Hyper-and-elliptic-curve cryptography

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

Includes recent joint work with:
Tanja Lange
Technische Universiteit Eindhoven

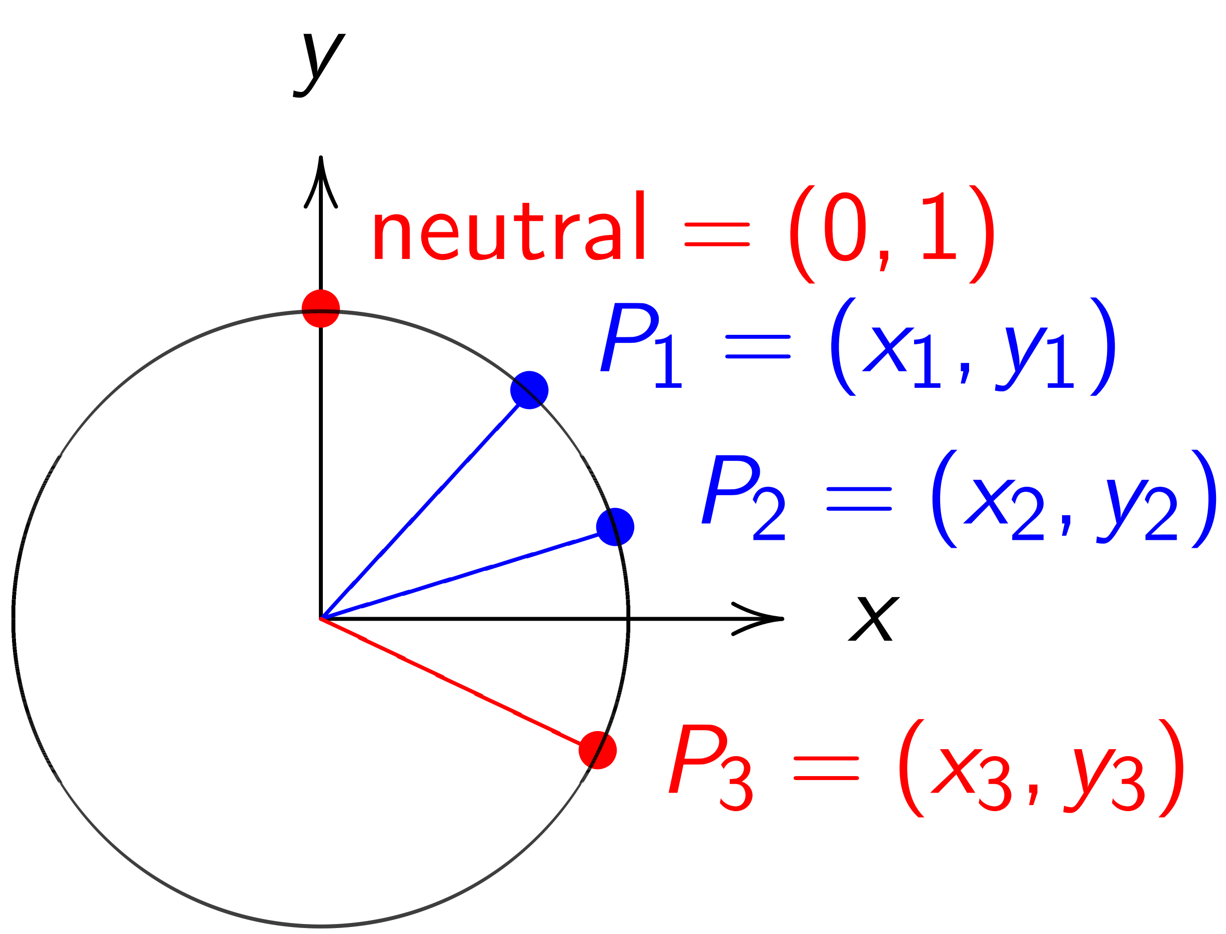
cr.yp.to/papers.html#hyperand

Clock($\mathbf{R}$): the commutative group $\{(x,y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$ under the operations

"0": $() \mapsto (0,1)$;

"−": $(x,y) \mapsto (-x,y)$;

"+": $(x_1,y_1),(x_2,y_2) \mapsto (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.



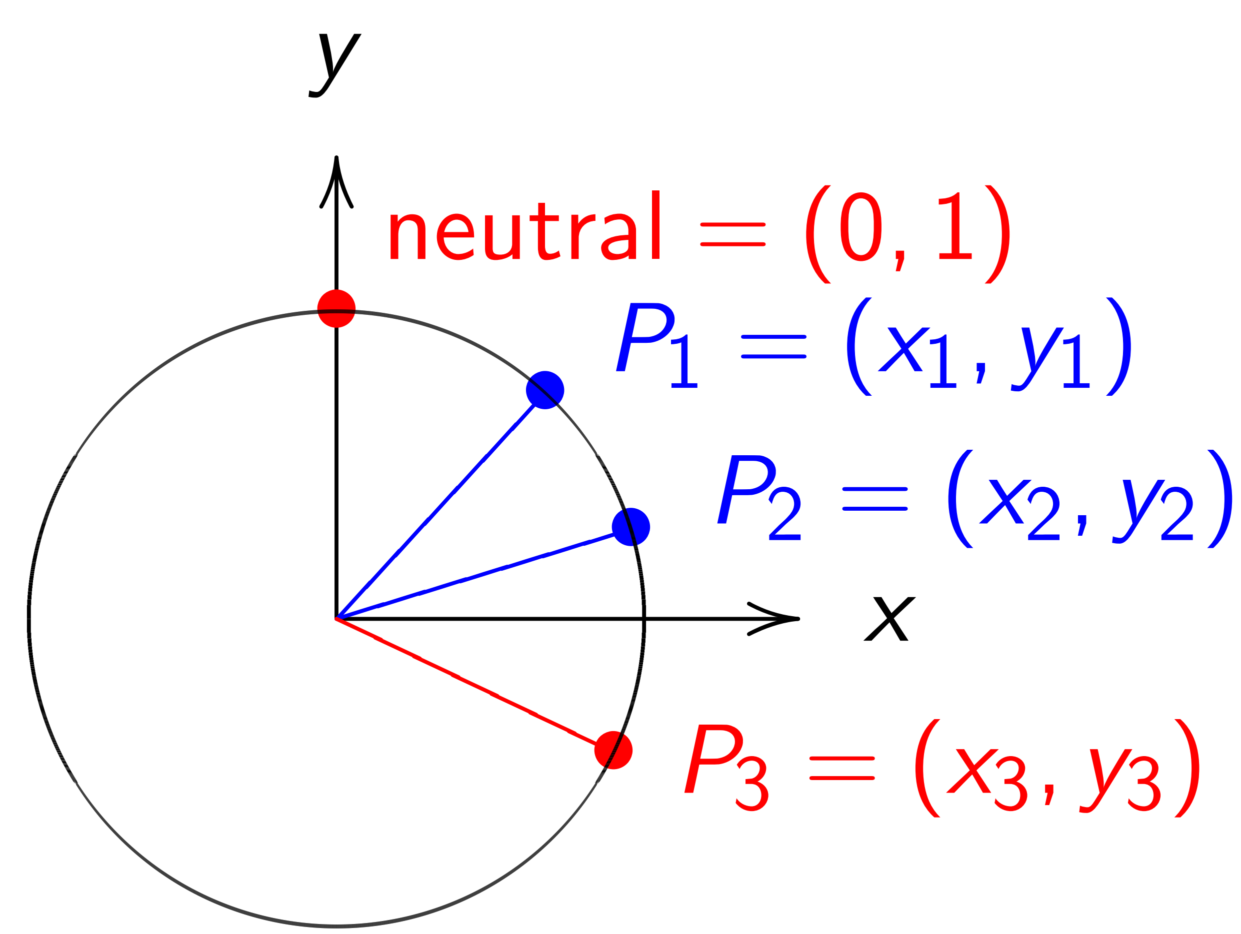
nd-elliptic-curve
aphy

. Bernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

recent joint work with:
ange
che Universiteit Eindhoven

to/papers.html#hyperand

Clock($\mathbf{R}$): the commutative group
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$
under the operations
"0": $() \mapsto (0, 1)$;
"−": $(x, y) \mapsto (-x, y)$;
"+": $(x_1, y_1), (x_2, y_2) \mapsto$
$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.



More clo

"A para
$t \mapsto$ (sin
is a grou
inducing

-curve

n

is at Chicago &

siteit Eindhoven

nt work with:

siteit Eindhoven

s.html#hyperand

Clock($\mathbf{R}$): the commutative group

$\{(x,y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$

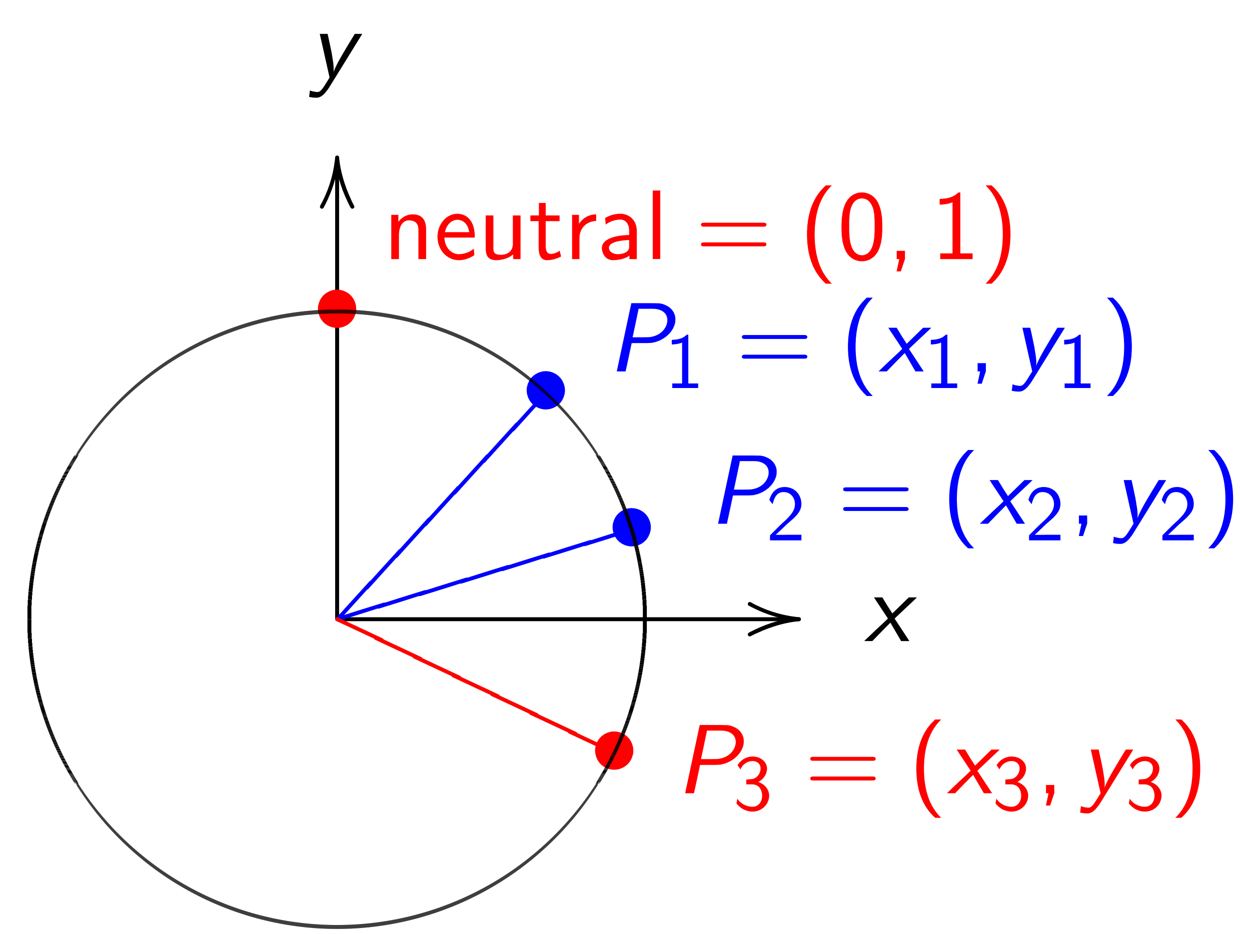
under the operations

"0": $() \mapsto (0,1)$;

"−": $(x,y) \mapsto (-x,y)$;

"+": $(x_1,y_1),(x_2,y_2) \mapsto$

$(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$.



More clock perspe

"A parametrized c

$t \mapsto (\sin t, \cos t)$

is a group hom $\mathbf{R}$

inducing $\mathbf{R}/2\pi\mathbf{Z}$

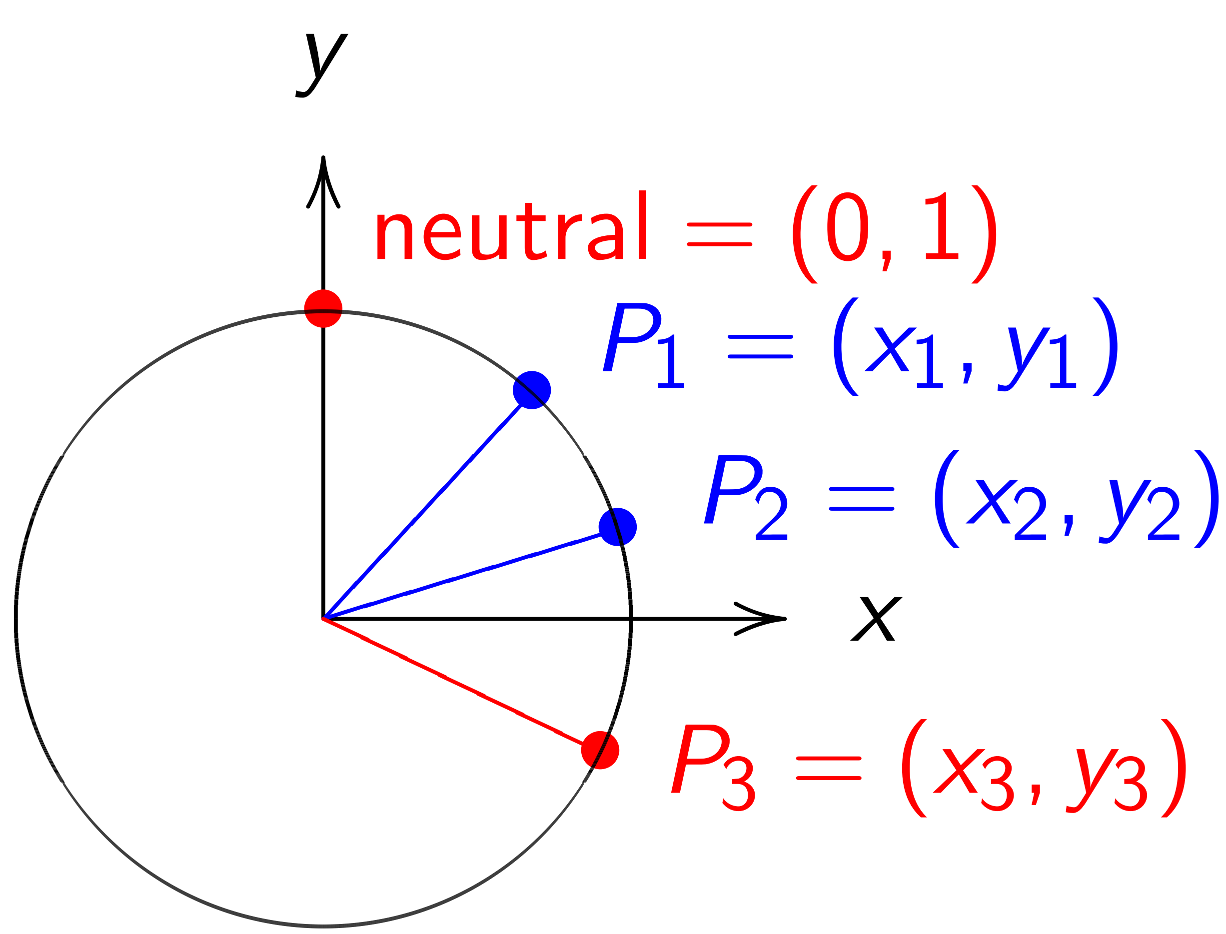
ago &
hoven

ith:

hoven

yperand

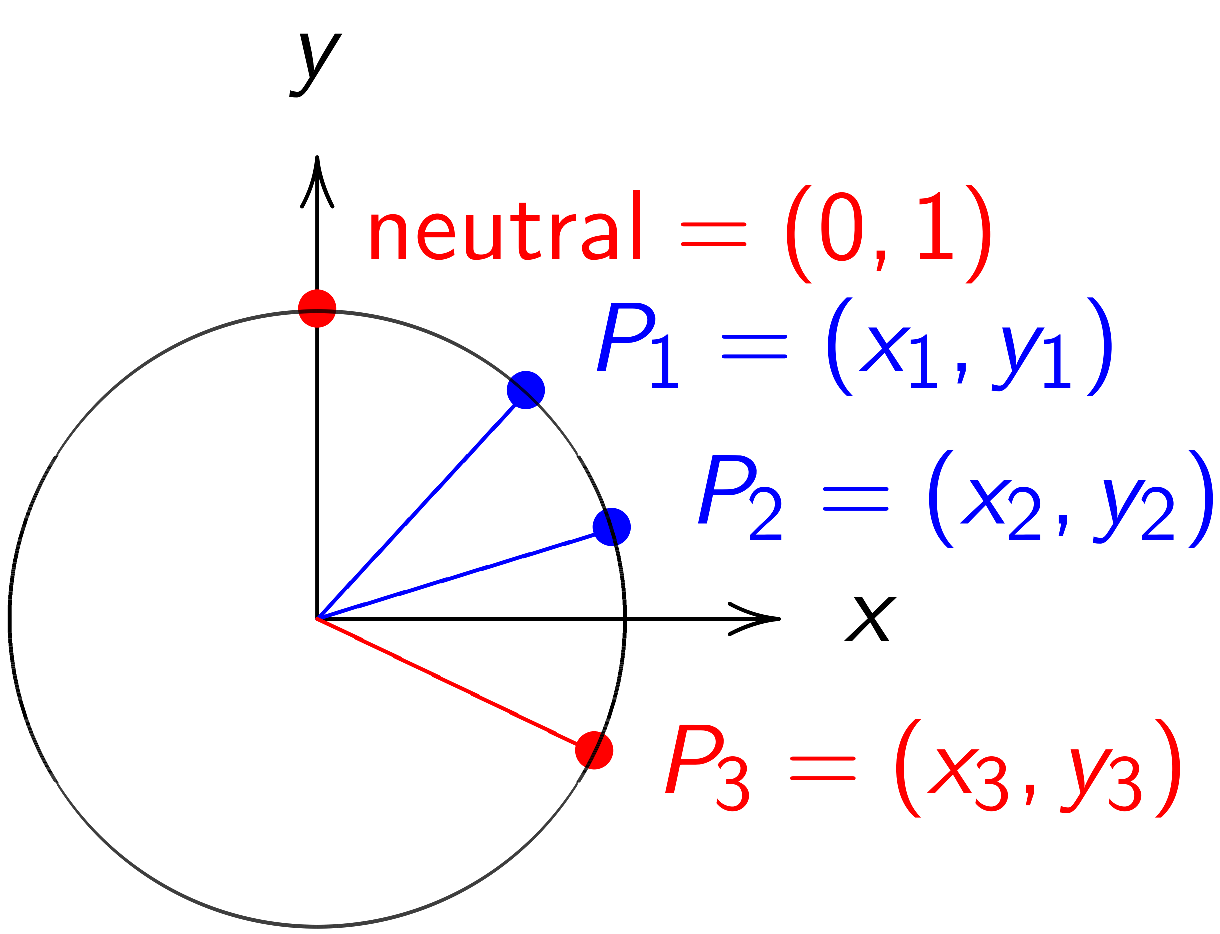
Clock(**R**): the commutative group
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$
under the operations
"0": $() \mapsto (0, 1)$;
"−": $(x, y) \mapsto (-x, y)$;
"+": $(x_1, y_1), (x_2, y_2) \mapsto$
$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.



More clock perspectives:

"A parametrized clock":
$t \mapsto (\sin t, \cos t)$
is a group hom $\mathbf{R} \twoheadrightarrow$ Clock(
inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\rightarrow$ Clock(**R**

Clock(**R**): the commutative group
$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$
under the operations
"0": $() \mapsto (0, 1)$;
"−": $(x, y) \mapsto (-x, y)$;
"+": $(x_1, y_1), (x_2, y_2) \mapsto$
$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.



More clock perspectives:

"A parametrized clock":
$t \mapsto (\sin t, \cos t)$
is a group hom $\mathbf{R} \twoheadrightarrow \mathrm{Clock}(\mathbf{R})$
inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\rightarrow \mathrm{Clock}(\mathbf{R})$.

Clock($\mathbf{R}$): the commutative group

$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$

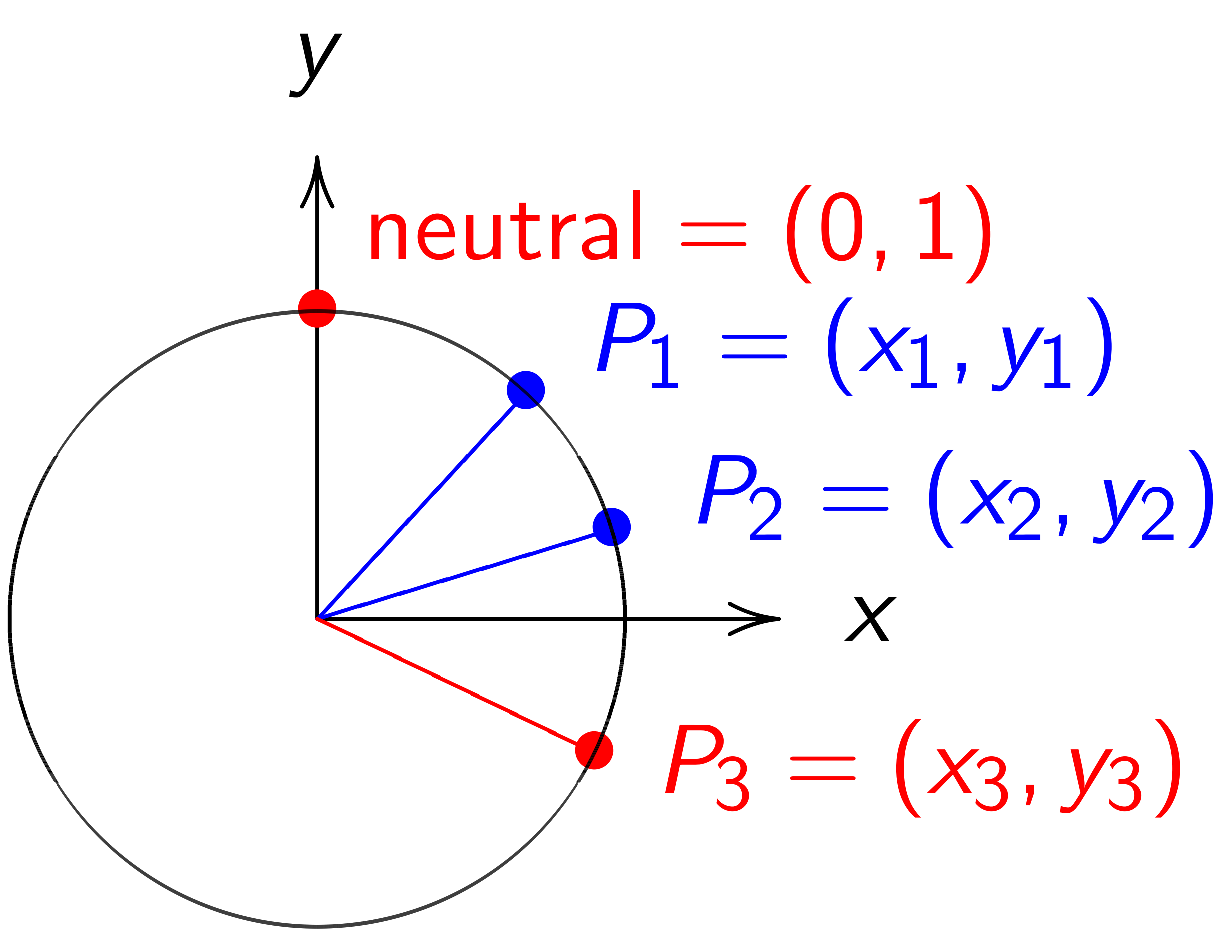
under the operations

"0": $() \mapsto (0, 1)$;

"$-$": $(x, y) \mapsto (-x, y)$;

"$+$": $(x_1, y_1), (x_2, y_2) \mapsto$

$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.



More clock perspectives:

"A parametrized clock":

$t \mapsto (\sin t, \cos t)$

is a group hom $\mathbf{R} \twoheadrightarrow$ Clock($\mathbf{R}$)

inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\twoheadrightarrow$ Clock($\mathbf{R}$).

"Complex numbers of norm 1":

$\{u \in \mathbf{C} : u\overline{u} = 1\}$ is a group under

1; $u \mapsto \overline{u}$; $u_1, u_2 \mapsto u_1 u_2$.

$(x, y) \mapsto y + ix$ is a group hom

Clock($\mathbf{R}$) $\hookrightarrow\!\!\!\!\twoheadrightarrow \{u \in \mathbf{C} : u\overline{u} = 1\}$.

Clock($\mathbf{R}$): the commutative group

$\{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$

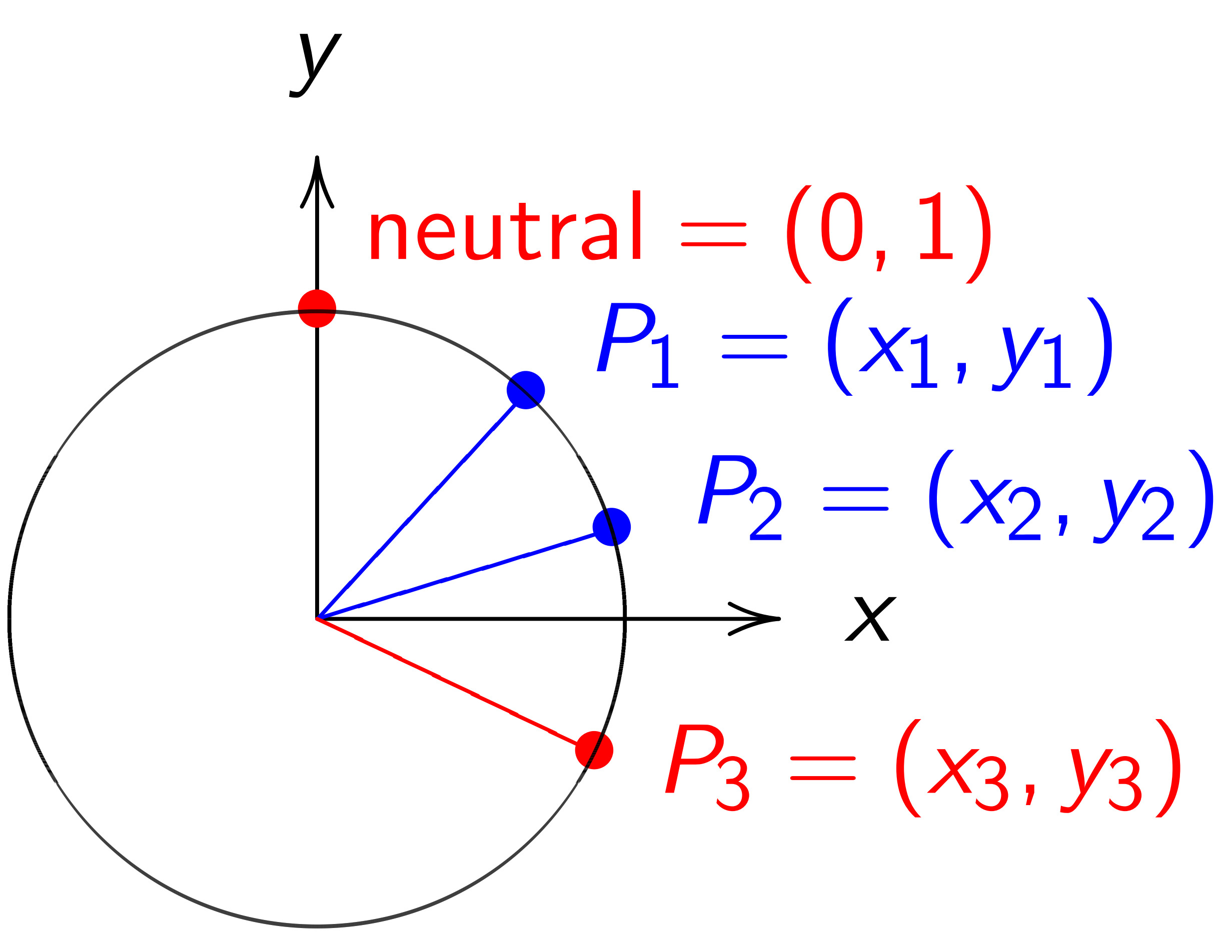
under the operations

"0": $() \mapsto (0, 1)$;

"−": $(x, y) \mapsto (-x, y)$;

"+": $(x_1, y_1), (x_2, y_2) \mapsto$

$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.



