Hyper-and-elliptic-curve cryptography

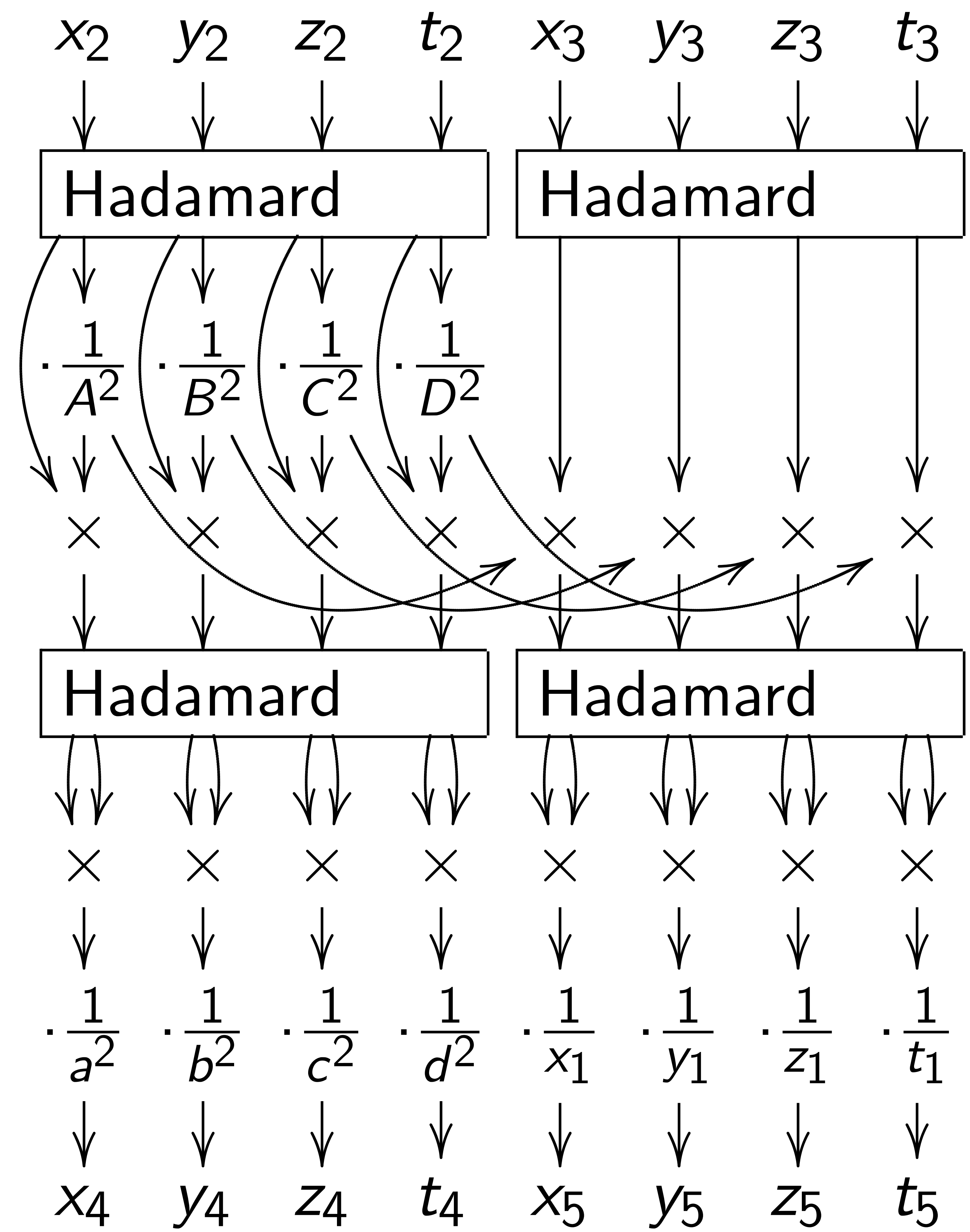
Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Joint work with: Tanja Lange
Technische Universiteit Eindhoven

cr.yp.to/papers.html#hyperand
(2014) + new examples (2015)

Rewind to 2012 Gaudry–Schost:
"the computation took
more than 1,000,000 CPU hours".

The Gaudry–Schost motivation:



nd-elliptic-curve

aphy

. Bernstein

ty of Illinois at Chicago &

che Universiteit Eindhoven

rk with: Tanja Lange

che Universiteit Eindhoven

to/papers.html#hyperand

+ new examples (2015)

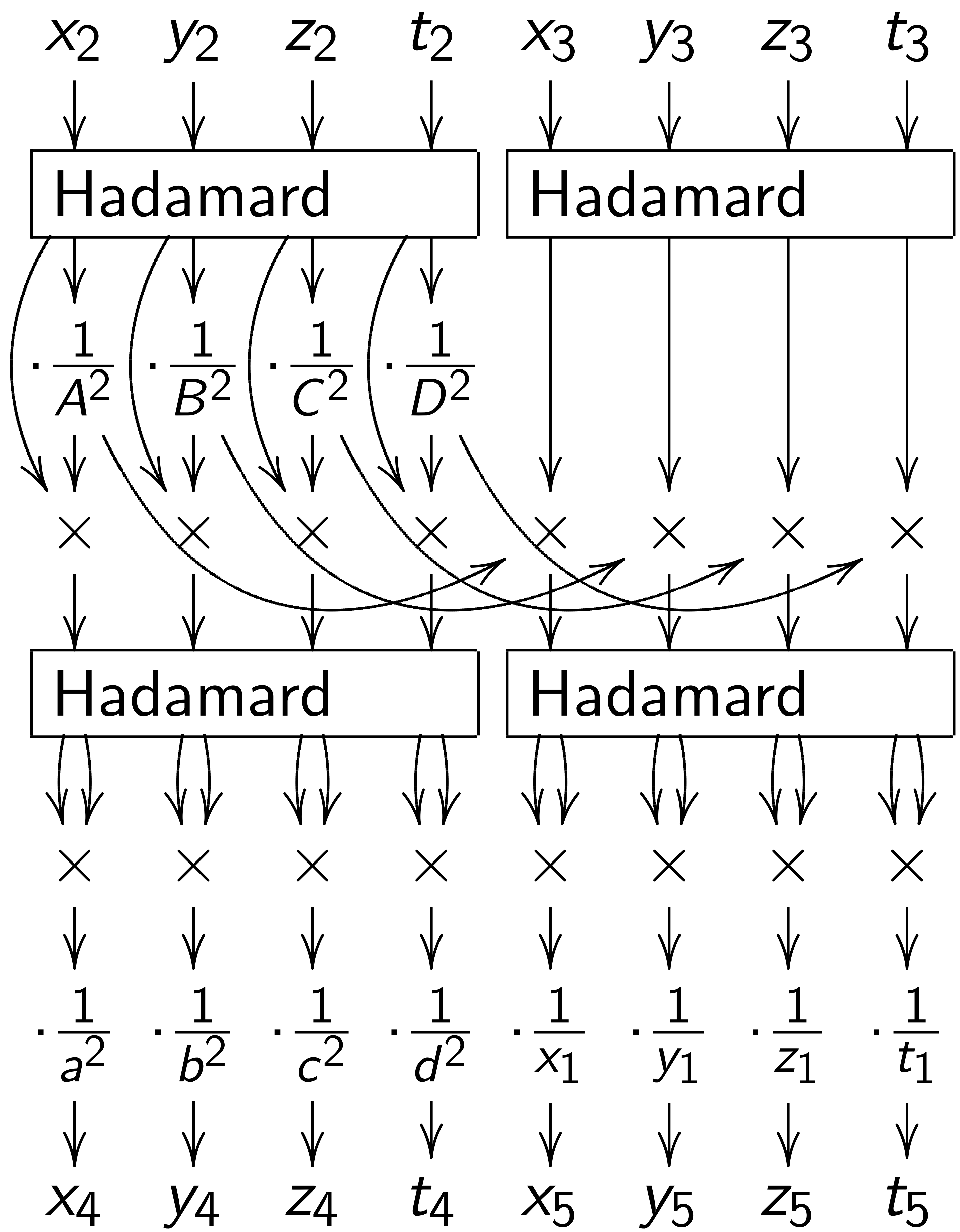
---

to 2012 Gaudry–Schost:

mputation took

an 1,000,000 CPU hours".

The Gaudry–Schost motivation:



Inputs:

$(x_2 : y_2 :$

$(x_3 : y_3 :$

$(x_1 : y_1 :$

This dia

$(x_4 : y_4 :$

$(x_5 : y_5 :$

-curve

n

is at Chicago &

siteit Eindhoven

Tanja Lange

siteit Eindhoven

s.html#hyperand

mples (2015)

