Hyper-and-elliptic-curve cryptography

(which is not the same as: hyperelliptic-curve cryptography and elliptic-curve cryptography)

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

Tanja Lange
Technische Universiteit Eindhoven

"Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use."
—Greenpeace UK

Hyper-and-elliptic-curve cryptography

(which is not the same as: hyperelliptic-curve cryptography and elliptic-curve cryptography)

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

Tanja Lange
Technische Universiteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)

nd-elliptic-curve
aphy

s not the same as:
ptic-curve cryptography
tic-curve cryptography)

. Bernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

ange
che Universiteit Eindhoven

"Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use."
—Greenpeace UK (mostly)

DH spee

Sandy B
security
("?" if r

2011 Be
Schwabe
2012 Ha
2012 Lo
2013 Bo
Lauter:
2013 Oli
Rodrígue
2013 Fa
Sánchez
2014 Be
Lange–S

-curve

same as:
cryptography
cryptography)

n
is at Chicago &
siteit Eindhoven

siteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)

DH speed records

Sandy Bridge cycl
security constant-t
(“?” if not SUPE

2011 Bernstein–D
Schwabe–Yang:
2012 Hamburg:
2012 Longa–Sica:
2013 Bos–Costell
Lauter:
2013 Oliveira–Lóp
Rodríguez-Henríq
2013 Faz-Hernánd
Sánchez:
2014 Bernstein–C
Lange–Schwabe:

phy
hy)

ago &
hoven

hoven

"Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use."
—Greenpeace UK (mostly)

DH speed records

Sandy Bridge cycles for high
security constant-time a, P
("?" if not SUPERCOP-ver

2011 Bernstein–Duif–Lange–
Schwabe–Yang: 19
2012 Hamburg: 15
2012 Longa–Sica: 13
2013 Bos–Costello–Hisil–
Lauter: 12
2013 Oliveira–López–Aranha
Rodríguez-Henríquez: 11
2013 Faz-Hernández–Longa–
Sánchez: 9
2014 Bernstein–Chuengsatia
Lange–Schwabe: 9

"Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use."
—Greenpeace UK (mostly)

DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

2011 Bernstein–Duif–Lange–Schwabe–Yang:	194036
2012 Hamburg:	153000?
2012 Longa–Sica:	137000?
2013 Bos–Costello–Hisil–Lauter:	122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez:	114800?
2013 Faz-Hernández–Longa–Sánchez:	96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:	91320

gh our inefficient use of
gas guzzling vehicles,
sulated buildings,
optimized crypto, etc)
lessly throw away almost
of the energy we use."
peace UK (mostly)

DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

2011 Bernstein–Duif–Lange–Schwabe–Yang:	194036
2012 Hamburg:	153000?
2012 Longa–Sica:	137000?
2013 Bos–Costello–Hisil–Lauter:	122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez:	114800?
2013 Faz-Hernández–Longa–Sánchez:	96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:	91320

Critical f

1986 Ch
tradition
allows fa
14**M** for

2006 Ga
25**M** for
$\mapsto X(2$
6**M** by s

2012 Ga
1000000
found se
surface c

fficient use of
ng vehicles,
ildings,
crypto, etc)
w away almost
rgy we use."
(mostly)

<u>DH speed records</u>

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

2011 Bernstein–Duif–Lange–Schwabe–Yang:	194036
2012 Hamburg:	153000?
2012 Longa–Sica:	137000?
2013 Bos–Costello–Hisil–Lauter:	122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez:	114800?
2013 Faz-Hernández–Longa–Sánchez:	96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:	91320

Critical for 122716

1986 Chudnovsky–
traditional Kumme
allows fast scalar r
14**M** for $X(P) \mapsto$

2006 Gaudry: ever
25**M** for $X(P), X($
$\mapsto X(2P), X(Q +$
6**M** by surface coe

2012 Gaudry–Scho
1000000-CPU-hou
found secure small
surface over $\mathbf{F}_{2^{127}}$

e of
s,

etc)
most
."

DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

2011 Bernstein–Duif–Lange–Schwabe–Yang: 194036
2012 Hamburg: 153000?
2012 Longa–Sica: 137000?
2013 Bos–Costello–Hisil–Lauter: 122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez: 114800?
2013 Faz-Hernández–Longa–Sánchez: 96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe: 91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovs
traditional Kummer surface
allows fast scalar mult.
14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster.
25**M** for $X(P), X(Q), X(Q$
$\mapsto X(2P), X(Q+P)$, inclu
6**M** by surface coefficients.

2012 Gaudry–Schost:
1000000-CPU-hour computa
found secure small-coefficier
surface over $\mathbf{F}_{2^{127}-1}$.

DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

2011 Bernstein–Duif–Lange–Schwabe–Yang:	194036
2012 Hamburg:	153000?
2012 Longa–Sica:	137000?
2013 Bos–Costello–Hisil–Lauter:	122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez:	114800?
2013 Faz-Hernández–Longa–Sánchez:	96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:	91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult. 14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster. 25**M** for $X(P), X(Q), X(Q-P)$ $\mapsto X(2P), X(Q+P)$, including 6**M** by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127}-1}$.

ed records

Bridge cycles for high-
constant-time $a, P \mapsto aP$
not SUPERCOP-verified):

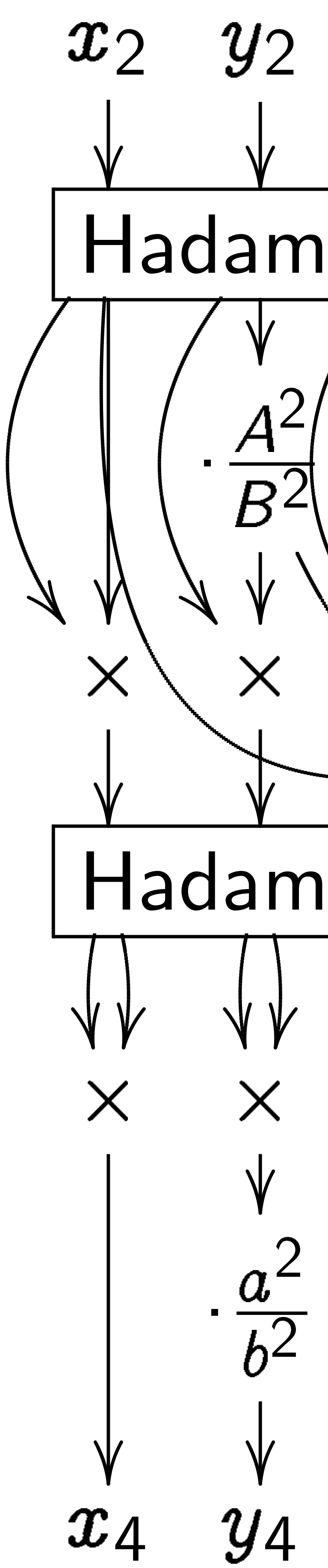
rnstein–Duif–Lange–
e–Yang: 194036
mburg: 153000?
nga–Sica: 137000?
s–Costello–Hisil–
122716
iveira–López–Aranha–
ez-Henríquez: 114800?
z-Hernández–Longa–
: 96000?
rnstein–Chuengsatiansup–
Schwabe: 91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult. 14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster. 25**M** for $X(P), X(Q), X(Q-P) \mapsto X(2P), X(Q+P)$, including 6**M** by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127}-1}$.



es for high-
time $a, P \mapsto aP$
RCOP-verified):

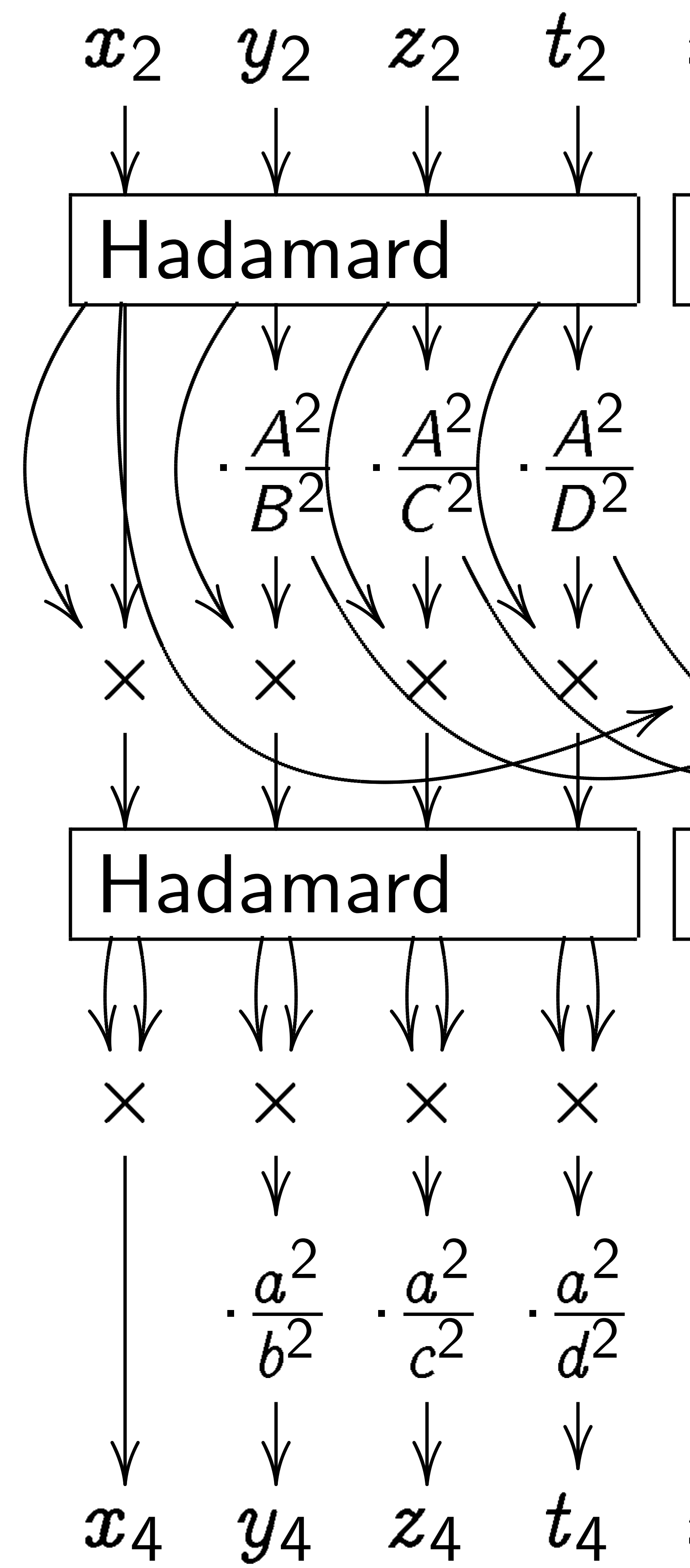
uif–Lange–
194036
153000?
137000?
–Hisil–
122716
ez–Aranha–
uez: 114800?
ez–Longa–
96000?
huengsatiansup–
91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult. 14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster. 25**M** for $X(P), X(Q), X(Q-P)$ $\mapsto X(2P), X(Q+P)$, including 6**M** by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127}-1}$.



n-

$\to aP$

ified):

–

94036

53000?