More clock perspectives:

"A parametrized clock":

$t \mapsto (\sin t, \cos t)$

is a group hom $\mathbf{R} \twoheadrightarrow \text{Clock}(\mathbf{R})$

inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\to \text{Clock}(\mathbf{R})$.

"Complex numbers of norm 1":

$\{u \in \mathbf{C} : u\overline{u} = 1\}$ is a group under

1; $u \mapsto \overline{u}$; $u_1, u_2 \mapsto u_1 u_2$.

$(x, y) \mapsto y + ix$ is a group hom

$\text{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\to \{u \in \mathbf{C} : u\overline{u} = 1\}$.

"2-dimensional rotations":

$(x, y) \mapsto \begin{pmatrix} y & x \\ -x & y \end{pmatrix}$ is a

group hom $\text{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\to \text{SO}_2(\mathbf{R})$.

): the commutative group

$\in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 1\}$

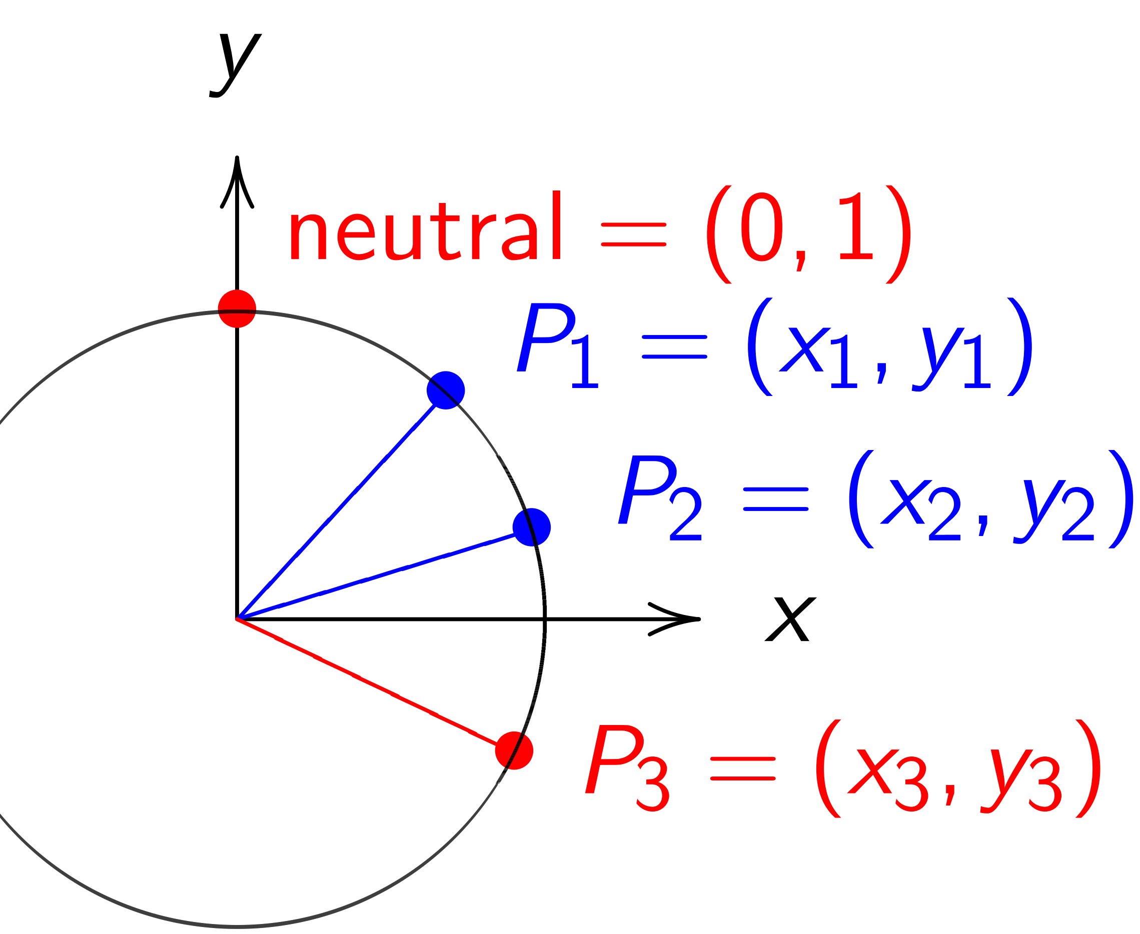
e operations

$\mapsto (0, 1)$;

$, y) \mapsto (-x, y)$;

$_1, y_1), (x_2, y_2) \mapsto$

$y_1 x_2, y_1 y_2 - x_1 x_2)$.



More clock perspectives:

"A parametrized clock":
$t \mapsto (\sin t, \cos t)$
is a group hom $\mathbf{R} \twoheadrightarrow \text{Clock}(\mathbf{R})$
inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\!\twoheadrightarrow \text{Clock}(\mathbf{R})$.

"Complex numbers of norm 1":
$\{u \in \mathbf{C} : u\overline{u} = 1\}$ is a group under
1; $u \mapsto \overline{u}$; $u_1, u_2 \mapsto u_1 u_2$.
$(x, y) \mapsto y + ix$ is a group hom
$\text{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\!\twoheadrightarrow \{u \in \mathbf{C} : u\overline{u} = 1\}$.

"2-dimensional rotations":
$(x, y) \mapsto \begin{pmatrix} y & x \\ -x & y \end{pmatrix}$ is a
group hom $\text{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\!\twoheadrightarrow \text{SO}_2(\mathbf{R})$.

Clocks o

Clock(**F**

$\{(x, y) \in$

Group o

Diagram

$-3, -2,$

mmutative group

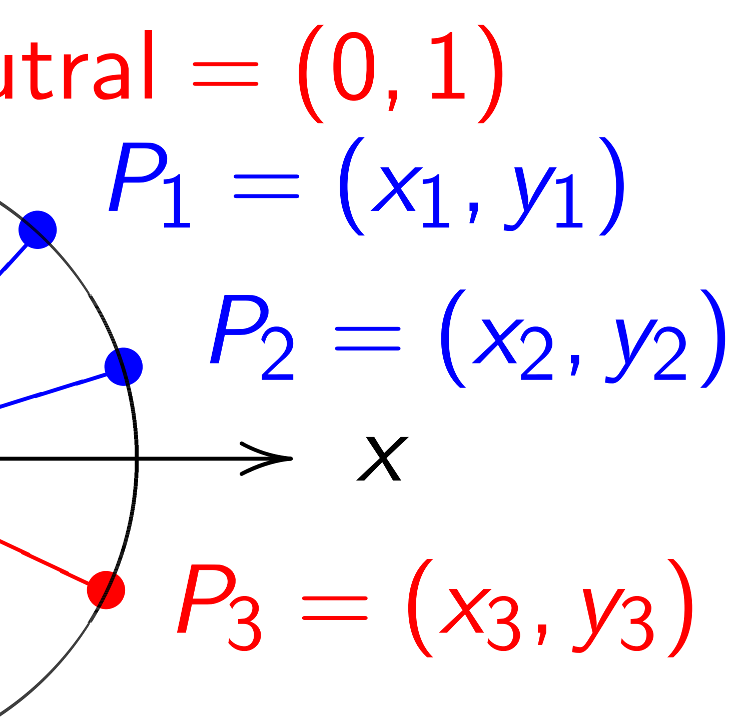
$x^2 + y^2 = 1\}$

ons

$x, y)$;

$y_2) \mapsto$

$- x_1 x_2)$.



More clock perspectives:

"A parametrized clock":
$t \mapsto (\sin t, \cos t)$
is a group hom $\mathbf{R} \twoheadrightarrow \mathrm{Clock}(\mathbf{R})$
inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\rightarrow \mathrm{Clock}(\mathbf{R})$.

"Complex numbers of norm 1":
$\{u \in \mathbf{C} : u\bar{u} = 1\}$ is a group under
1; $u \mapsto \bar{u}$; $u_1, u_2 \mapsto u_1 u_2$.
$(x, y) \mapsto y + ix$ is a group hom
$\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\rightarrow \{u \in \mathbf{C} : u\bar{u} = 1\}$.

"2-dimensional rotations":
$(x, y) \mapsto \begin{pmatrix} y & x \\ -x & y \end{pmatrix}$ is a
group hom $\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\rightarrow \mathrm{SO}_2(\mathbf{R})$.

Clocks over finite

$\mathrm{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7$
Group operations

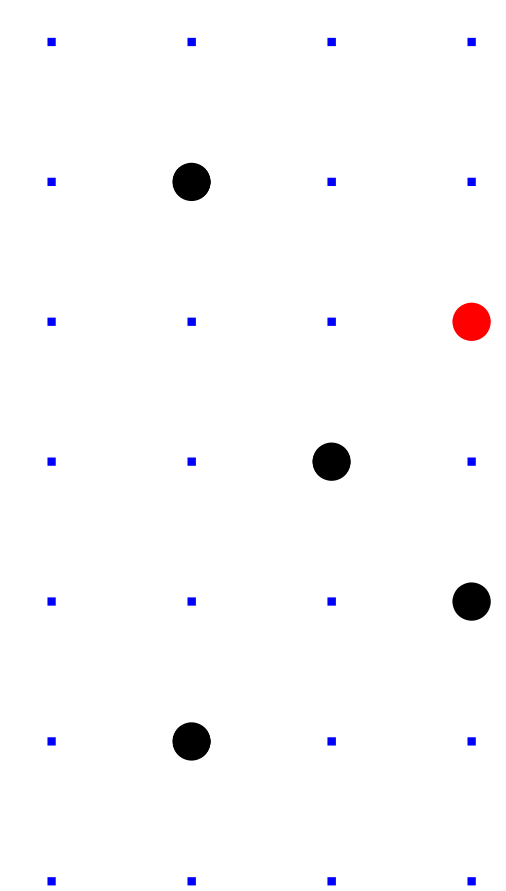


Diagram plots $\mathbf{F}_7$
$-3, -2, -1, 0, 1, 2$

group

$= 1\}$

$1)$

$x_1, y_1)$

(x_2, y_2)

(x_3, y_3)

More clock perspectives:

"A parametrized clock":
$t \mapsto (\sin t, \cos t)$
is a group hom $\mathbf{R} \twoheadrightarrow \mathrm{Clock}(\mathbf{R})$
inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{Clock}(\mathbf{R})$.

"Complex numbers of norm 1":
$\{u \in \mathbf{C} : u\overline{u} = 1\}$ is a group under
1; $u \mapsto \overline{u}$; $u_1, u_2 \mapsto u_1 u_2$.
$(x, y) \mapsto y + ix$ is a group hom
$\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\twoheadrightarrow \{u \in \mathbf{C} : u\overline{u} = 1\}$.

"2-dimensional rotations":
$(x, y) \mapsto \begin{pmatrix} y & x \\ -x & y \end{pmatrix}$ is a
group hom $\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{SO}_2(\mathbf{R})$.

Clocks over finite fields

$\mathrm{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2$
Group operations as before.

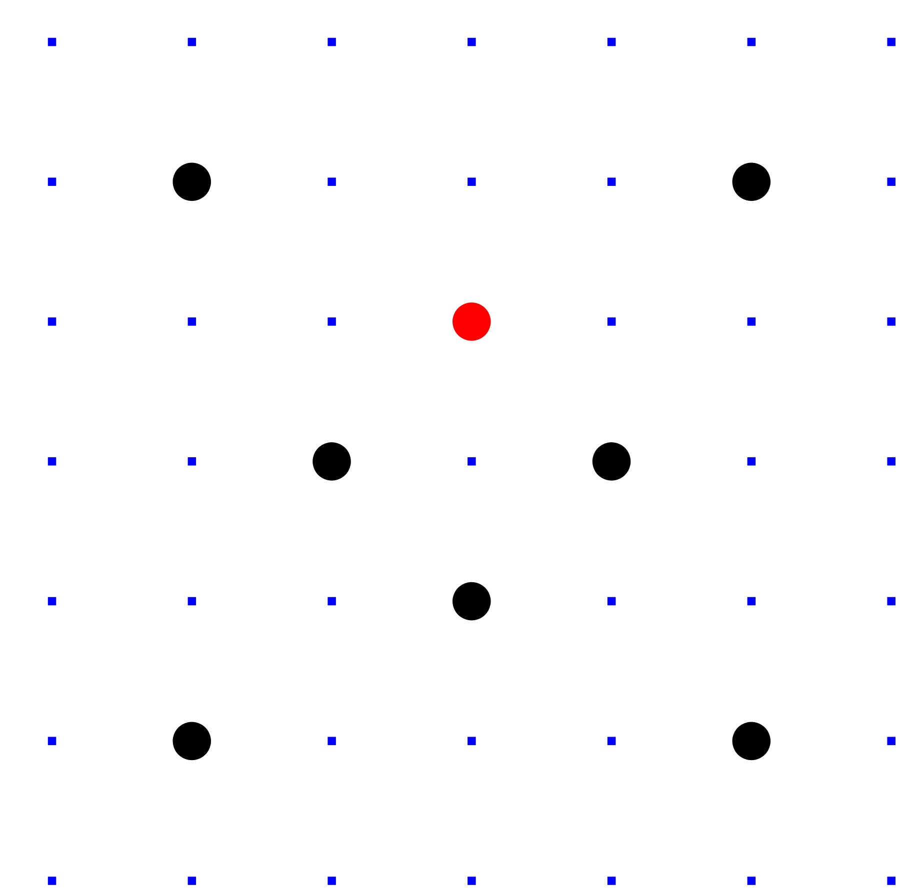


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

More clock perspectives:

"A parametrized clock":
$t \mapsto (\sin t, \cos t)$
is a group hom $\mathbf{R} \twoheadrightarrow \mathrm{Clock}(\mathbf{R})$
inducing $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{Clock}(\mathbf{R})$.

"Complex numbers of norm 1":
$\{u \in \mathbf{C} : u\overline{u} = 1\}$ is a group under
1; $u \mapsto \overline{u}$; $u_1, u_2 \mapsto u_1 u_2$.
$(x, y) \mapsto y + ix$ is a group hom
$\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\twoheadrightarrow \{u \in \mathbf{C} : u\overline{u} = 1\}$.

"2-dimensional rotations":
$(x, y) \mapsto \begin{pmatrix} y & x \\ -x & y \end{pmatrix}$ is a
group hom $\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{SO}_2(\mathbf{R})$.

Clocks over finite fields

$\mathrm{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

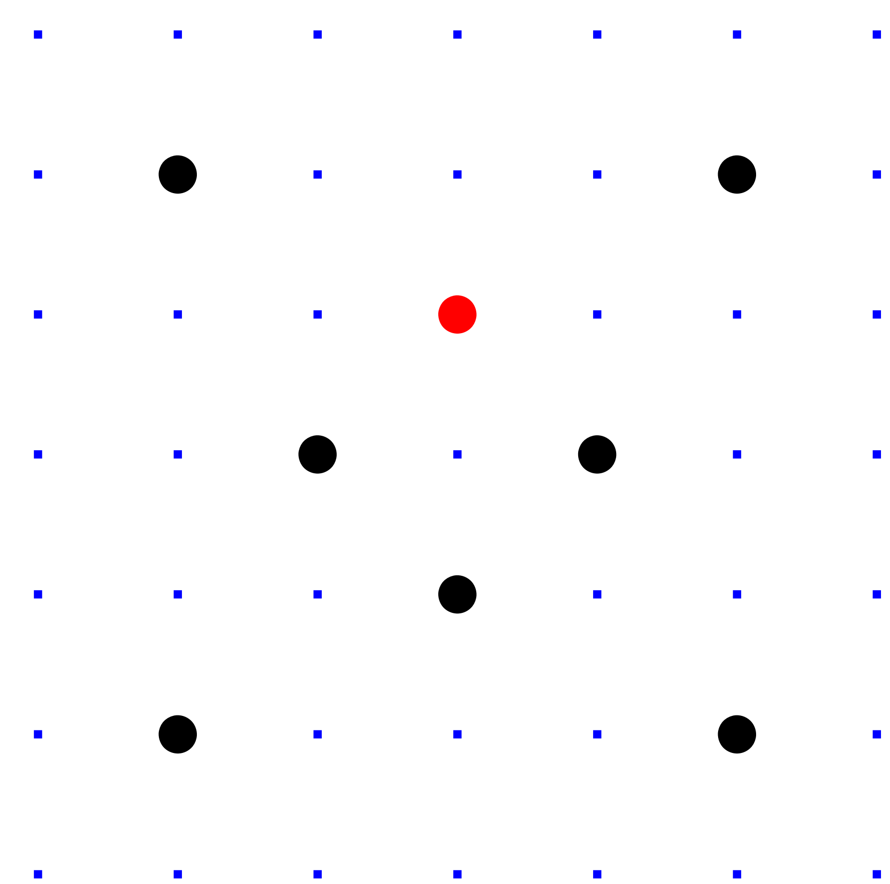


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

ock perspectives:

metrized clock”:

$t, \cos t)$

up hom $\mathbf{R} \twoheadrightarrow \mathrm{Clock}(\mathbf{R})$

; $\mathbf{R}/2\pi\mathbf{Z} \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{Clock}(\mathbf{R})$.

ex numbers of norm 1”:

: $u\overline{u} = 1\}$ is a group under

$\overline{u}$; $u_1, u_2 \mapsto u_1 u_2$.

→ $y + ix$ is a group hom

$) \hookrightarrow\!\!\!\!\twoheadrightarrow \{u \in \mathbf{C} : u\overline{u} = 1\}$.

nsional rotations”:

→ $\begin{pmatrix} y & x \\ -x & y \end{pmatrix}$ is a

om $\mathrm{Clock}(\mathbf{R}) \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{SO}_2(\mathbf{R})$.

Clocks over finite fields

$\mathrm{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

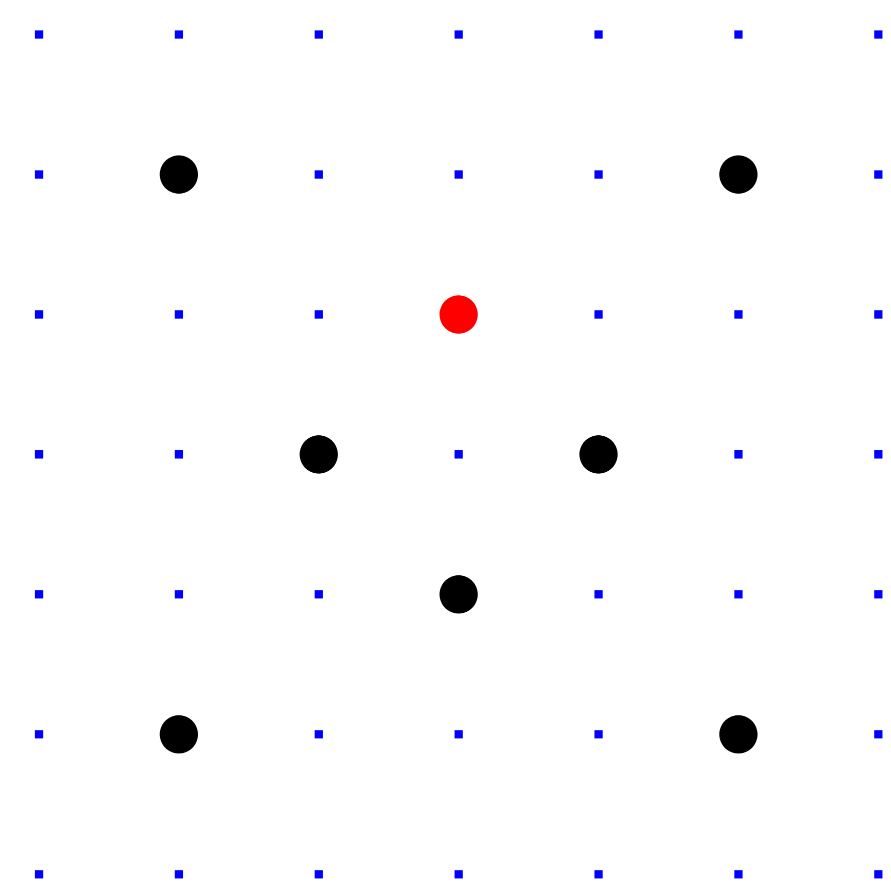


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger e

Example

in Clock

2(1000,

ectives:

lock":

$\twoheadrightarrow$ Clock($\mathbf{R}$)

$\twoheadrightarrow$ Clock($\mathbf{R}$).

s of norm 1":

is a group under

$\to u_1 u_2$.

a group hom

$\mathbf{C} : u\overline{u} = 1\}$.

tations":

is a

$\mathbf{R}) \hookrightarrow\!\!\!\!\twoheadrightarrow \mathrm{SO}_2(\mathbf{R})$.

Clocks over finite fields

$\mathrm{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

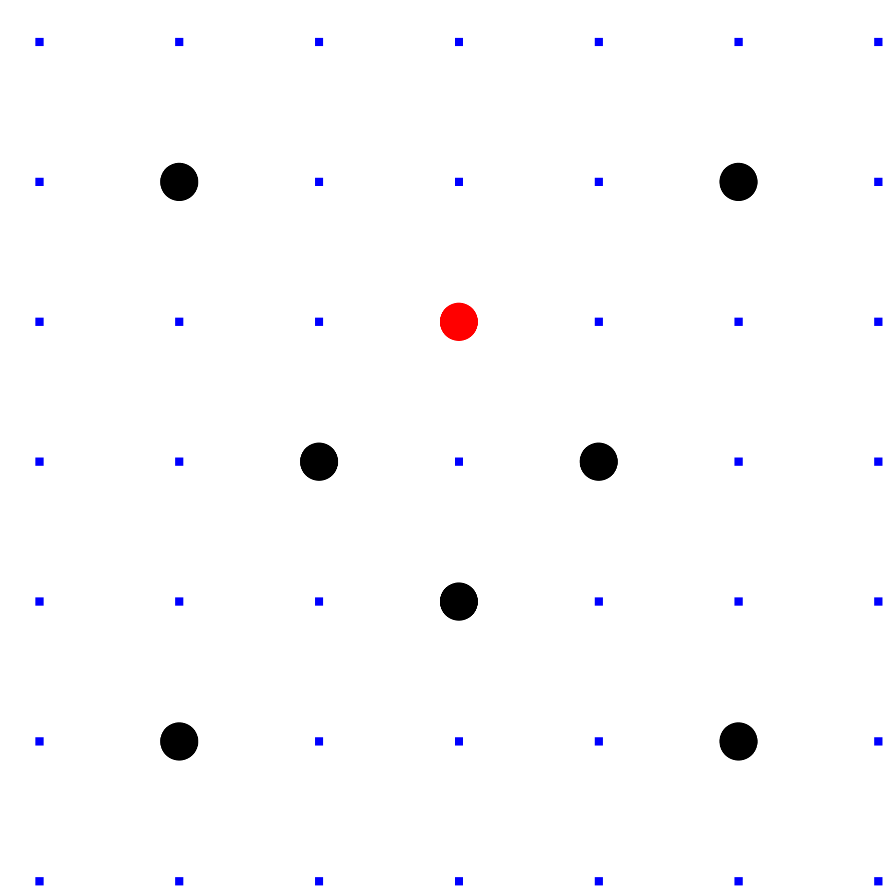


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: C

Examples of addit

in Clock($\mathbf{F}_{1000003}$)

$2(1000, 2) = (400$

R)

R).

1”:

under

nom

1}.

$_2$(**R**).

Clocks over finite fields

Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

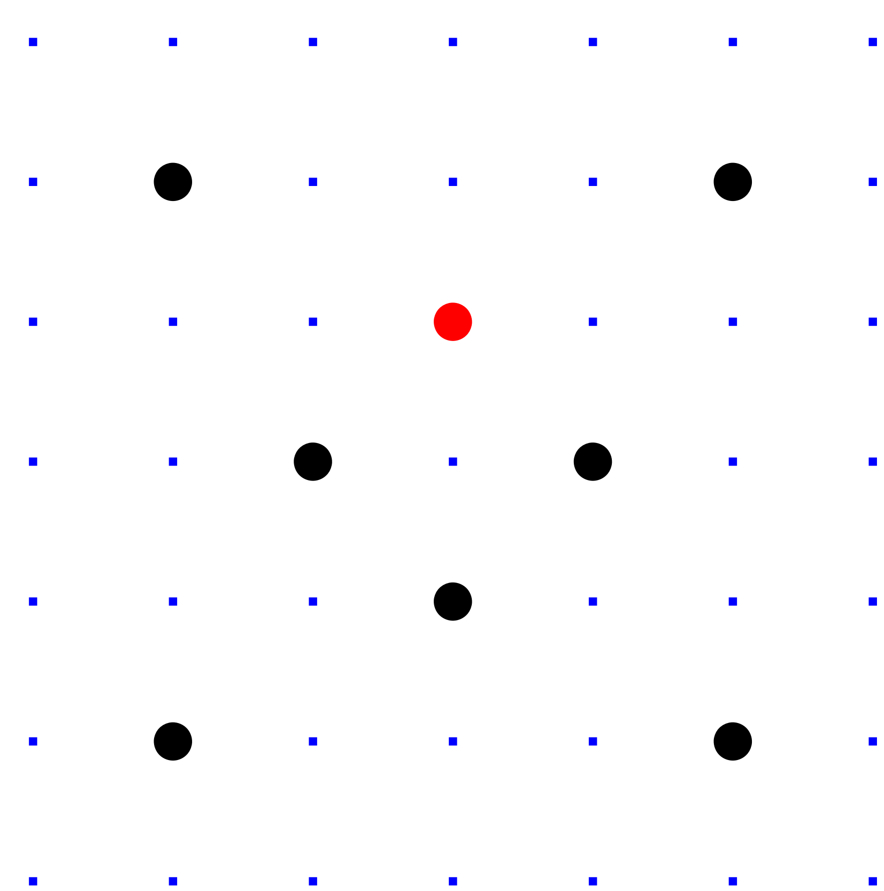


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: Clock($\mathbf{F}_{100}$

Examples of addition
in Clock($\mathbf{F}_{1000003}$):
$2(1000, 2) = (4000, 7)$.