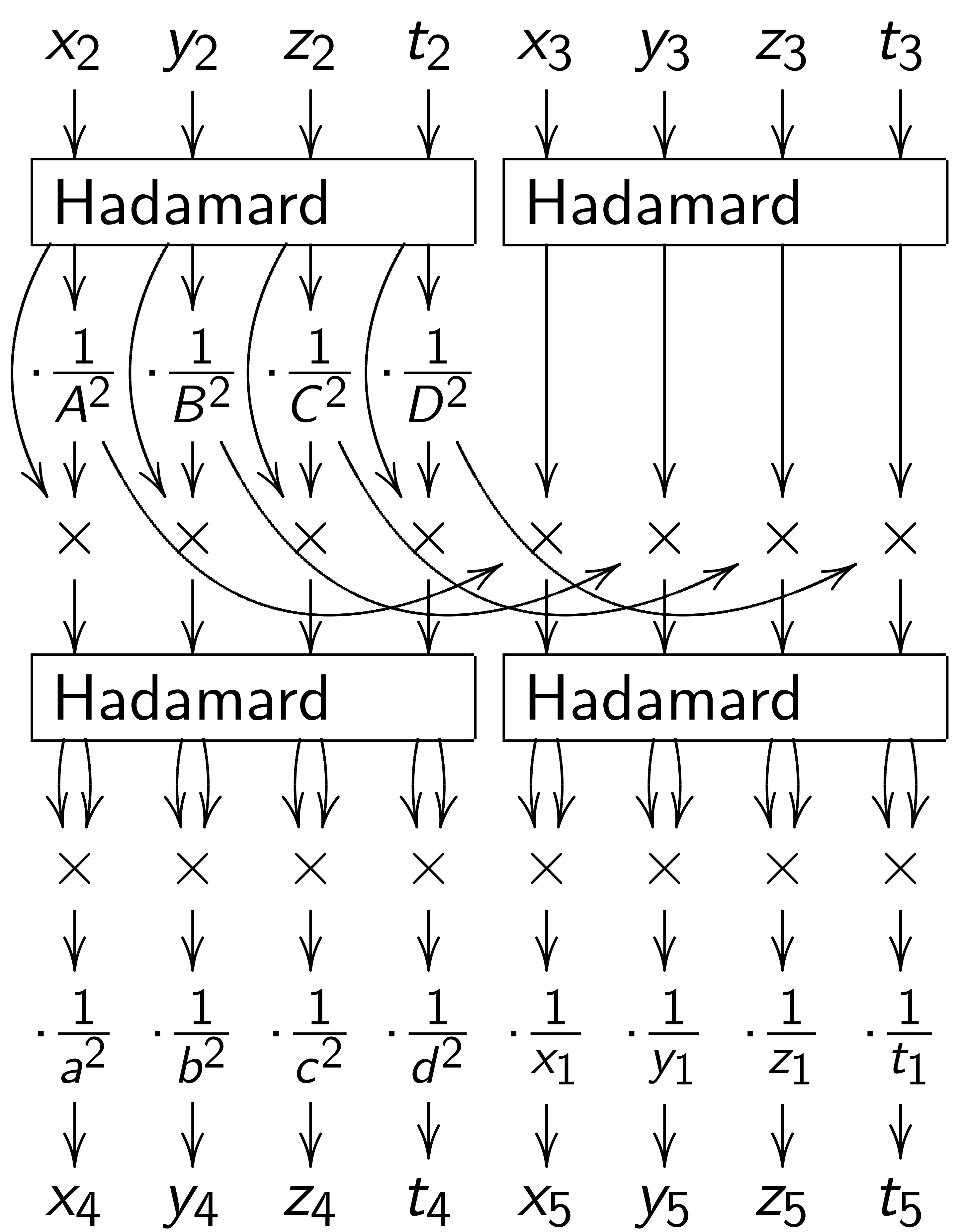
---

audry–Schost:

took

00 CPU hours”.

The Gaudry–Schost motivation:



Inputs: “squared 6

$(x_2 : y_2 : z_2 : t_2)$ for

$(x_3 : y_3 : z_3 : t_3)$ for

$(x_1 : y_1 : z_1 : t_1)$ for

This diagram com

$(x_4 : y_4 : z_4 : t_4)$ for

$(x_5 : y_5 : z_5 : t_5)$ for

ago &
hoven

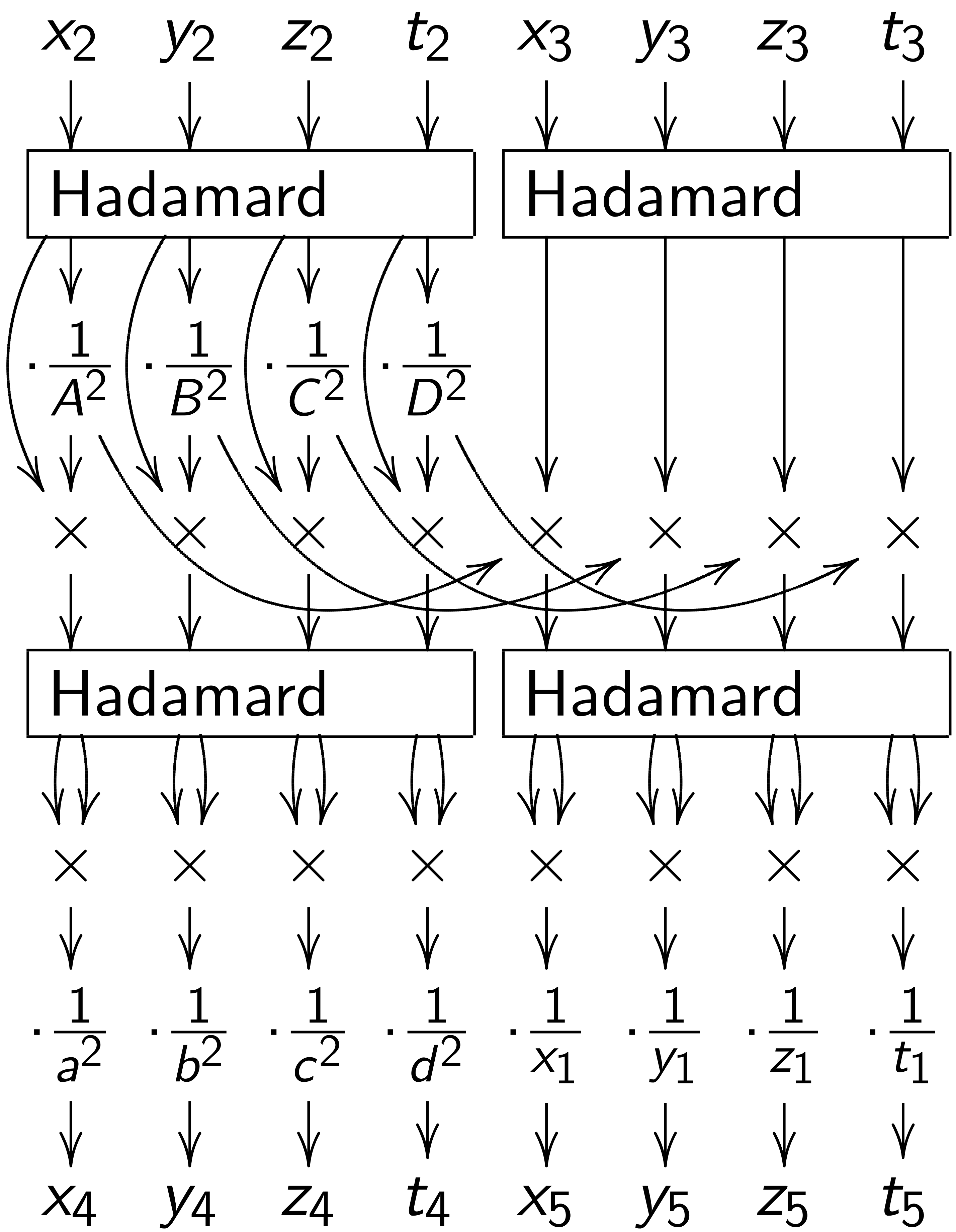
ge
hoven

yperand
15)

host:

ours".

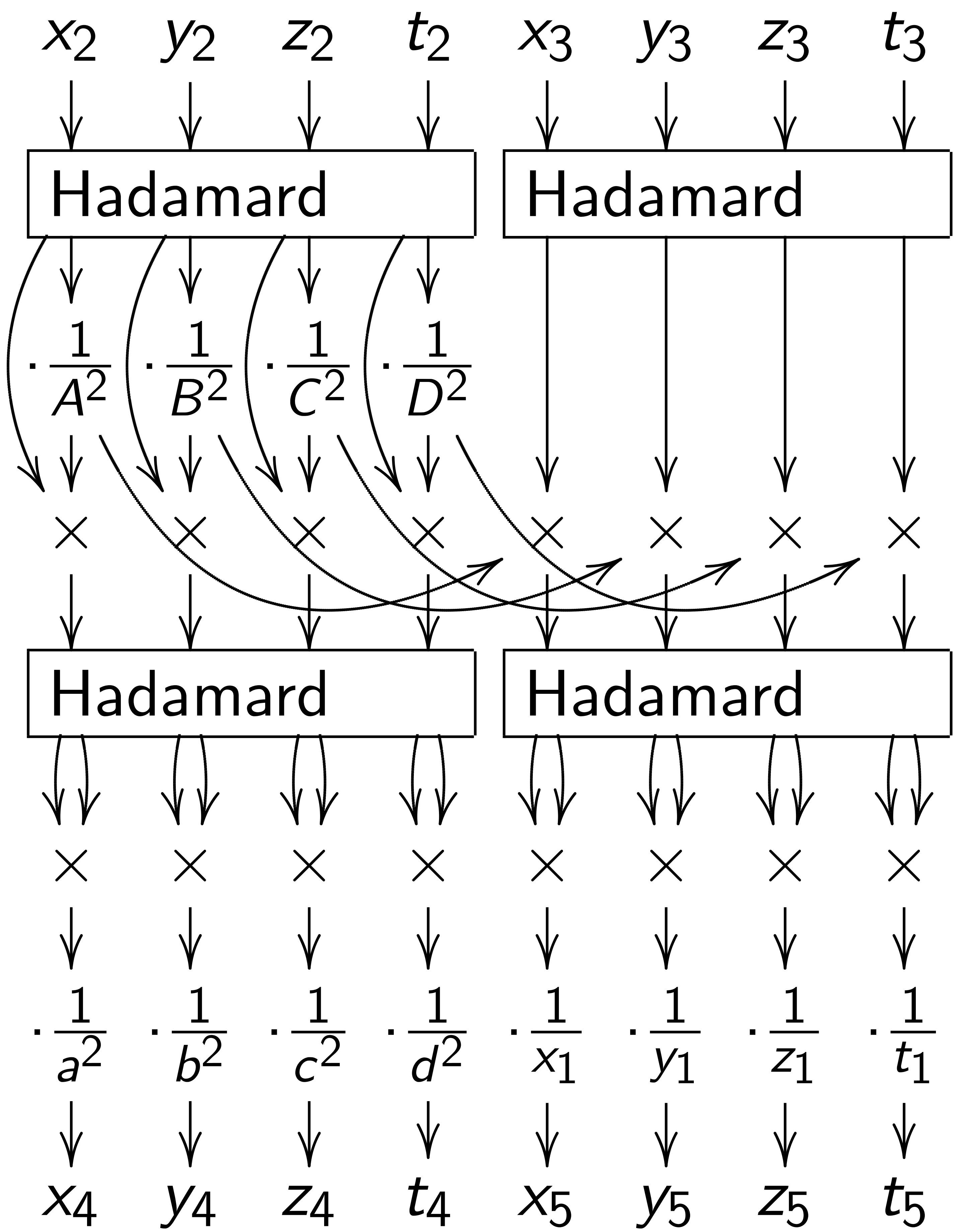
The Gaudry–Schost motivation:



Inputs: "squared θ coordina
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3$

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q$
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3$

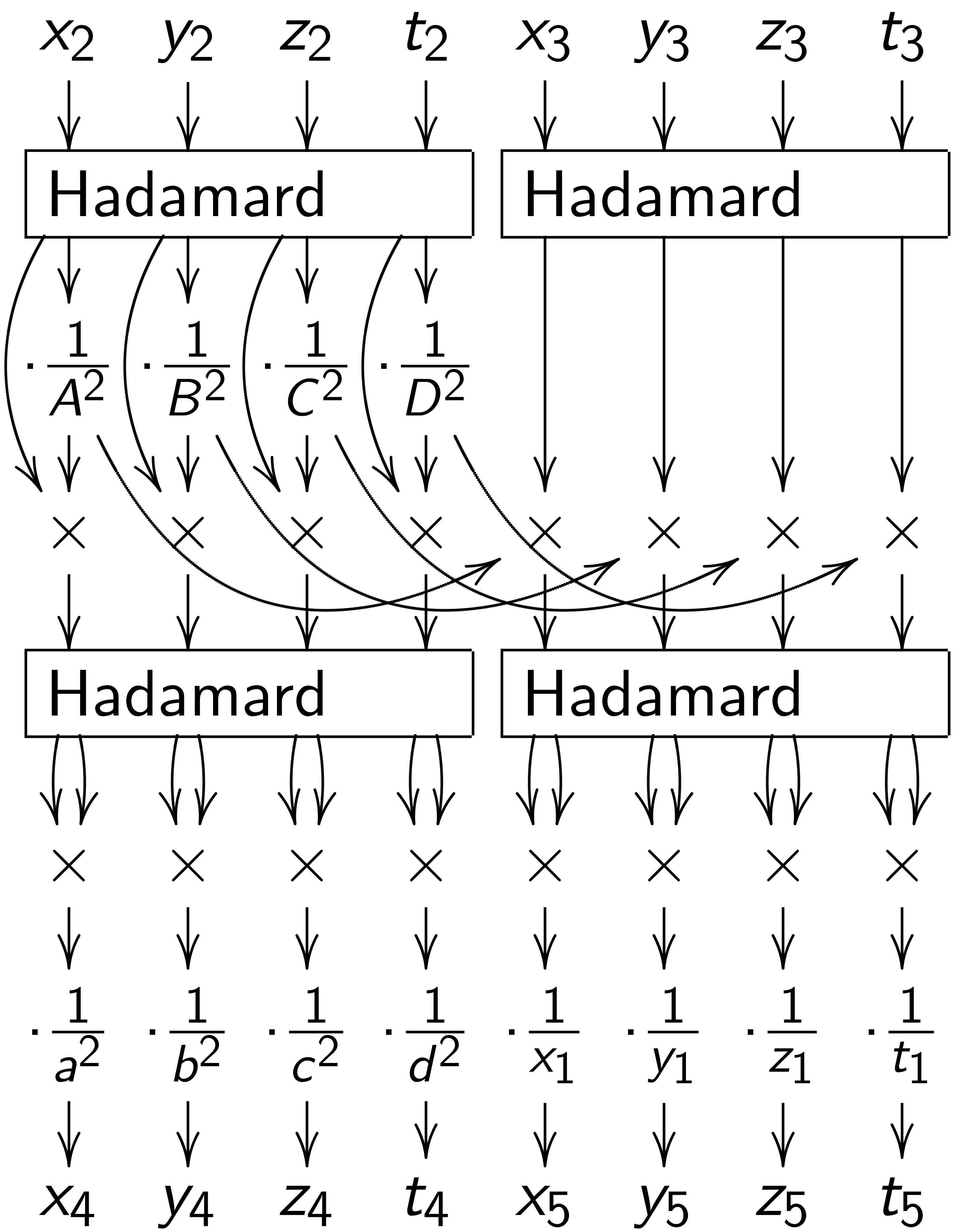
The Gaudry–Schost motivation:



Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

The Gaudry–Schost motivation:

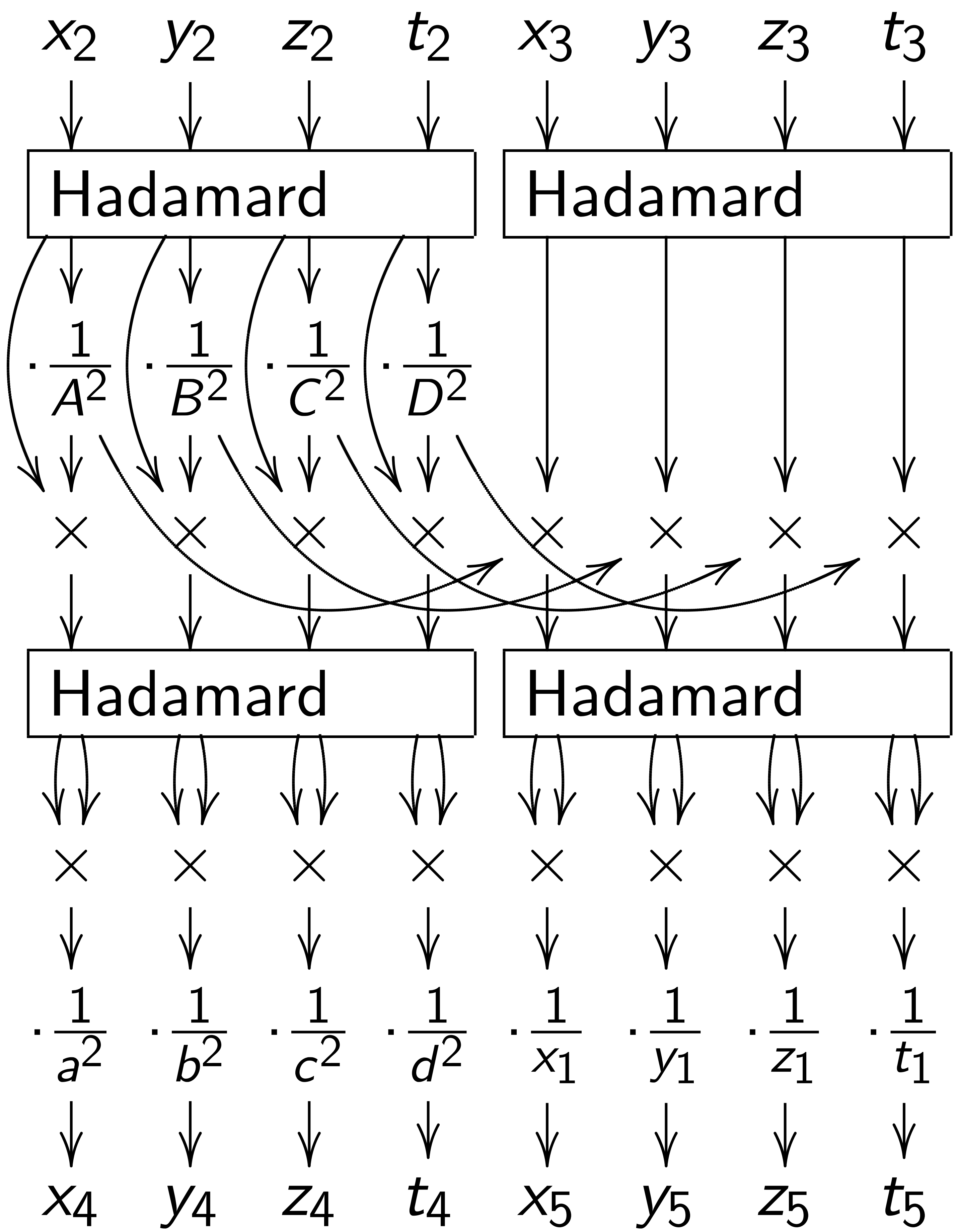


Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

The Gaudry–Schost motivation:



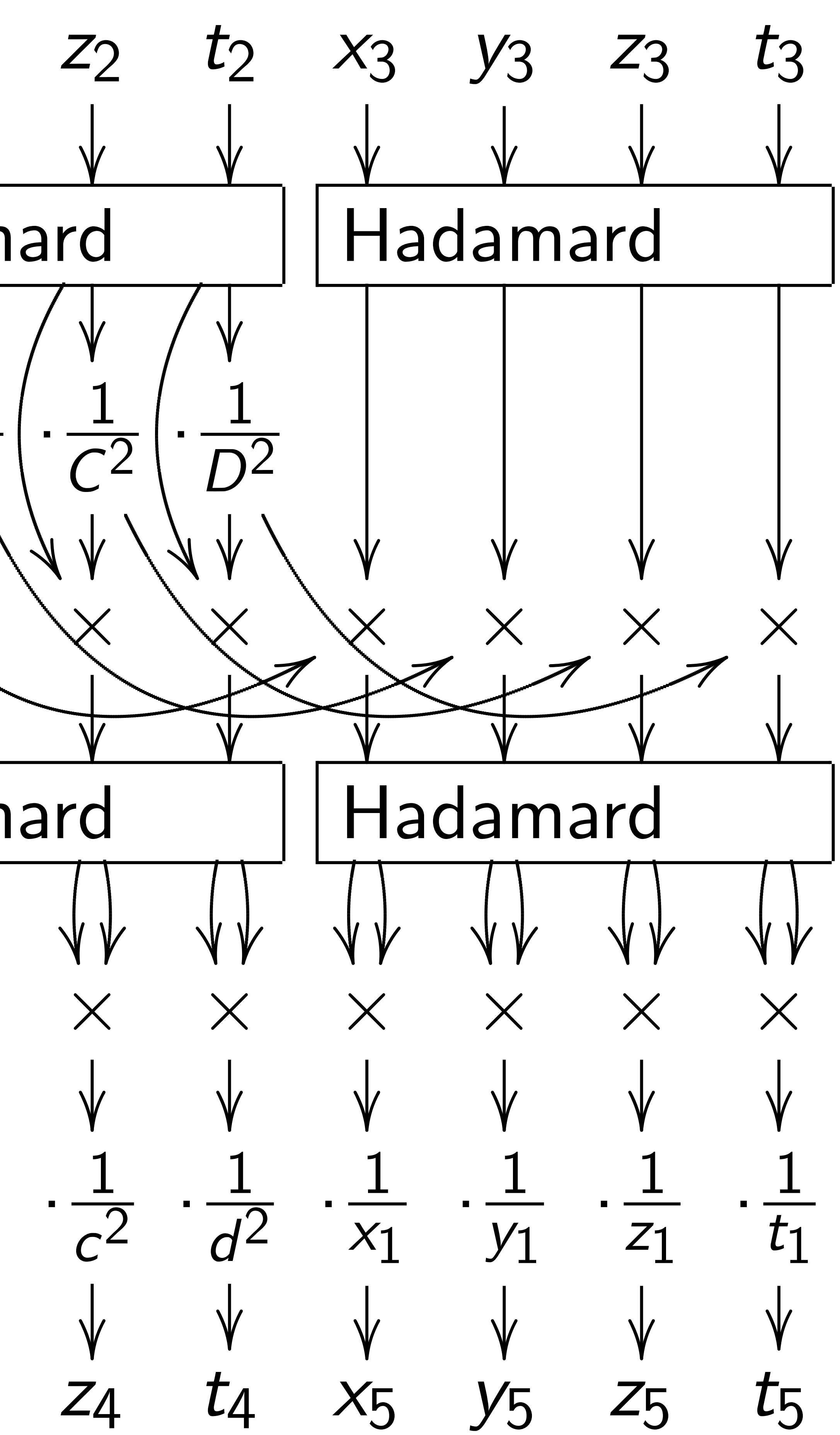
Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Just 25 mults for Q_4, Q_5
(2006 Gaudry) after Q_1 precomp.