37000?

22716

a–

14800?

–

96000?

nsup–

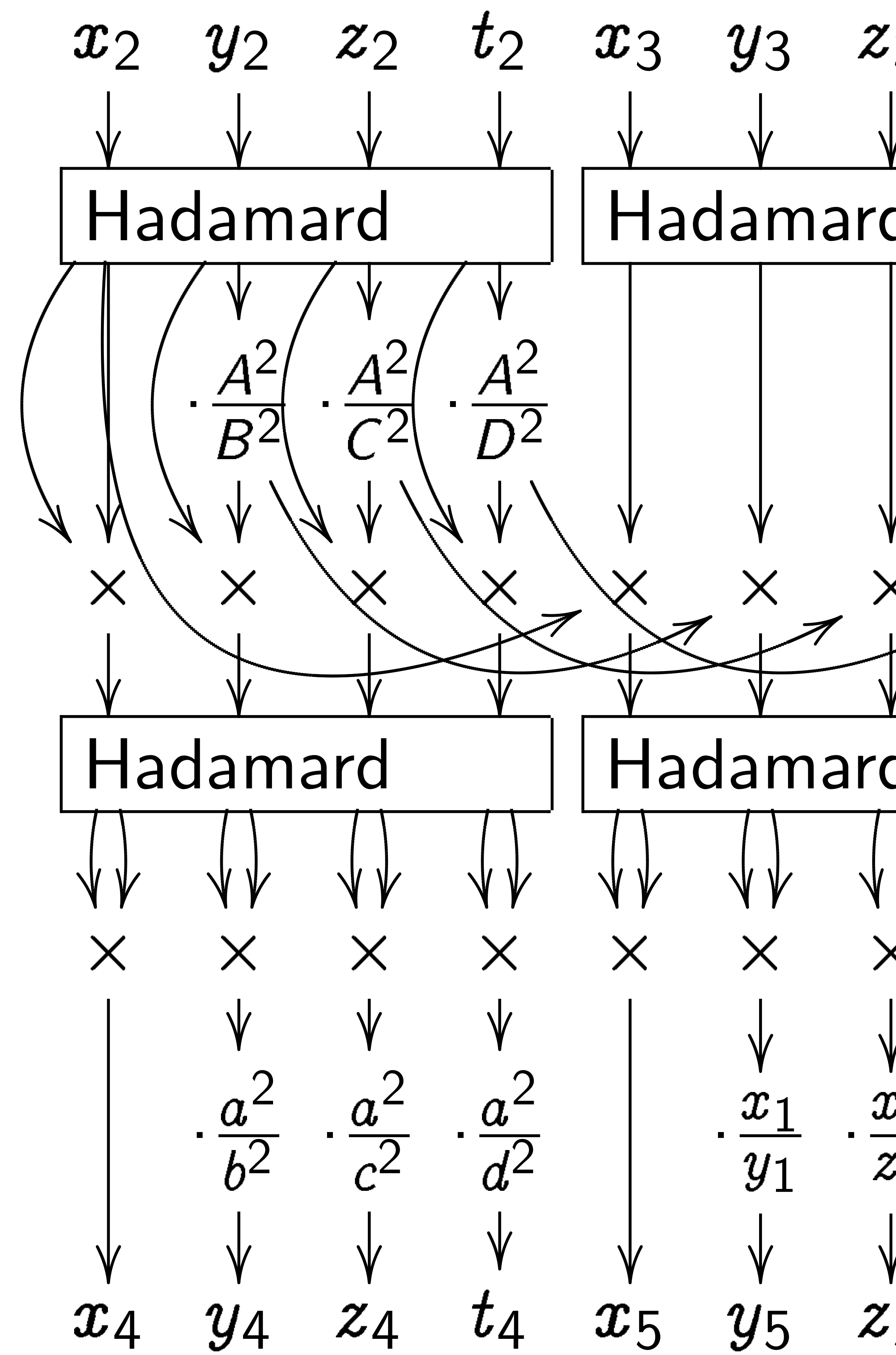
91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult. 14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster. 25**M** for $X(P), X(Q), X(Q-P)$ $\mapsto X(2P), X(Q+P)$, including 6**M** by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127}-1}$.

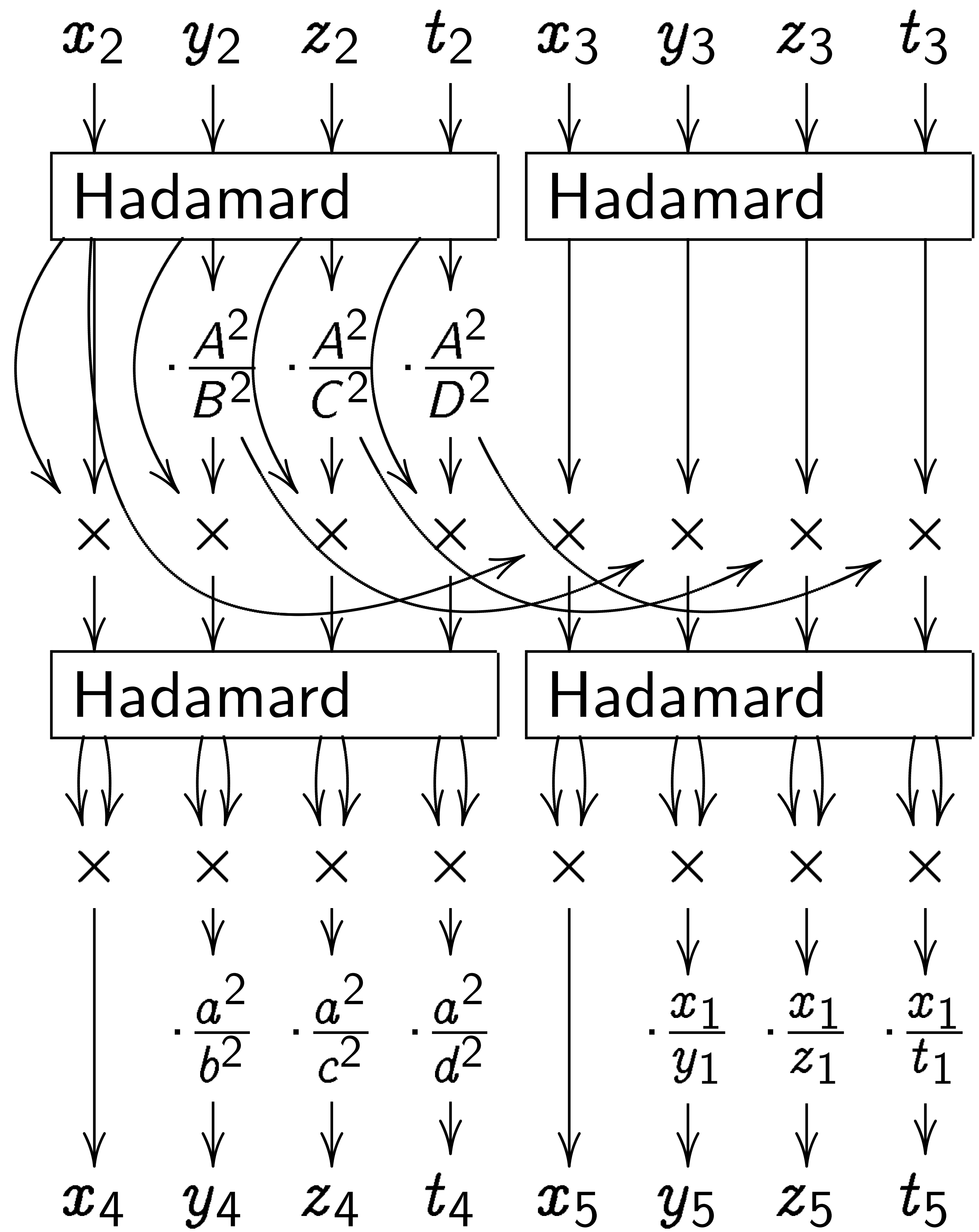


Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult. 14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster. 25**M** for $X(P), X(Q), X(Q-P)$ $\mapsto X(2P), X(Q+P)$, including 6**M** by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127}-1}$.



for 122716, 91320:

udnovsky–Chudnovsky:

nal Kummer surface

ast scalar mult.

$X(P) \mapsto X(2P)$.

udry: even faster.