Clocks over finite fields

$\text{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

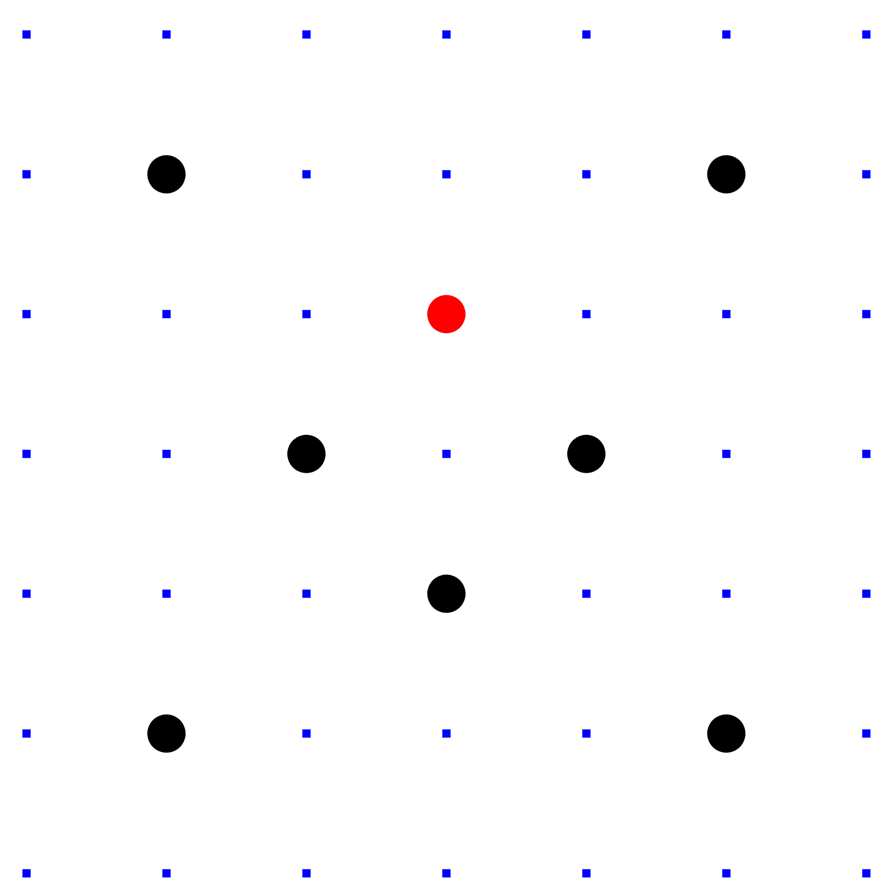


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: $\text{Clock}(\mathbf{F}_{1000003})$.

Examples of addition
in $\text{Clock}(\mathbf{F}_{1000003})$:
$2(1000, 2) = (4000, 7)$.

Clocks over finite fields

Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

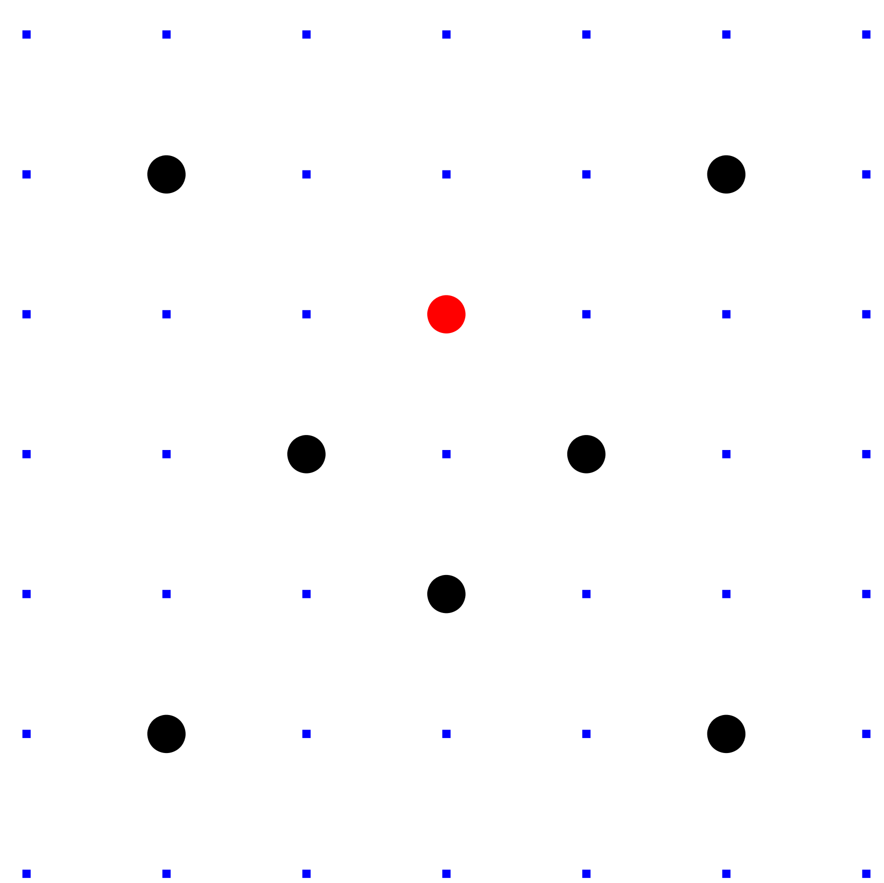


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: Clock($\mathbf{F}_{1000003}$).

Examples of addition
in Clock($\mathbf{F}_{1000003}$):
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.

Clocks over finite fields

$\text{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

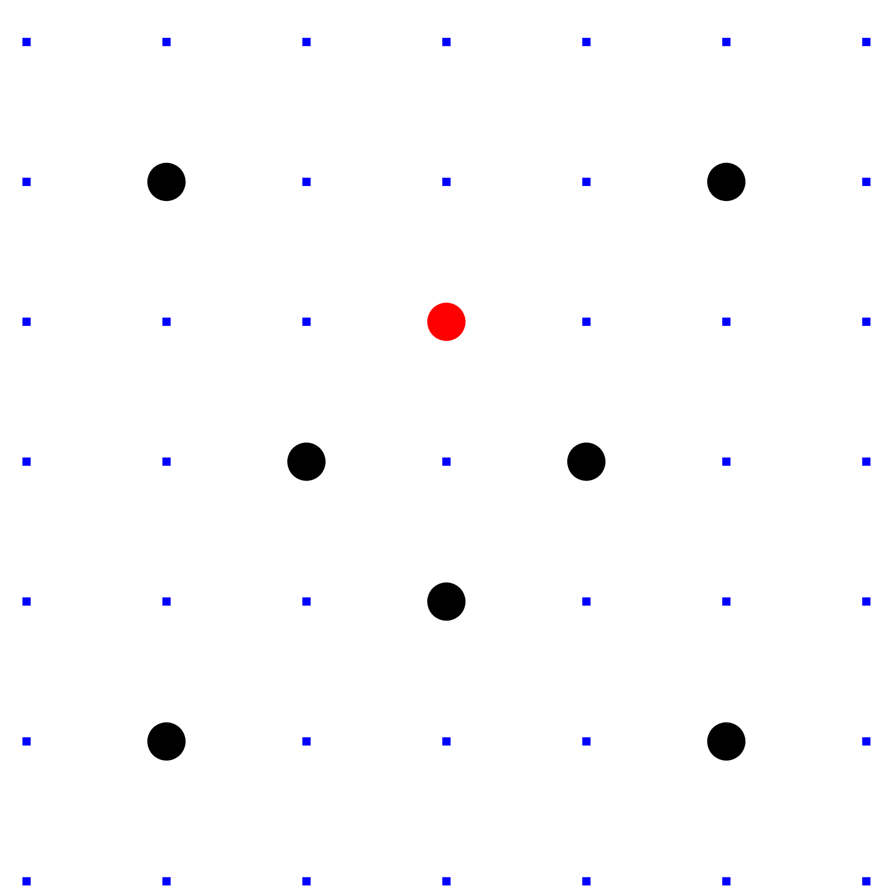


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: $\text{Clock}(\mathbf{F}_{1000003})$.

Examples of addition
in $\text{Clock}(\mathbf{F}_{1000003})$:
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.

Clocks over finite fields

Clock($\mathbf{F}_7$) =
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

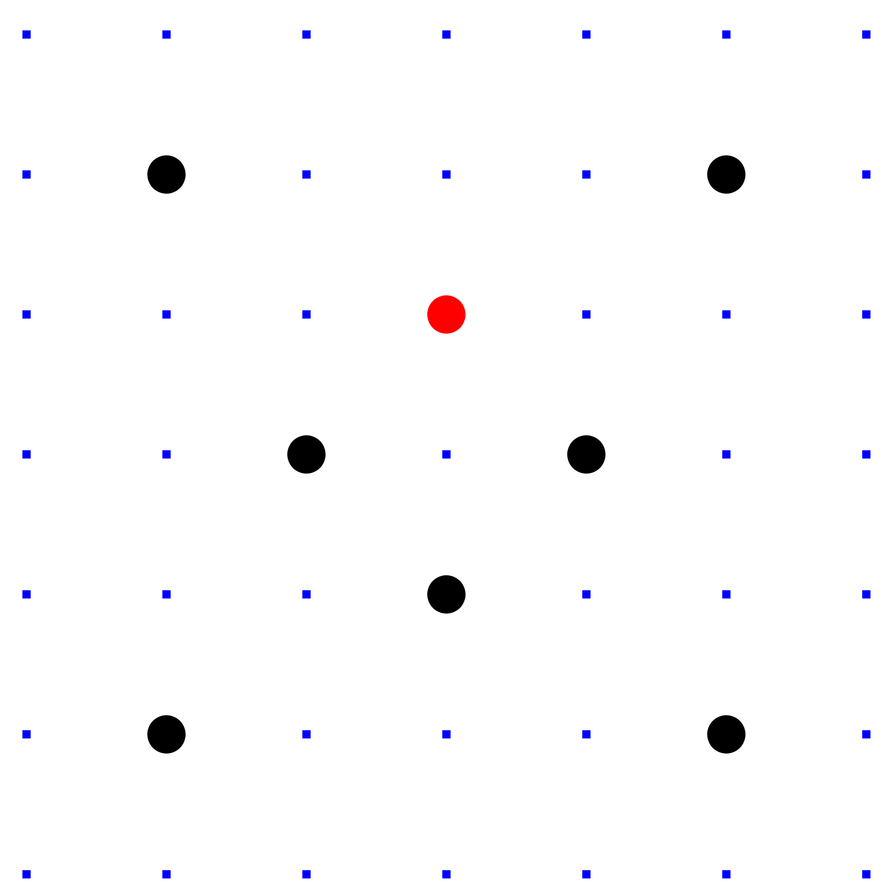


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: Clock($\mathbf{F}_{1000003}$).

Examples of addition
in Clock($\mathbf{F}_{1000003}$):
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.

Clocks over finite fields

$\text{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

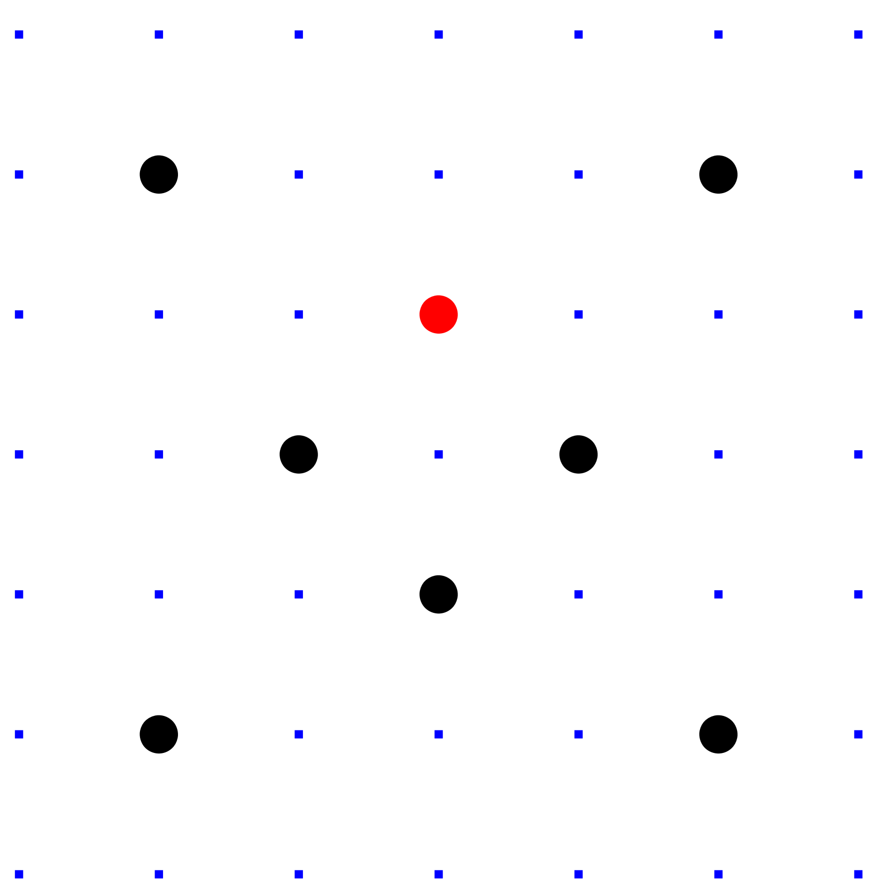


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: $\text{Clock}(\mathbf{F}_{1000003})$.

Examples of addition
in $\text{Clock}(\mathbf{F}_{1000003})$:
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.
$17(1000, 2) = (951405, 877356)$.

Clocks over finite fields

$\text{Clock}(\mathbf{F}_7) =$
$\{(x, y) \in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.
Group operations as before.

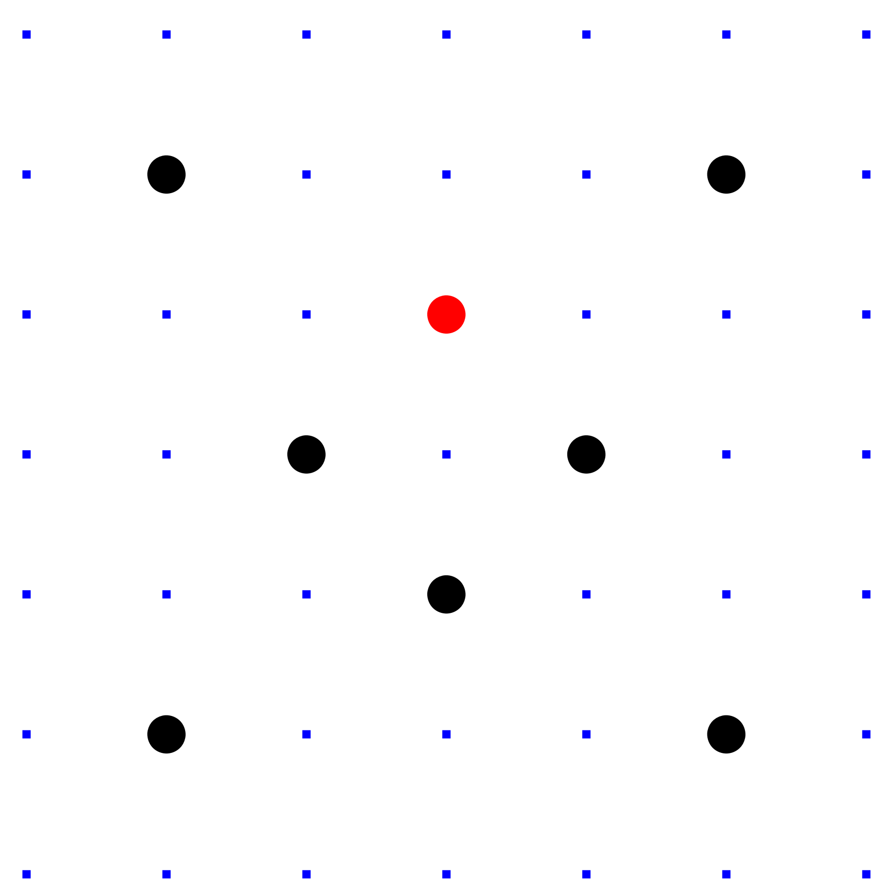


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3$.

Larger example: $\text{Clock}(\mathbf{F}_{1000003})$.

Examples of addition
in $\text{Clock}(\mathbf{F}_{1000003})$:
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.
$17(1000, 2) = (951405, 877356)$.

"Scalar multiplication" maps
$\mathbf{Z} \times \text{Clock}(\mathbf{F}_q) \to \text{Clock}(\mathbf{F}_q)$
by $n, P \mapsto nP$.

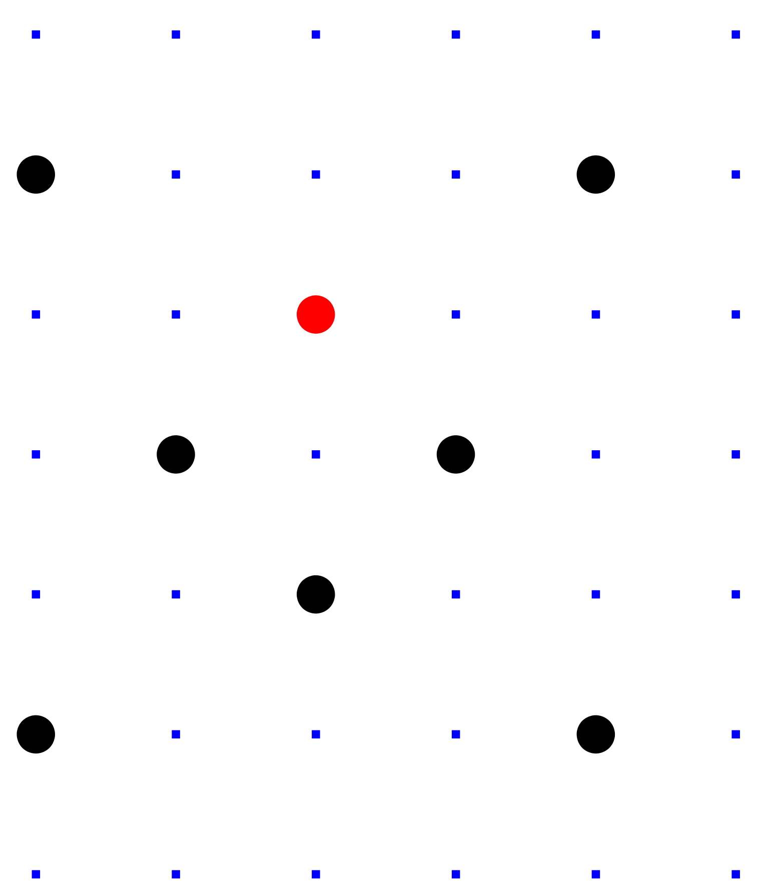
We'll build cryptography
from scalar multiplication.

over finite fields

$_7) =$

$\in \mathbf{F}_7 \times \mathbf{F}_7 : x^2 + y^2 = 1\}$.

perations as before.



plots $\mathbf{F}_7$ as

$-1, 0, 1, 2, 3$.

Larger example: $\text{Clock}(\mathbf{F}_{1000003})$.

Examples of addition
in $\text{Clock}(\mathbf{F}_{1000003})$:

$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.
$17(1000, 2) = (951405, 877356)$.

"Scalar multiplication" maps
$\mathbf{Z} \times \text{Clock}(\mathbf{F}_q) \to \text{Clock}(\mathbf{F}_q)$
by $n, P \mapsto nP$.

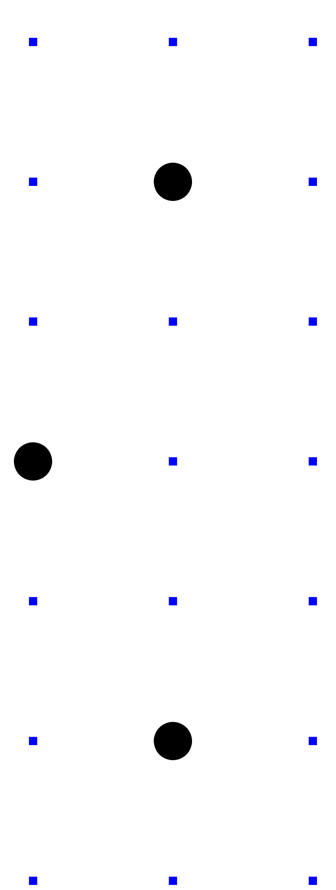
We'll build cryptography
from scalar multiplication.

A fast m
take 0 if
negate (
double (
add P to
else subt

fields

$: x^2 + y^2 = 1\}$.

as before.



as

, 3.

Larger example: Clock($\mathbf{F}_{1000003}$).

Examples of addition
in Clock($\mathbf{F}_{1000003}$):
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.
$17(1000, 2) = (951405, 877356)$.

"Scalar multiplication" maps
$\mathbf{Z} \times \text{Clock}(\mathbf{F}_q) \to \text{Clock}(\mathbf{F}_q)$
by $n, P \mapsto nP$.

We'll build cryptography
from scalar multiplication.

A fast method to
take 0 if $n = 0$;
negate $(-n)P$ if n
double $(n/2)P$ if n
add P to $(n-1)P$
else subtract P fro

$= 1\}$.

Larger example: Clock($\mathbf{F}_{1000003}$).

Examples of addition
in Clock($\mathbf{F}_{1000003}$):
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.
$17(1000, 2) = (951405, 877356)$.

"Scalar multiplication" maps
$\mathbf{Z} \times \text{Clock}(\mathbf{F}_q) \to \text{Clock}(\mathbf{F}_q)$
by $n, P \mapsto nP$.

We'll build cryptography
from scalar multiplication.

A fast method to compute n
take 0 if $n = 0$;
negate $(-n)P$ if $n < 0$;
double $(n/2)P$ if $n \in 2\mathbf{Z}$;
add P to $(n-1)P$ if $n - 1$
else subtract P from $(n+1)$

Larger example: Clock($\mathbf{F}_{1000003}$).

Examples of addition in Clock($\mathbf{F}_{1000003}$):

$2(1000, 2) = (4000, 7)$.

$4(1000, 2) = (56000, 97)$.

$8(1000, 2) = (863970, 18817)$.

$16(1000, 2) = (549438, 156853)$.

$17(1000, 2) = (951405, 877356)$.

"Scalar multiplication" maps $\mathbf{Z} \times \text{Clock}(\mathbf{F}_q) \to \text{Clock}(\mathbf{F}_q)$ by $n, P \mapsto nP$.

We'll build cryptography from scalar multiplication.

A fast method to compute nP:

take 0 if $n = 0$;

negate $(-n)P$ if $n < 0$;

double $(n/2)P$ if $n \in 2\mathbf{Z}$;

add P to $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;

else subtract P from $(n+1)P$.

Larger example: Clock($\mathbf{F}_{1000003}$).

Examples of addition
in Clock($\mathbf{F}_{1000003}$):
$2(1000, 2) = (4000, 7)$.
$4(1000, 2) = (56000, 97)$.
$8(1000, 2) = (863970, 18817)$.
$16(1000, 2) = (549438, 156853)$.
$17(1000, 2) = (951405, 877356)$.

"Scalar multiplication" maps
$\mathbf{Z} \times \text{Clock}(\mathbf{F}_q) \to \text{Clock}(\mathbf{F}_q)$
by $n, P \mapsto nP$.

We'll build cryptography
from scalar multiplication.

A fast method to compute nP:
take 0 if $n = 0$;
negate $(-n)P$ if $n < 0$;
double $(n/2)P$ if $n \in 2\mathbf{Z}$;
add P to $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;
else subtract P from $(n+1)P$.

But figuring out n
given P and nP
is much more difficult.

30 clock additions produce
$n(1000, 2) = (947472, 736284)$
for some 6-digit n.
Can you figure out n?

xample: Clock($\mathbf{F}_{1000003}$).

es of addition

($\mathbf{F}_{1000003}$):

$2) = (4000, 7)$.

$2) = (56000, 97)$.

$2) = (863970, 18817)$.

$, 2) = (549438, 156853)$.

$, 2) = (951405, 877356)$.

multiplication" maps

ck($\mathbf{F}_q$) $\to$ Clock($\mathbf{F}_q$)

$\to nP$.

ild cryptography

alar multiplication.

A fast method to compute nP:

take 0 if $n = 0$;

negate $(-n)P$ if $n < 0$;

double $(n/2)P$ if $n \in 2\mathbf{Z}$;

add P to $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;

else subtract P from $(n+1)P$.

But figuring out n

given P and nP

is much more difficult.

30 clock additions produce

$n(1000, 2) = (947472, 736284)$

for some 6-digit n.

Can you figure out n?

Clock cr

Standard

and $(x, y$

of large

Alice ch

Comput

Bob cho

Comput

Alice co

Bob com

They us

to encry

Clock($\mathbf{F}_{1000003}$).

ion

:

$0, 7)$.

$00, 97)$.

$970, 18817)$.

$9438, 156853)$.

$1405, 877356)$.

tion" maps

Clock($\mathbf{F}_q$)

graphy

lication.

A fast method to compute nP:

take 0 if $n = 0$;

negate $(-n)P$ if $n < 0$;

double $(n/2)P$ if $n \in 2\mathbf{Z}$;

add P to $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;

else subtract P from $(n+1)P$.

But figuring out n
given P and nP
is much more difficult.

30 clock additions produce
$n(1000, 2) = (947472, 736284)$
for some 6-digit n.
Can you figure out n?

Clock cryptograph

Standardize odd p
and $(x, y) \in$ Clock
of large prime orde

Alice chooses big s
Computes her pub

Bob chooses big s
Computes his pub

Alice computes $a($
Bob computes $b(a$
They use this shar
to encrypt with "A

0003).

7).

353).

356).

s

)

A fast method to compute nP:
take 0 if $n = 0$;
negate $(-n)P$ if $n < 0$;
double $(n/2)P$ if $n \in 2\mathbf{Z}$;
add P to $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;
else subtract P from $(n+1)P$.

But figuring out n
given P and nP
is much more difficult.

30 clock additions produce
$n(1000, 2) = (947472, 736284)$
for some 6-digit n.
Can you figure out n?

Clock cryptography

Standardize odd prime powe
and $(x, y) \in \text{Clock}(\mathbf{F}_q)$
of large prime order.

Alice chooses big secret a.
Computes her public key $a(x$

Bob chooses big secret b.
Computes his public key $b(x$

Alice computes $a(b(x, y))$.
Bob computes $b(a(x, y))$.
They use this shared secret
to encrypt with "AES-GCM"

A fast method to compute nP:
take 0 if $n = 0$;
negate $(-n)P$ if $n < 0$;
double $(n/2)P$ if $n \in 2\mathbf{Z}$;
add P to $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;
else subtract P from $(n+1)P$.

But figuring out n
given P and nP
is much more difficult.

30 clock additions produce
$n(1000, 2) = (947472, 736284)$
for some 6-digit n.
Can you figure out n?

Clock cryptography

Standardize odd prime power q
and $(x, y) \in \text{Clock}(\mathbf{F}_q)$
of large prime order.

Alice chooses big secret a.
Computes her public key $a(x, y)$.

Bob chooses big secret b.
Computes his public key $b(x, y)$.

Alice computes $a(b(x, y))$.
Bob computes $b(a(x, y))$.
They use this shared secret
to encrypt with "AES-GCM" etc.

nethod to compute nP:

f $n = 0$;

$-n)P$ if $n < 0$;

$n/2)P$ if $n \in 2\mathbf{Z}$;

o $(n-1)P$ if $n - 1 \in 4\mathbf{Z}$;

tract P from $(n+1)P$.

ring out n

and nP

more difficult.

additions produce

$2) = (947472, 736284)$

e 6-digit n.

figure out n?

Clock cryptography

Standardize odd prime power q
and $(x, y) \in \text{Clock}(\mathbf{F}_q)$
of large prime order.

Alice chooses big secret a.
Computes her public key $a(x, y)$.

Bob chooses big secret b.
Computes his public key $b(x, y)$.