udry–Schost motivation:



Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

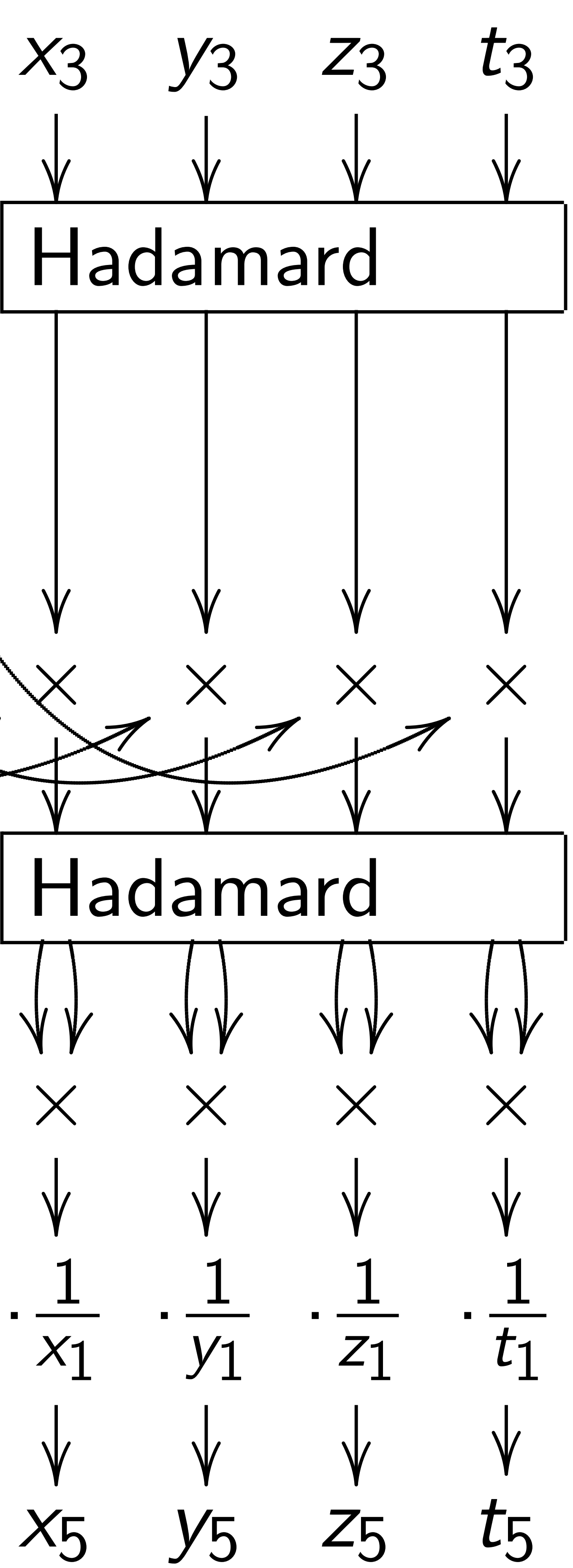
This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Just 25 mults for Q_4, Q_5
(2006 Gaudry) after Q_1 precomp.

$(x_i : y_i : z$
original
$4E^2xyz$
$-F$
$-H$
where
$A^2 = a^2$
$B^2 = a^2$
$C^2 = a^2$
$D^2 = a^2$
$F = (a^4$
$G = (a^4$
$H = (a^4$
$E^2 = F^2$

st motivation:



Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

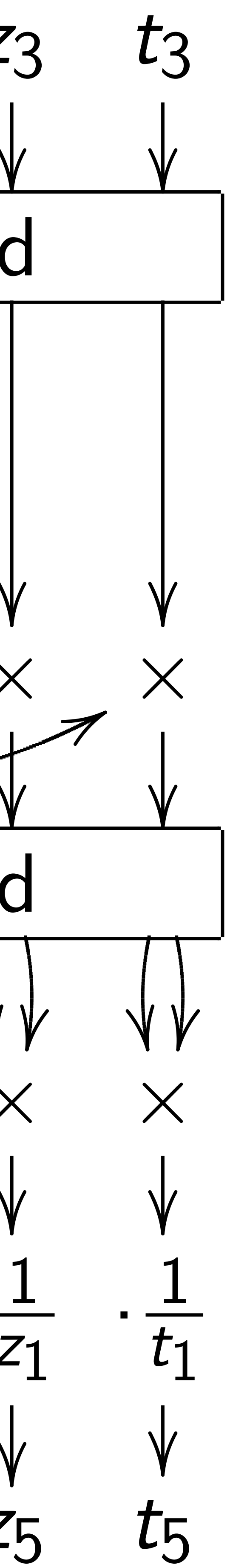
This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Just 25 mults for Q_4, Q_5
(2006 Gaudry) after Q_1 precomp.

$(x_i : y_i : z_i : t_i)$ are
original Kummer s
$4E^2xyzt = ((x^2 +$
$-F(xt + yz)$
$-H(xy + zt)$
where
$A^2 = a^2 + b^2 + c$
$B^2 = a^2 + b^2 - c$
$C^2 = a^2 - b^2 + c$
$D^2 = a^2 - b^2 - c$
$F = (a^4 - b^4 - c^4 +$
$G = (a^4 - b^4 + c^4 -$
$H = (a^4 + b^4 - c^4 -$
$E^2 = F^2 + G^2 +$

ion:



Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Just 25 mults for Q_4, Q_5
(2006 Gaudry) after Q_1 precomp.

$(x_i : y_i : z_i : t_i)$ are points on
original Kummer surface K
$4E^2xyzt = ((x^2 + y^2 + z^2$
$\quad -F(xt + yz) - G(xz +$
$\quad -H(xy + zt))^2$

where
$A^2 = a^2 + b^2 + c^2 + d^2$,
$B^2 = a^2 + b^2 - c^2 - d^2$,
$C^2 = a^2 - b^2 + c^2 - d^2$,
$D^2 = a^2 - b^2 - c^2 + d^2$,
$F = (a^4 - b^4 - c^4 + d^4)/(a^2 d^2$
$G = (a^4 - b^4 + c^4 - d^4)/(a^2 c^2$
$H = (a^4 + b^4 - c^4 - d^4)/(a^2 b^2$
$E^2 = F^2 + G^2 + H^2 + FGH$

Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Just 25 mults for Q_4, Q_5
(2006 Gaudry) after Q_1 precomp.

$(x_i : y_i : z_i : t_i)$ are points on
original Kummer surface K :

$$4E^2xyzt = ((x^2 + y^2 + z^2 + t^2) - F(xt + yz) - G(xz + yt) - H(xy + zt))^2$$

where

$A^2 = a^2 + b^2 + c^2 + d^2$,
$B^2 = a^2 + b^2 - c^2 - d^2$,
$C^2 = a^2 - b^2 + c^2 - d^2$,
$D^2 = a^2 - b^2 - c^2 + d^2$,
$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2)$,
$G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2)$,
$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2)$,
$E^2 = F^2 + G^2 + H^2 + FGH - 4$.

“squared θ coordinates”

$z_2 : t_2)$ for Q_2,

$z_3 : t_3)$ for Q_3,

$z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

gram computes

$z_4 : t_4)$ for $Q_4 = 2Q_2$,

$z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

mults for Q_4

hudnovsky–Chudnovsky).

eedup if constants

$: \frac{1}{c^2} : \frac{1}{d^2})$ etc. are small.

mults for Q_4, Q_5

audry) after Q_1 precomp.

$(x_i : y_i : z_i : t_i)$ are points on original Kummer surface K :

$$4E^2xyzt = ((x^2 + y^2 + z^2 + t^2) \\ -F(xt + yz) - G(xz + yt) \\ -H(xy + zt))^2$$

where

$A^2 = a^2 + b^2 + c^2 + d^2$,

$B^2 = a^2 + b^2 - c^2 - d^2$,

$C^2 = a^2 - b^2 + c^2 - d^2$,

$D^2 = a^2 - b^2 - c^2 + d^2$,

$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2)$,

$G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2)$,

$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2)$,

$E^2 = F^2 + G^2 + H^2 + FGH - 4$.

Surface

Über die

mit sech

Endlich

werden, welc

men kann. V

singulären Ta

als die Fundar

genen Coordir

teren durch r

chung:

10.,

wo

$\phi = p^2 +$

$K =$

in welcher die

auf die richtige

ist. Wählt m

Ausdrücke p,

ϑ coordinates"

Q_2,

Q_3,

$Q_1 = Q_3 - Q_2$.

putes

$Q_4 = 2Q_2$,

$Q_5 = Q_3 + Q_2$.