$X(P), X(Q), X(Q-P)$

$P), X(Q+P)$, including

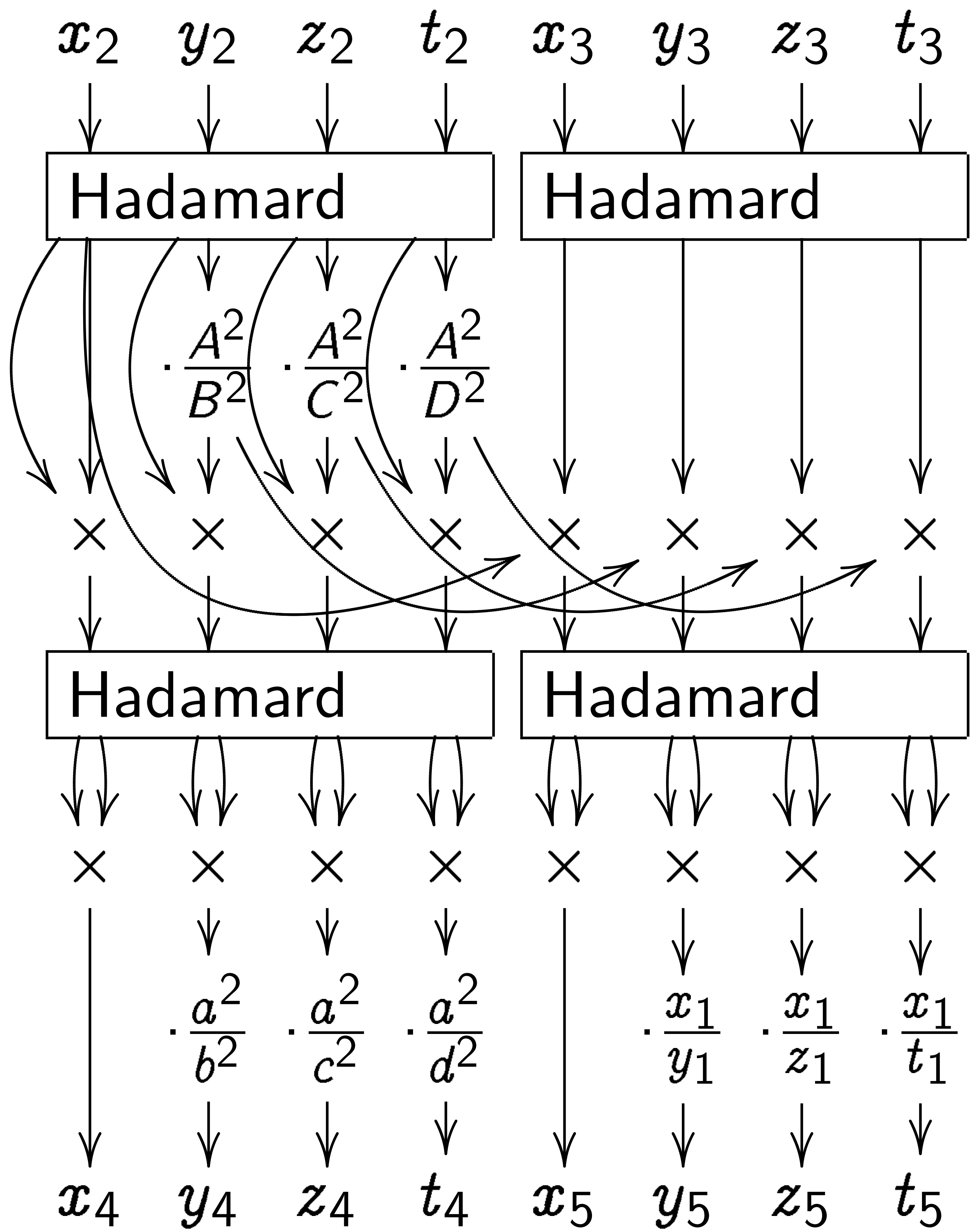
surface coefficients.

udry–Schost:

0-CPU-hour computation

ecure small-coefficient

over $\mathbf{F}_{2^{127}-1}$.



Strategie

with kno

fast buil

any curv

many cu

secure c

twist-sec

Kumme

small co

fastest I

fastest k

complet

6, 91320:

-Chudnovsky:

er surface

mult.

$X(2P)$.

n faster.

$(Q), X(Q-P)$

$-P)$, including

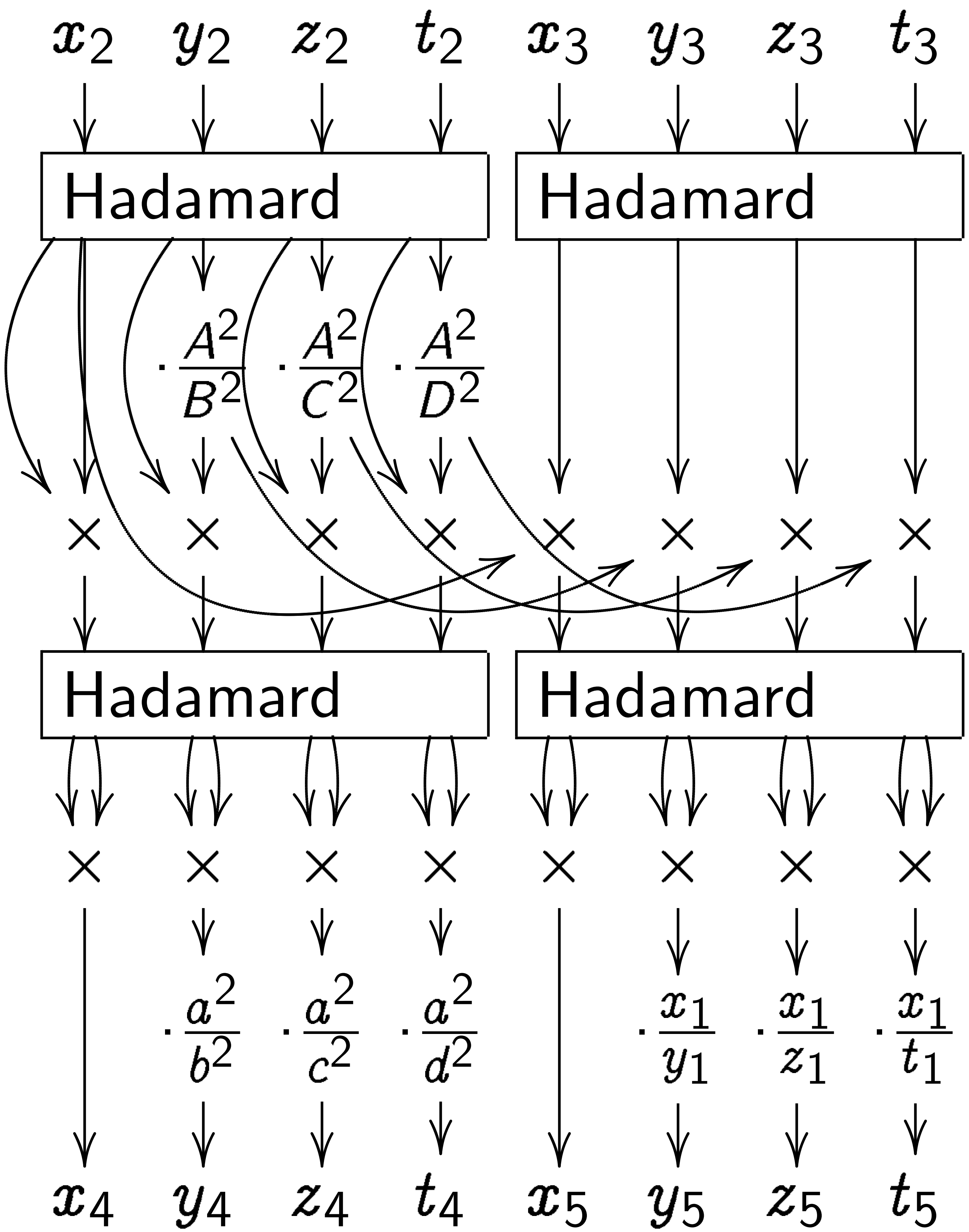
efficients.

ost:

ur computation

l-coefficient

-1.



Strategies to build

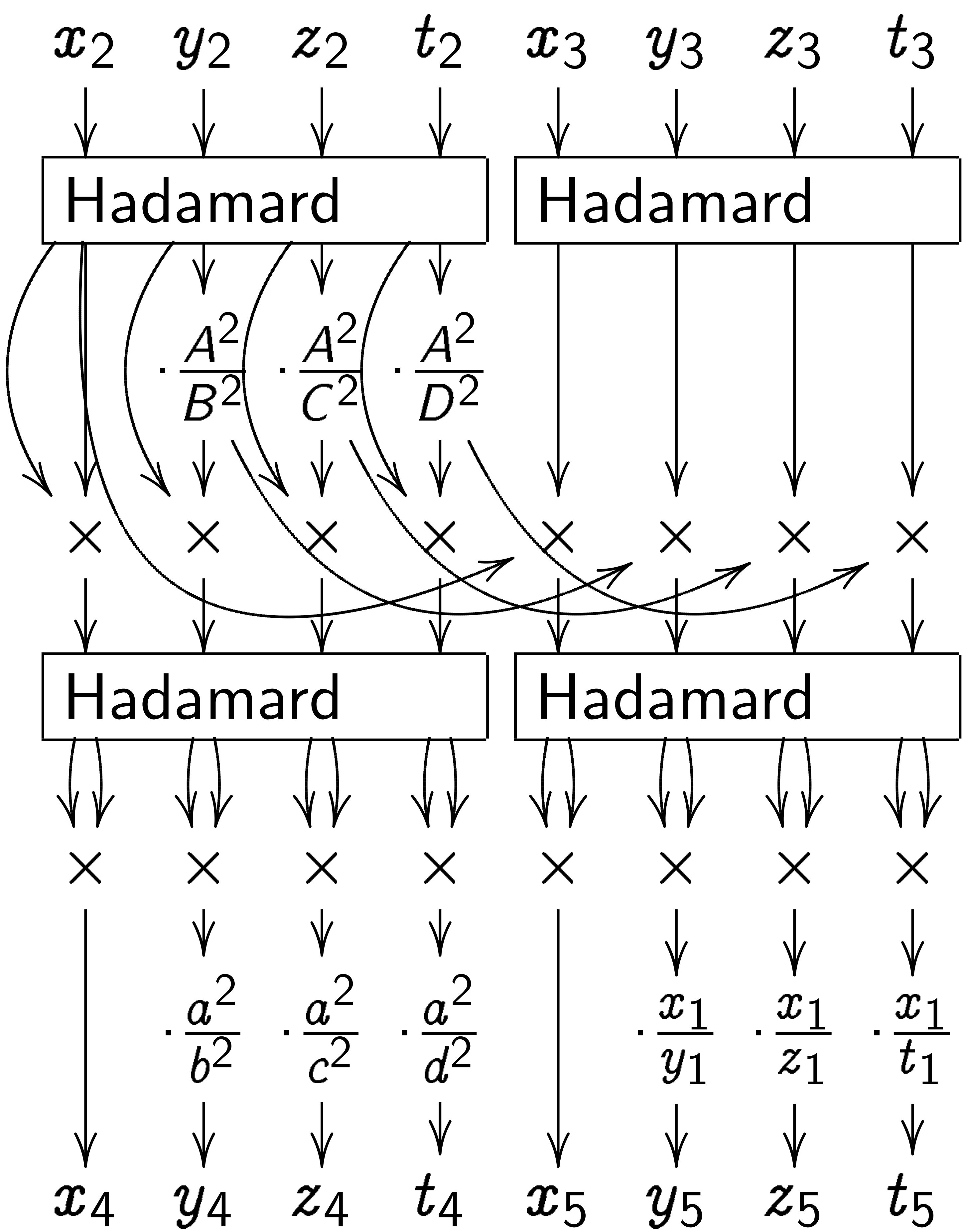
with known $\#J(\mathbf{F}$

	CM
fast build	yes
any curve	no
many curves	no
secure curves	yes
twist-secure	yes
Kummer	yes
small coeff	no
fastest DH	no
fastest keygen	no
complete add	no

sky:

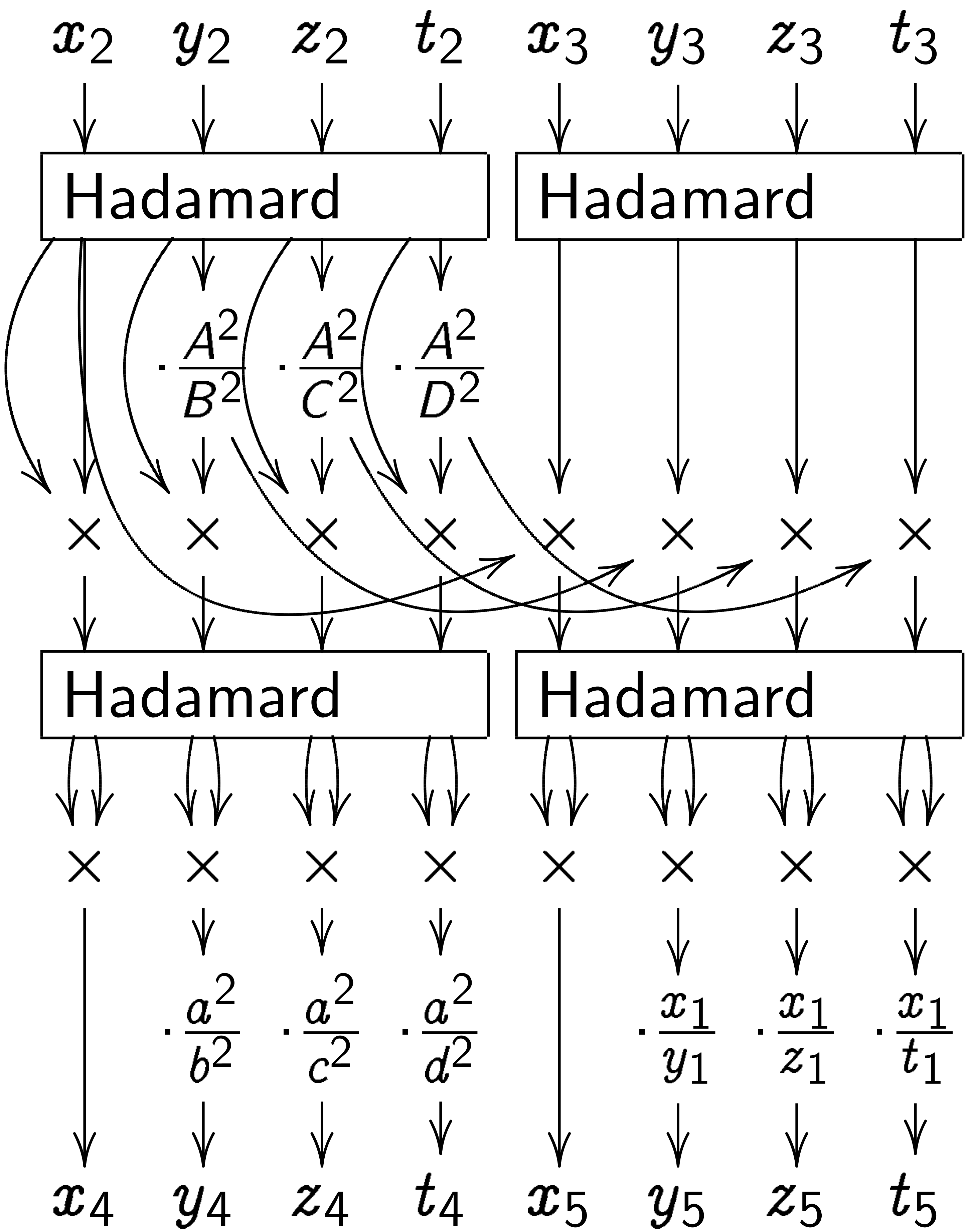
– P)
ding

ation
nt



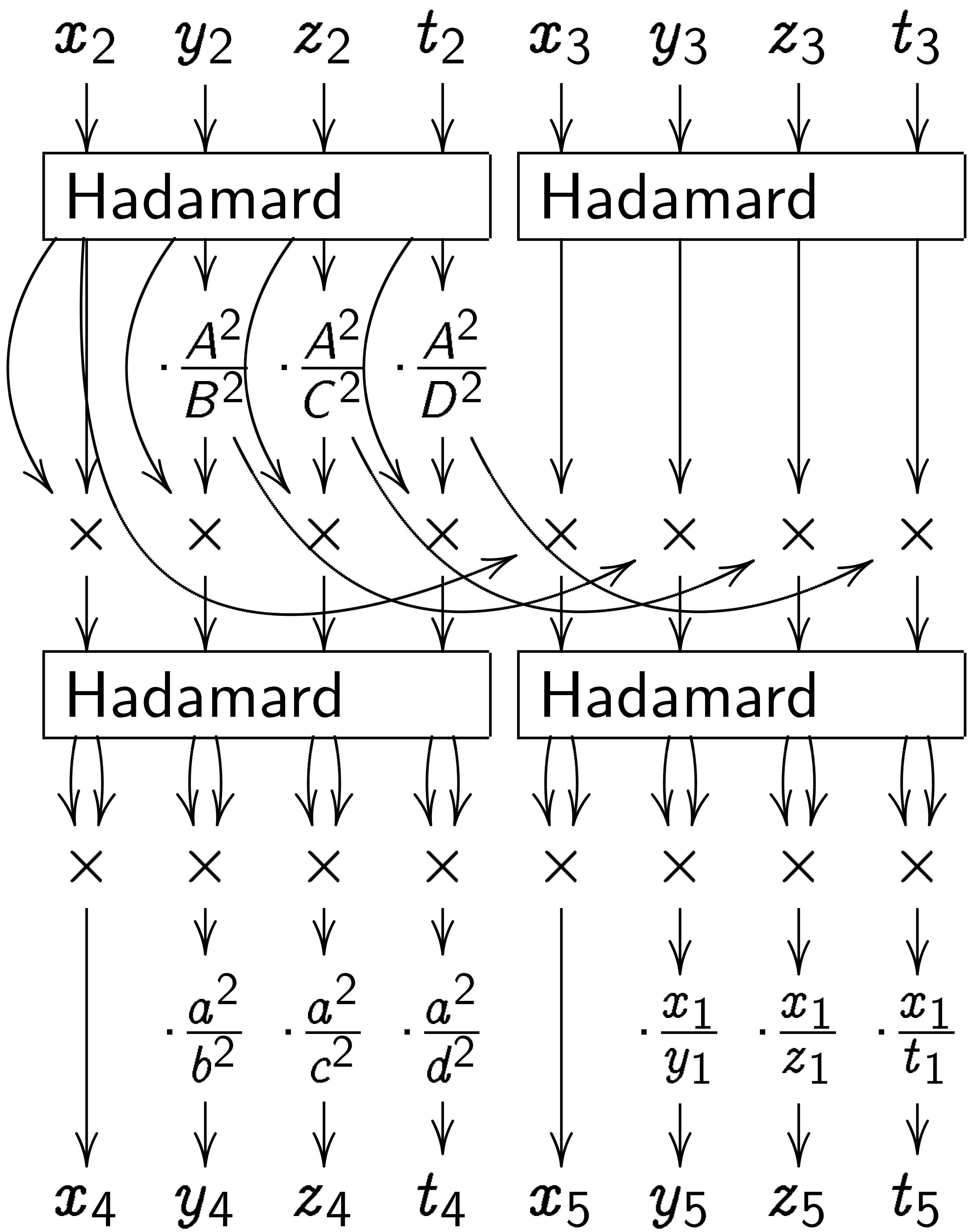
Strategies to build dim-2 J/
with known $\#J(\mathbf{F}_p)$, large p

	CM	Pila	nev
fast build	yes	no	yes
any curve	no	yes	no
many curves	no	yes	yes
secure curves	yes	yes	yes
twist-secure	yes	yes	yes
Kummer	yes	yes	yes
small coeff	no	yes	yes
fastest DH	no	yes	yes
fastest keygen	no	no	yes
complete add	no	no	yes



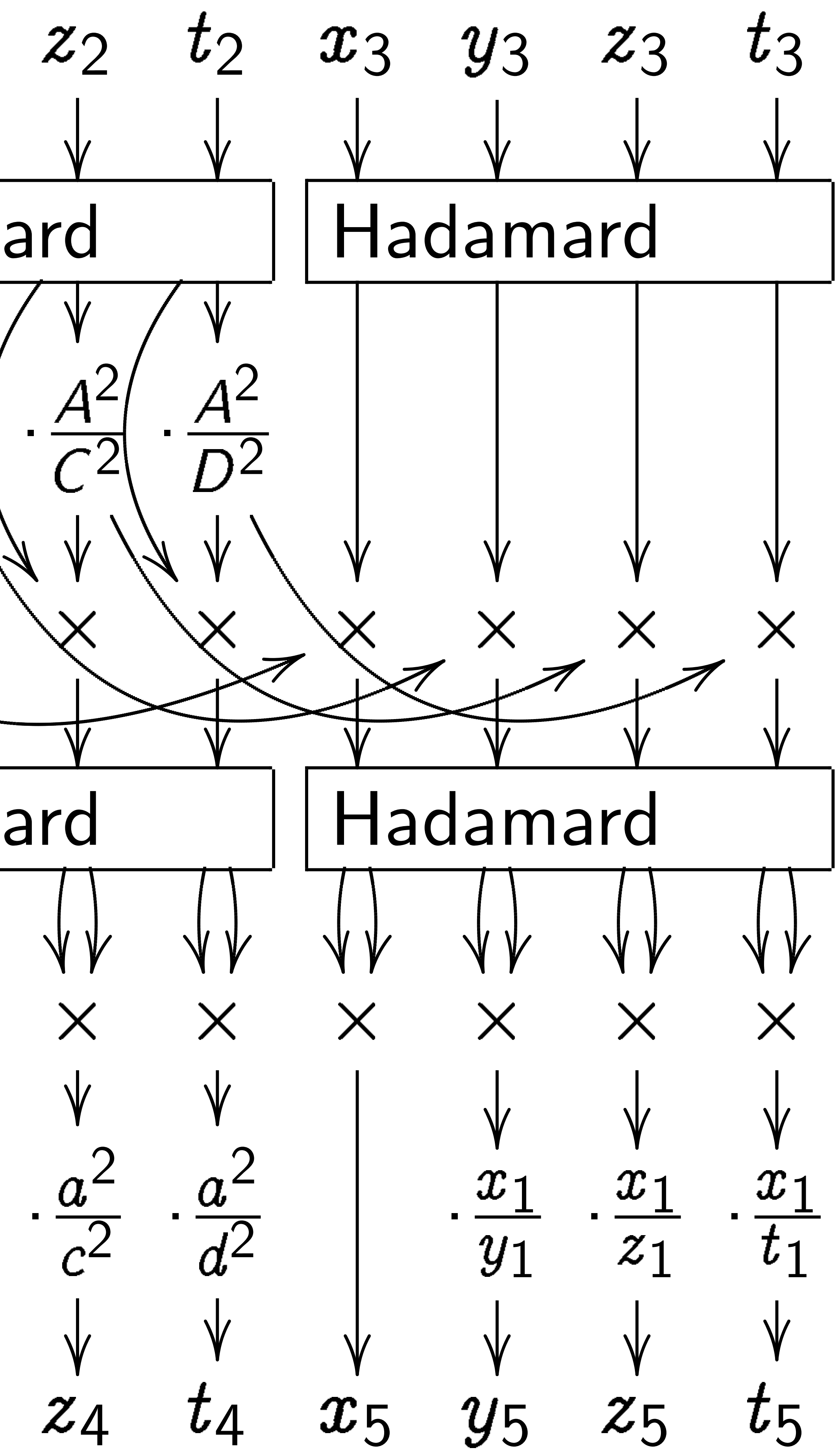
Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	new
fast build	**yes**	no	**yes**
any curve	no	**yes**	no
many curves	no	**yes**	**yes**
secure curves	**yes**	**yes**	**yes**
twist-secure	**yes**	**yes**	**yes**
Kummer	**yes**	**yes**	**yes**
small coeff	no	**yes**	**yes**
fastest DH	no	**yes**	**yes**
fastest keygen	no	no	**yes**
complete add	no	no	**yes**



Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	**yes**	no	**yes**	**yes**
any curve	no	**yes**	no	no
many curves	no	**yes**	**yes**	**yes**
secure curves	**yes**	**yes**	**yes**	**yes**
twist-secure	**yes**	**yes**	**yes**	**yes**
Kummer	**yes**	**yes**	**yes**	**yes**
small coeff	no	**yes**	no	**yes**
fastest DH	no	**yes**	no	**yes**
fastest keygen	no	no	no	**yes**
complete add	no	no	no	**yes**



Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	**yes**	no	**yes**	**yes**
any curve	no	**yes**	no	no
many curves	no	**yes**	**yes**	**yes**
secure curves	**yes**	**yes**	**yes**	**yes**
twist-secure	**yes**	**yes**	**yes**	**yes**
Kummer	**yes**	**yes**	**yes**	**yes**
small coeff	no	**yes**	no	**yes**
fastest DH	no	**yes**	no	**yes**
fastest keygen	no	no	no	**yes**
complete add	no	no	no	**yes**

Hyper-a

Typical

$H : y^2 =$

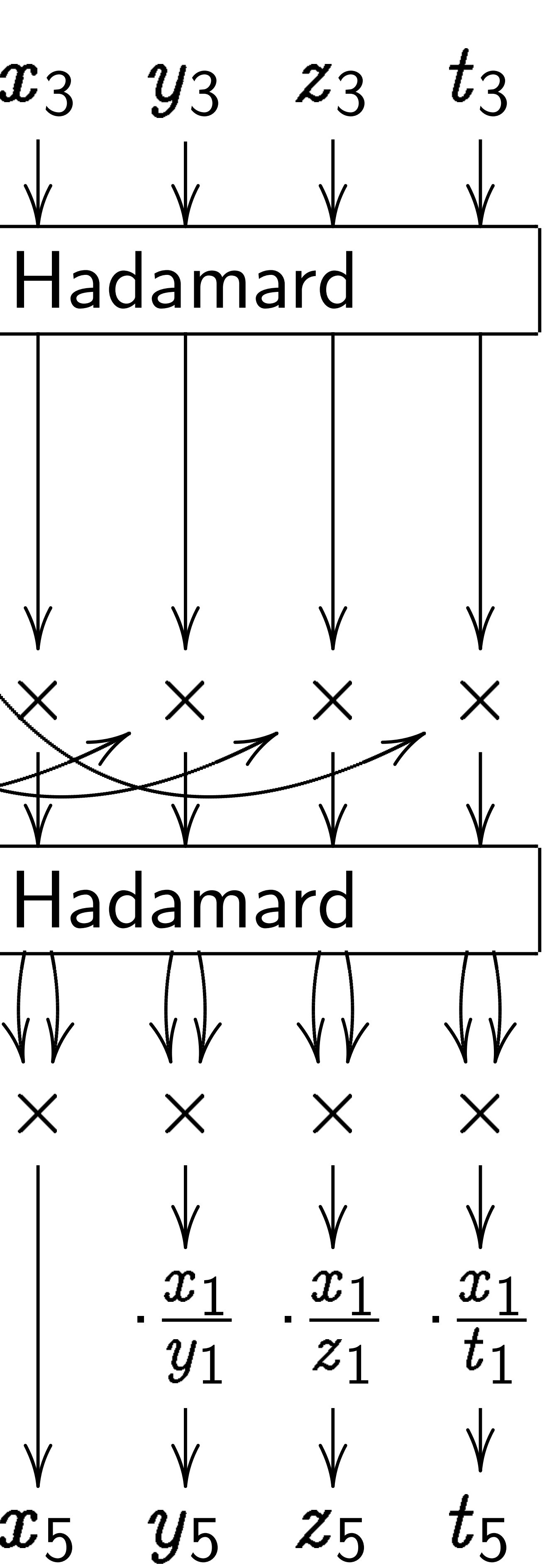
$(z$

over $\mathbf{F}_p$

$J =$ Jac

surface

Small K



Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	**yes**	no	**yes**	**yes**
any curve	no	**yes**	no	no
many curves	no	**yes**	**yes**	**yes**
secure curves	**yes**	**yes**	**yes**	**yes**
twist-secure	**yes**	**yes**	**yes**	**yes**
Kummer	**yes**	**yes**	**yes**	**yes**
small coeff	no	**yes**	no	**yes**
fastest DH	no	**yes**	no	**yes**
fastest keygen	no	no	no	**yes**
complete add	no	no	no	**yes**

Hyper-and-elliptic-

Typical example:

$H : y^2 = (z-1)($

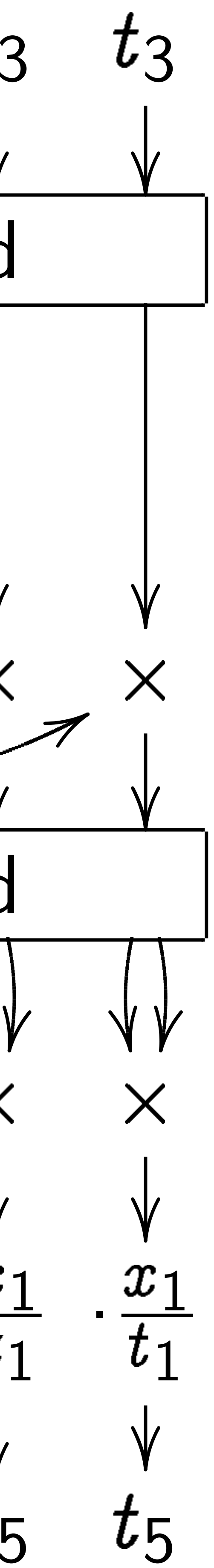
$(z - 1/2)(z +$

over $\mathbf{F}_p$ with $p =$

$J = \mathrm{Jac}\,H$; traditi

surface K; traditio

Small K coeffs (2



Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	yes	no	yes	yes
any curve	no	yes	no	no
many curves	no	yes	yes	yes
secure curves	yes	yes	yes	yes
twist-secure	yes	yes	yes	yes
Kummer	yes	yes	yes	yes
small coeff	no	yes	no	yes
fastest DH	no	yes	no	yes
fastest keygen	no	no	no	yes
complete add	no	no	no	yes

Hyper-and-elliptic-curve cryp

Typical example: Define

$H : y^2 = (z-1)(z+1)(z+$
$(z-1/2)(z+3/2)(z-$

over $\mathbf{F}_p$ with $p = 2^{127} - 309$

$J = \mathrm{Jac}\, H$; traditional Kumm

surface K; traditional $X : J$

Small K coeffs $(20 : 1 : 20 :$

Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	yes	no	yes	yes
any curve	no	yes	no	no
many curves	no	yes	yes	yes
secure curves	yes	yes	yes	yes
twist-secure	yes	yes	yes	yes
Kummer	yes	yes	yes	yes
small coeff	no	yes	no	yes
fastest DH	no	yes	no	yes
fastest keygen	no	no	no	yes
complete add	no	no	no	yes

Hyper-and-elliptic-curve crypto

Typical example: Define

$$H : y^2 = (z-1)(z+1)(z+2)(z-1/2)(z+3/2)(z-2/3)$$

over $\mathbf{F}_p$ with $p = 2^{127} - 309$; $J = \text{Jac}\, H$; traditional Kummer surface K; traditional $X : J \to K$. Small K coeffs $(20 : 1 : 20 : 40)$.

Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	yes	no	yes	yes
any curve	no	yes	no	no
many curves	no	yes	yes	yes
secure curves	yes	yes	yes	yes
twist-secure	yes	yes	yes	yes
Kummer	yes	yes	yes	yes
small coeff	no	yes	no	yes
fastest DH	no	yes	no	yes
fastest keygen	no	no	no	yes
complete add	no	no	no	yes

Hyper-and-elliptic-curve crypto

Typical example: Define
$H : y^2 = (z-1)(z+1)(z+2)$
$(z-1/2)(z+3/2)(z-2/3)$
over $\mathbf{F}_p$ with $p = 2^{127} - 309$;
$J = \text{Jac}\, H$; traditional Kummer surface K; traditional $X : J \to K$.
Small K coeffs $(20 : 1 : 20 : 40)$.

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

es to build dim-2 $J/\mathbf{F}_p$

own $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
ld	**yes**	no	**yes**	**yes**
ve	no	**yes**	no	no
urves	no	**yes**	**yes**	**yes**
curves	**yes**	**yes**	**yes**	**yes**
cure	**yes**	**yes**	**yes**	**yes**
r	**yes**	**yes**	**yes**	**yes**
oeff	no	**yes**	no	**yes**
DH	no	**yes**	no	**yes**
keygen	no	no	no	**yes**
e add	no	no	no	**yes**

Hyper-and-elliptic-curve crypto

Typical example: Define

$H : y^2 = (z-1)(z+1)(z+2)$
$\quad (z-1/2)(z+3/2)(z-2/3)$

over $\mathbf{F}_p$ with $p = 2^{127} - 309$;

$J = \operatorname{Jac} H$; traditional Kummer surface K; traditional $X : J \to K$.

Small K coeffs $(20 : 1 : 20 : 40)$.