Alice computes $a(b(x, y))$.
Bob computes $b(a(x, y))$.
They use this shared secret
to encrypt with "AES-GCM" etc.

Alic
secret

Alic
publi
$a(x,$

{Alice,
shared
$ab(x$

compute nP:

< 0;

$n \in 2\mathbf{Z}$;

P if $n - 1 \in 4\mathbf{Z}$;

om $(n+1)P$.

.

cult.

produce

$472, 736284)$

.

t n?

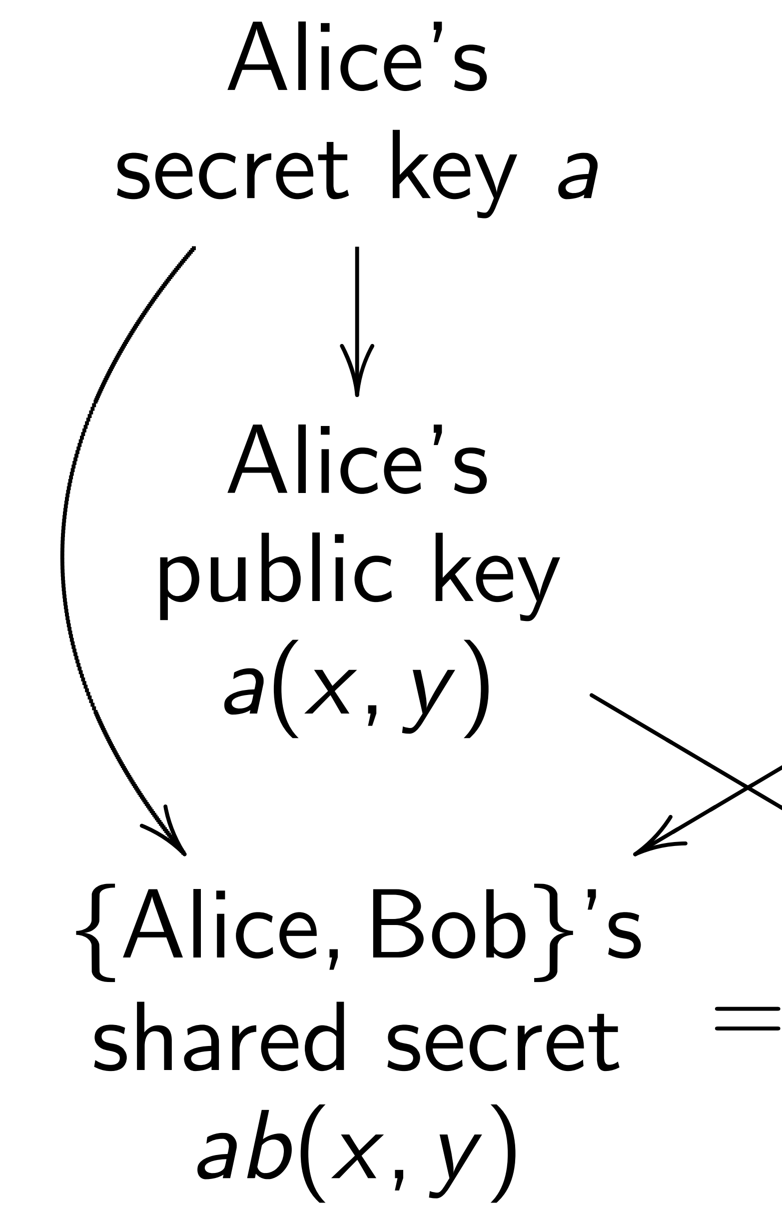
Clock cryptography

Standardize odd prime power q
and $(x, y) \in \text{Clock}(\mathbf{F}_q)$
of large prime order.

Alice chooses big secret a.
Computes her public key $a(x, y)$.

Bob chooses big secret b.
Computes his public key $b(x, y)$.

Alice computes $a(b(x, y))$.
Bob computes $b(a(x, y))$.
They use this shared secret
to encrypt with "AES-GCM" etc.



nP:

$\in 4\mathbf{Z}$;

$)P$.

34)

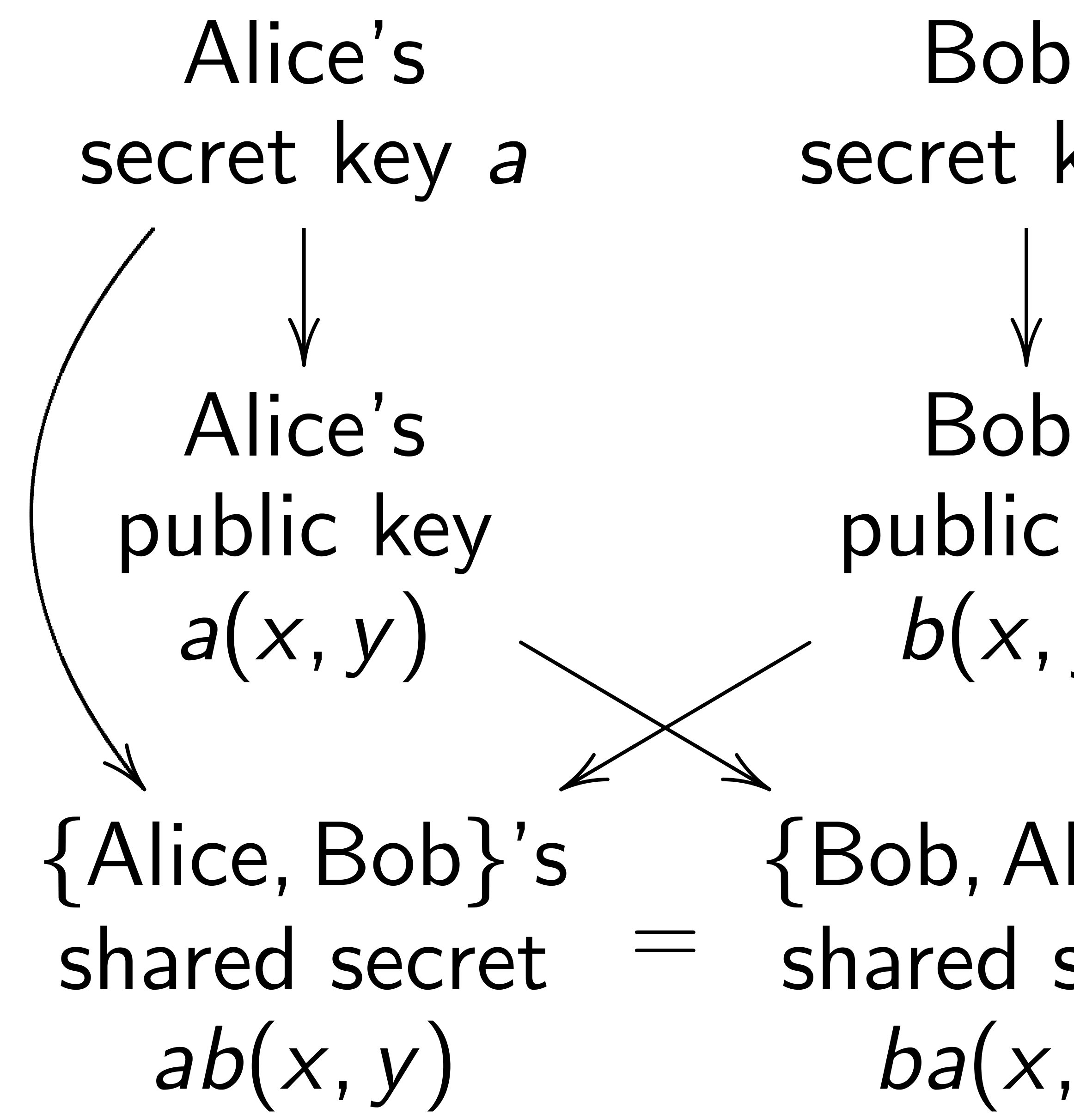
Clock cryptography

Standardize odd prime power q and $(x, y) \in \text{Clock}(\mathbf{F}_q)$ of large prime order.

Alice chooses big secret a. Computes her public key $a(x, y)$.

Bob chooses big secret b. Computes his public key $b(x, y)$.

Alice computes $a(b(x, y))$. Bob computes $b(a(x, y))$. They use this shared secret to encrypt with "AES-GCM" etc.



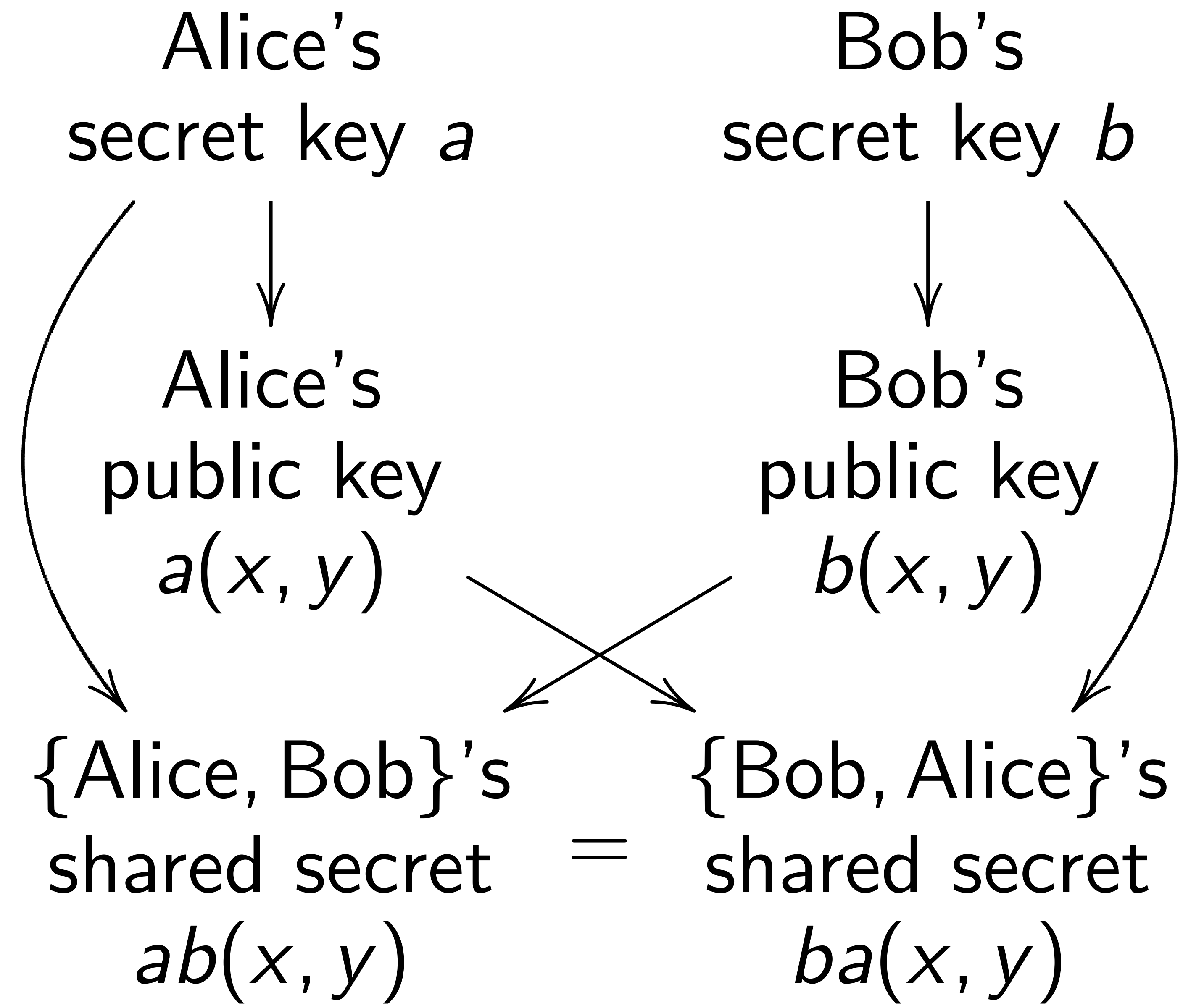
Clock cryptography

Standardize odd prime power q and $(x, y) \in \text{Clock}(\mathbf{F}_q)$ of large prime order.

Alice chooses big secret a.
Computes her public key $a(x, y)$.

Bob chooses big secret b.
Computes his public key $b(x, y)$.

Alice computes $a(b(x, y))$.
Bob computes $b(a(x, y))$.
They use this shared secret to encrypt with "AES-GCM" etc.



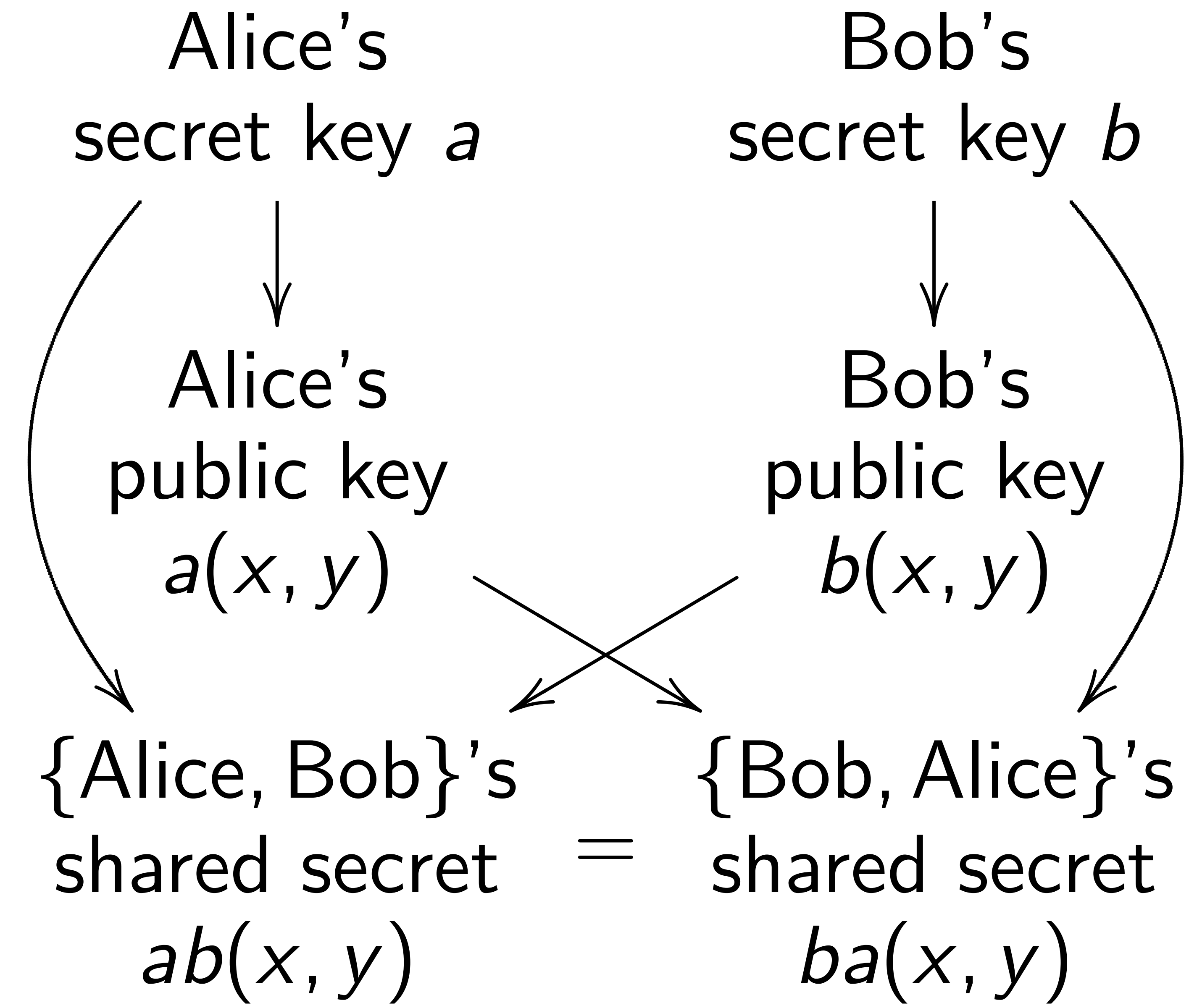
<u>Clock cryptography</u>

Standardize odd prime power q and $(x, y) \in \text{Clock}(\mathbf{F}_q)$ of large prime order.

Alice chooses big secret a. Computes her public key $a(x, y)$.

Bob chooses big secret b. Computes his public key $b(x, y)$.

Alice computes $a(b(x, y))$. Bob computes $b(a(x, y))$. They use this shared secret to encrypt with "AES-GCM" etc.



Need surprisingly large q to avoid state-of-the-art attacks. Recommendation: $q > 2^{1500}$. Better: Switch to elliptic curves.

yptography

dize odd prime power q

$y) \in \mathrm{Clock}(\mathbf{F}_q)$

prime order.

ooses big secret a.

es her public key $a(x, y)$.

oses big secret b.

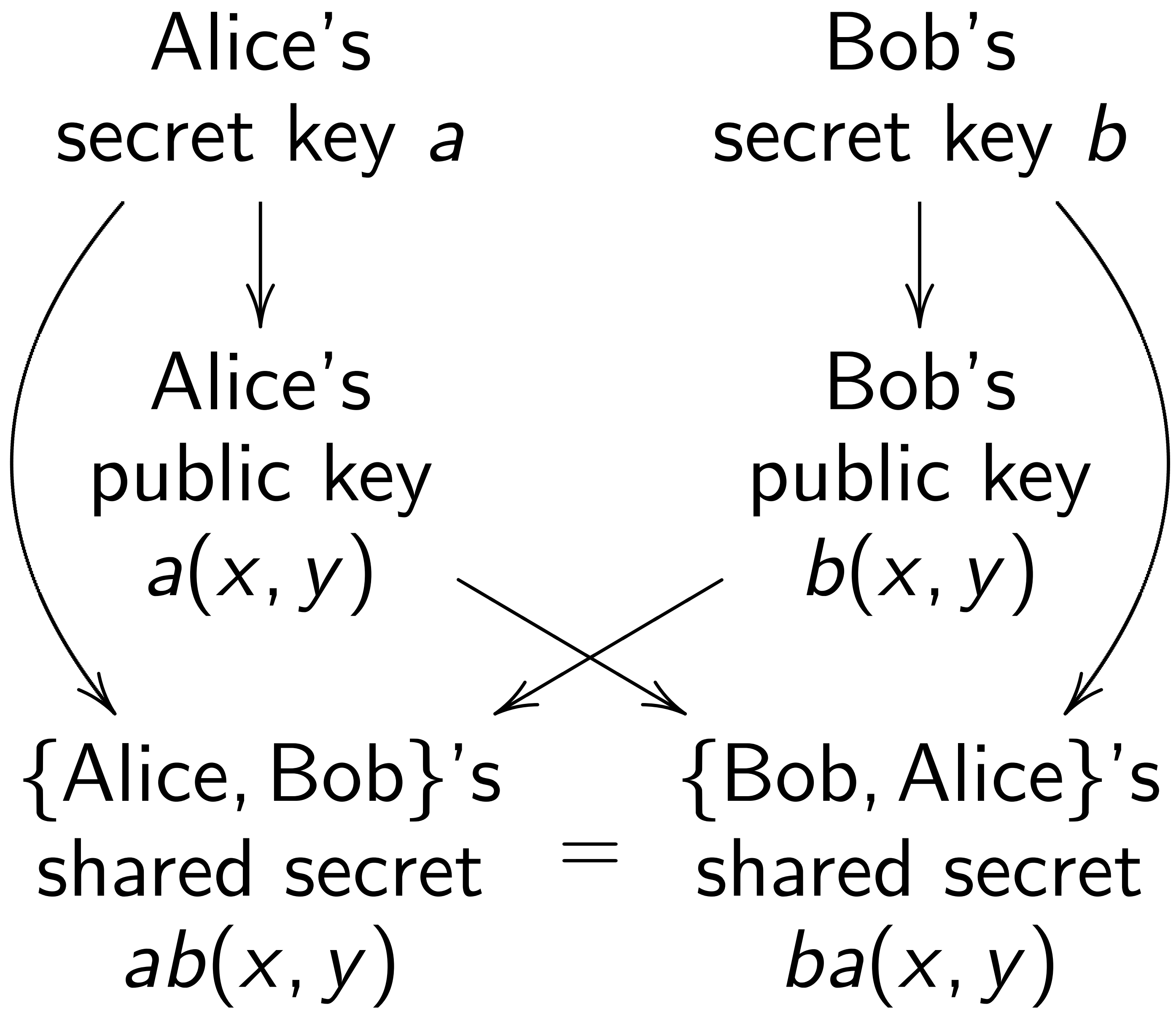
es his public key $b(x, y)$.

mputes $a(b(x, y))$.

nputes $b(a(x, y))$.

e this shared secret

pt with “AES-GCM” etc.



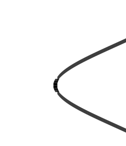
Need surprisingly large q

to avoid state-of-the-art attacks.

Recommendation: $q > 2^{1500}$.

Better: Switch to elliptic curves.

Addition



$x^2 + y^2$

Sum of (

$((x_1 y_2 +$

$(y_1 y_2 -$

y

rime power q

$k(\mathbf{F}_q)$

er.

secret a.

lic key $a(x, y)$.

ecret b.

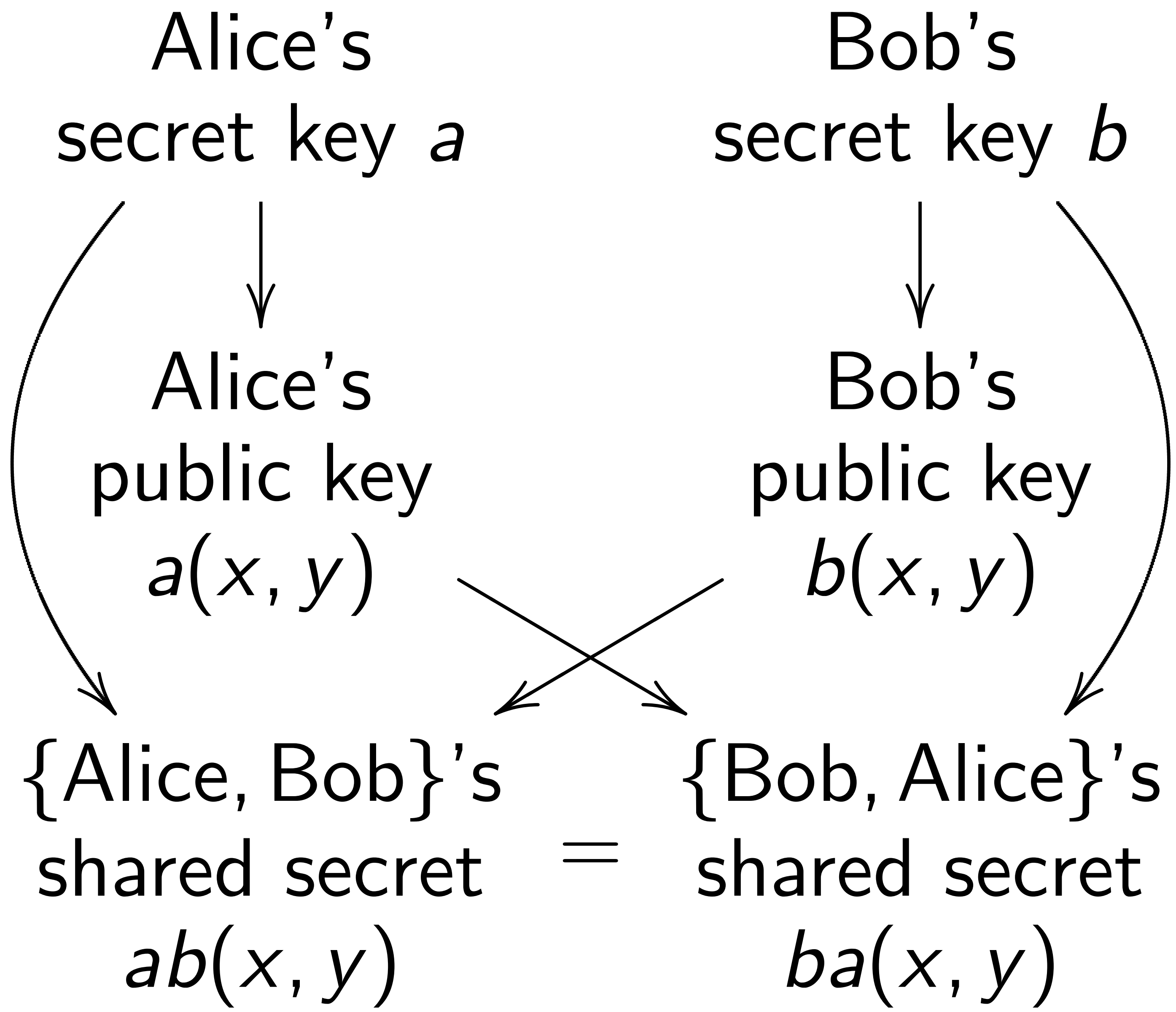
lic key $b(x, y)$.

$b(x, y))$.

$a(x, y))$.

red secret

AES-GCM" etc.



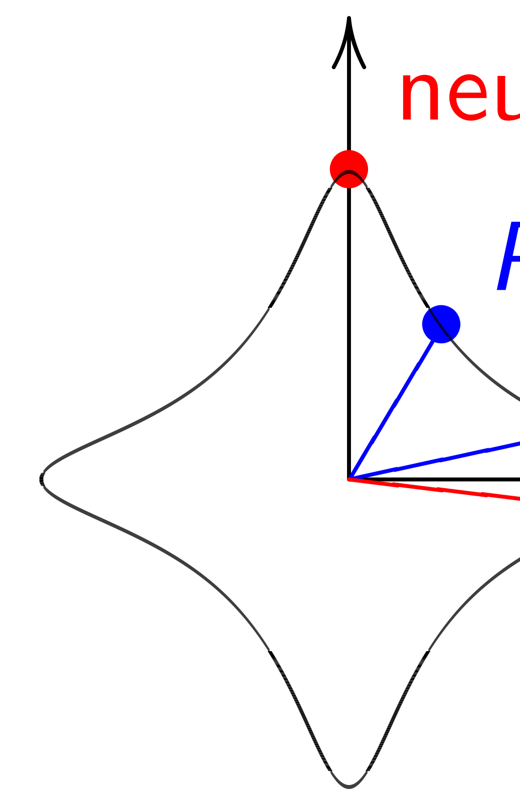
Need surprisingly large q

to avoid state-of-the-art attacks.

Recommendation: $q > 2^{1500}$.

Better: Switch to elliptic curves.