Q_4

y–Chudnovsky).

onstants

etc. are small.

Q_4, Q_5

er Q_1 precomp.

$(x_i : y_i : z_i : t_i)$ are points on original Kummer surface K :

$$4E^2xyzt = ((x^2+y^2+z^2+t^2) - F(xt+yz) - G(xz+yt) - H(xy+zt))^2$$

where

$$A^2 = a^2+b^2+c^2+d^2,$$
$$B^2 = a^2+b^2-c^2-d^2,$$
$$C^2 = a^2-b^2+c^2-d^2,$$
$$D^2 = a^2-b^2-c^2+d^2,$$
$$F = (a^4-b^4-c^4+d^4)/(a^2d^2-b^2c^2),$$
$$G = (a^4-b^4+c^4-d^4)/(a^2c^2-b^2d^2),$$
$$H = (a^4+b^4-c^4-d^4)/(a^2b^2-c^2d^2),$$
$$E^2 = F^2+G^2+H^2+FGH-4.$$

Surface is from 18

Über die Flächen

mit sechzehn singu

---

vom 18. *A*

Endlich möge hier noch
werden, welche man mit der G
men kann. Wählt man die vie
singulären Tangentialebenen

$p = 0, \; q = 0,$

als die Fundamentalebenen, also
genen Coordinaten, und bezeic
teren durch r und s, so erhält
chung:

10., $\phi^2 =$

wo

$\phi = p^2 + q^2 + r^2 + s^2 + 2a(q$

$K = a^2 + b^2 + c^2 - 2a$

in welcher die sieben Constante
auf die richtige Anzahl von drei C
ist. Wählt man in dieser For
Ausdrücke p, q, r, s real, und d

tes"

$- Q_2.$

^{2,}

$+ Q_2.$

vsky).

nall.

comp.

$(x_i : y_i : z_i : t_i)$ are points on original Kummer surface K :

$$4E^2xyzt = ((x^2 + y^2 + z^2 + t^2) - F(xt + yz) - G(xz + yt) - H(xy + zt))^2$$

where

$$A^2 = a^2 + b^2 + c^2 + d^2,$$
$$B^2 = a^2 + b^2 - c^2 - d^2,$$
$$C^2 = a^2 - b^2 + c^2 - d^2,$$
$$D^2 = a^2 - b^2 - c^2 + d^2,$$
$$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2),$$
$$G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2),$$
$$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2),$$
$$E^2 = F^2 + G^2 + H^2 + FGH - 4.$$

Surface is from 1864 Kumm

Über die Flächen vierten Gr

mit sechzehn singulären Pur

---

vom 18. *April* 1864.

Endlich möge hier noch eine Formverände
werden, welche man mit der Gleichung dieser Fl
men kann. Wählt man die vier in der Form (4
singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als d
genen Coordinaten, und bezeichnet demgemäſs di
teren durch r und s, so erhält man folgende Fo
chung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f,
auf die richtige Anzahl von drei Constanten a, b, c
ist. Wählt man in dieser Form die Coefficienten
Ausdrücke p, q, r, s real, und die drei Constanten

$(x_i : y_i : z_i : t_i)$ are points on original Kummer surface K :

$$4E^2xyzt = ((x^2 + y^2 + z^2 + t^2) \\ -F(xt + yz) - G(xz + yt) \\ -H(xy + zt))^2$$

where

$$A^2 = a^2 + b^2 + c^2 + d^2,$$
$$B^2 = a^2 + b^2 - c^2 - d^2,$$
$$C^2 = a^2 - b^2 + c^2 - d^2,$$
$$D^2 = a^2 - b^2 - c^2 + d^2,$$
$$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2),$$
$$G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2),$$
$$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2),$$
$$E^2 = F^2 + G^2 + H^2 + FGH - 4.$$

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäſs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

$z_i : t_i)$ are points on
Kummer surface K :
$t = ((x^2 + y^2 + z^2 + t^2)$
$(xt + yz) - G(xz + yt)$
$(xy + zt))^2$

$+ b^2 + c^2 + d^2,$
$+ b^2 - c^2 - d^2,$
$- b^2 + c^2 - d^2,$
$- b^2 - c^2 + d^2,$
$-b^4-c^4+d^4)/(a^2d^2-b^2c^2),$
$-b^4+c^4-d^4)/(a^2c^2-b^2d^2),$
$+b^4-c^4-d^4)/(a^2b^2-c^2d^2),$
$^2 + G^2 + H^2 + FGH - 4.$

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$
wo
$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 a
Jacobiar
genus-2
“Standa
defines s

points on
surface K :
$- y^2 + z^2 + t^2)$
$- G(xz + yt)$
$)^2$

$^2 + d^2,$
$^2 - d^2,$
$^2 - d^2,$
$^2 + d^2,$
$d^4)/(a^2d^2 - b^2c^2),$
$d^4)/(a^2c^2 - b^2d^2),$
$d^4)/(a^2b^2 - c^2d^2),$
$H^2 + FGH - 4.$

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 are points
Jacobian J of a re
genus-2 hyperellip
"Standard" $X : J/$
defines squared θ

:

$+ t^2)$

$- yt)$

$-b^2c^2),$

$-b^2d^2),$

$-c^2d^2),$

$I - 4.$

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

---

vom 18. *April* 1864. 253

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C

“Standard” $X : J/\{\pm 1\} \hookrightarrow$

defines squared θ coords on

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C.

"Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C.
"Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

---

vom 18. April 1864. 253

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C. "Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\to K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

is from 1864 Kummer,
e Flächen vierten Grades
nzehn singulären Punkten:

vom 18. April 1864. 253

möge hier noch eine Formveränderung erwähnt
he man mit der Gleichung dieser Flächen vorneh-
Vählt man die vier in der Form (4.) enthaltenen
gentialebenen

$$p = 0,\; q = 0,\; p' = 0,\; q' = 0$$

nentalebenen, also p, q, p', q', als die vier homo-
naten, und bezeichnet demgemäfs die beiden letz-
und s, so erhält man folgende Form der Glei-

$$\phi^2 = 16Kpqrs,$$

$$q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$a^2 + b^2 + c^2 - 2abc - 1.$$

sieben Constanten a, b, c, d, e, f, k jener Form
e Anzahl von drei Constanten a, b, c eingeschränkt
an in dieser Form die Coefficienten der linearen
q, r, s real, und die drei Constanten a, b, c eben-

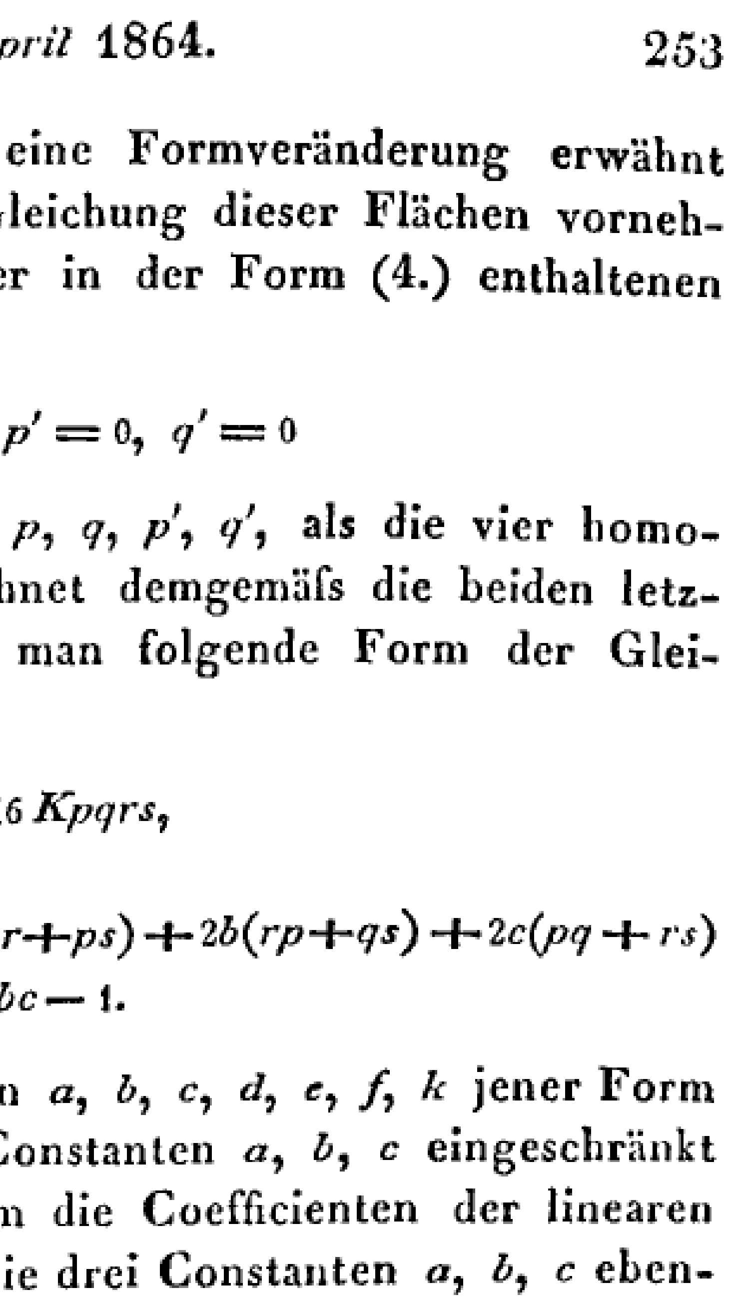
Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C.
"Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

1966 Mu
defining
"There a
formulas
allow on
ambiguit
symmetr
reformul
definitio
made a
achieve
make *co*
still cann

64 Kummer, *vierten Grades ulären Punkten*:



pril 1864. 253

eine Formveränderung erwähnt
leichung dieser Flächen vorneh-
er in der Form (4.) enthaltenen

$p' = 0,\ q' = 0$

$p, q, p', q',$ als die vier homo-
hnet demgemäſs die beiden letz-
man folgende Form der Glei-