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

$\#J(\mathbf{F}_p)$

where ℓ

1809251

4076074

2895314

Security

Order of

1215294

1225631

Twist se

(Want n

Switch t

cofactor

l dim-2 $J/\mathbf{F}_p$

p), large p:

M	Pila	Stn	new
s	no	yes	yes
	yes	no	no
	yes	yes	yes
s	yes	yes	yes
s	yes	yes	yes
s	yes	yes	yes
	yes	no	yes
	yes	no	yes
	no	no	yes
	no	no	yes

Hyper-and-elliptic-curve crypto

Typical example: Define

$$H : y^2 = (z-1)(z+1)(z+2)$$
$$(z-1/2)(z+3/2)(z-2/3)$$

over $\mathbf{F}_p$ with $p = 2^{127} - 309$;

$J = \operatorname{Jac} H$; traditional Kummer surface K; traditional $X : J \to K$.

Small K coeffs $(20:1:20:40)$.

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

$\#J(\mathbf{F}_p) = 16\ell$

where ℓ is the prin

180925139433306

407607485536491

289531455285792

Security $\approx 2^{125}$ ag

Order of ℓ in $(\mathbf{Z}/p$

121529416757478

122563150387.

Twist security ≈ 2

(Want more twist

Switch to $p = 2^{127}$

cofactors $16 \cdot 326$

$\mathbf{F}_p$

):

n	new
s	yes
	no
s	yes
s	yes
s	yes
s	yes
	yes
	yes
	yes
	yes

Hyper-and-elliptic-curve crypto

Typical example: Define

$H : y^2 = (z-1)(z+1)(z+2)$
$\quad (z-1/2)(z+3/2)(z-2/3)$

over $\mathbf{F}_p$ with $p = 2^{127} - 309$;

$J = \text{Jac}\, H$; traditional Kummer surface K; traditional $X : J \to K$.

Small K coeffs $(20:1:20:40)$.

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

$\#J(\mathbf{F}_p) = 16\ell$

where ℓ is the prime

180925139433306555349329

407607485536491946060108

289531455285792829679923

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is

121529416757478022665490

122563150387.

Twist security $\approx 2^{75}$.

(Want more twist security?

Switch to $p = 2^{127} - 94825$

cofactors $16 \cdot 3269239$, 4.)

Hyper-and-elliptic-curve crypto

Typical example: Define
$H : y^2 = (z-1)(z+1)(z+2)$
$(z-1/2)(z+3/2)(z-2/3)$
over $\mathbf{F}_p$ with $p = 2^{127} - 309$;
$J = \text{Jac}\, H$; traditional Kummer surface K; traditional $X : J \to K$.
Small K coeffs $(20 : 1 : 20 : 40)$.

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is 121529416757478022665490931225631503 87.

Twist security $\approx 2^{75}$.

(Want more twist security? Switch to $p = 2^{127} - 94825$; cofactors $16 \cdot 3269239$, 4.)

nd-elliptic-curve crypto

example: Define

= $(z-1)(z+1)(z+2)$

$- 1/2)(z+3/2)(z-2/3)$

with $p = 2^{127} - 309$;

H; traditional Kummer

K; traditional $X : J \to K$.

coeffs (20 : 1 : 20 : 40).

: There are typos in the

in/Mumford/Kummer

s in 2007 Gaudry, 2010

2013 Bos–Costello–

uter. We have simpler,

er-verified formulas.

$\#J(\mathbf{F}_p) = 16\ell$

where ℓ is the prime

1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is

1215294167574780226654909312256315038 7.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast poi

Define **F**

$r = (7 +$

$s = 159$

$C : y^2 =$

-curve crypto

Define

$z+1)(z+2)$

$+3/2)(z-2/3)$

$2^{127}-309$;

onal Kummer

onal $X : J \to K$.

$0:1:20:40)$.

re typos in the

rd/Kummer

Gaudry, 2010

-Costello–

have simpler,

formulas.

$\#J(\mathbf{F}_p) = 16\ell$

where ℓ is the prime

1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is 1215294167574780226654909 3122563150387.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-countin

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i$

$r = (7+4i)^2 = 3$

$s = 159 + 56i$; ω

$C : y^2 = rx^6 + sx$

oto

- 2)

- 2/3)

9;

mer

$\to K$.

40).

n the

ner

010

ler,

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
180925139433306555349329664076074856020734292531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is
1215294167574780226654909312256315038 7.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 +$

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
180925139433306555349329664076074855364919460601081428953145528579282967992 3.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is
1215294167574780226654909312256315 0387.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2 + 1)$;
$r = (7 + 4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is
12152941675747802266549093122563150387.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2 + 1)$;
$r = (7 + 4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is
12152941675747802266549093122563150387.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r$.

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is 1215294167574780226654909312 2563150387.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2 + 1)$;
$r = (7 + 4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

$$(z, y) \mapsto \left(\frac{1 + iz}{1 - iz}, \frac{\omega y}{(1 - iz)^3}\right)$$
takes H over $\mathbf{F}_{p^2}$ to C.

$= 16\ell$
is the prime
3943330655534932966
8553649194606010814
55285792829679923.

$\approx 2^{125}$ against rho.

f ℓ in $(\mathbf{Z}/p)^*$ is
1675747802266549093
50387.

ecurity $\approx 2^{75}$.

nore twist security?
to $p = 2^{127} - 94825$;
s $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$(x,y) \mapsto (x^2,y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

$(x,y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r$.

$$(z,y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$$
takes H over $\mathbf{F}_{p^2}$ to C.

J is isog
Weil res
computi

me
55534932966
94606010814
829679923.

gainst rho.

$)^*$ is
02266549093

^{75}.

security?
$^7 - 94825$;
9239, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

$$(z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$$
takes H over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W
computing $\#J(\mathbf{F}_p$

966

314

3.

093

;

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$(x,y) \mapsto (x^2,y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

$(x,y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r$.

$$(z,y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$$
takes H over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r$.

$$(z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$$

takes H over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

$$(z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$$
takes H over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x,y) \mapsto (x^2,y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x,y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

$(z,y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$
takes H over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over $\mathbf{F}_{p^2}$ with full 2-torsion
(and more elliptic curves).
Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.

nt-counting

$_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$4i)^2 = 33 + 56i$;
$+ 56i$; $\omega = \sqrt{-384}$;
$= rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

(x^2, y) takes C to E :
$^3 + sx^2 + \overline{s}x + \overline{r}$.

$(1/x^2, y/x^3)$ takes C to
$^3 + \overline{s}x^2 + sx + r$.

$\left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$
over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over $\mathbf{F}_{p^2}$ with full 2-torsion
(and more elliptic curves).
Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.

New: no

Alice ge
Bob gen

Alice co
using st
Top spe

Alice se

Bob vie
applies
compute
Top spe

ng

$]/(i^2+1)$;
$3+56i$;
$= \sqrt{-384}$;
$^4+\bar{s}x^2+\bar{r}$.

akes C to E :
$\bar{s}x+\bar{r}$.

$/x^3)$ takes C to
$sx+r$.

$, \frac{\omega y}{(1-iz)^3}\Big)$
to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over $\mathbf{F}_{p^2}$ with full 2-torsion
(and more elliptic curves).
Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.

New: not just poi

Alice generates se
Bob generates sec

Alice computes aG
using standard G
Top speed: Edwar

Alice sends aG to

Bob views aG in W
applies isogeny W
computes $b(aG)$ in
Top speed: Kumm

;

;

$\overline{r}$.

E :

C to

)

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over $\mathbf{F}_{p^2}$ with full 2-torsion
(and more elliptic curves).
Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.

New: not just point-countin

Alice generates secret $a \in \mathbf{Z}$
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2}$
using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordin

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$,
applies isogeny $W(\mathbf{F}_p) \to J($
computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordi

J is isogenous to Weil restriction W of E, so computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten: this strategy for building many genus-2 curves with fast point-counting.

Handles all elliptic curves over $\mathbf{F}_{p^2}$ with full 2-torsion (and more elliptic curves). Geometrically: all elliptic curves; codim 1 in hyperelliptic curves.

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$. Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$ using standard $G \in E(\mathbf{F}_{p^2})$. Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$, applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$, computes $b(aG)$ in $J(\mathbf{F}_p)$. Top speed: Kummer coordinates.

genous to
triction W of E, so
ng $\#J(\mathbf{F}_p)$ is fast.

holten:
tegy for
many genus-2 curves
t point-counting.

all elliptic curves
with full 2-torsion
ore elliptic curves).
rically: all elliptic curves;
in hyperelliptic curves.

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$.
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$
using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$,
applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$,
computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordinates.

In gener
$\iota : W \to$
dynamic
between

But do v
for ι' an

of E, so
) is fast.

us-2 curves
unting.

curves
2-torsion
curves).
elliptic curves;
lliptic curves.

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$.
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$
using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$,
applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$,
computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordinates.

In general: use iso
$\iota : W \to J$ and ι' :
dynamically move
between $E(\mathbf{F}_{p^2})$ a

But do we have **fa**
for ι' and for dual

es

rves;

ves.

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$.
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$
using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$,
applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$,
computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies
$\iota : W \to J$ and $\iota' : J \to W$ t
dynamically move computat
between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formul**
for ι' and for dual isogeny ι

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$.
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$
using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$,
applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$,
computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies
$\iota : W \to J$ and $\iota' : J \to W$ to
dynamically move computations
between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas**
for ι' and for dual isogeny ι?

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$.
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$ using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$, applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$, computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

Scholten: Define $\phi : H \to E$ as

$$(z, y) \mapsto \left(\frac{(1+iz)^2}{(1-iz)^2}, \frac{\omega y}{(1-iz)^3} \right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1)+\phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

ot just point-counting

nerates secret $a \in \mathbf{Z}$.

erates secret $b \in \mathbf{Z}$.

mputes $aG \in E(\mathbf{F}_{p^2})$

andard $G \in E(\mathbf{F}_{p^2})$.

ed: Edwards coordinates.

nds aG to Bob.

ws aG in $W(\mathbf{F}_p)$,

sogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$,

es $b(aG)$ in $J(\mathbf{F}_p)$.

ed: Kummer coordinates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

Scholten: Define $\phi : H \to E$ as

$$(z, y) \mapsto \left(\frac{(1+iz)^2}{(1-iz)^2}, \frac{\omega y}{(1-iz)^3}\right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1)+\phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The con

1. Prove

by analy

2. Obse

for some

3. Comp

$P_i = (z_i$

over $\mathbf{F}_p($

$/(y_1^2 -$

compose

with add

eliminate

in favor

nt-counting

cret $a \in \mathbf{Z}$.
ret $b \in \mathbf{Z}$.

$G \in E(\mathbf{F}_{p^2})$
$\in E(\mathbf{F}_{p^2})$.
rds coordinates.

Bob.