Addition on an elli



$x^2 + y^2 = 1 - 30x$

Sum of (x_1, y_1) an

$((x_1y_2 + y_1x_2)/(1-$

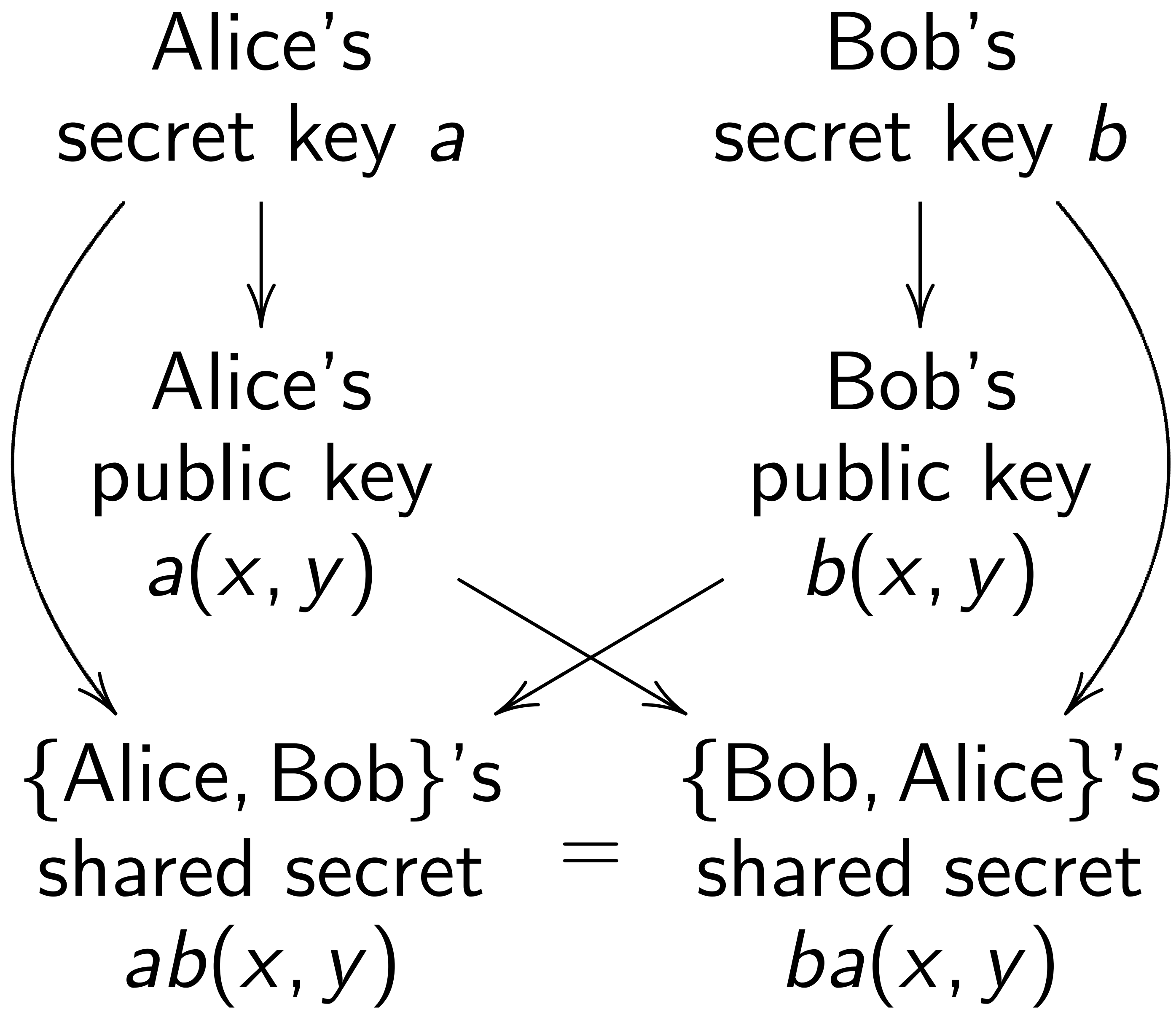
$(y_1y_2 - x_1x_2)/(1+$

er q

$x, y)$.

$x, y)$.

, etc.



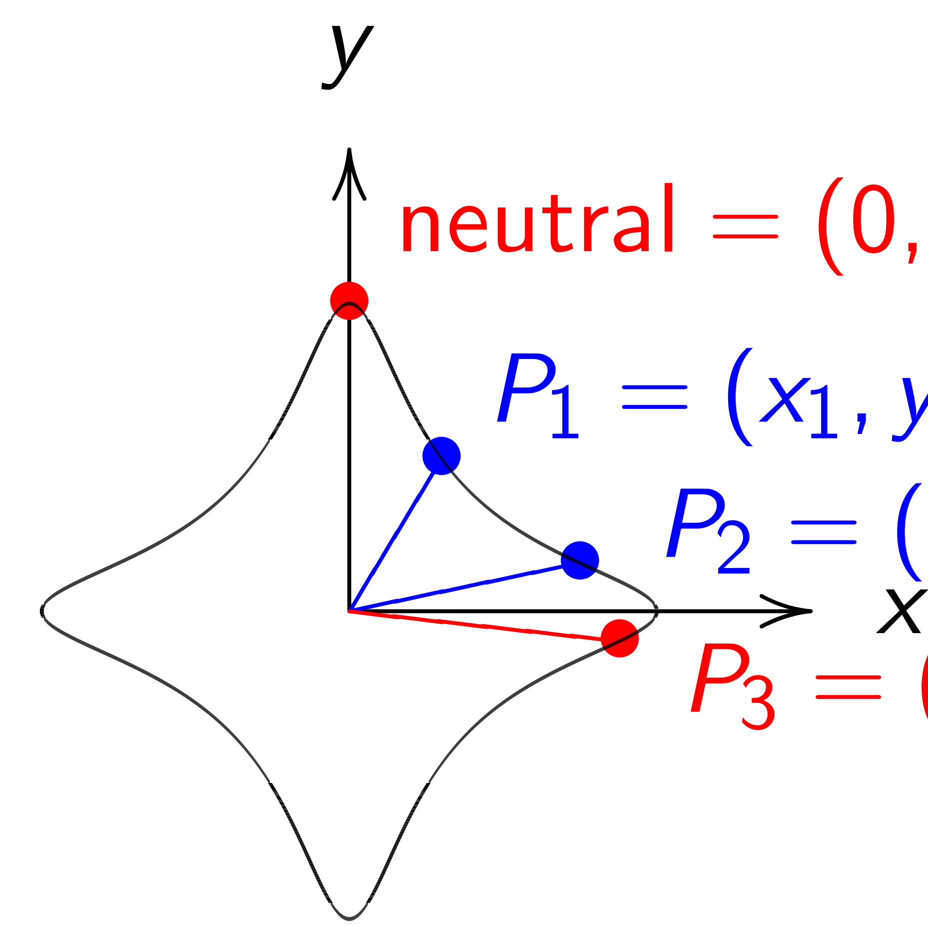
Need surprisingly large q

to avoid state-of-the-art attacks.

Recommendation: $q > 2^{1500}$.

Better: Switch to elliptic curves.

Addition on an elliptic curve

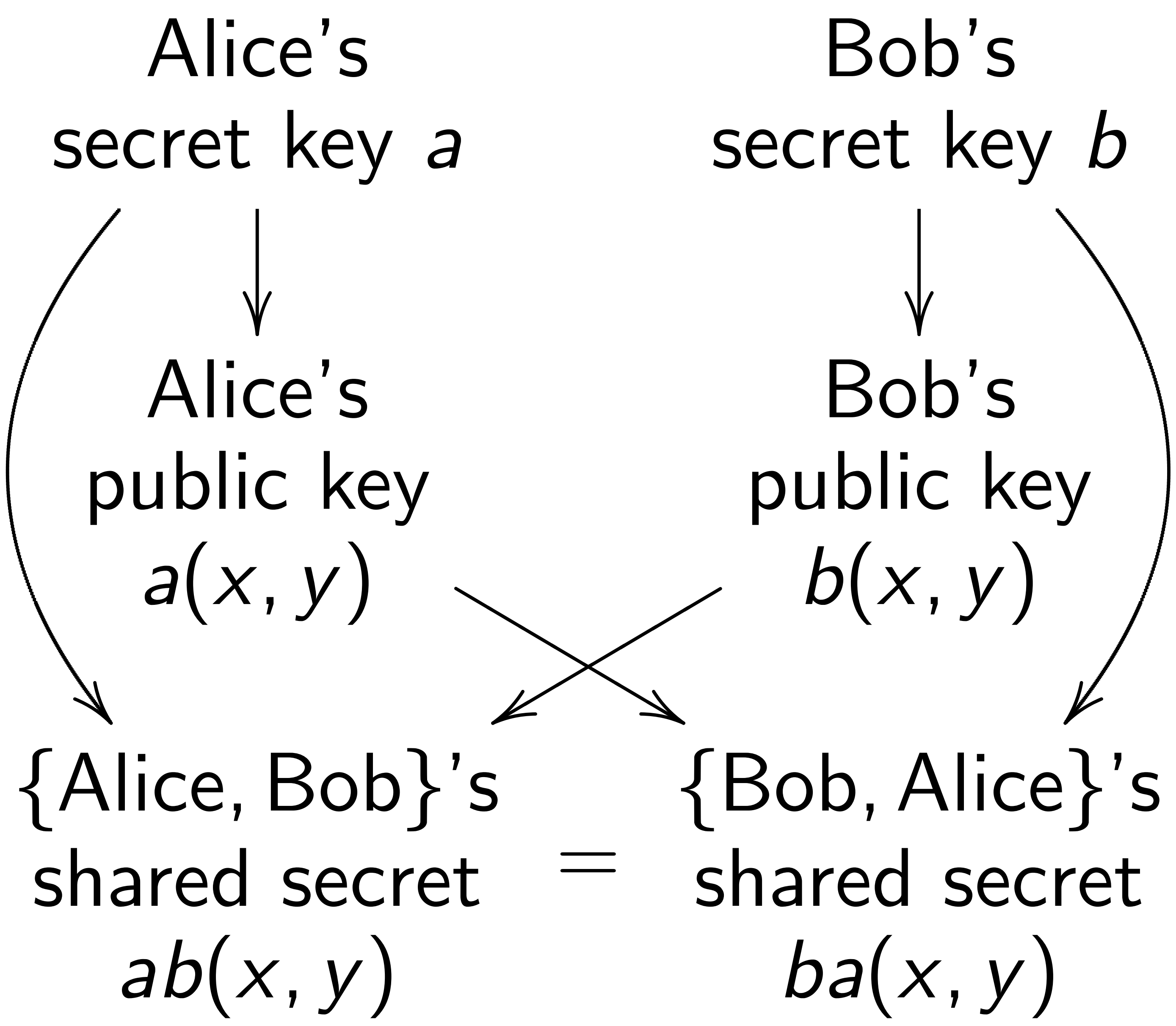


$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2)

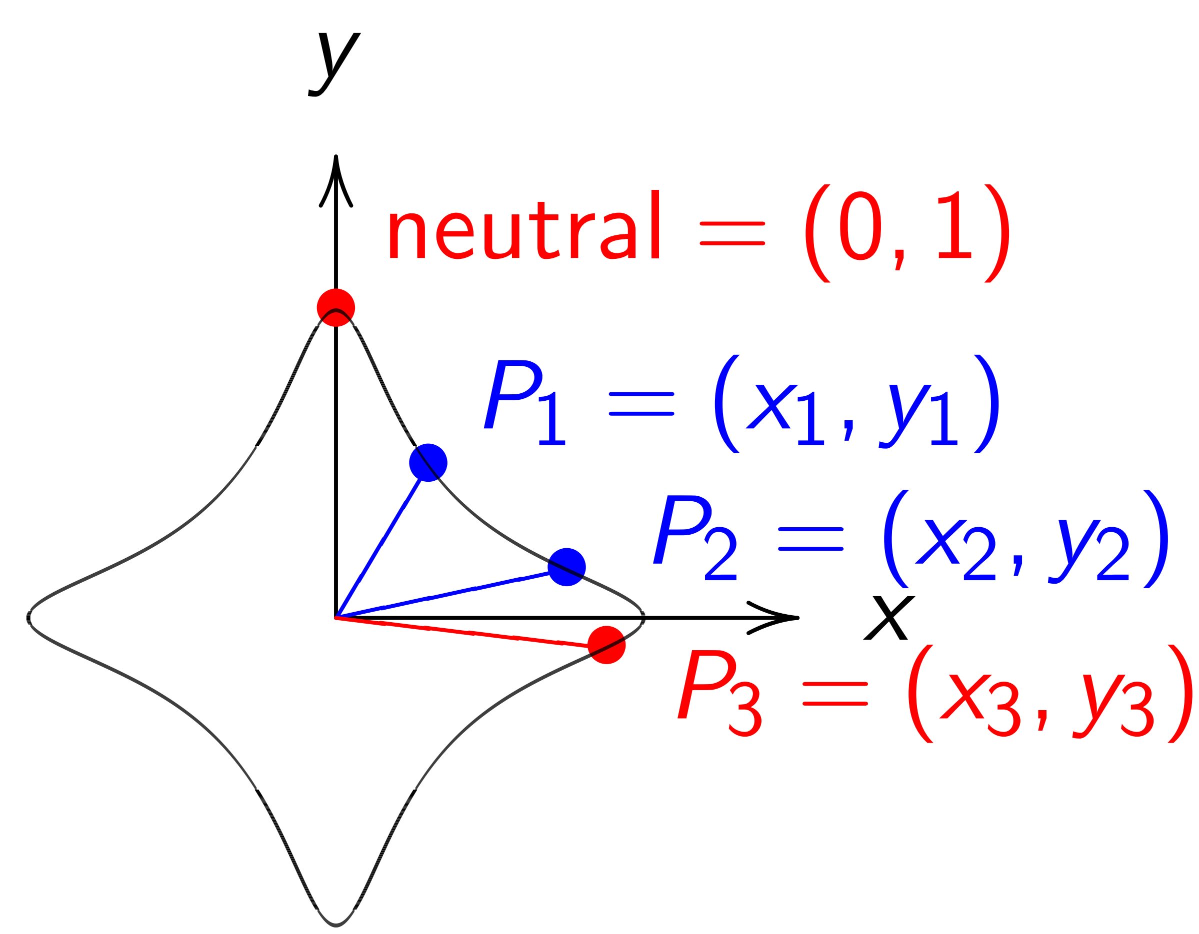
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y$

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y$



Need surprisingly large q
to avoid state-of-the-art attacks.
Recommendation: $q > 2^{1500}$.
Better: Switch to elliptic curves.

Addition on an elliptic curve



$x^2 + y^2 = 1 - 30x^2y^2$.
Sum of (x_1, y_1) and (x_2, y_2) is
$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

ce's
key a

Bob's
secret key b

ce's
c key
$, y)$

Bob's
public key
$b(x, y)$

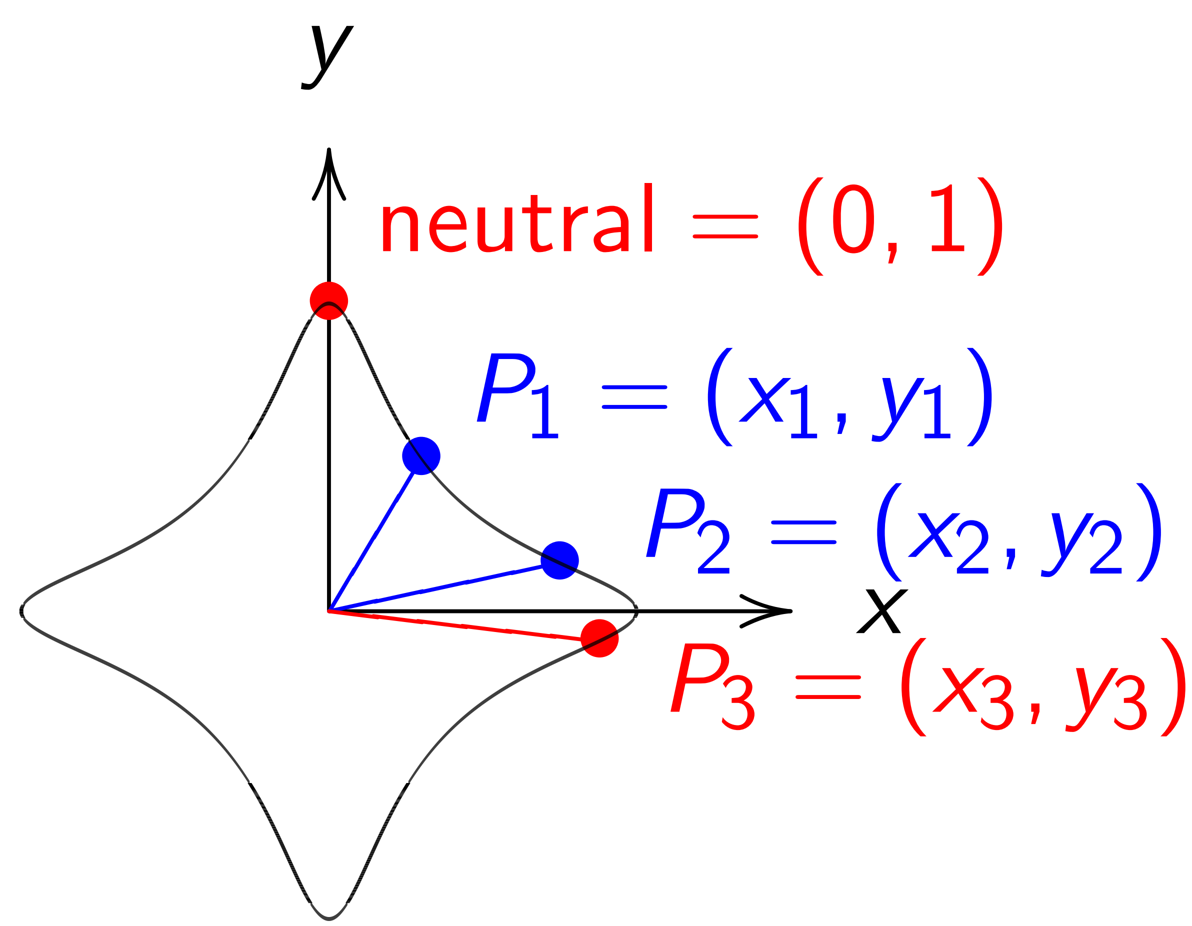
Bob}'s
secret
$x, y)$

=

{Bob, Alice}'s
shared secret
$ba(x, y)$

rprisingly large q
state-of-the-art attacks.
mendation: $q > 2^{1500}$.
Switch to elliptic curves.

Addition on an elliptic curve

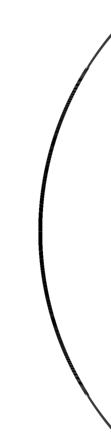


$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The cloc



$x^2 + y^2$

Sum of (

$(x_1y_2 +$

$y_1y_2 -$

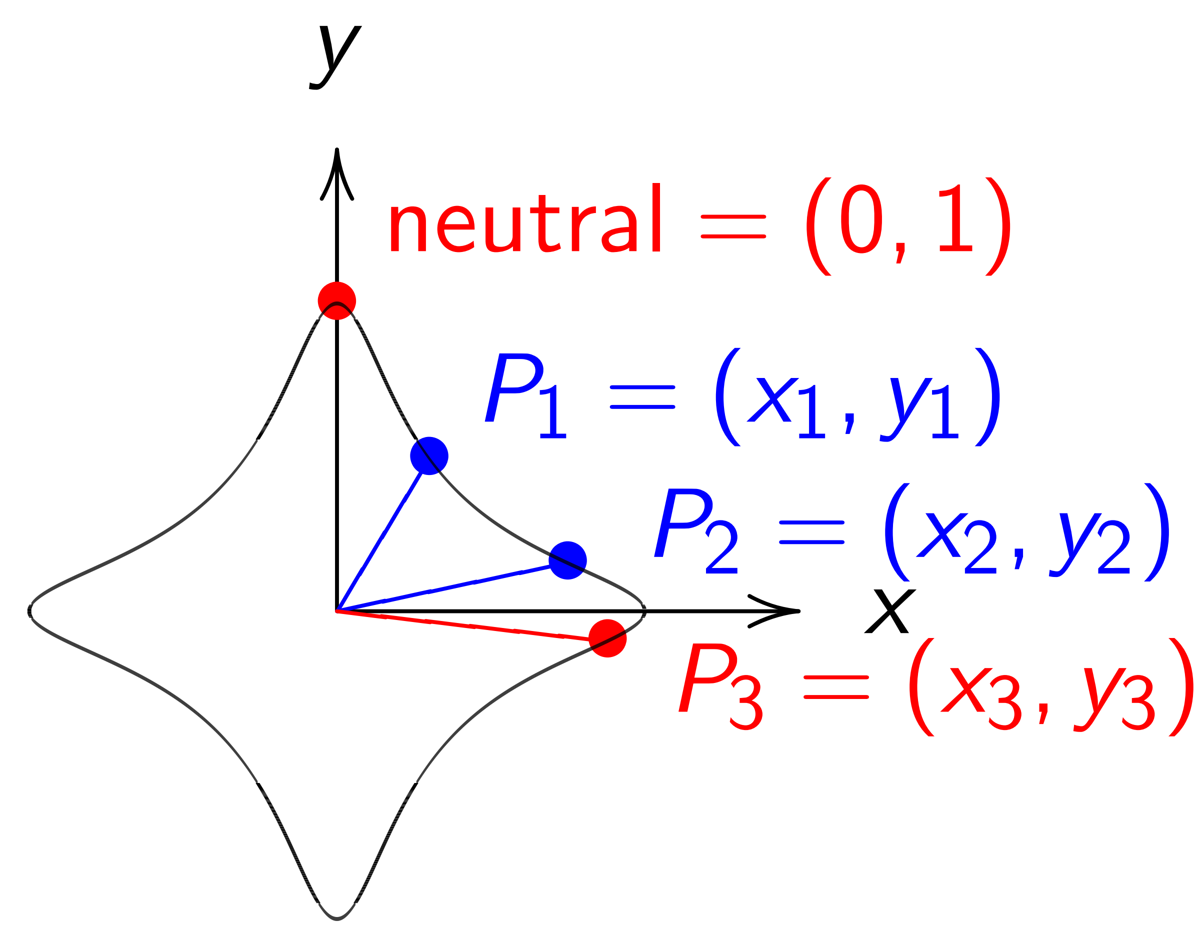
Bob's
secret key b

Bob's
public key
$b(x, y)$

$\{$Bob, Alice$\}$'s
shared secret
$ba(x, y)$

large q
he-art attacks.
$q > 2^{1500}$.
elliptic curves.

Addition on an elliptic curve

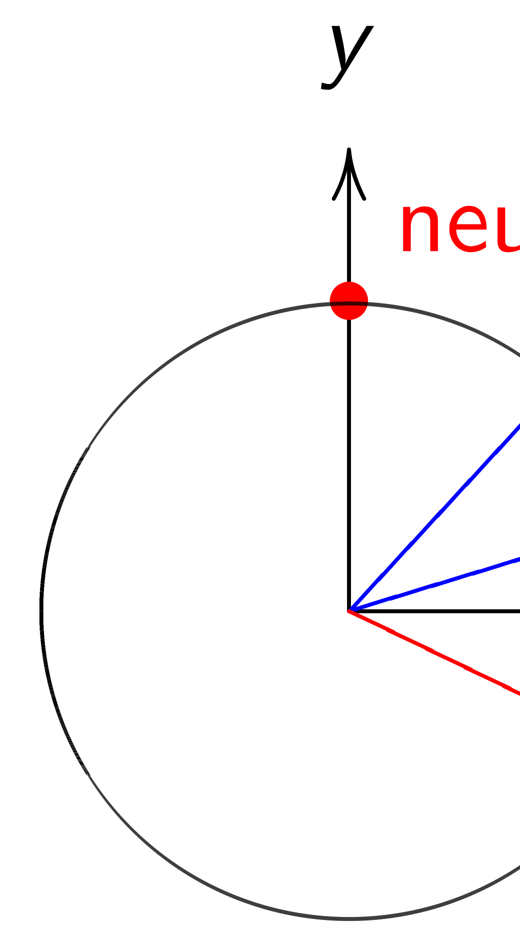


$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$
$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, f



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) an

$(x_1y_2 + y_1x_2,$
$y_1y_2 - x_1x_2)$.

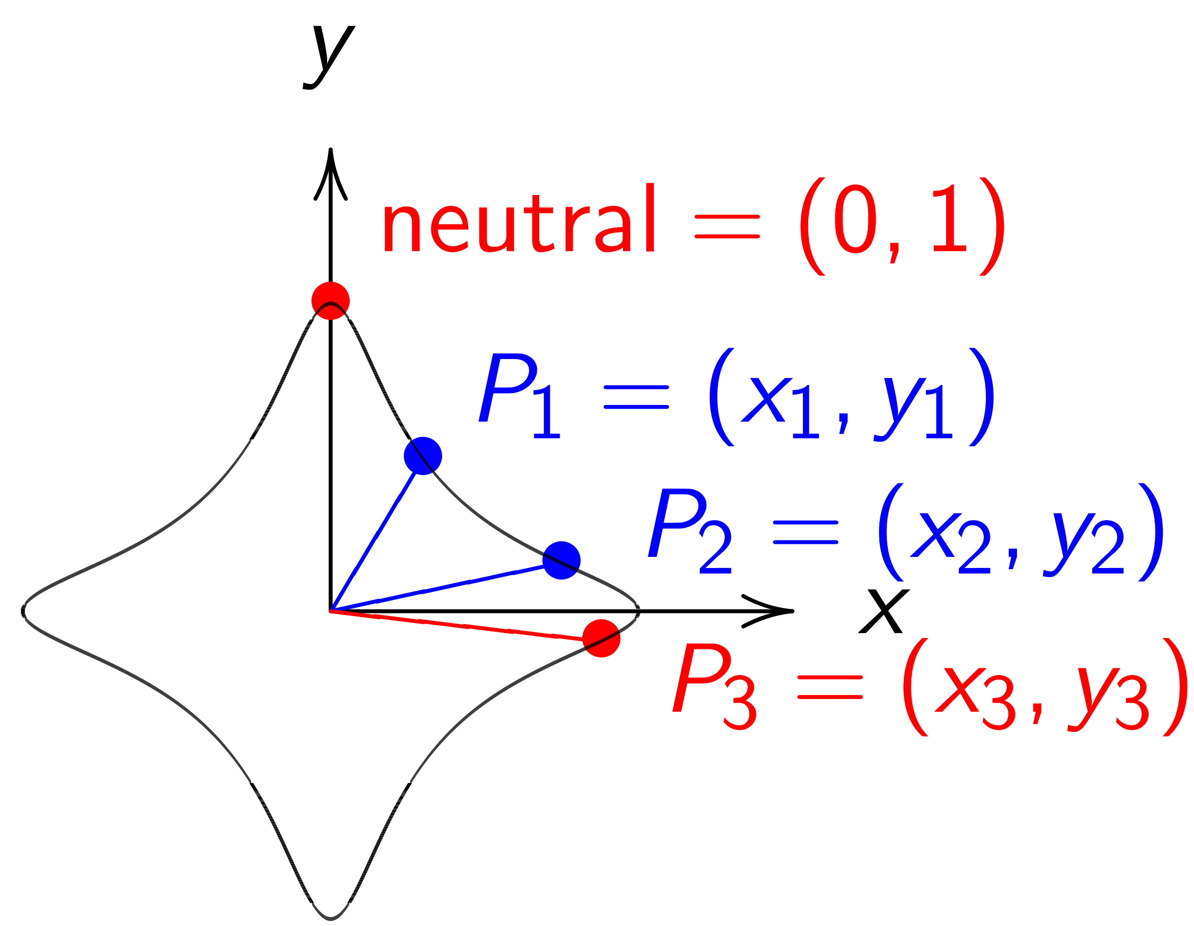
's
key b

's
key
$y)$

lice}'s
secret
$y)$

acks.
0.
rves.