6 $Kpqrs$,

$r+ps) + 2b(rp+qs) + 2c(pq+rs)$
$bc - 1.$

n a, b, c, d, e, f, k jener Form
Constanten a, b, c eingeschränkt
n die Coefficienten der linearen
ie drei Constanten a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C. "Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

1966 Mumford, *O defining Abelian v*
"There are several formulas in this pa allow one *or more* ambiguities': i.e., symmetric but nor reformulations. Th definitions and the made a superhuma achieve consistenc make *correct* state still cannot guaran

er,
ades
nkten:

253

rung erwähnt
ächen vorneh-
4.) enthaltenen

ie vier homo-
e beiden letz-
rm der Glei-

$) + 2c(pq + rs)$

k jener Form
eingeschränkt
n der linearen
a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C. "Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

1966 Mumford, *On the equa*
defining Abelian varieties. I
"There are several thousand
formulas in this paper which
allow one *or more* 'sign-like
ambiguities': i.e., alternate
symmetric but non-equivaler
reformulations. These occur
definitions and theorems. I
made a superhuman effort t
achieve consistency and eve
make *correct* statements: bu
still cannot guarantee the re

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C. "Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C. "Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Sage is better than superhuman!

are points on
n J of a related
hyperelliptic curve C.
rd" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\rightarrow K$
squared θ coords on J.

gram k times to compute
$\to X(nQ_1), X((n+1)Q_1)$
$n \in \{0, 1, \ldots, 2^k - 1\}$.

typos in the "standard"
in/Mumford/Kummer
s in 2007 Gaudry, 2010
2013 Bos–Costello–Hisil–
See our paper for simpler
s **as Sage scripts**.

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Sage is better than superhuman!

1975 We
that fam
without
tool prov
actually,
theta-fu
only in 1
Borchard
particula
it is aga
geomete
study of
varieties
to progr

on
lated
tic curve C.
$/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$
coords on J.

nes to compute
$, X((n+1)Q_1)$
$\ldots, 2^k - 1\}$.

ne "standard"
ord/Kummer
Gaudry, 2010
-Costello–Hisil–
aper for simpler
scripts.

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Sage is better than superhuman!

1975 Weil: "Kum
that family of surf
without the help o
tool provided by t
actually, the conn
theta-functions wa
only in 1877, by C
Borchardt . . . His
particular value at
it is again realized
geometers that th
study of well-chos
varieties remains o
to progress in thei

C.
K
J.
npute
$)Q_1)$
}.
rd"
ner
010
Hisil–
mpler

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Sage is better than superhuman!

1975 Weil: "Kummer discov
that family of surfaces . . . e
without the help of the pow
tool provided by theta-funct
actually, the connection with
theta-functions was noticed
only in 1877, by Cayley and
Borchardt . . . His example i
particular value at a time wh
it is again realized by algebr
geometers that the detailed
study of well-chosen special
varieties remains one major
to progress in their field."

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Sage is better than superhuman!

1975 Weil: "Kummer discovered that family of surfaces . . . entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt . . . His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field."

umford, *On the equations* *Abelian varieties. I*: are several thousand s in this paper which e *or more* 'sign-like ties': i.e., alternate and ric but non-equivalent ations. These occur in ns and theorems. I have superhuman effort to consistency and even to *rrect* statements: but I not guarantee the result."

better than superhuman!

1975 Weil: "Kummer discovered that family of surfaces . . . entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt . . . His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field."

2012 Ga
"We wa
of genus
that is s
a public-

n the equations
arieties. I:
thousand
aper which
'sign-like
alternate and
n-equivalent
hese occur in
eorems. I have
an effort to
y and even to
ements: but I
ntee the result."

n superhuman!

1975 Weil: "Kummer discovered that family of surfaces ... entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt ... His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field."

2012 Gaudry–Scho
"We want to find
of genus 2 over a
that is suitable for
a public-key crypto

ations
:
n

and
nt
r in
have
o
n to
ut I
sult.”

man!

1975 Weil: “Kummer discovered that family of surfaces . . . entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt . . . His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field.”

2012 Gaudry–Schost: “We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem.”

1975 Weil: “Kummer discovered that family of surfaces . . . entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt . . . His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field.”

2012 Gaudry–Schost: “We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem.”

1975 Weil: “Kummer discovered that family of surfaces . . . entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt . . . His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field.”

2012 Gaudry–Schost: “We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem.”

Obvious choice of field: $\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast. $\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1975 Weil: "Kummer discovered that family of surfaces ... entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt ... His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field."

2012 Gaudry–Schost: "We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field: $\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast. $\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found $(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$, primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$. Here J' is Jacobian of nontrivial quadratic twist of curve C.

eil: "Kummer discovered
nily of surfaces . . . entirely
the help of the powerful
vided by theta-functions;
the connection with
nctions was noticed
1877, by Cayley and by
dt . . . His example is of
ar value at a time when
in realized by algebraic
ers that the detailed
well-chosen special
remains one major road
ess in their field."

2012 Gaudry–Schost:
"We want to find a curve
of genus 2 over a prime field
that is suitable for building
a public-key cryptosystem."

Obvious choice of field:
$\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast.
$\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found
$(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$,
primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$.
Here J' is Jacobian of nontrivial
quadratic twist of curve C.

Is this fa
security
or a sim

mer discovered
aces . . . entirely
of the powerful
heta-functions;
ection with
as noticed
Cayley and by
example is of
a time when
by algebraic
e detailed
en special
one major road
r field."

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field: $\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast. $\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found $(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$, primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$. Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than
security elliptic cu
or a similar-size pr

vered
ntirely
erful
ions;
n

by
s of
hen
aic

road

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field:
$\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast.
$\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found
$(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$,
primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$.
Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than a similar-security elliptic curve over **F**
or a similar-size prime field?

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field:
$\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast.
$\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found
$(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$,
primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$.
Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field:
$\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast.
$\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found $(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$, primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$.
Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

2012 Gaudry–Schost: "We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field: $\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast. $\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found $(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$, primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$. Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field:
$\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast.
$\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found $(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$, primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$.
Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

udry–Schost:
nt to find a curve
s 2 over a prime field
uitable for building
-key cryptosystem."

choice of field:
e $p = 2^{127} - 1$. Fast.
$\approx 2^{254}$; big enough.

CPU hours found
$c^2, d^2) = (-11, 22, 19, 3)$,
$\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$.
is Jacobian of nontrivial
c twist of curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summar
holds sp
high-sec

ost:
a curve
prime field
r building
osystem."

field:
$^{7} - 1$. Fast.
ig enough.

urs found
$(-11, 22, 19, 3)$,
$6, \#J'(\mathbf{F}_p)/16$.
n of nontrivial
curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry
holds speed record
high-security n, Q

d

t.

$19, 3)$,

$/16$.

ivial

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

aster than a similar-
elliptic curve over $\mathbf{F}_{p^2}$
ilar-size prime field?

g ops suggests: Yes,
y with small a^2 etc.

entations (2006 Bernstein,
os–Costello–Hisil–Lauter,
rnstein–Chuengsatiansup–
Schwabe): Yes.

ostello–Longa E with
CM, 2-isogeny to $\overline{E}$: faster
e CPUs but not others,
pressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is
E is an
curve; W
Note: 2

a similar-
rve over $\mathbf{F}_{p^2}$
ime field?

gests: Yes,
all a^2 etc.

2006 Bernstein,
–Hisil–Lauter,
nuengsatiansup–
Yes.

nga E with
eny to $\overline{E}$: faster
t not others,
ot twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) =$
E is an $\mathbf{F}_{p^2}$-compl
curve; W is Weil r
Note: 2 paramete

$_{p^2}$

nstein,

uter,

nsup–

n

faster

rs,

ecure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$. E is an $\mathbf{F}_{p^2}$-complete Edwar curve; W is Weil restriction. Note: 2 parameters for W.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$. E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction. Note: 2 parameters for W.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$. E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction. Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$. Note: 3 parameters for K.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$. E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction. Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$. Note: 3 parameters for K.

Surprise: We have examples where a^2, b^2, c^2, d^2 are small! This allows fastest $n, P \mapsto nP$.

Explanation: Can lift from $\mathbf{F}_{p^2}/\mathbf{F}_p$ to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

y: Gaudry–Schost J
eed records for
urity $n, Q \mapsto nQ$.

nt about $P, Q \mapsto P + Q$?
? $m, n, P, Q \mapsto mP + nQ$?

known addition formulas
er for E than for J.
't competitive for
eration, signing, etc.

and-elliptic curve
raphy: Build *one* group
ng the fastest formulas
nus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$.
Note: 3 parameters for K.

Surprise: We have examples where a^2, b^2, c^2, d^2 are small!
This allows fastest $n, P \mapsto nP$.

Explanation: Can lift from $\mathbf{F}_{p^2}/\mathbf{F}_p$ to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

Another
genus-1
(Use Ma

History
for genu
via genu

2002 Ga
in char 2
2001 Ga
2003 Die
2003 Sch
2004 Die
2011 Fre
odd-char

–Schost J
ls for
$\mapsto nQ$.

$P, Q \mapsto P + Q$?
$Q \mapsto mP + nQ$?

dition formulas
an for J.
itive for
gning, etc.

ic curve
uild *one* group
test formulas
genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$.
Note: 3 parameters for K.

Surprise: We have examples where a^2, b^2, c^2, d^2 are small!
This allows fastest $n, P \mapsto nP$.

Explanation: Can lift from $\mathbf{F}_{p^2}/\mathbf{F}_p$ to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

Another virtue of
genus-1 point-cou
(Use Magma; Sag

History of using W
for genus-2 point-
via genus-1 point-

2002 Gaudry–Hess
in char 2; odd cha
2001 Galbraith: "
2003 Diem, 2003
2003 Scholten, 20
2004 Diem–Scholt
2011 Freeman–Sat
odd-char construc

/

$-\ Q$?

$+\ nQ$?

ulas

roup

ulas

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$.
Note: 3 parameters for K.

Surprise: We have examples where a^2, b^2, c^2, d^2 are small!
This allows fastest $n, P \mapsto nP$.

