(X : Y : Z) \mapsto$

$$(XYZ : \omega^2 \alpha^2 X^2 Z + \omega \alpha XY^2 + YZ^2 : \omega^2 \alpha^2 X^2 Y + \omega \alpha XZ^2 + Y^2 Z),$$

where  $\alpha^3 = a$ ,  $a_4 = 9(\omega \alpha d^2 + \omega^2 \alpha^2 d + a)$  and  $d_4 = \omega d + 2\omega^2 \alpha$ .

## Proposition

The isogenies  $\phi_i : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_i,d_i}$ , with  $i \in \{1, 2\}$  induce “isogenies”  $\varphi_i : \mathcal{HK}_{a,d} \rightarrow \mathcal{HK}_{a_i,d_i}$  which are given by

$$\varphi_1 : (X : U) \mapsto (aX^3 + U^3 : 3d(2aX^3 - U^3) + 9aX^2U)$$

$$\varphi_2 : (X : U) \mapsto (X(\alpha^2 X^2 - \alpha XU + U^2) : \\ -2aX^3 + 3\alpha(\alpha + d)X^2U + U^3),$$

# Hessian Kummer line 3-isogenies

## Proposition

The isogenies  $\phi_i : \mathcal{H}_{a,d} \rightarrow \mathcal{H}_{a_i,d_i}$ , with  $i \in \{1, 2\}$  induce “isogenies”  $\varphi_i : \mathcal{HK}_{a,d} \rightarrow \mathcal{HK}_{a_i,d_i}$  which are given by

$$\varphi_1 : (X : U) \mapsto (aX^3 + U^3 : 3d(2aX^3 - U^3) + 9aX^2U)$$

$$\varphi_2 : (X : U) \mapsto (X(\alpha^2 X^2 - \alpha XU + U^2) : \\ -2aX^3 + 3\alpha(\alpha + d)X^2U + U^3),$$

## Proof.

- $dX + Y + Z = 0$  iff  $(X : Y : Z) = (0 : -1 : 1)$
- $YZ = \frac{aX^3 + U^3}{3(dX + U)}$



# Hessian Kummer line 3-isogenies efficiently

## Proposition

Define the following maps:

- $C_a : (X : U) \mapsto (aX^2(U + dX) : U(dU^2 - aX^2))$
- $M : (X : U) \mapsto (X + U : 2X - U)$
- $\mu_{x,u} : (X : U) \mapsto (xX : uU)$ .

Then

$$\varphi_1(X : U) = \mu_{1,3d} \circ M \circ C_a(X : U),$$

$$\varphi_2(X : U) = \mu_{1,3(d-\alpha)^3} \circ M \circ C_a \circ M \circ \mu_{\alpha,1}(X : U).$$

# Hessian Kummer line 3-isogenies efficiently

## Proposition

Define the following maps:

- $C_a : (X : U) \mapsto (aX^2(U + dX) : U(dU^2 - aX^2))$
- $M : (X : U) \mapsto (X + U : 2X - U)$
- $\mu_{x,u} : (X : U) \mapsto (xX : uU)$ .

Then

$$\varphi_1(X : U) = \mu_{1,3d} \circ M \circ C_a(X : U),$$

$$\varphi_2(X : U) = \mu_{1,3(d-\alpha)^3} \circ M \circ C_a \circ M \circ \mu_{\alpha,1}(X : U).$$

Multiplication-by-3 on  $\mathcal{HK}_{a,d}$  is given by  $\widehat{\varphi}_1 \circ \varphi_1!$

# Hessian Kummer line tripling

---

**Algorithm 1** Tripling on the Kummer line  $\mathcal{HK}_{a,1}$  in twisted Hessian normal form

---

**Require:**  $\overline{P} = (x : u)$  on  $\mathcal{HK}_{a,1}$ .

**Ensure:**  $\overline{3 \cdot P}$ .

1:  $s, t \leftarrow a \cdot x^2, u^2$  ▷  $1M_a + 2S$

2:  $x_1, u_1 \leftarrow s \cdot (u + x), u \cdot (t - s)$  ▷  $2M$

3:  $x_2, u_2 \leftarrow x_1 + u_1, 2x_1 - u_1$

4:  $s', t' \leftarrow (1 - a) \cdot x_2^2, u_2^2$  ▷  $1M_a + 2S$

5:  $x_3, u_3 \leftarrow s' \cdot (u_2 + x_2), u_2 \cdot (t' - s')$  ▷  $2M$

6:  $x_4, u_4 \leftarrow x_3 + u_3, 2x_3 - u_3$

7: **return**  $(x_4 : u_4)$  ▷ Total Cost:  $4M + 4S + 1M_a$

---

# Hessian Kummer line tripling

For well chosen curve parameters (i.e.  $d = 1$  and  $a$  is small), the cost of tripling on  $\mathcal{HK}_{a,1}$  is  $4\mathbf{M} + 4\mathbf{S}$ .