Addition on an elliptic curve



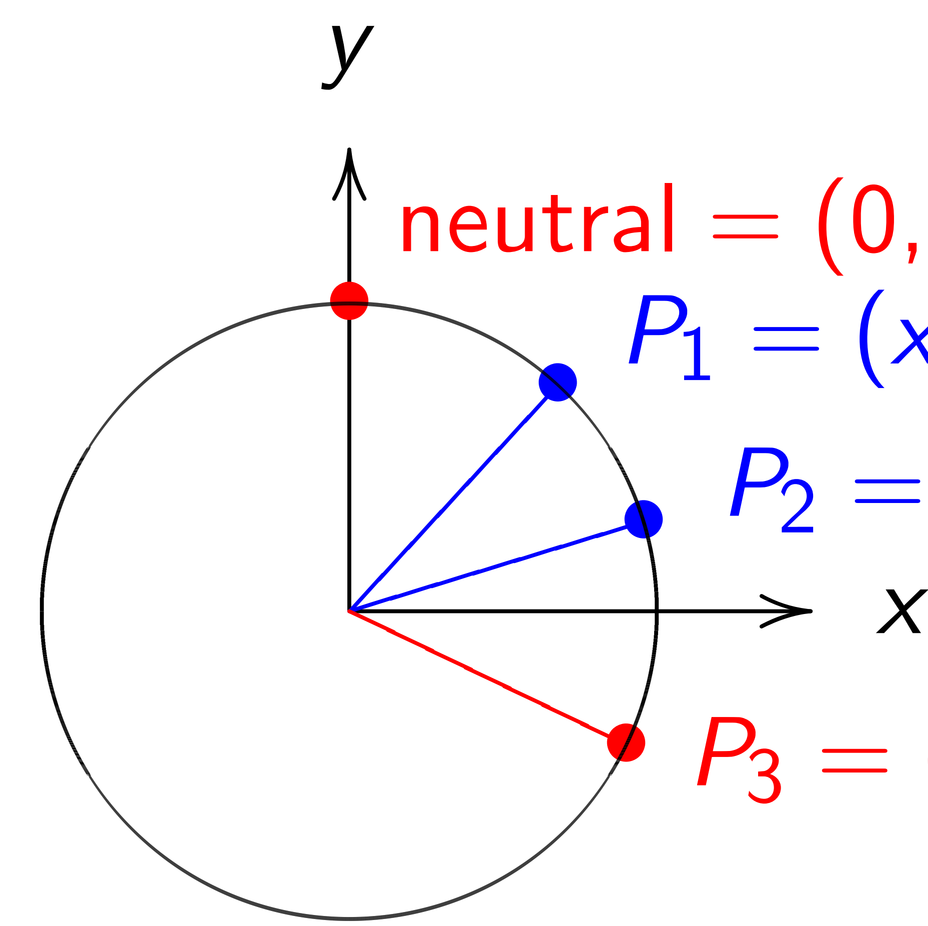
$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, for compar



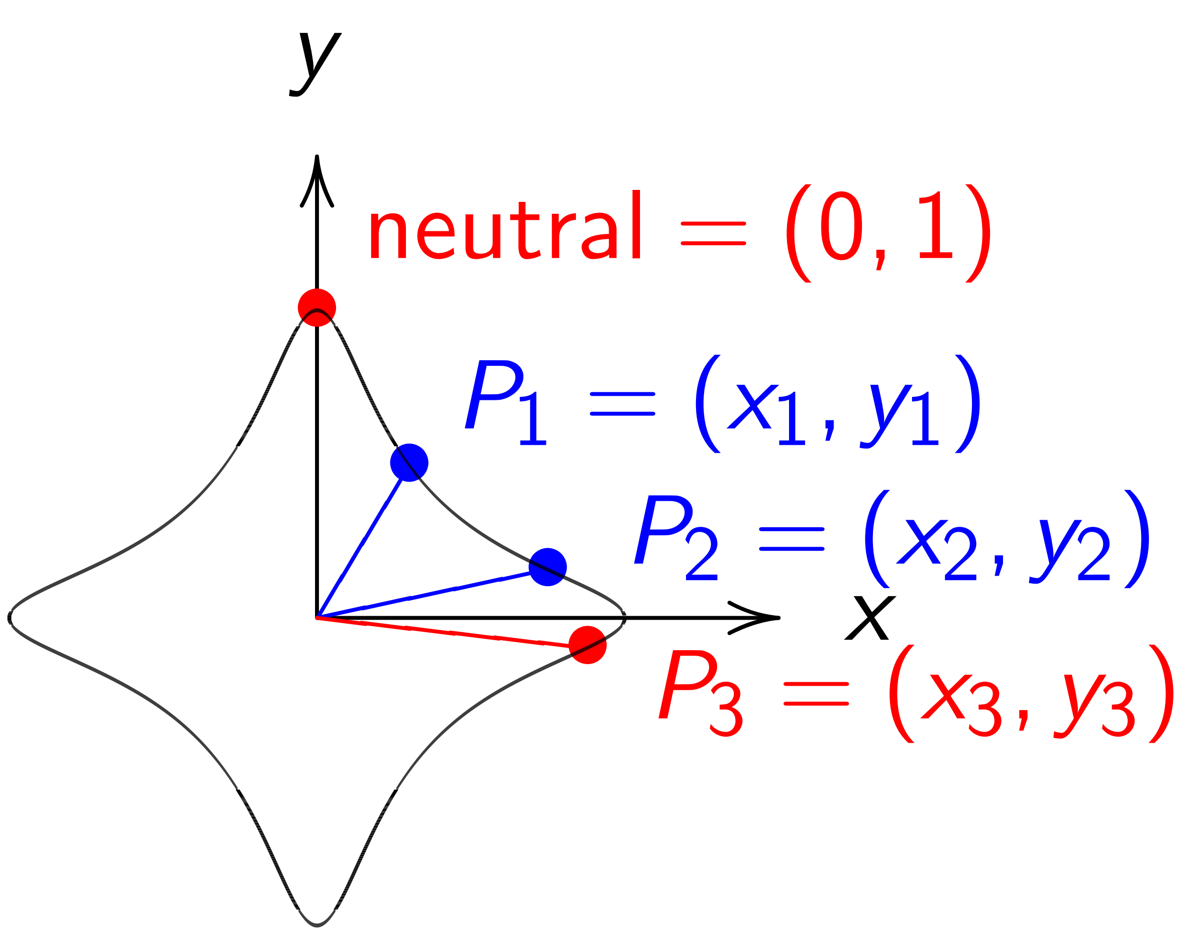
$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2)

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

Addition on an elliptic curve



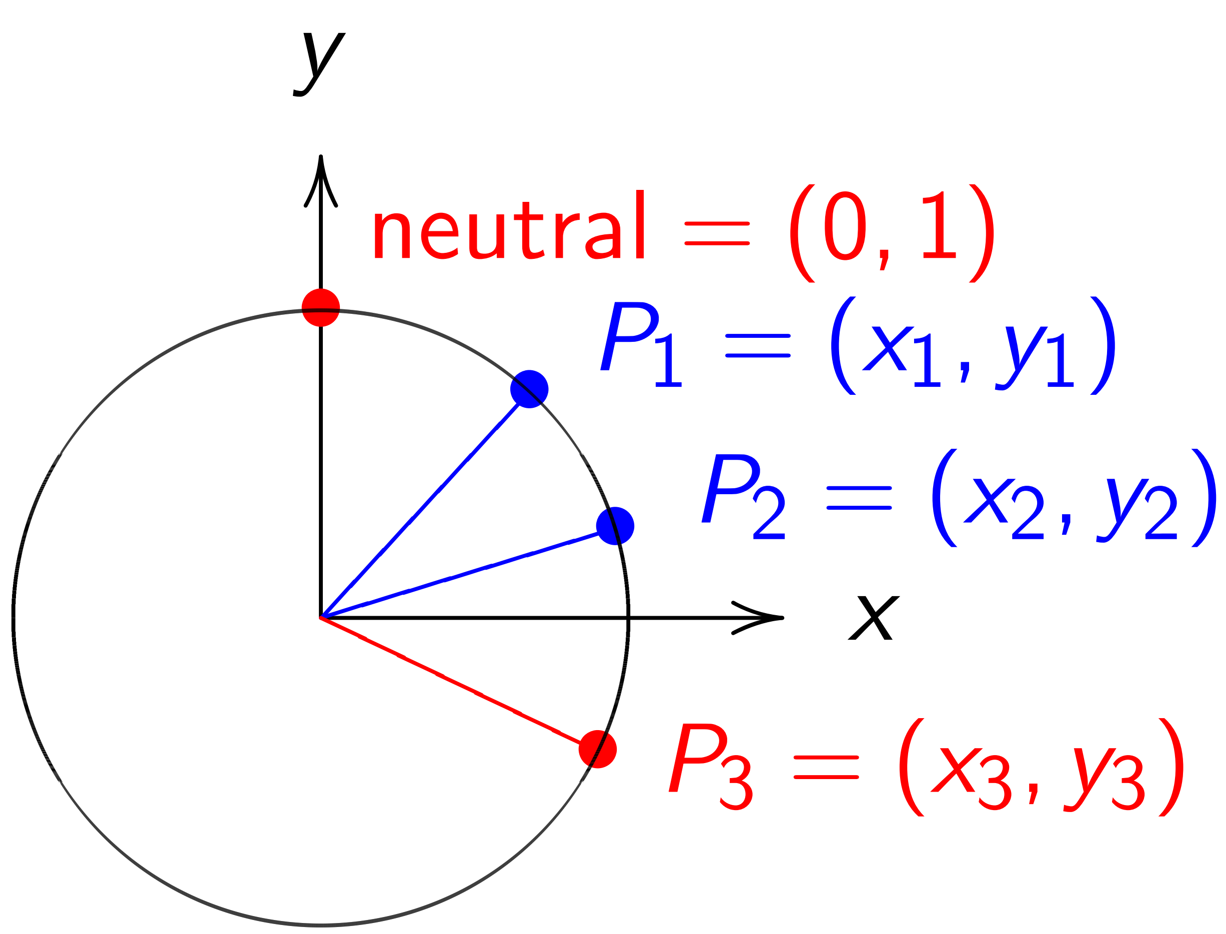
$x^2 + y^2 = 1 - 30x^2y^2$.

Sum of (x_1, y_1) and (x_2, y_2) is

$((x_1y_2+y_1x_2)/(1-30x_1x_2y_1y_2),$

$(y_1y_2-x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, for comparison:



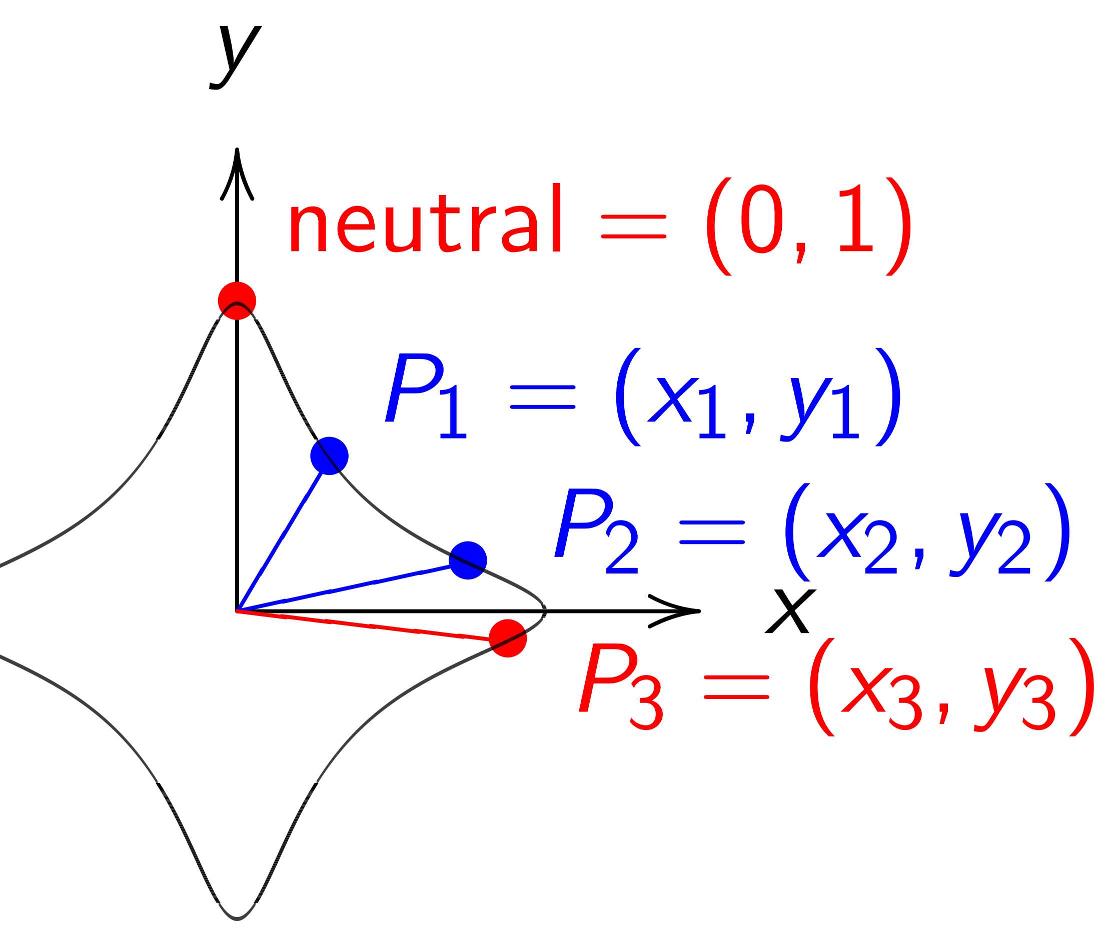
$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

n on an elliptic curve



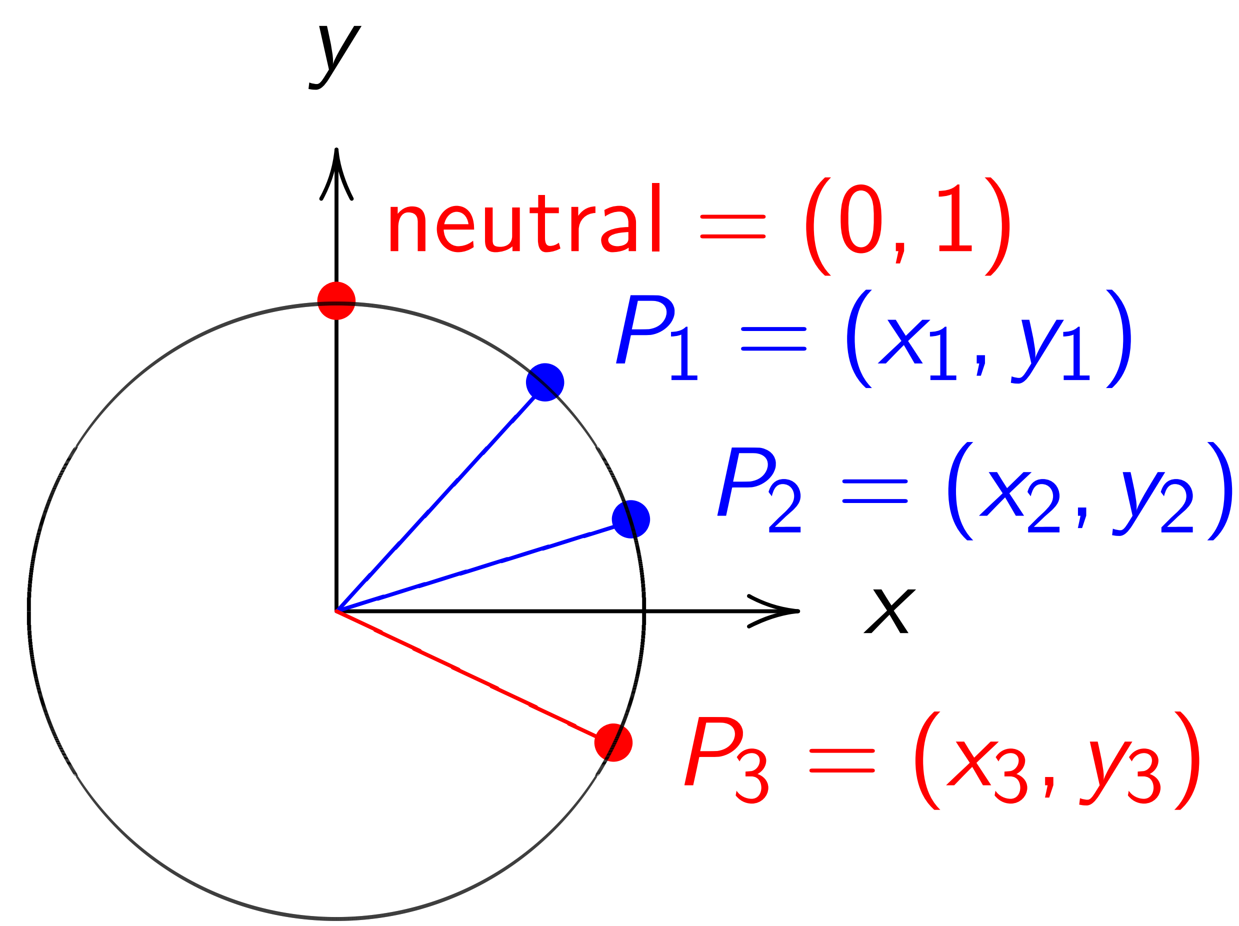
$= 1 - 30x^2y^2$.

(x_1, y_1) and (x_2, y_2) is

$y_1x_2)/(1-30x_1x_2y_1y_2)$,

$x_1x_2)/(1+30x_1x_2y_1y_2))$.

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

More ell

Choose a

Choose a

$\{(x, y) \in$

x^2 -

is a “cor

“The Ed

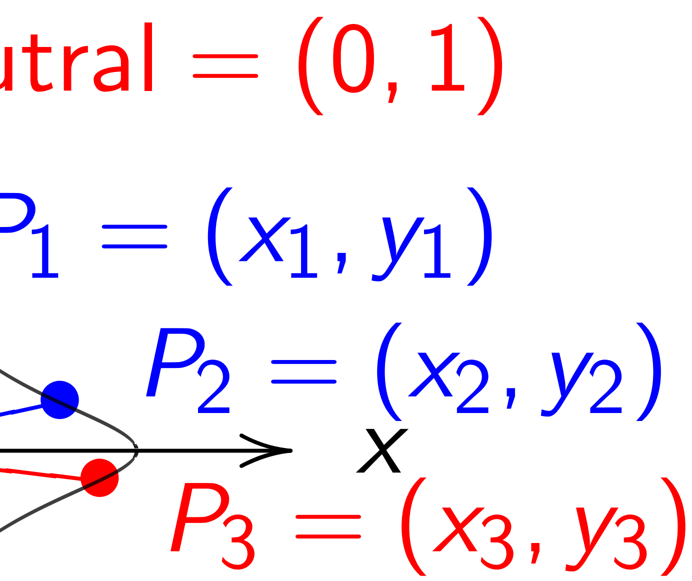
(x_1, y_1) +

where

$x_3 = \frac{x}{1 -}$

$y_3 = \frac{y}{1 -}$

iptic curve



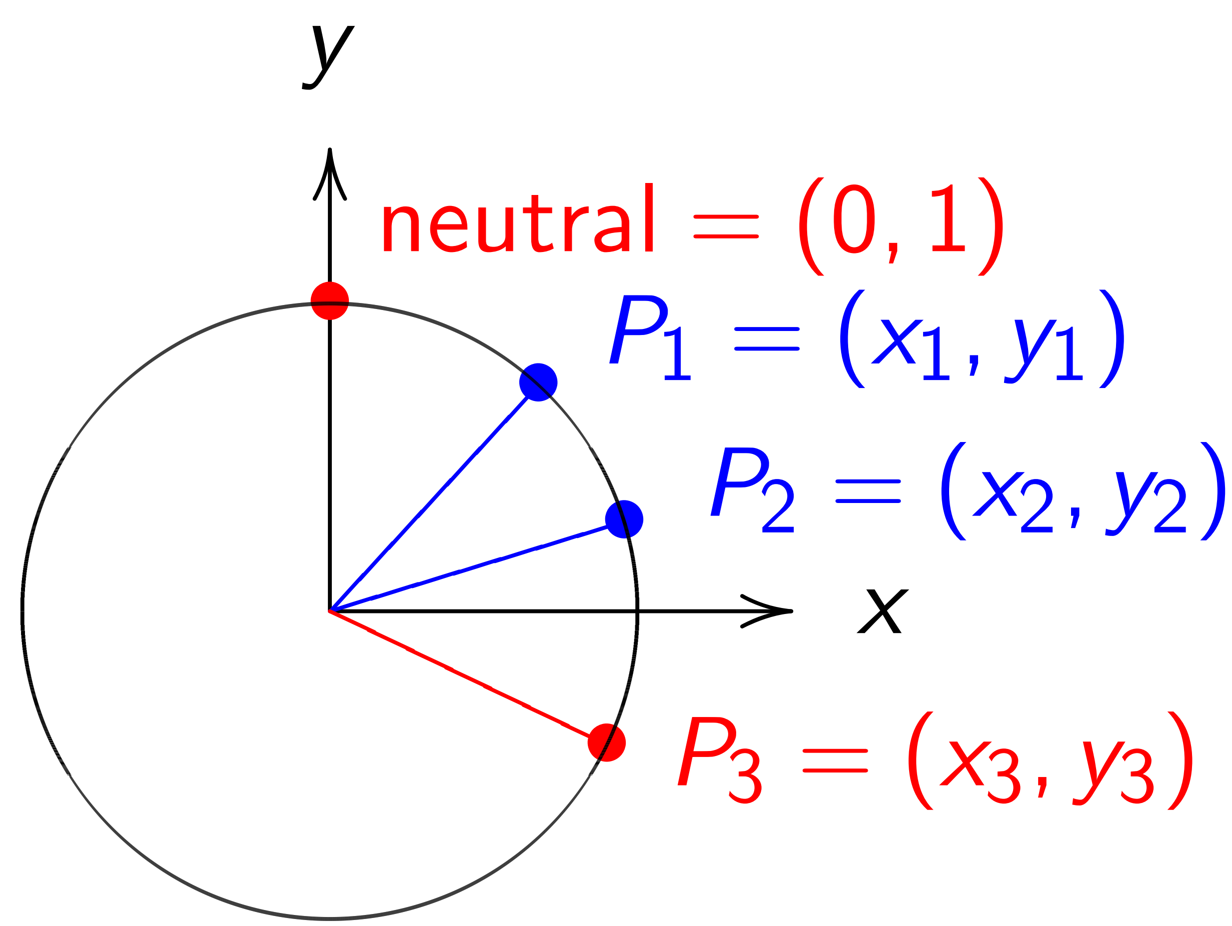
x^2y^2.

nd (x_2, y_2) is

$-30x_1x_2y_1y_2)$,

$-30x_1x_2y_1y_2))$.

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1y_2 + y_1x_2,$

$y_1y_2 - x_1x_2)$.

More elliptic curve

Choose an odd pri

Choose a *non-squa*

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q$

$x^2 + y^2 = 1 -$

is a “complete Edw

“The Edwards add

$(x_1, y_1) + (x_2, y_2)$

where

$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1}$

$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1}$

e

1)

$y_1)$

$x_2, y_2)$

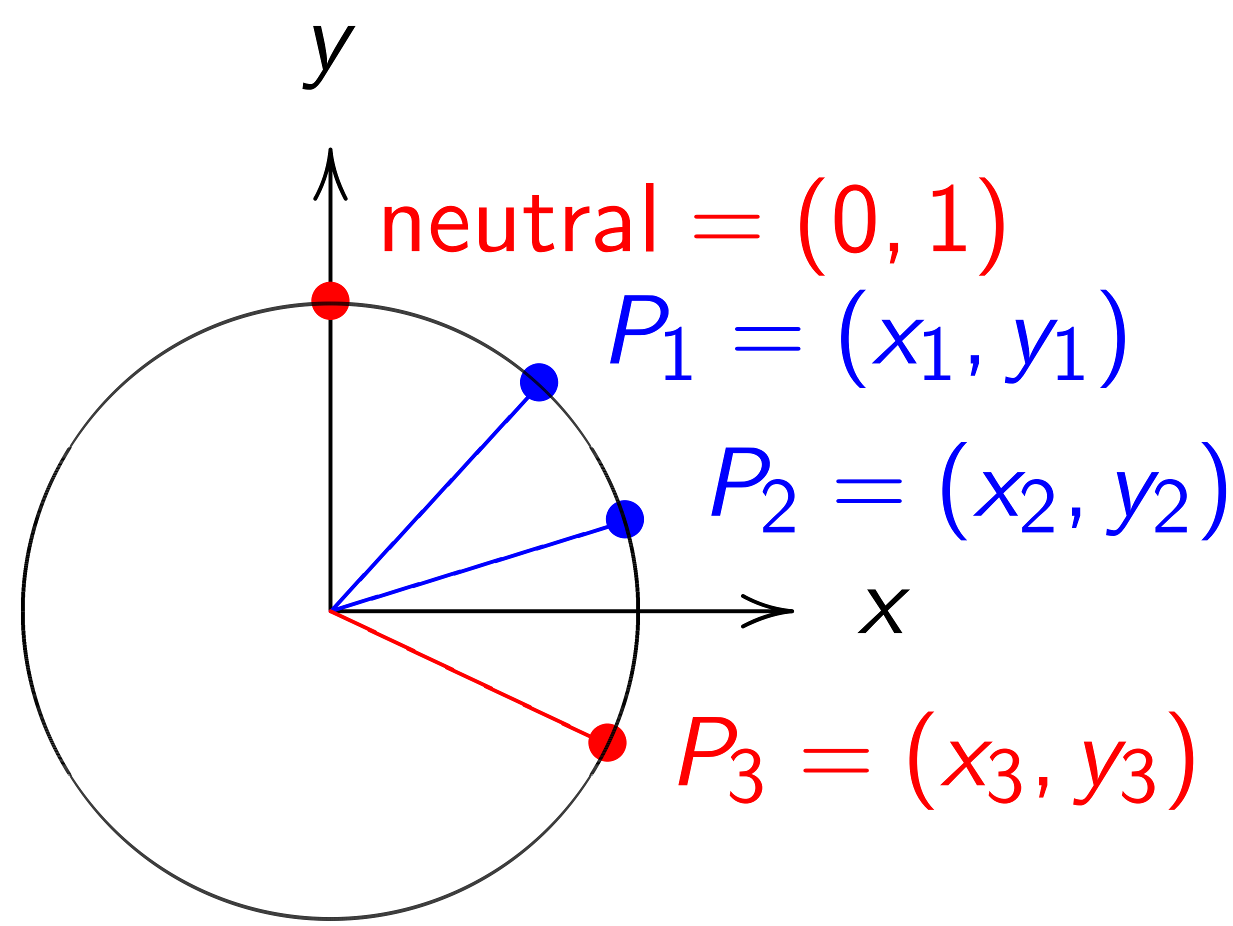
(x_3, y_3)

is

$y_2),$

$y_2)).$

The clock again, for comparison:



$x^2 + y^2 = 1.$

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1 y_2 + y_1 x_2,$

$y_1 y_2 - x_1 x_2).$

More elliptic curves

Choose an odd prime power

Choose a *non-square* $d \in \mathbf{F}_q$

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$x^2 + y^2 = 1 + dx^2y^2\}$

is a "complete Edwards curv

"The Edwards addition law"

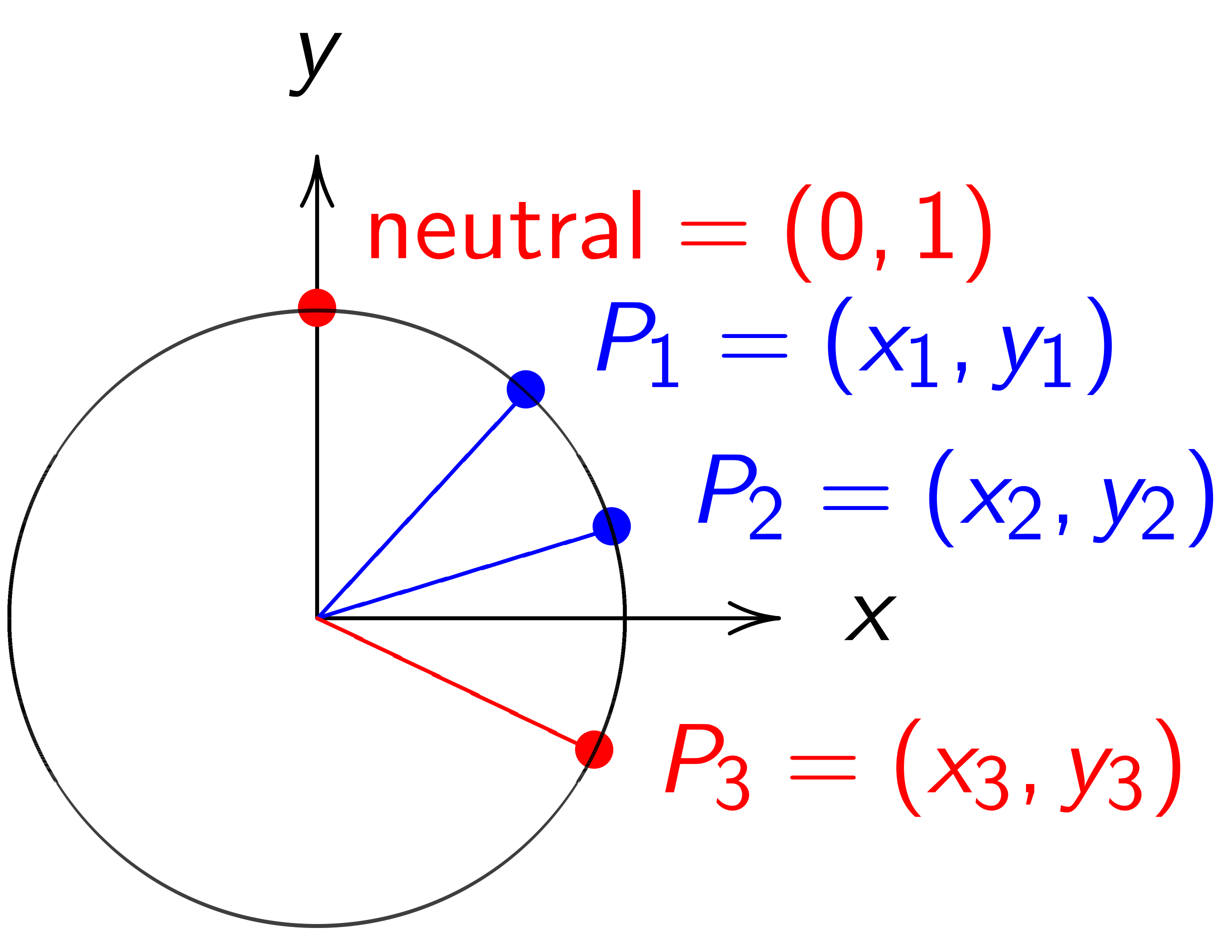
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

where

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}.$$

The clock again, for comparison:



$x^2 + y^2 = 1$.