$W(\mathbf{F}_p)$,
$(\mathbf{F}_p) \to J(\mathbf{F}_p)$,
n $J(\mathbf{F}_p)$.
ner coordinates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

Scholten: Define $\phi : H \to E$ as

$$(z, y) \mapsto \left(\frac{(1+iz)^2}{(1-iz)^2}, \frac{\omega y}{(1-iz)^3} \right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1)+\phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional

1. Prove that ι' is
by analyzing fibers

2. Observe that ι
for some isogeny ι

3. Compute formu
$P_i = (z_i, y_i)$ on H
over $\mathbf{F}_p(z_1, z_2)[y_1$
$/(y_1^2 - f(z_1), y_2^2 -$
compose definition
with addition form
eliminate z_1, z_2, y_1
in favor of Mumfo

g

.

t.

)

nates.

$(\mathbf{F}_p)$,

nates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

Scholten: Define $\phi : H \to E$ as

$$(z, y) \mapsto \left(\frac{(1 + iz)^2}{(1 - iz)^2}, \frac{\omega y}{(1 - iz)^3} \right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional continuati

1. Prove that ι' is an isoger by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': $P_i = (z_i, y_i)$ on $H : y^2 = f($ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordin

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

Scholten: Define $\phi : H \to E$ as $(z, y) \mapsto \left(\frac{(1+iz)^2}{(1-iz)^2}, \frac{\omega y}{(1-iz)^3}\right)$.

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1)+\phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

al: use isogenies
J and $\iota' : J \to W$ to
ally move computations
$E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

we have **fast formulas**
d for dual isogeny ι?

n: Define $\phi : H \to E$ as
$$\left(\frac{(1+iz)^2}{(1-iz)^2}, \frac{\omega y}{(1-iz)^3}\right).$$
ition of $\phi_2 : (P_1, P_2) \mapsto$
$\phi(P_2)$ and standard $E \to W$
osition of standard
$\to J$ and some $\iota' : J \to W$.

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

4. Simp
using, e.
"rationa

5. Find

ogenies

: $J \to W$ to

computations

nd $J(\mathbf{F}_p)$.

ast formulas

isogeny ι?

$\phi : H \to E$ as

$)^2$ ... $)^2$, $\dfrac{\omega y}{(1 - iz)^3}\Bigg)$.

$_2 : (P_1, P_2) \mapsto$

standard $E \to W$

standard

ome $\iota' : J \to W$.

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

4. Simplify formul

using, e.g., 2006 M

“rational simplifica

5. Find ι: norm–c

to
ions

las
?

as
$z)^3$).
$) \mapsto$
$E \to W$

$\to W$.

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

4. Simplify formulas for ι' using, e.g., 2006 Monagan–
“rational simplification” met

5. Find ι: norm–conorm etc

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

4. Simplify formulas for ι' using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find ι: norm–conorm etc.

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2]$ $/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

4. Simplify formulas for ι' using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$, interpolated coefficients of ι'. Similarly interpolated formulas for ι; verified composition.

Easy computer calculation. "Wasting brain power is bad for the environment."

ventional continuation:

e that ι' is an isogeny
zing fibers of ϕ_2.

rve that $\iota \circ \iota' = 2$
e isogeny ι.

pute formulas for ι': take
$, y_i)$ on $H : y^2 = f(z)$
$(z_1, z_2)[y_1, y_2]$
$f(z_1), y_2^2 - f(z_2))$;
e definition of ϕ
dition formulas on E;
e z_1, z_2, y_1, y_2
of Mumford coordinates.

4. Simplify formulas for ι'
using, e.g., 2006 Monagan–Pearce
"rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to
random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$,
interpolated coefficients of ι'.
Similarly interpolated formulas
for ι; verified composition.

Easy computer calculation.
"Wasting brain power
is bad for the environment."

New: sn

K define
Only 2 c

Can't ex
. . . unle

continuation:

s an isogeny
s of ϕ_2.

$\circ\, \iota' = 2$

.

ulas for ι': take
$' : y^2 = f(z)$
$, y_2]$
$- f(z_2))$;
n of ϕ
nulas on E;
$_1, y_2$
rd coordinates.

4. Simplify formulas for ι'
using, e.g., 2006 Monagan–Pearce
"rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to
random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$,
interpolated coefficients of ι'.
Similarly interpolated formulas
for ι; verified composition.

Easy computer calculation.
"Wasting brain power
is bad for the environment."

New: small coeffic

K defined by 3 co
Only 2 degrees of

Can't expect smal
... unless everyth

on:

ny

take

(z)

;

ates.

4. Simplify formulas for ι' using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$, interpolated coefficients of ι'. Similarly interpolated formulas for ι; verified composition.

Easy computer calculation. "Wasting brain power is bad for the environment."

New: small coefficients

K defined by 3 coeffs. Only 2 degrees of freedom i

Can't expect small-height c

. . . unless everything lifts to

4. Simplify formulas for ι' using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$, interpolated coefficients of ι'. Similarly interpolated formulas for ι; verified composition.

Easy computer calculation. "Wasting brain power is bad for the environment."

New: small coefficients

K defined by 3 coeffs. Only 2 degrees of freedom in E.

Can't expect small-height coeffs. ... unless everything lifts to $\mathbf{Q}$.

4. Simplify formulas for ι' using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$, interpolated coefficients of ι'. Similarly interpolated formulas for ι; verified composition.

Easy computer calculation. "Wasting brain power is bad for the environment."

New: small coefficients

K defined by 3 coeffs. Only 2 degrees of freedom in E.

Can't expect small-height coeffs. . . . unless everything lifts to $\mathbf{Q}$.

Choose non-square $\Delta \in \mathbf{Q}$; distinct squares ρ_1, ρ_2, ρ_3 of norm-1 elements of $\mathbf{Q}(\sqrt{\Delta})$; $r \in \mathbf{Q}(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$. Then $rx^3 + sx^2 + \overline{s}x + \overline{r} = r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

lify formulas for ι'
g., 2006 Monagan–Pearce
l simplification" method.

ι: norm–conorm etc.

---

asier: We applied ϕ_2 to
points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$,
ated coefficients of ι'.
interpolated formulas
rified composition.

mputer calculation.
g brain power
or the environment."

New: small coefficients

K defined by 3 coeffs.
Only 2 degrees of freedom in E.

Can't expect small-height coeffs.
... unless everything lifts to $\mathbf{Q}$.

Choose non-square $\Delta \in \mathbf{Q}$;
distinct squares ρ_1, ρ_2, ρ_3
of norm-1 elements of $\mathbf{Q}(\sqrt{\Delta})$;
$r \in \mathbf{Q}(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.
Then $rx^3 + sx^2 + \overline{s}x + \overline{r} =$
$r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

Choose
and $(\overline{\beta}/$

Then th
$(r\overline{\beta}^6 + s$
$r(1-\overline{\beta}z$
$\overline{s}(1-\overline{\beta}z$
has full

In many
Rosenha
have $\frac{\lambda\mu}{\nu}$
both squ
so K is
(Degene

as for ι'
Monagan–Pearce
ation" method.

conorm etc.

---

applied ϕ_2 to
$H(\mathbf{F}_p) \times H(\mathbf{F}_p)$,
cients of ι'.
ted formulas
position.

lculation.
wer
ronment."

<u>New: small coefficients</u>

K defined by 3 coeffs.
Only 2 degrees of freedom in E.

Can't expect small-height coeffs.
. . . unless everything lifts to $\mathbf{Q}$.

Choose non-square $\Delta \in \mathbf{Q}$;
distinct squares ρ_1, ρ_2, ρ_3
of norm-1 elements of $\mathbf{Q}(\sqrt{\Delta})$;
$r \in \mathbf{Q}(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.
Then $rx^3 + sx^2 + \overline{s}x + \overline{r} =$
$r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

Choose $\beta \in \mathbf{Q}(\sqrt{}$
and $(\overline{\beta}/\beta)^2 \notin \{\rho_1$

Then the Scholten
$(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}$
$r(1-\overline{\beta}z)^6 + s(1-$
$\overline{s}(1-\overline{\beta}z)^2(1-\beta z$
has full 2-torsion o

In many cases corr
Rosenhain parame
have $\frac{\lambda\mu}{\nu}$ and $\frac{\mu(\mu}{\nu(\nu}$
both squares in $\mathbf{Q}$
so K is defined ov
(Degenerate cases

Pearce
thod.

c.

---

to
$H(\mathbf{F}_p)$,
$'$.
las

New: small coefficients

K defined by 3 coeffs.
Only 2 degrees of freedom in E.

Can't expect small-height coeffs.
. . . unless everything lifts to $\mathbf{Q}$.

Choose non-square $\Delta \in \mathbf{Q}$;
distinct squares ρ_1, ρ_2, ρ_3
of norm-1 elements of $\mathbf{Q}(\sqrt{\Delta})$;
$r \in \mathbf{Q}(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.
Then $rx^3 + sx^2 + \overline{s}x + \overline{r} =$
$r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with β
and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve
$(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6$
$r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-$
$\overline{s}(1 - \overline{\beta}z)^2(1 - \beta z)^4 + \overline{r}(1 -$
has full 2-torsion over $\mathbf{Q}$.

In many cases correspondin
Rosenhain parameters $\lambda, \mu,$
have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu - 1)(\lambda -}{\nu(\nu - 1)(\lambda -}$
both squares in $\mathbf{Q}$,
so K is defined over $\mathbf{Q}$.
(Degenerate cases: see pape

New: small coefficients

K defined by 3 coeffs.
Only 2 degrees of freedom in E.

Can't expect small-height coeffs.
... unless everything lifts to $\mathbf{Q}$.

Choose non-square $\Delta \in \mathbf{Q}$;
distinct squares ρ_1, ρ_2, ρ_3
of norm-1 elements of $\mathbf{Q}(\sqrt{\Delta})$;
$r \in \mathbf{Q}(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.
Then $rx^3 + sx^2 + \overline{s}x + \overline{r} =$
$r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$
and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve
$(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 =$
$r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 +$
$\overline{s}(1-\overline{\beta}z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$
has full 2-torsion over $\mathbf{Q}$.

In many cases corresponding
Rosenhain parameters λ, μ, ν
have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$
both squares in $\mathbf{Q}$,
so K is defined over $\mathbf{Q}$.
(Degenerate cases: see paper.)

nall coefficients

ed by 3 coeffs.

degrees of freedom in E.

xpect small-height coeffs.

ss everything lifts to $\mathbf{Q}$.

non-square $\Delta \in \mathbf{Q}$;

squares ρ_1, ρ_2, ρ_3

-1 elements of $\mathbf{Q}(\sqrt{\Delta})$;

$\overline{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

$= -r(\rho_1 + \rho_2 + \rho_3)$.