Previous state-of-the-art was

- $4\mathbf{M} + 8\mathbf{S}$  on Hessian curves
- $4\mathbf{M} + 6\mathbf{S}$  on Hessian curves iff multiplication-by- $\omega$  is cheap
- $5\mathbf{M} + 5\mathbf{S}$  on Montgomery Kummer lines

Where do these efficient maps come from? If we lift back to  $\mathcal{H}_{a,d}$  instead of  $\mathcal{HK}_{a,d}$  they are

- $C_a$ : Coordinate-wise cubing; i.e.  
 $C_a(X : Y : Z) = (aX^3 : Y^3 : Z^3)$
- $M$ : Discrete Fourier transform; i.e.

$$M(X : Y : Z) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

- $\mu_{x,y}$ : Scaling; i.e.  $\mu_{x,u}(X : Y : Z) = (xX : uY : uZ)$

# Action of 3-torsion

For  $(X : Y : Z) \in \mathcal{H}_{1,d}$ , we have

$$(X : Y : Z) + (-1 : 1 : 0) = (Y : Z : X)$$

and

$$(X : Y : Z) + (0 : -\omega : 1) = (\omega^2 X : \omega Y : Z)$$

and...

# Hessian ladder?

- Montgomery arithmetic uses double-and-add and works with bits

# Hessian ladder?

- Montgomery arithmetic uses double-and-add and works with bits
- Hessian ladder would use triple-and-add-or-subtract and work with trits?
- The difference between bits and trits gives us a factor  $\log_2 3$  to play with.

# Hessian ladder?

- Montgomery arithmetic uses double-and-add and works with bits
- Hessian ladder would use triple-and-add-or-subtract and work with trits?
- The difference between bits and trits gives us a factor  $\log_2 3$  to play with.
- Differential addition is not good enough (yet?)

---

**Algorithm 2** Differential addition on the Kummer line  $\mathcal{HK}_{a,d}$ 

---

**Require:**  $\overline{P} = (x_1 : u_1)$ ,  $\overline{Q} = (x_2 : u_2)$  and  $\overline{P - Q} = (x_3 : u_3) \neq (0 : 0)$  on  $\mathcal{HK}_{a,d}$ .

**Ensure:**  $\overline{P + Q}$ .

- 1:  $r_1, r_2, r_3, r_4 \leftarrow x_1 \cdot x_2, x_1 \cdot u_2, x_2 \cdot u_1, u_1 \cdot u_2$  ▷ 4M
  - 2:  $s_1 \leftarrow a \cdot r_1$  ▷ 1M<sub>a</sub>
  - 3:  $t_1, t_2, t_3, t_4 \leftarrow d \cdot r_1, d \cdot r_2, d \cdot r_3, d \cdot r_4$  ▷ 4M<sub>d</sub>
  - 4:  $t_5 \leftarrow (3d^2 - 2) \cdot r_1$  ▷ 1M<sub>d</sub>
  - 5:  $x'_4 \leftarrow -r_1 \cdot (s_1 - t_4) + r_3 \cdot (t_3 + r_4) + r_2 \cdot (t_2 + r_4)$  ▷ 3M
  - 6:  $u'_4 \leftarrow -2s_1 \cdot (t_1 + r_2 + r_3) - r_4 \cdot (t_2 + t_3 + t_5 + 2r_1 + r_4)$  ▷ 2M
  - 7:  $x_4, u_4 \leftarrow x_3 \cdot x'_4, u'_4 x_3 - u_3 x'_4$  ▷ 3M
  - 8: **return**  $(x_4 : u_4)$  ▷ Total Cost: 12M + 1M<sub>a</sub> + 5M<sub>d</sub>
-

# Efficient 3-isogenies on Hessian Kummer lines?

A chain of 3-isogenies can be done relatively cheaply at  $6\mathbf{M} + 4\mathbf{S}$  per step!

# Efficient 3-isogenies on Hessian Kummer lines?

A chain of 3-isogenies can be done relatively cheaply at  $6\mathbf{M} + 4\mathbf{S}$  per step!

- still slightly worse than Montgomery form 3-isogenies
- curve constants  $a, d$  change at every step so  $\mathbf{M}_a = \mathbf{M}_d = \mathbf{M}$
- problem: dual isogeny is always “easiest” so we need to base change at each step which costs  $2\mathbf{M}$

# Conclusion

- Montgomery curve arithmetic still wins on almost all fronts
- New state-of-the-art tripling costs at only  $4\mathbf{M} + 4\mathbf{S}$