Sum of (x_1, y_1) and (x_2, y_2) is

$(x_1 y_2 + y_1 x_2,$

$y_1 y_2 - x_1 x_2)$.

More elliptic curves

Choose an odd prime power q.

Choose a *non-square* $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : x^2 + y^2 = 1 + d x^2 y^2\}$$

is a "complete Edwards curve".

"The Edwards addition law":

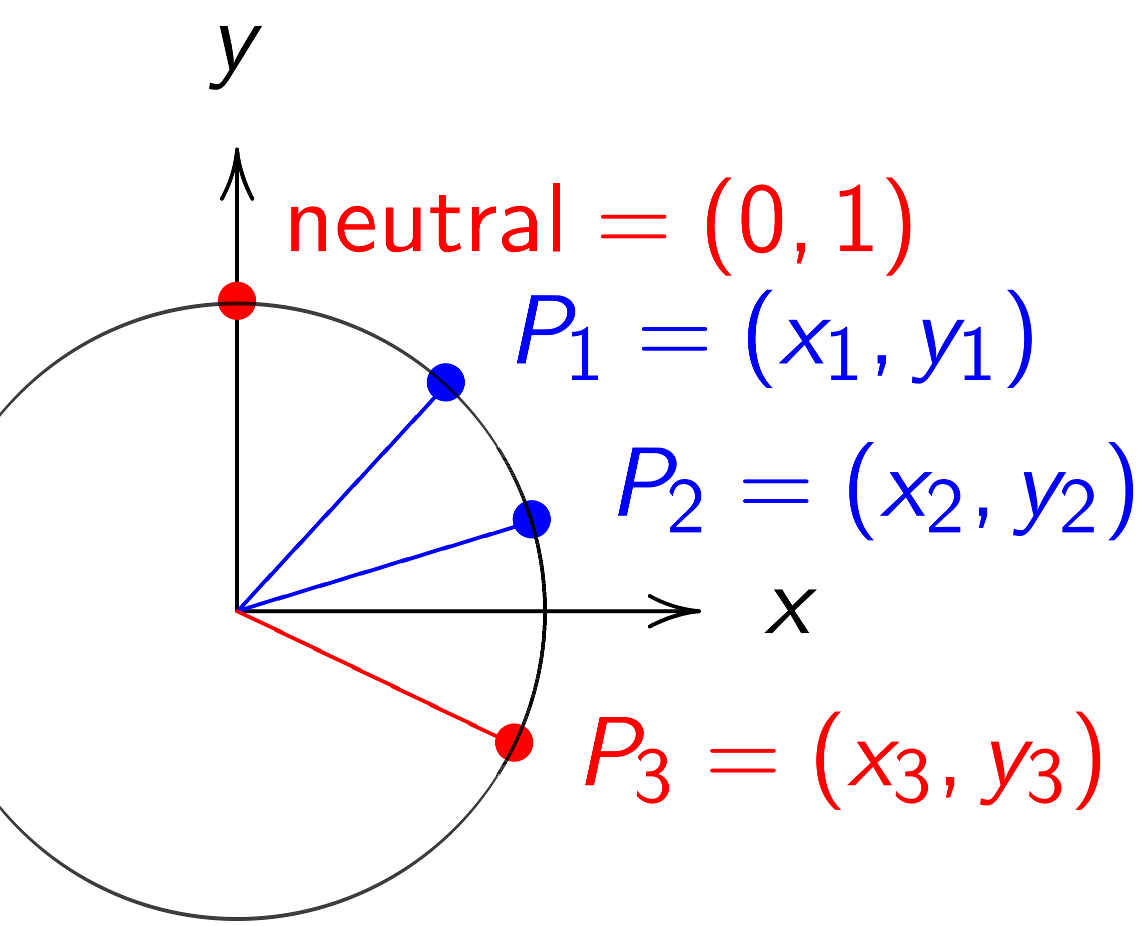
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

where

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}.$$

ck again, for comparison:



$= 1.$

(x_1, y_1) and (x_2, y_2) is

$y_1 x_2,$

$x_1 x_2).$

More elliptic curves

Choose an odd prime power q.

Choose a *non-square* $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a "complete Edwards curve".

"The Edwards addition law":

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

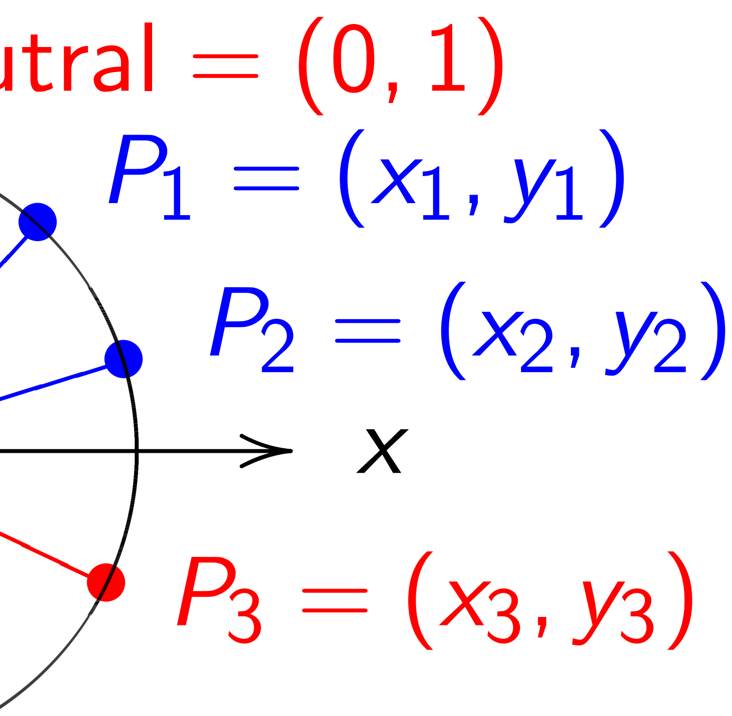
where

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}.$$

"What i

or comparison:



nd (x_2, y_2) is

More elliptic curves

Choose an odd prime power q.
Choose a *non-square* $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a "complete Edwards curve".

"The Edwards addition law":
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
where

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}.$$

"What if denomin

rison:

$1)$

$x_1, y_1)$

(x_2, y_2)

(x_3, y_3)

is

More elliptic curves

Choose an odd prime power q.

Choose a *non-square* $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : \\ x^2 + y^2 = 1 + dx^2y^2\}$$

is a "complete Edwards curve".

"The Edwards addition law":

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

where

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

"What if denominators are 0

More elliptic curves

Choose an odd prime power q.

Choose a *non-square* $d \in \mathbf{F}_q$.

$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q :$
$x^2 + y^2 = 1 + dx^2y^2\}$
is a "complete Edwards curve".

"The Edwards addition law":

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
where

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2},$$

$$y_3 = \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}.$$

"What if denominators are 0?"

More elliptic curves

Choose an odd prime power q.
Choose a *non-square* $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : x^2 + y^2 = 1 + dx^2y^2\}$$

is a "complete Edwards curve".

"The Edwards addition law":
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
where

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
then $dx_1x_2y_1y_2$ can't be ± 1.

More elliptic curves

Choose an odd prime power q.
Choose a *non-square* $d \in \mathbf{F}_q$.

$$\{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q : x^2 + y^2 = 1 + dx^2y^2\}$$

is a "complete Edwards curve".

"The Edwards addition law":
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
where

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
then $dx_1x_2y_1y_2$ can't be ± 1.

Main steps in proof:
If $(dx_1x_2y_1y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1x_2y_1y_2y_1)^2 =$
$dx_1^2y_1^2(x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

iptic curves

an odd prime power q.

a *non-square* $d \in \mathbf{F}_q$.

$\in \mathbf{F}_q \times \mathbf{F}_q$:

$+ y^2 = 1 + dx^2y^2\}$

mplete Edwards curve".

lwards addition law":

$+ (x_2, y_2) = (x_3, y_3)$

$\frac{{}_1y_2 + y_1x_2}{+ dx_1x_2y_1y_2}$,

$\frac{{}_1y_2 - x_1x_2}{- dx_1x_2y_1y_2}$.

"What if denominators are 0?"

Answer: They aren't!

If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
then $dx_1x_2y_1y_2$ can't be ± 1.

Main steps in proof:

If $(dx_1x_2y_1y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1x_2y_1y_2y_1)^2 =$
$dx_1^2y_1^2(x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

"Doesn'
standard

e.g. "Ev
is linear.

e.g. "Th
cardinali
of additi
two." (1

es

me power q.

are $d \in \mathbf{F}_q$.

:

$+ dx^2y^2\}$

wards curve".

dition law":

$= (x_3, y_3)$

$\frac{2}{y_2}$,

$\frac{2}{y_2}$.

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$
then $dx_1x_2y_1y_2$ can't be ± 1.

Main steps in proof:
If $(dx_1x_2y_1y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1x_2y_1y_2y_1)^2 =$
$dx_1^2y_1^2(x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

"Doesn't this cont
standard structure

e.g. "Every affine
is linear."

e.g. "Theorem 1.
cardinality of a co
of addition laws o
two." (1995 Bosm

q.

q.

ve".

:

"What if denominators are 0?"

Answer: They aren't!

If $x_1^2 + y_1^2 = 1 + dx_1^2 y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2 y_2^2$
then $dx_1 x_2 y_1 y_2$ can't be ± 1.

Main steps in proof:

If $(dx_1 x_2 y_1 y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1 x_2 y_1 y_2 y_1)^2 =$
$dx_1^2 y_1^2 (x_2 + y_2)^2$.
Conclude that d is a square.

But d is not a square! Q.E.D.

"Doesn't this contradict
standard structure theorems

e.g. "Every affine algebraic g
is linear."

e.g. "Theorem 1. The small
cardinality of a complete sys
of addition laws on E equals
two." (1995 Bosma–Lenstra

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = 1 + dx_1^2 y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2 y_2^2$
then $dx_1 x_2 y_1 y_2$ can't be ± 1.

Main steps in proof:
If $(dx_1 x_2 y_1 y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1 x_2 y_1 y_2 y_1)^2 =$
$dx_1^2 y_1^2 (x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

"Doesn't this contradict standard structure theorems?"

e.g. "Every affine algebraic group is linear."

e.g. "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma–Lenstra)

"What if denominators are 0?"

Answer: They aren't!
If $x_1^2 + y_1^2 = 1 + dx_1^2 y_1^2$
and $x_2^2 + y_2^2 = 1 + dx_2^2 y_2^2$
then $dx_1x_2y_1y_2$ can't be ± 1.

Main steps in proof:
If $(dx_1x_2y_1y_2)^2 = 1$ then
curve equation implies
$(x_1 + dx_1x_2y_1y_2y_1)^2 =$
$dx_1^2 y_1^2 (x_2 + y_2)^2$.
Conclude that d is a square.
But d is not a square! Q.E.D.

"Doesn't this contradict
standard structure theorems?"

e.g. "Every affine algebraic group
is linear."

e.g. "Theorem 1. The smallest
cardinality of a complete system
of addition laws on E equals
two." (1995 Bosma–Lenstra)

The way out: Don't confuse
geometry with arithmetic.
The Edwards addition law is
complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

f denominators are 0?"

They aren't!

$y_1^2 = 1 + dx_1^2 y_1^2$

$+ y_2^2 = 1 + dx_2^2 y_2^2$

$_1x_2y_1y_2$ can't be ± 1.

eps in proof:

$_2y_1y_2)^2 = 1$ then

uation implies

$x_1x_2y_1y_2y_1)^2 =$

$x_2 + y_2)^2$.

e that d is a square.

not a square! Q.E.D.

"Doesn't this contradict standard structure theorems?"

e.g. "Every affine algebraic group is linear."

e.g. "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma–Lenstra)

The way out: Don't confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, co

Choose

Choose

this is n

Use x^2

ators are 0?"

n't!

$dx_1^2 y_1^2$

$- dx_2^2 y_2^2$

n't be ± 1.

of:

1 then

plies

$)^2 =$

s a square.

are! Q.E.D.

"Doesn't this contradict standard structure theorems?"

e.g. "Every affine algebraic group is linear."

e.g. "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma–Lenstra)

The way out: Don't confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative

Choose prime $q =$

Choose $d = 1216$

this is non-square

Use $x^2 + y^2 = 1 +$

0?”

.

D.

“Doesn’t this contradict standard structure theorems?”

e.g. “Every affine algebraic group is linear.”

e.g. “Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two.” (1995 Bosma–Lenstra)

The way out: Don’t confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$
Choose $d = 121665/121666$
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

"Doesn't this contradict standard structure theorems?"

e.g. "Every affine algebraic group is linear."

e.g. "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma–Lenstra)

The way out: Don't confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

"Doesn't this contradict standard structure theorems?"

e.g. "Every affine algebraic group is linear."

e.g. "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma–Lenstra)

The way out: Don't confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk
will switch to square q.

"Doesn't this contradict standard structure theorems?"

e.g. "Every affine algebraic group is linear."

e.g. "Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two." (1995 Bosma–Lenstra)

The way out: Don't confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk will switch to square q.

Disadvantage:
Maybe attacker can exploit nontrivial subfield of $\mathbf{F}_q$.

“Doesn’t this contradict standard structure theorems?”

e.g. “Every affine algebraic group is linear.”

e.g. “Theorem 1. The smallest cardinality of a complete system of addition laws on E equals two.” (1995 Bosma–Lenstra)

The way out: Don’t confuse geometry with arithmetic.
The Edwards addition law is complete for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk
will switch to square q.

Disadvantage:
Maybe attacker can exploit
nontrivial subfield of $\mathbf{F}_q$.

Advantage:
Will speed up scalar mult.

t this contradict
l structure theorems?"

ery affine algebraic group
"

heorem 1. The smallest
ty of a complete system
on laws on E equals
1995 Bosma–Lenstra)

out: Don't confuse
y with arithmetic.
vards addition law is
e for $\mathbf{F}_q$, not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk
will switch to square q.

Disadvantage:
Maybe attacker can exploit
nontrivial subfield of $\mathbf{F}_q$.

Advantage:
Will speed up scalar mult.

A class g

Fix prim
e.g. $p =$

Define C
$\delta t(t - 1$
over $\mathbf{F}_p$
with spe

Define J
surface c
$\delta t(t - 1$
$- ($
mod t^2
in variab

tradict
theorems?"

algebraic group

The smallest
mplete system
n E equals
na–Lenstra)

n't confuse
thmetic.
tion law is
not $\mathbf{F}_q(\sqrt{d})$.

Safe, conservative crypto:
Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk
will switch to square q.

Disadvantage:
Maybe attacker can exploit
nontrivial subfield of $\mathbf{F}_q$.

Advantage:
Will speed up scalar mult.

A class group of a

Fix prime $p \in 3 +$
e.g. $p = 2^{127} - 30$

Define C as the cu
$\delta t(t-1)(t-10)($
over $\mathbf{F}_p$ where $\delta =$
with specified poir

Define J as "Jac C
surface defined by
$\delta t(t-1)(t-10)($
$- (v_1 t + v_0)^2$
mod $t^2 + u_1 t + u_0$
in variables $(u_0, u_1$

?"

group

est

stem

s

n)

e

s

/).

Safe, conservative crypto:

Choose prime $q = 2^{255} - 19$.

Choose $d = 121665/121666$;

this is non-square in $\mathbf{F}_q$.

Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk

will switch to square q.

Disadvantage:

Maybe attacker can exploit

nontrivial subfield of $\mathbf{F}_q$.

Advantage:

Will speed up scalar mult.

<u>A class group of a quadratic</u>

Fix prime $p \in 3 + 4\mathbf{Z}$ with p

e.g. $p = 2^{127} - 309$.

Define C as the curve $y^2 =$

$\delta t(t-1)(t-10)(t-5/8)(t$

over $\mathbf{F}_p$ where $\delta = -2/3^5 5^4$

with specified point ∞.

Define J as "Jac C":

surface defined by equation

$\delta t(t-1)(t-10)(t-5/8)(t$

$\quad - (v_1 t + v_0)^2$

mod $t^2 + u_1 t + u_0 = 0$

in variables (u_0, u_1, v_0, v_1).

Safe, conservative crypto:

Choose prime $q = 2^{255} - 19$.
Choose $d = 121665/121666$;
this is non-square in $\mathbf{F}_q$.
Use $x^2 + y^2 = 1 + dx^2y^2$.

Rest of this talk
will switch to square q.

Disadvantage:
Maybe attacker can exploit
nontrivial subfield of $\mathbf{F}_q$.

Advantage:
Will speed up scalar mult.

A class group of a quadratic field

Fix prime $p \in 3 + 4\mathbf{Z}$ with $p \geq 19$.
e.g. $p = 2^{127} - 309$.

Define C as the curve $y^2 = \delta t(t-1)(t-10)(t-5/8)(t-25)$
over $\mathbf{F}_p$ where $\delta = -2/3^5 5^4$,
with specified point ∞.

Define J as "$\mathrm{Jac}\, C$":
surface defined by equation

$$\delta t(t-1)(t-10)(t-5/8)(t-25) - (v_1 t + v_0)^2$$

mod $t^2 + u_1 t + u_0 = 0$
in variables (u_0, u_1, v_0, v_1).

nservative crypto:
prime $q = 2^{255} - 19$.
$d = 121665/121666$;
on-square in $\mathbf{F}_q$.
$+\, y^2 = 1 + dx^2y^2$.

this talk
ch to square q.

ntage:
ttacker can exploit
al subfield of $\mathbf{F}_q$.

ge:
ed up scalar mult.

A class group of a quadratic field

Fix prime $p \in 3 + 4\mathbf{Z}$ with $p \geq 19$.
e.g. $p = 2^{127} - 309$.

Define C as the curve $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
over $\mathbf{F}_p$ where $\delta = -2/3^5 5^4$,
with specified point ∞.

Define J as “Jac C”:
surface defined by equation

$$\delta t(t-1)(t-10)(t-5/8)(t-25) - (v_1 t + v_0)^2$$

mod $t^2 + u_1 t + u_0 = 0$
in variables (u_0, u_1, v_0, v_1).

View J p
handling
Define ra
$0, -, +$ r
J is an “

Rational
taking ∞
J is a “C

J is initi
maps un
any C-A

crypto:
$2^{255} - 19$.
$55/121666$;
in $\mathbf{F}_q$.
$- dx^2y^2$.

are q.

an exploit
of $\mathbf{F}_q$.

ar mult.

A class group of a quadratic field

Fix prime $p \in 3 + 4\mathbf{Z}$ with $p \geq 19$.
e.g. $p = 2^{127} - 309$.

Define C as the curve $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
over $\mathbf{F}_p$ where $\delta = -2/3^5 5^4$,
with specified point ∞.

Define J as "Jac C":
surface defined by equation
$$\delta t(t-1)(t-10)(t-5/8)(t-25) - (v_1 t + v_0)^2$$
mod $t^2 + u_1 t + u_0 = 0$
in variables (u_0, u_1, v_0, v_1).

View J projectively
handling ∞ carefu
Define rational op
$0, -, +$ making J
J is an "Abelian v

Rationally map C
taking ∞ to 0.
J is a "C-Abelian

J is initial:
maps uniquely to
any C-Abelian var

A class group of a quadratic field

Fix prime $p \in 3 + 4\mathbf{Z}$ with $p \geq 19$.
e.g. $p = 2^{127} - 309$.

Define C as the curve $y^2 = \delta t(t-1)(t-10)(t-5/8)(t-25)$ over $\mathbf{F}_p$ where $\delta = -2/3^5 5^4$, with specified point ∞.

Define J as "Jac C":
surface defined by equation

$$\delta t(t-1)(t-10)(t-5/8)(t-25) - (v_1 t + v_0)^2$$

mod $t^2 + u_1 t + u_0 = 0$
in variables (u_0, u_1, v_0, v_1).

View J projectively,
handling ∞ carefully.
Define rational operations $0, -, +$ making J a group.
J is an "Abelian variety".

Rationally map C to J,
taking ∞ to 0.
J is a "C-Abelian variety".

J is initial:
maps uniquely to
any C-Abelian variety.

A class group of a quadratic field

Fix prime $p \in 3 + 4\mathbf{Z}$ with $p \geq 19$.
e.g. $p = 2^{127} - 309$.

Define C as the curve $y^2 = \delta t(t-1)(t-10)(t-5/8)(t-25)$ over $\mathbf{F}_p$ where $\delta = -2/3^5 5^4$, with specified point ∞.

Define J as "Jac C": surface defined by equation

$$\delta t(t-1)(t-10)(t-5/8)(t-25) - (v_1 t + v_0)^2$$

mod $t^2 + u_1 t + u_0 = 0$
in variables (u_0, u_1, v_0, v_1).

View J projectively, handling ∞ carefully.
Define rational operations $0, -, +$ making J a group.
J is an "Abelian variety".

Rationally map C to J, taking ∞ to 0.
J is a "C-Abelian variety".

J is initial:
maps uniquely to any C-Abelian variety.

group of a quadratic field

e $p \in 3 + 4\mathbf{Z}$ with $p \geq 19$.
$2^{127} - 309$.

C as the curve $y^2 =$
$)(t - 10)(t - 5/8)(t - 25)$
where $\delta = -2/3^5 5^4$,
ecified point ∞.

J as "Jac C":
defined by equation
$)(t - 10)(t - 5/8)(t - 25)$
$(v_1 t + v_0)^2$
$+ u_1 t + u_0 = 0$
bles (u_0, u_1, v_0, v_1).

View J projectively,
handling ∞ carefully.
Define rational operations
$0, -, +$ making J a group.
J is an "Abelian variety".

Rationally map C to J,
taking ∞ to 0.
J is a "C-Abelian variety".

J is initial:
maps uniquely to
any C-Abelian variety.

Kummer

J has co
supporti
of $P_5 =$
given P_3
(1986 C
2006 Ga

Linear co
$1, u_0, u_1$
$x = 16u$
$5u_1^2 - 1$
$175u_1 -$
wrong fo
always u

quadratic field

4**Z** with $p \geq 19$.
09.

urve $y^2 =$
$t - 5/8)(t - 25)$
$= -2/3^5 5^4$,
nt ∞.

C":
equation
$t - 5/8)(t - 25)$
2

$_0 = 0$
$_1, v_0, v_1)$.

View J projectively,
handling ∞ carefully.
Define rational operations
$0, -, +$ making J a group.
J is an "Abelian variety".

Rationally map C to J,
taking ∞ to 0.
J is a "C-Abelian variety".

J is initial:
maps uniquely to
any C-Abelian variety.

Kummer coordinat

J has coordinates
supporting very fa
of $P_5 = P_3 + P_2$ a
given P_3 and P_2 a
(1986 Chudnovsky
2006 Gaudry)

Linear combinatio
$1, u_0, u_1, u_0^2, u_0 u_1,$
$x = 16 u_0 u_1^2 - 8 u_0^2$
$5 u_1^2 - 1215000 v_0 v$
$175 u_1 - 1250$, etc.
wrong formulas in
always use a comp

field

$\geq 19.$

$t - 25)$

,

$t - 25)$

View J projectively,
handling ∞ carefully.
Define rational operations
$0, -, +$ making J a group.
J is an "Abelian variety".

Rationally map C to J,
taking ∞ to 0.
J is a "C-Abelian variety".

J is initial:
maps uniquely to
any C-Abelian variety.

Kummer coordinates

J has coordinates $(x : y : z$
supporting very fast comput
of $P_5 = P_3 + P_2$ and $P_4 = 2$
given P_3 and P_2 and $P_1 = F$
(1986 Chudnovsky–Chudnov
2006 Gaudry)

Linear combinations of
$1, u_0, u_1, u_0^2, u_0 u_1, u_1^2, u_0 u_1^2, v$
$x = 16 u_0 u_1^2 - 8 u_0^2 + 573 u_0$
$5 u_1^2 - 1215000 v_0 v_1 + 2460 u$
$175 u_1 - 1250$, etc. Warning:
wrong formulas in literature;
always use a computer!

View J projectively, handling ∞ carefully. Define rational operations $0, -, +$ making J a group. J is an "Abelian variety".

Rationally map C to J, taking ∞ to 0. J is a "C-Abelian variety".

J is initial: maps uniquely to any C-Abelian variety.

Kummer coordinates

J has coordinates $(x : y : z : t)$ supporting very fast computation of $P_5 = P_3 + P_2$ and $P_4 = 2P_2$ given P_3 and P_2 and $P_1 = P_3 - P_2$. (1986 Chudnovsky–Chudnovsky, 2006 Gaudry)

Linear combinations of $1, u_0, u_1, u_0^2, u_0u_1, u_1^2, u_0u_1^2, v_0v_1$: $x = 16u_0u_1^2 - 8u_0^2 + 573u_0u_1 - 5u_1^2 - 1215000v_0v_1 + 2460u_0 - 175u_1 - 1250$, etc. Warning: many wrong formulas in literature; always use a computer!

projectively,
; ∞ carefully.
ational operations
making J a group.
"Abelian variety".