Explanation: Can lift from $\mathbf{F}_{p^2}/\mathbf{F}_p$ to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

Another virtue of these grou
genus-1 point-counting is fa
(Use Magma; Sage needs $\mathbf{F}_{\!p}$

History of using $W \to J$
for genus-2 point-counting
via genus-1 point-counting:

2002 Gaudry–Hess–Smart
in char 2; odd char is "hard"
2001 Galbraith: "rather diffi
2003 Diem, 2003 Diem–Sch
2003 Scholten, 2003 Thériau
2004 Diem–Scholten, 2009 S
2011 Freeman–Satoh: vario
odd-char constructions.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$.
Note: 3 parameters for K.

Surprise: We have examples where a^2, b^2, c^2, d^2 are small!
This allows fastest $n, P \mapsto nP$.

Explanation: Can lift from $\mathbf{F}_{p^2}/\mathbf{F}_p$ to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

Another virtue of these groups: genus-1 point-counting is fast.
(Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is “hard”.
2001 Galbraith: “rather difficult”.
2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

s $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
$\mathbf{F}_{p^2}$-complete Edwards
/ is Weil restriction.
parameters for W.

$(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using
geny $W \to J = \text{Jac}\, H$ for
and fast $X : J \to K$.
parameters for K.

: We have examples
$^2, b^2, c^2, d^2$ are small!
ows fastest $n, P \mapsto nP$.

tion: Can lift from
to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is "hard".
2001 Galbraith: "rather difficult".
2003 Diem, 2003 Diem–Scholten,
2003 Scholten, 2003 Thériault,
2004 Diem–Scholten, 2009 Satoh,
2011 Freeman–Satoh: various odd-char constructions.

Scholten

(2003 Sc

Assume:
$r, s, \beta \in$
minor ac

Write $\overline{r}$

$= W(\mathbf{F}_p)$.
lete Edwards
estriction.
rs for W.

$(\mathbf{F}_p)$ using
$J = \text{Jac}\, H$ for
$X : J \to K$.
rs for K.

e examples
^{2} are small!
t $n, P \mapsto nP$.

lift from
$)/\mathbf{Q}$.

Another virtue of these groups:
genus-1 point-counting is fast.
(Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$
for genus-2 point-counting
via genus-1 point-counting:

2002 Gaudry–Hess–Smart
in char 2; odd char is "hard".
2001 Galbraith: "rather difficult".
2003 Diem, 2003 Diem–Scholten,
2003 Scholten, 2003 Thériault,
2004 Diem–Scholten, 2009 Satoh,
2011 Freeman–Satoh: various
odd-char constructions.

Scholten curves

(2003 Scholten +

Assume: odd prim
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin$
minor additional h

Write $\bar{r} = r^p$, $\bar{s} =$

rds

;

H for

K.

s

ll!

nP.

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is "hard". 2001 Galbraith: "rather difficult". 2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

Scholten curves

(2003 Scholten + simplificat

Assume: odd prime p; $r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$; minor additional hypotheses

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta$

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is "hard". 2001 Galbraith: "rather difficult". 2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p; $r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$; minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is "hard".
2001 Galbraith: "rather difficult".
2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p; $r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$; minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$. Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is "hard". 2001 Galbraith: "rather difficult". 2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p; $r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$; minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$. Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$. Note that $g \in \mathbf{F}_p[z]$.

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is "hard".
2001 Galbraith: "rather difficult".
2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

<u>Scholten curves</u>

(2003 Scholten + simplifications)

Assume: odd prime p; $r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$; minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$. Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$. Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

virtue of these groups:
point-counting is fast.
agma; Sage needs $\mathbf{F}_p$.)

of using $W \to J$
s-2 point-counting
s-1 point-counting:

udry–Hess–Smart
2; odd char is "hard".
lbraith: "rather difficult".
em, 2003 Diem–Scholten,
holten, 2003 Thériault,
em–Scholten, 2009 Satoh,
eeman–Satoh: various
r constructions.

<u>Scholten curves</u>

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denomin
Choose

these groups:
nting is fast.
e needs $\mathbf{F}_p$.)

$/ \to J$
counting
counting:

s–Smart
r is "hard".
rather difficult".
Diem–Scholten,
03 Thériault,
ten, 2009 Satoh,
toh: various
tions.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1 - \beta z$, $v = 1 - \overline{\beta} z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g
Choose square roo

ps:
st.
p.)

”,
”.
cult”.
olten,
ult,
Satoh,
us

<u>Scholten curves</u>

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1 - \beta z$, $v = 1 - \overline{\beta} z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1 - \beta z$, $v = 1 - \overline{\beta} z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

n curves

cholten + simplifications)

odd prime p;

$\mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;

dditional hypotheses.

$= r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.

$\in \mathbf{F}_{p^2}[z]$ as

$$\frac{\ldots sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{\ldots s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

$= 1-\beta z$, $v = 1-\overline{\beta}z$.

at $g \in \mathbf{F}_p[z]$.

n curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our pap

obtain lo

on Mum

simplifications)

ne p;

$\mathbf{F}_p$;

ypotheses.

s^p, $\overline{\beta} = \beta^p$.

as

$$\frac{\overline{s}v^2u^4 + \overline{r}u^6}{\overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

$v = 1 - \overline{\beta}z$.

$z]$.

: $y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpo
obtain low-degree
on Mumford coord

tions)

.

β^p.

$\frac{u^6}{\beta^6}$

z.

z).

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to
obtain low-degree formulas f
on Mumford coordinates for

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve $y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

Define $\phi : H \to E$ as $(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$, hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces $\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$ W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to
obtain low-degree formulas for ι'
on Mumford coordinates for J.
Also low-degree formulas for $\iota :$
$W \to J$ with $\iota'(\iota(P)) = 2P$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to
obtain low-degree formulas for ι'
on Mumford coordinates for J.
Also low-degree formulas for ι :
$W \to J$ with $\iota'(\iota(P)) = 2P$.
All formulas are defined over $\mathbf{F}_p$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to
obtain low-degree formulas for ι'
on Mumford coordinates for J.
Also low-degree formulas for ι :
$W \to J$ with $\iota'(\iota(P)) = 2P$.
All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum
of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002
Gaudry–Hess–Smart, 2003 Diem,
2004 Arita–Matsuo–Nagao–Shimura. But this doesn't
give a very fast algorithm.)

nator of g is in $\mathbf{F}_p$.
square root $\omega \in \mathbf{F}_{p^2}$.

E as the elliptic curve
${}^3 + sx^2 + \bar{s}x + \bar{r}$.

$\phi : H \to E$ as
$\mapsto (v^2/u^2, \omega y/u^3)$.

an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
Weil restriction W of E.
es $H \to W$, which induces
W where $J = \mathrm{Jac}\, H$.

ely: $\iota'(P_1 + P_2) =$
ds of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to
obtain low-degree formulas for ι'
on Mumford coordinates for J.
Also low-degree formulas for ι :
$W \to J$ with $\iota'(\iota(P)) = 2P$.
All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum
of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002
Gaudry–Hess–Smart, 2003 Diem,
2004 Arita–Matsuo–Nagao–Shimura. But this doesn't
give a very fast algorithm.)

Scholten

Given Sc
compute
original

Factor g

is in $\mathbf{F}_p$.

pt $\omega \in \mathbf{F}_{p^2}$.

lliptic curve

$\bar{s}x + \bar{r}$.

as

$\omega y/u^3)$.

is for $\mathbf{F}_{p^2}$,

iction W of E.

, which induces

$J = \operatorname{Jac} H$.

$+ P_2) =$

$) + \phi(P_2)$.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$. All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002 Gaudry–Hess–Smart, 2003 Diem, 2004 Arita–Matsuo–Nagao–Shimura. But this doesn't give a very fast algorithm.)

Scholten with fast

Given Scholten cu

compute correspon

original Kummer s

Factor g into linea

.

e

of E.

duces

J.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$. All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum of ϕ-preimages of P; “norm-conorm” map used in, e.g., 2002 Gaudry–Hess–Smart, 2003 Diem, 2004 Arita–Matsuo–Nagao–Shimura. But this doesn’t give a very fast algorithm.)

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$. All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002 Gaudry–Hess–Smart, 2003 Diem, 2004 Arita–Matsuo–Nagao–Shimura. But this doesn't give a very fast algorithm.)

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$. All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002 Gaudry–Hess–Smart, 2003 Diem, 2004 Arita–Matsuo–Nagao–Shimura. But this doesn't give a very fast algorithm.)

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$. All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002 Gaudry–Hess–Smart, 2003 Diem, 2004 Arita–Matsuo–Nagao–Shimura. But this doesn't give a very fast algorithm.)

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute

$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

er interpolates to
ow-degree formulas for ι'
nford coordinates for J.
-degree formulas for ι :
with $\iota'(\iota(P)) = 2P$.
ulas are defined over $\mathbf{F}_p$.

ow: $\iota(P)$ is trace of sum
images of P; "norm-
map used in, e.g., 2002
-Hess–Smart, 2003 Diem,
ita–Matsuo–Nagao–
. But this doesn't
ery fast algorithm.)

Scholten with fast Kummer?

Given Scholten curve,
compute corresponding
original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation
move to twisted Rosenhain form
$\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute

$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take s_1,
with s_1^2,

$-s_1^2 s_2^2 s_3^2$
Write it

lates to
formulas for ι'
dinates for J.
ormulas for ι :
$P)) = 2P$.
efined over $\mathbf{F}_p$.

s trace of sum
P; "norm-
d in, e.g., 2002
art, 2003 Diem,
o–Nagao–
doesn't
gorithm.)

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute
$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$
$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}$
with s_1^2, s_2^2, s_3^2 dist
$-s_1^2 s_2^2 s_3^2$ has norm
Write it as $\overline{r}/r$ wit

for ι'
J.
ι :

$\mathbf{F}_p$.

sum

2002
Diem,

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute

$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute

$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1. Write it as $\bar{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute
$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$
$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1. Write it as $\bar{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$. Then g has 6 distinct roots $(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute
$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$
$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1. Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$. Then g has 6 distinct roots $(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$; i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.

Scholten with fast Kummer?