$c^3 + sx^2 + \overline{s}x + \overline{r} =$

$_1)(x - \rho_2)(x - \rho_3)$.

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$ and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve

$$(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 = r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 + \overline{s}(1-\overline{\beta}z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$$

has full 2-torsion over $\mathbf{Q}$.

In many cases corresponding Rosenhain parameters λ, μ, ν have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$ both squares in $\mathbf{Q}$,
so K is defined over $\mathbf{Q}$.
(Degenerate cases: see paper.)

Example

$\rho_1 = (i)$

$\rho_3 = ((5$

$s = 159$

One Ros

$\lambda = 10,$

Then $\dfrac{\lambda\mu}{\nu}$

and $\dfrac{\mu(\mu}{\nu(\nu}$

Larger e

$r = 864$

$s = -40$

coeffs (6

cients

effs.

freedom in E.

l-height coeffs.

ing lifts to $\mathbf{Q}$.

e $\Delta \in \mathbf{Q}$;

$, \rho_2, \rho_3$

ts of $\mathbf{Q}(\sqrt{\Delta})$;

$-\rho_1\rho_2\rho_3 = \overline{r}/r$.

$+ \rho_2 + \rho_3)$.

$\overline{s}x + \overline{r} =$

$(x - \rho_3)$.

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$ and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve
$(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 =$
$r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 +$
$\overline{s}(1-\overline{\beta}z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$
has full 2-torsion over $\mathbf{Q}$.

In many cases corresponding
Rosenhain parameters λ, μ, ν
have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$
both squares in $\mathbf{Q}$,
so K is defined over $\mathbf{Q}$.
(Degenerate cases: see paper.)

Example: Choose
$\rho_1 = (i)^2$, $\rho_2 = (($
$\rho_3 = ((5+12i)/13$
$s = 159 + 56i$, β
One Rosenhain ch
$\lambda = 10$, $\mu = 5/8$,
Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$
and $\dfrac{\mu(\mu-1)(\lambda -}{\nu(\nu-1)(\lambda -}$

Larger example:
$r = 8648575 - 15$
$s = -40209279 -$
coeffs (6137 : 833

n E.

oeffs.

$\mathbf{Q}$.

$\overline{\Delta})$;

$= \overline{r}/r$.

).

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$ and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve

$$(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 = r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 + \overline{s}(1-\overline{\beta}z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$$

has full 2-torsion over $\mathbf{Q}$.

In many cases corresponding Rosenhain parameters λ, μ, ν have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$ both squares in $\mathbf{Q}$,

so K is defined over $\mathbf{Q}$.

(Degenerate cases: see paper.)

Example: Choose $\Delta = -1$;

$\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5$

$\rho_3 = ((5+12i)/13)^2$; $r = 3$

$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is $\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$

and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$

Larger example:

$r = 8648575 - 15615600i$,

$s = -40209279 - 33245520$

coeffs $(6137 : 833 : 2275 : 2$

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$ and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve $(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 = r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 + \overline{s}(1-\overline{\beta}z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$ has full 2-torsion over $\mathbf{Q}$.

In many cases corresponding Rosenhain parameters λ, μ, ν have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$ both squares in $\mathbf{Q}$, so K is defined over $\mathbf{Q}$. (Degenerate cases: see paper.)

Example: Choose $\Delta = -1$; $\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5)^2$, $\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$, $s = 159+56i$, $\beta = i$.
One Rosenhain choice is $\lambda = 10$, $\mu = 5/8$, $\nu = 25$.
Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$.

Larger example:
$r = 8648575 - 15615600i$,
$s = -40209279 - 33245520i$;
coeffs $(6137 : 833 : 2275 : 2275)$.

$\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$

$\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

e Scholten curve

$s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 =$

$)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 +$

$z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$

2-torsion over $\mathbf{Q}$.

cases corresponding

in parameters λ, μ, ν

and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$

uares in $\mathbf{Q}$,

defined over $\mathbf{Q}$.

rate cases: see paper.)

Example: Choose $\Delta = -1$;
$\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5)^2$,
$\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$,
$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is
$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$

and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$.

Larger example:
$r = 8648575 - 15615600i$,
$s = -40209279 - 33245520i$;
coeffs (6137 : 833 : 2275 : 2275).

$\overline{\Delta}$) with $\beta \notin \mathbf{Q}$

, $\rho_2, \rho_3\}$.

n curve

$\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 =$

$\overline{\beta}z)^4(1-\beta z)^2+$

$z)^4 + \overline{r}(1-\beta z)^6$

over $\mathbf{Q}$.

responding

ters λ, μ, ν

$-1)(\lambda-\nu)$

$-1)(\lambda-\mu)$

,

er $\mathbf{Q}$.

: see paper.)

Example: Choose $\Delta = -1$;

$\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5)^2$,

$\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$,

$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is

$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$

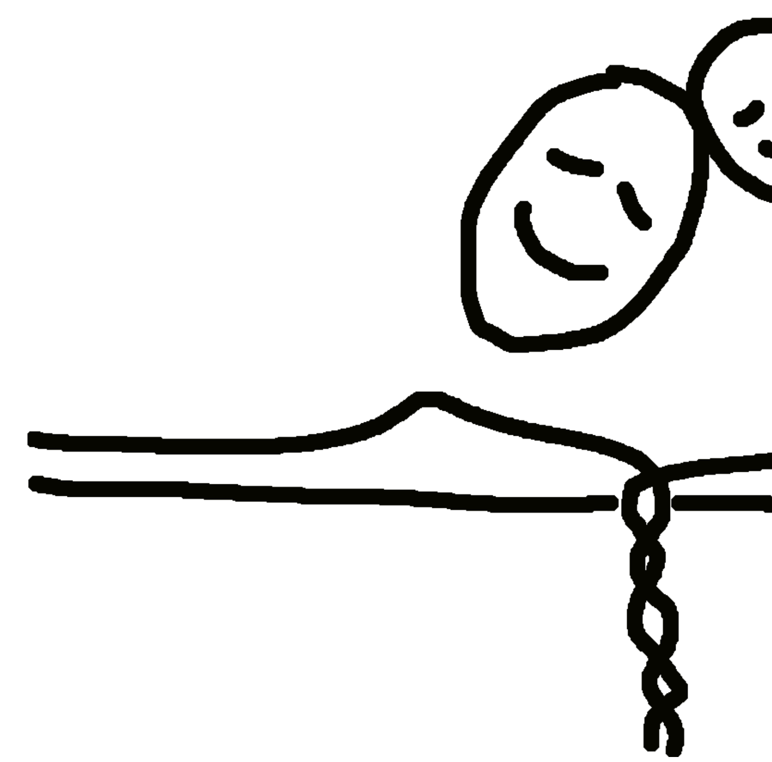
and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$.

Larger example:

$r = 8648575 - 15615600i$,

$s = -40209279 - 33245520i$;

coeffs (6137 : 833 : 2275 : 2275).



$\notin$ **Q**

$)y^2 =$

$\beta z)^2 +$

$-\beta z)^6$

g

ν

$\nu)$

$\mu)$

er.)

Example: Choose $\Delta = -1$;

$\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5)^2$,

$\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$,

$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is

$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$

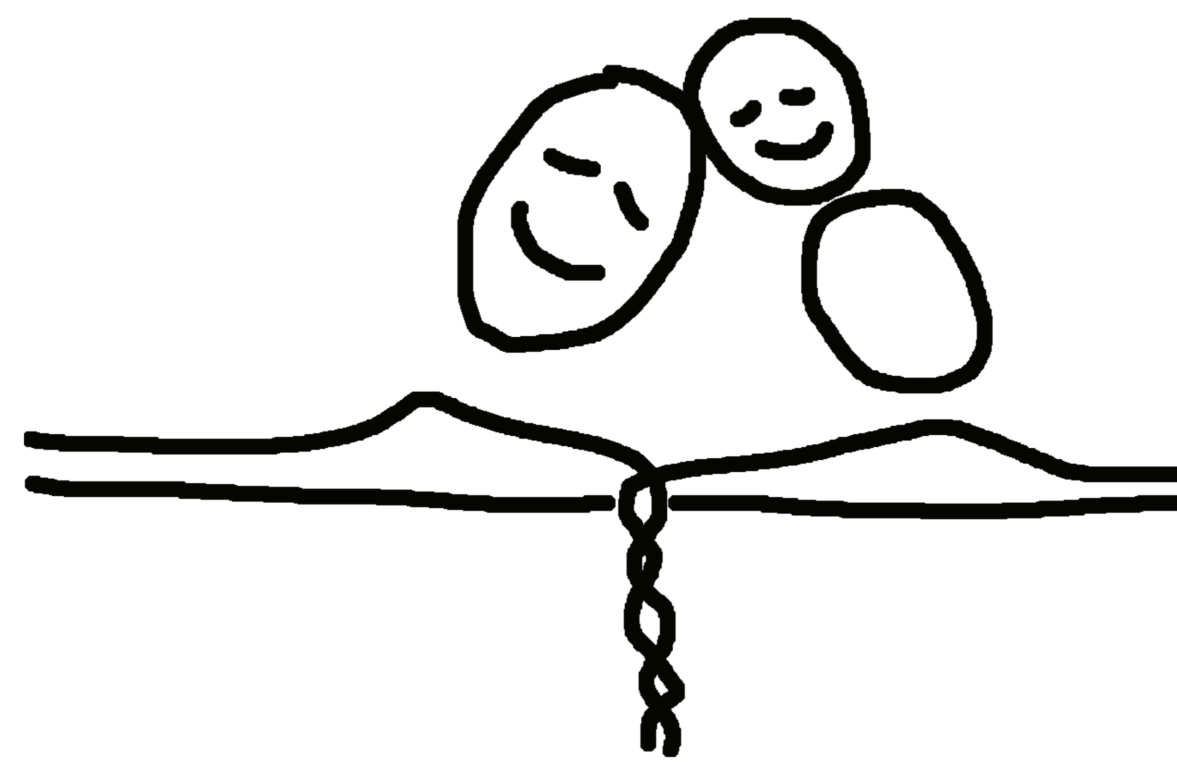
and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$.

Larger example:

$r = 8648575 - 15615600i$,

$s = -40209279 - 33245520i$;

coeffs $(6137 : 833 : 2275 : 2275)$.



Example: Choose $\Delta = -1$;
$\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5)^2$,
$\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$,
$s = 159+56i$, $\beta = i$.

One Rosenhain choice is
$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$

and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$.

Larger example:
$r = 8648575 - 15615600i$,
$s = -40209279 - 33245520i$;
coeffs $(6137 : 833 : 2275 : 2275)$.