Given Scholten curve, compute corresponding original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation move to twisted Rosenhain form $\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute

$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\bar{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $(\bar{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots $(1 \pm s_j)/(\bar{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$; i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

n with fast Kummer?

cholten curve,
e corresponding
Kummer surface K:

: into linear factors.

r-fractional transformation
twisted Rosenhain form
$(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

e
$\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$,
$\frac{\lambda\mu}{\nu}$, $a^2 = \frac{b^2c^2\nu}{\mu}$, $d^2 = 1$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots
$(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

Lifting t

$\mathbf{F}_{p^2} = \mathbf{F}$
small sq

Kummer?

rve,

nding

surface K:

ar factors.

l transformation

osenhain form

$-\lambda)(x-\mu)(x-\nu)$.

$\overline{\lambda-\nu)}$

$\lambda-\mu)$,

$\frac{b^2c^2\nu}{\mu}$, $d^2=1$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1+s_2+s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots $(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$; i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

Lifting to $\mathbf{Q}(\sqrt{\Delta})$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ fo

small squarefree i

?

mation
form
$(x-\nu)$.

$^2 = 1$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots
$(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
i.e., $\sqrt{\dfrac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots
$(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many
small squarefree integers Δ.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}^*_{p^2}$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots
$(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

<u>Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$</u>

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many
small squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements
$s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$;
$g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots
$(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many
small squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements
$s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$;
$g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist,
giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

$s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
s_2^2, s_3^2 distinct.

has norm 1.

as $\bar{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

$= -r(s_1 + s_2 + s_3)$.

y $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
$/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
has 6 distinct roots
$/(\bar{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

at $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
$\frac{\mu}{\nu}, \sqrt{\cdots} \in \mathbf{F}_p$.
small height.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many
small squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements
$s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$;
$g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist,
giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

For each
We tried

$_{p^2}$, norm 1,
inct.

1.

th $r \in \mathbf{F}^*_{p^2}$.

$+ s_2 + s_3)$.

$- \mathbf{F}_p$
$, s_2^2, s_3^2\}$.
inct roots
$\in \mathbf{F}_p$.

$c^2, d^2 \in \mathbf{F}_p$;

$\mathbf{F}_p$.
ght.

<u>Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$</u>

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many
small squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements
$s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$;
$g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist,
giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

For each small qua
We tried all small

1,

.

.

p;

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements $s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$; $g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist, giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

For each small quadratic fiel
We tried all small s_1, s_2, s_3.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements $s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$; $g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist, giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

For each small quadratic field:
We tried all small s_1, s_2, s_3.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements $s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$; $g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist, giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

For each small quadratic field:
We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that
$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,
$s_2 = (189 + 32\sqrt{\Delta})/323$,
$s_3 = (333 - 40\sqrt{\Delta})/467$
produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)(x - 1/16)(x + 16/67)(x + 1/20)(x - 20/67)$$

with Kummer surface
$a^2 = 194769$, $b^2 = 126939$,
$c^2 = 64009$, $d^2 = 126939$.

o $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$_p(\sqrt{\Delta})$ for many
quarefree integers Δ.

y, $\beta = \sqrt{\Delta}$.
nall norm-1 elements
$\in \mathbf{Q}(\sqrt{\Delta})$.

re define $r, s \in \mathbf{Q}(\sqrt{\Delta})$;
$\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

re small.
the square roots exist,
mall $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

be there's an obstruction.

For each small quadratic field:
We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that
$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,
$s_2 = (189 + 32\sqrt{\Delta})/323$,
$s_3 = (333 - 40\sqrt{\Delta})/467$
produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)$$
$$(x - 1/16)(x + 16/67)$$
$$(x + 1/20)(x - 20/67)$$

with Kummer surface
$a^2 = 194769$, $b^2 = 126939$,
$c^2 = \ 64009$, $d^2 = 126939$.

Found m
for vario
$\Rightarrow$ thous
$\#E(\mathbf{F}_{p^2}$

$/\mathbf{Q}$

r many

ntegers Δ.

Δ.

1 elements

).

$, s \in \mathbf{Q}(\sqrt{\Delta})$;

nd $\lambda, \mu, \nu \in \mathbf{Q}$.

roots exist,

$, c^2, d^2 \in \mathbf{Q}$.

an obstruction.

For each small quadratic field:
We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that
$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,
$s_2 = (189 + 32\sqrt{\Delta})/323$,
$s_3 = (333 - 40\sqrt{\Delta})/467$
produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)$$
$$(x - 1/16)(x + 16/67)$$
$$(x + 1/20)(x - 20/67)$$

with Kummer surface
$a^2 = 194769$, $b^2 = 126939$,
$c^2 = \ 64009$, $d^2 = 126939$.

Found many more

for various choices

$\Rightarrow$ thousands of d

$\#E(\mathbf{F}_{p^2})$ for $p =$

For each small quadratic field:
We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that
$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,
$s_2 = (189 + 32\sqrt{\Delta})/323$,
$s_3 = (333 - 40\sqrt{\Delta})/467$
produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)(x - 1/16)(x + 16/67)(x + 1/20)(x - 20/67)$$

with Kummer surface
$a^2 = 194769$, $b^2 = 126939$,
$c^2 = \ 64009$, $d^2 = 126939$.

Found many more examples
for various choices of Δ
$\Rightarrow$ thousands of different
$\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

For each small quadratic field:
We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that
$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,
$s_2 = (189 + 32\sqrt{\Delta})/323$,
$s_3 = (333 - 40\sqrt{\Delta})/467$
produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)(x - 1/16)(x + 16/67)(x + 1/20)(x - 20/67)$$

with Kummer surface
$a^2 = 194769$, $b^2 = 126939$,
$c^2 = 64009$, $d^2 = 126939$.

Found many more examples
for various choices of Δ
$\Rightarrow$ thousands of different
$\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

For each small quadratic field:

We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that

$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,

$s_2 = (189 + 32\sqrt{\Delta})/323$,

$s_3 = (333 - 40\sqrt{\Delta})/467$

produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)(x - 1/16)(x + 16/67)(x + 1/20)(x - 20/67)$$

with Kummer surface

$a^2 = 194769$, $b^2 = 126939$,

$c^2 = 64009$, $d^2 = 126939$.

Found many more examples for various choices of Δ

$\Rightarrow$ thousands of different $\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z + 3)(z + 1/9)(z - 1/7)(z - 7/3)(z - 8/7)(z - 7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.

$a^2 = -46893$, $b^2 = 20020$,

$c^2 = 20020$, $d^2 = 5800$.

n small quadratic field:
d all small s_1, s_2, s_3.

, $\Delta = -67$ found that
$17143 + 96\sqrt{\Delta})/17161$,
$39 + 32\sqrt{\Delta})/323$,
$33 - 40\sqrt{\Delta})/467$
d Scholten curve
$- 16/3)(x + 3/1072)$
$- 1/16)(x + 16/67)$
$+ 1/20)(x - 20/67)$
mmer surface
$4769, b^2 = 126939$,
$4009, d^2 = 126939$.

Found many more examples
for various choices of Δ
$\Rightarrow$ thousands of different
$\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z + 3)(z + 1/9)(z - 1/7)(z - 7/3)(z - 8/7)(z - 7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = 20020$, $d^2 = 5800$.

Another
$y^2 = (z$
$(z$
$(z$

adratic field:

s_1, s_2, s_3.

7 found that

$6\sqrt{\Delta})/17161$,

$\Delta)/323$,

$\Delta)/467$

curve

$x + 3/1072)$

$x + 16/67)$

$x - 20/67)$

ace

$= 126939$,

$= 126939$.

Found many more examples for various choices of Δ $\Rightarrow$ thousands of different $\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z+3)(z+1/9)$$
$$(z-1/7)(z-7/3)$$
$$(z-8/7)(z-7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$ $= 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = 20020$, $d^2 = 5800$.

Another good exa

$$y^2 = (z-1)(z+$$
$$(z-1/4)(z$$
$$(z+5/7)(z$$

ld:

hat

161,

2)

)

)

Found many more examples for various choices of Δ $\Rightarrow$ thousands of different $\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z+3)(z+1/9)(z-1/7)(z-7/3)(z-8/7)(z-7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$ $= 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = \ \ 20020$, $d^2 = \ \ 5800$.

Another good example:

$$y^2 = (z-1)(z+1/11)(z-1/4)(z+4/11)(z+5/7)(z-7/55).$$

Found many more examples for various choices of Δ $\Rightarrow$ thousands of different $\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z+3)(z+1/9)(z-1/7)(z-7/3)(z-8/7)(z-7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2}) = 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = 20020$, $d^2 = 5800$.

Another good example:

$$y^2 = (z-1)(z+1/11)(z-1/4)(z+4/11)(z+5/7)(z-7/55).$$

Found many more examples
for various choices of Δ
$\Rightarrow$ thousands of different
$\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z+3)(z+1/9)(z-1/7)(z-7/3)(z-8/7)(z-7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = 20020$, $d^2 = 5800$.

Another good example:

$$y^2 = (z-1)(z+1/11)(z-1/4)(z+4/11)(z+5/7)(z-7/55).$$

Slightly lower security level:
$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 720\ell$ for a prime $\ell \approx 2^{244.5}$.
$\#E'(\mathbf{F}_{p^2}) = 260 \cdot \text{prime}$.

Found many more examples for various choices of Δ $\Rightarrow$ thousands of different $\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z+3)(z+1/9)(z-1/7)(z-7/3)(z-8/7)(z-7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2}) = 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = 20020$, $d^2 = 5800$.

Another good example:

$$y^2 = (z-1)(z+1/11)(z-1/4)(z+4/11)(z+5/7)(z-7/55).$$

Slightly lower security level:
$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2}) = 720\ell$ for a prime $\ell \approx 2^{244.5}$.
$\#E'(\mathbf{F}_{p^2}) = 260 \cdot \text{prime}$.

Particularly nice arithmetic:
$(a^2 : b^2 : c^2 : d^2) = (20:12:12:5)$;
$(A^2 : \ldots) = (49:15:15:1)$;
$(\frac{1}{a^2} : \cdots) = (3:5:5:12)$;
$(\frac{1}{A^2} : \cdots) = (15:49:49:735)$.