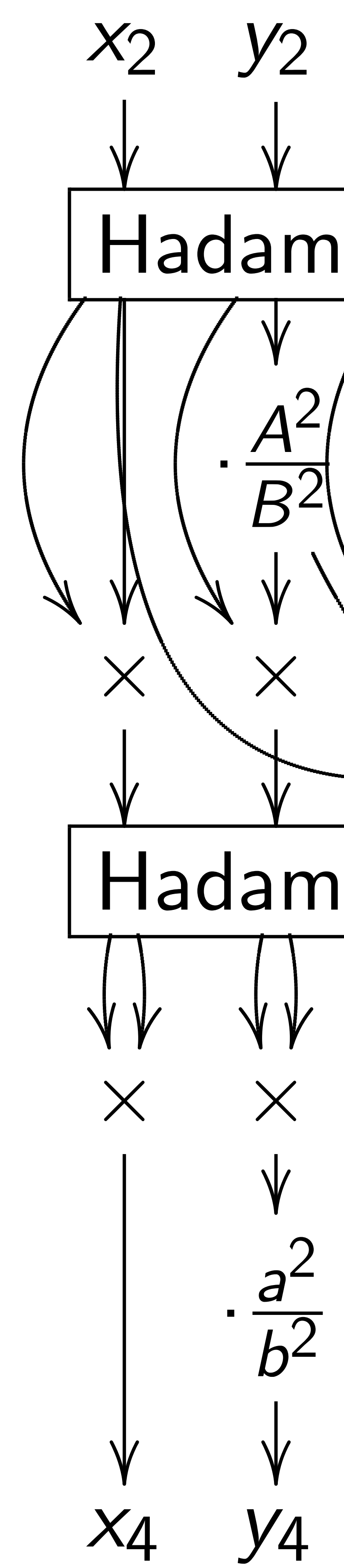
ly map C to J,
o to 0.
C-Abelian variety".

al:
niquely to
belian variety.

Kummer coordinates

J has coordinates $(x : y : z : t)$ supporting very fast computation of $P_5 = P_3 + P_2$ and $P_4 = 2P_2$ given P_3 and P_2 and $P_1 = P_3 - P_2$. (1986 Chudnovsky–Chudnovsky, 2006 Gaudry)

Linear combinations of $1, u_0, u_1, u_0^2, u_0 u_1, u_1^2, u_0 u_1^2, v_0 v_1$: $x = 16u_0 u_1^2 - 8u_0^2 + 573u_0 u_1 - 5u_1^2 - 1215000v_0 v_1 + 2460u_0 - 175u_1 - 1250$, etc. Warning: many wrong formulas in literature; always use a computer!



y,
lly.
erations
a group.
ariety".

to J,

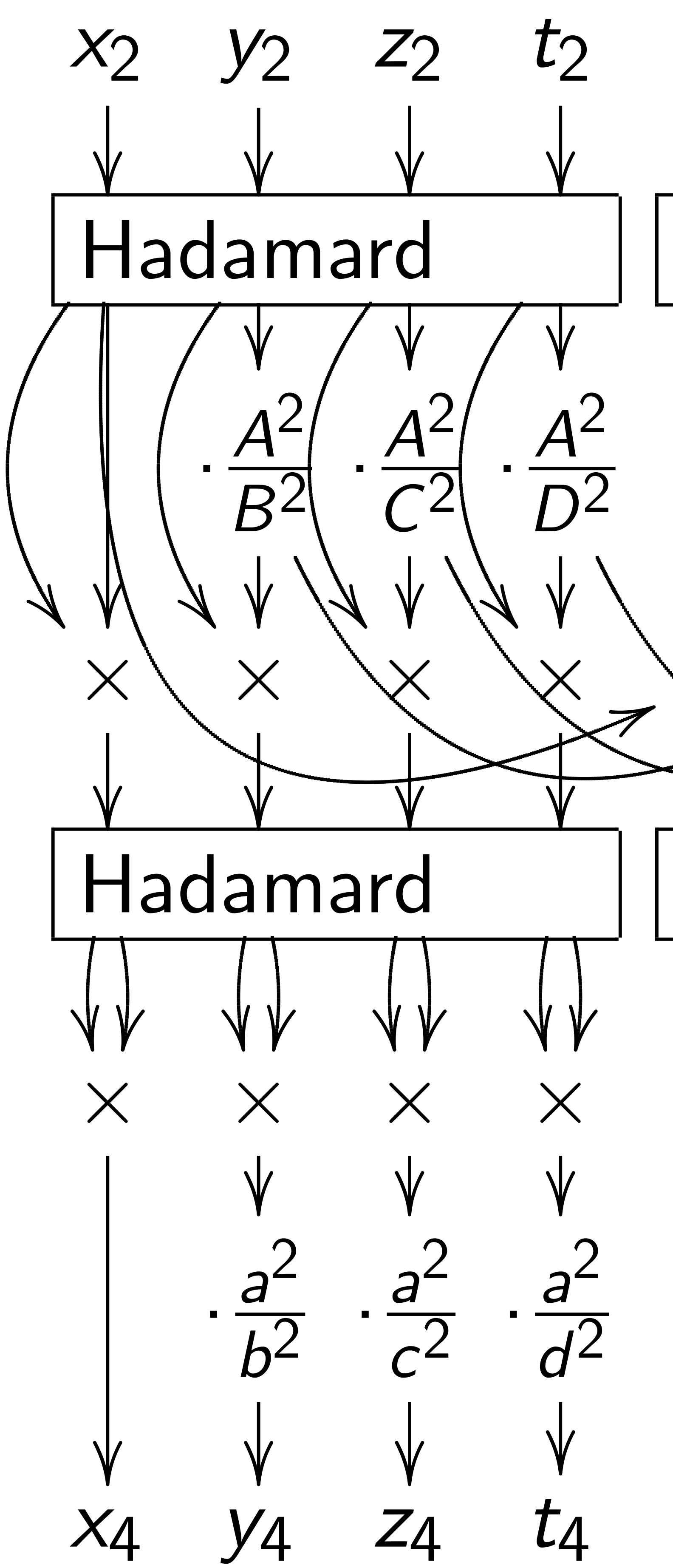
variety".

iety.

Kummer coordinates

J has coordinates $(x : y : z : t)$ supporting very fast computation of $P_5 = P_3 + P_2$ and $P_4 = 2P_2$ given P_3 and P_2 and $P_1 = P_3 - P_2$. (1986 Chudnovsky–Chudnovsky, 2006 Gaudry)

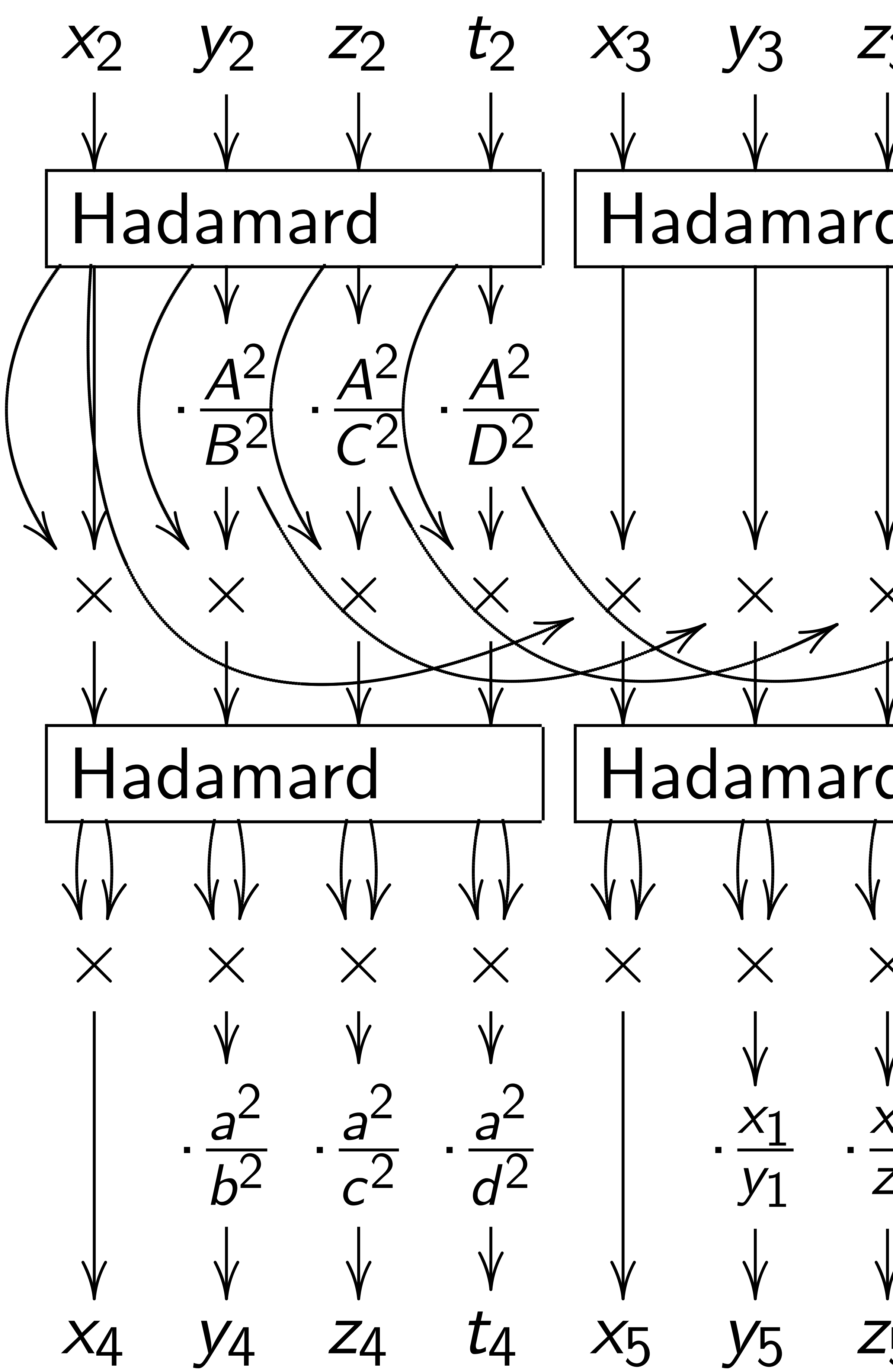
Linear combinations of $1, u_0, u_1, u_0^2, u_0 u_1, u_1^2, u_0 u_1^2, v_0 v_1$: $x = 16 u_0 u_1^2 - 8 u_0^2 + 573 u_0 u_1 - 5 u_1^2 - 1215000 v_0 v_1 + 2460 u_0 - 175 u_1 - 1250$, etc. Warning: many wrong formulas in literature; always use a computer!



Kummer coordinates

J has coordinates $(x : y : z : t)$ supporting very fast computation of $P_5 = P_3 + P_2$ and $P_4 = 2P_2$ given P_3 and P_2 and $P_1 = P_3 - P_2$. (1986 Chudnovsky–Chudnovsky, 2006 Gaudry)

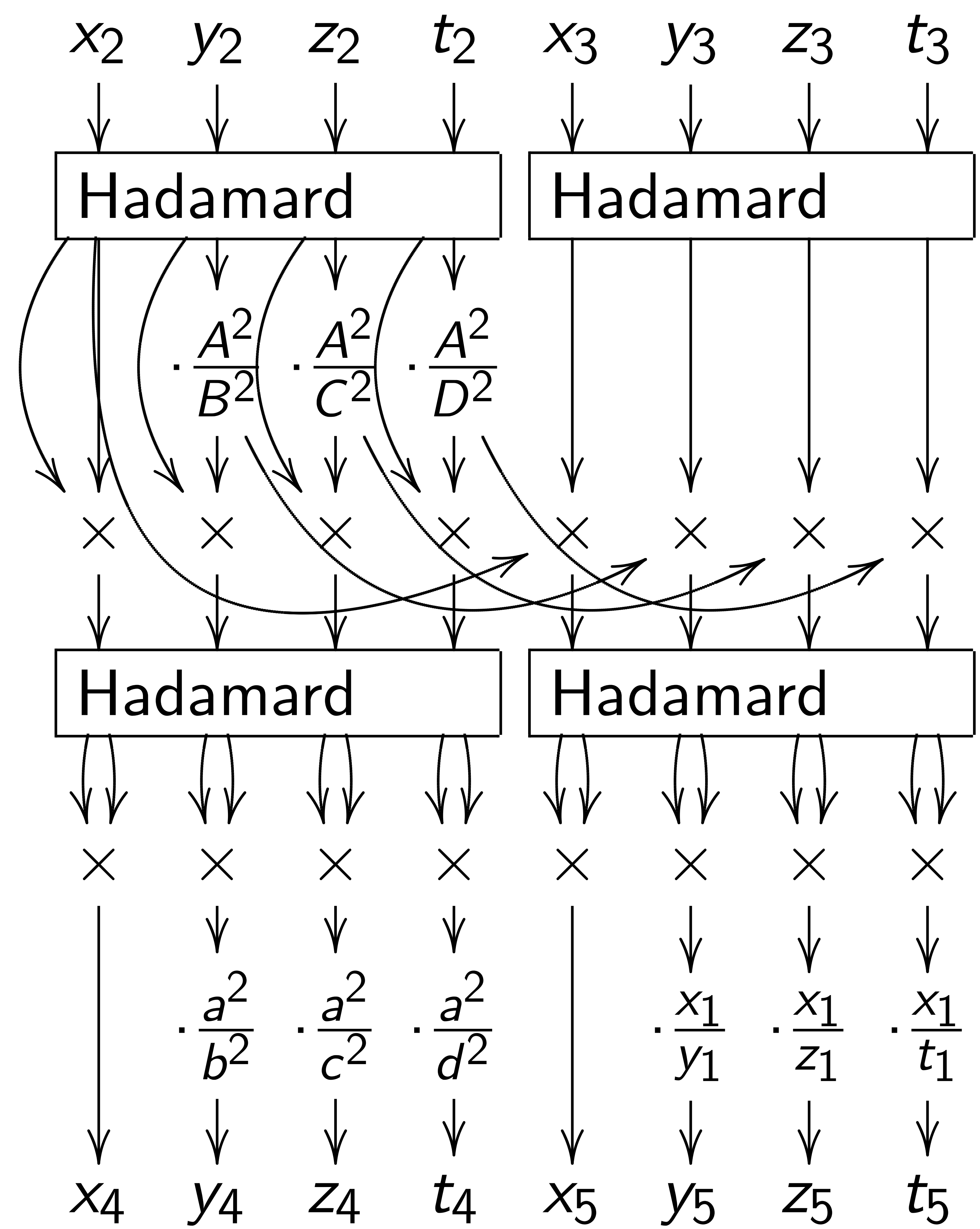
Linear combinations of $1, u_0, u_1, u_0^2, u_0u_1, u_1^2, u_0u_1^2, v_0v_1$: $x = 16u_0u_1^2 - 8u_0^2 + 573u_0u_1 - 5u_1^2 - 1215000v_0v_1 + 2460u_0 - 175u_1 - 1250$, etc. Warning: many wrong formulas in literature; always use a computer!



Kummer coordinates

J has coordinates $(x : y : z : t)$ supporting very fast computation of $P_5 = P_3 + P_2$ and $P_4 = 2P_2$ given P_3 and P_2 and $P_1 = P_3 - P_2$. (1986 Chudnovsky–Chudnovsky, 2006 Gaudry)

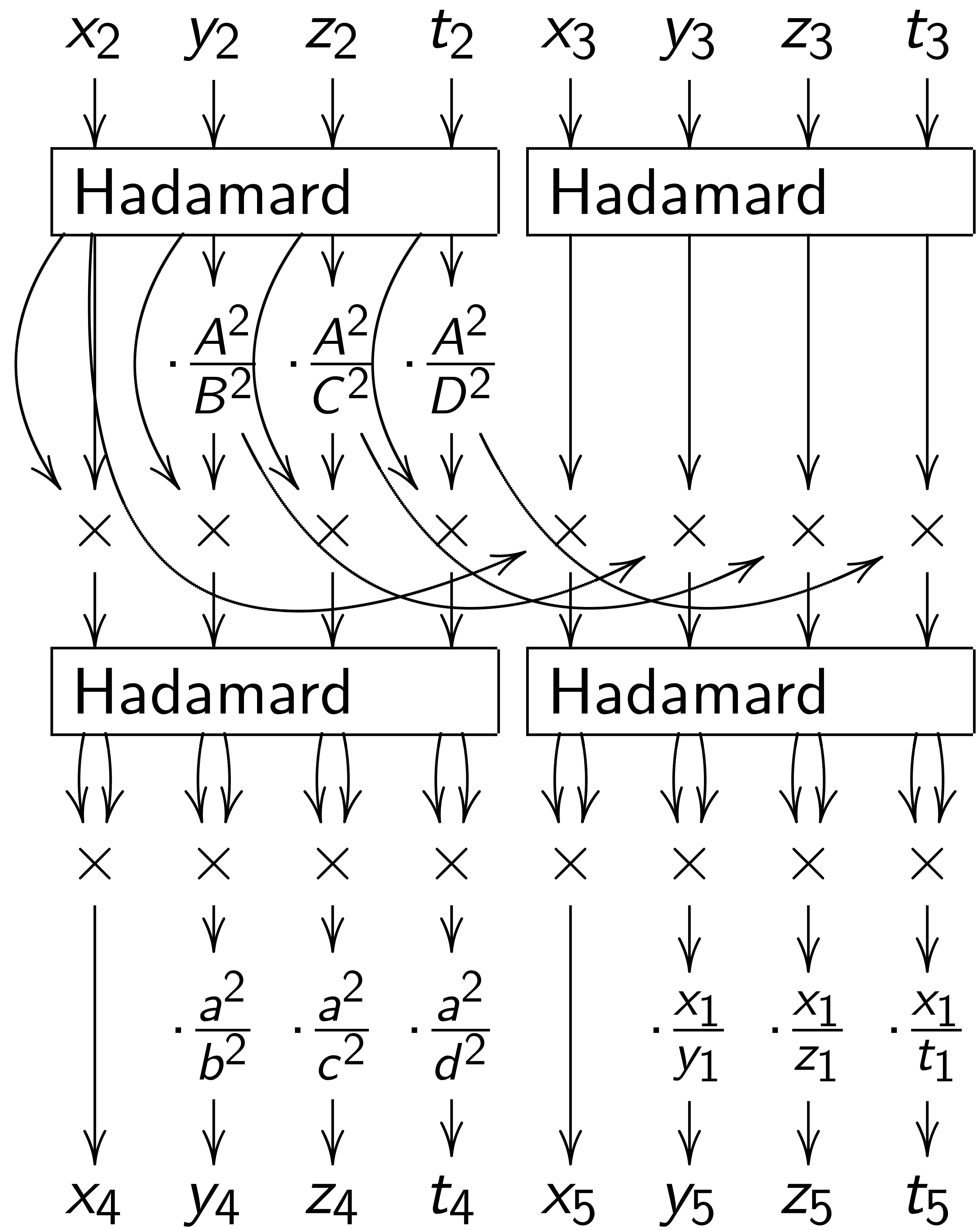
Linear combinations of $1, u_0, u_1, u_0^2, u_0u_1, u_1^2, u_0u_1^2, v_0v_1$: $x = 16u_0u_1^2 - 8u_0^2 + 573u_0u_1 - 5u_1^2 - 1215000v_0v_1 + 2460u_0 - 175u_1 - 1250$, etc. Warning: many wrong formulas in literature; always use a computer!



r coordinates

oordinates $(x : y : z : t)$
ng very fast computation
$P_3 + P_2$ and $P_4 = 2P_2$
, and P_2 and $P_1 = P_3 - P_2$.
hudnovsky–Chudnovsky,
udry)

ombinations of
$, u_0^2, u_0 u_1, u_1^2, u_0 u_1^2, v_0 v_1$:
$u_0 u_1^2 - 8u_0^2 + 573 u_0 u_1 -$
$215000 v_0 v_1 + 2460 u_0 -$
1250, etc. Warning: many
ormulas in literature;
use a computer!



These co
induce c
so they c
rational
but they
rational

Coefficie
are all sr
$(a^2 : b^2$
$= (20$
$(A^2 : B^2$
$= (81$

tes

$(x : y : z : t)$

st computation

nd $P_4 = 2P_2$

nd $P_1 = P_3 - P_2$.

y–Chudnovsky,

ns of

$u_1^2, u_0 u_1^2, v_0 v_1$:

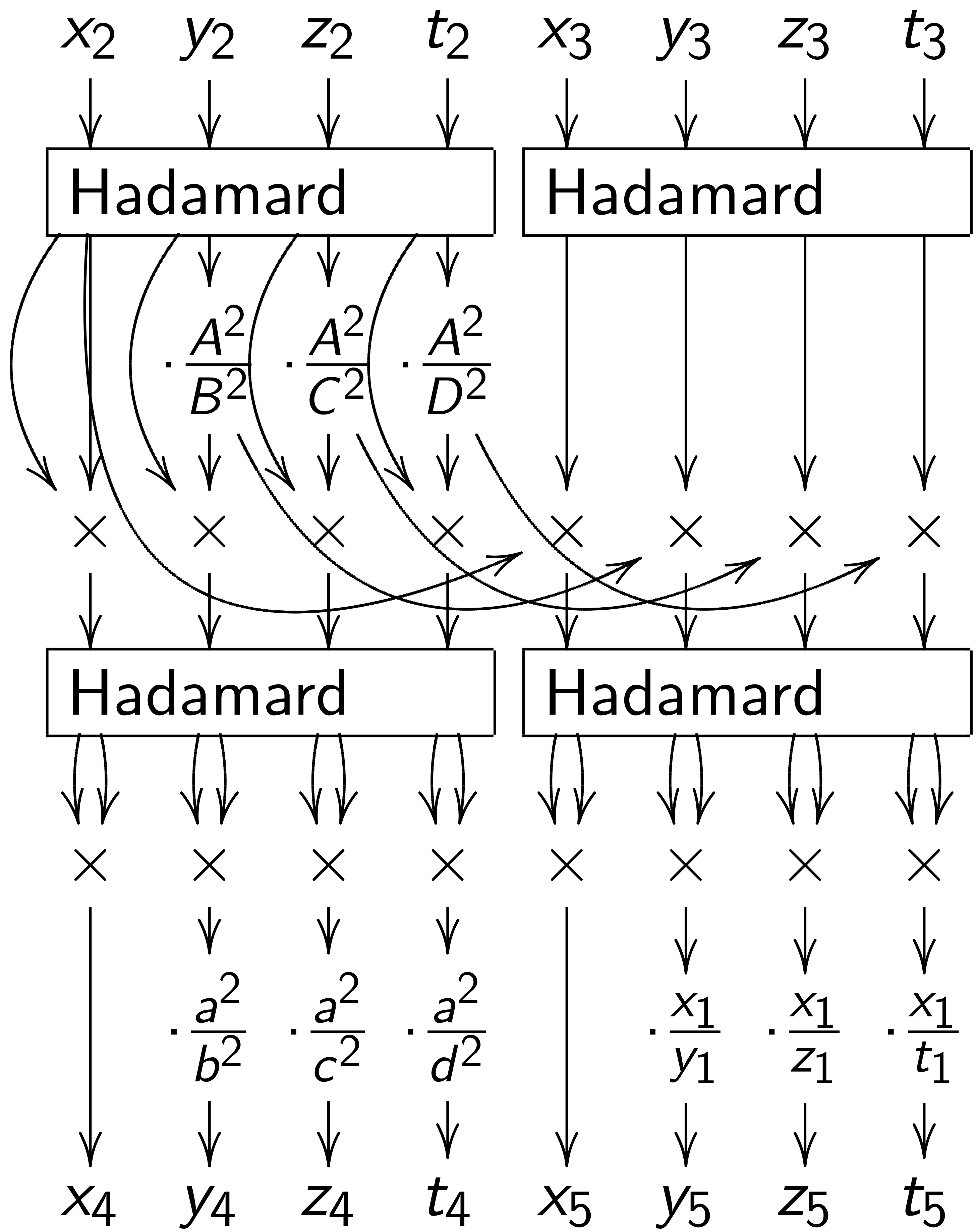
$_0^2 + 573 u_0 u_1 -$

$v_1 + 2460 u_0 -$

Warning: many

literature;

uter!



These coordinates

induce coordinates

so they don't supp

rational group ope

but they do suppo

rational scalar mul

Coefficients in con

are all small, savin

$(a^2 : b^2 : c^2 : d^2)$

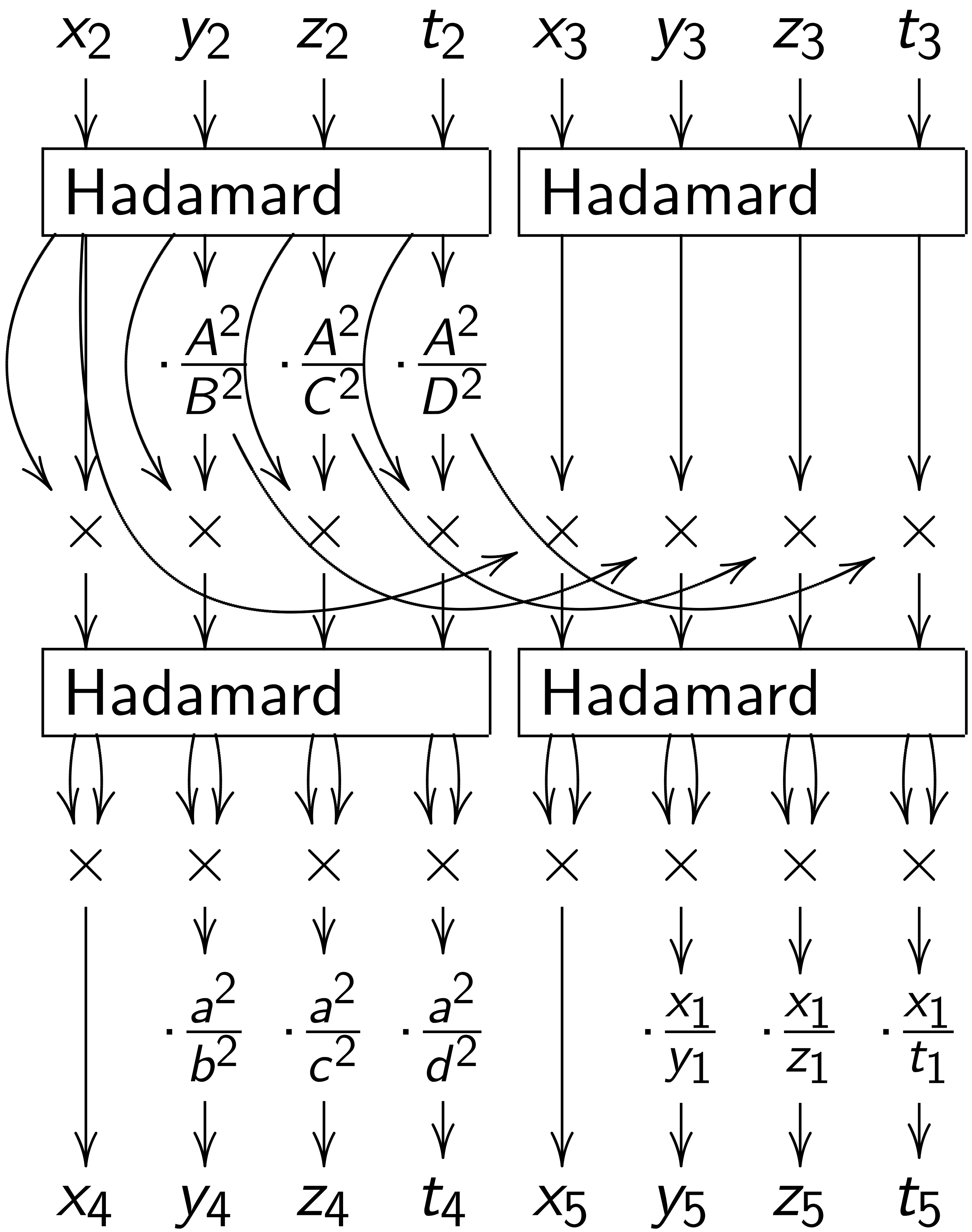
$= (20 : 1 : 20 :$

$(A^2 : B^2 : C^2 : D^2$

$= (81 : -39 : -$

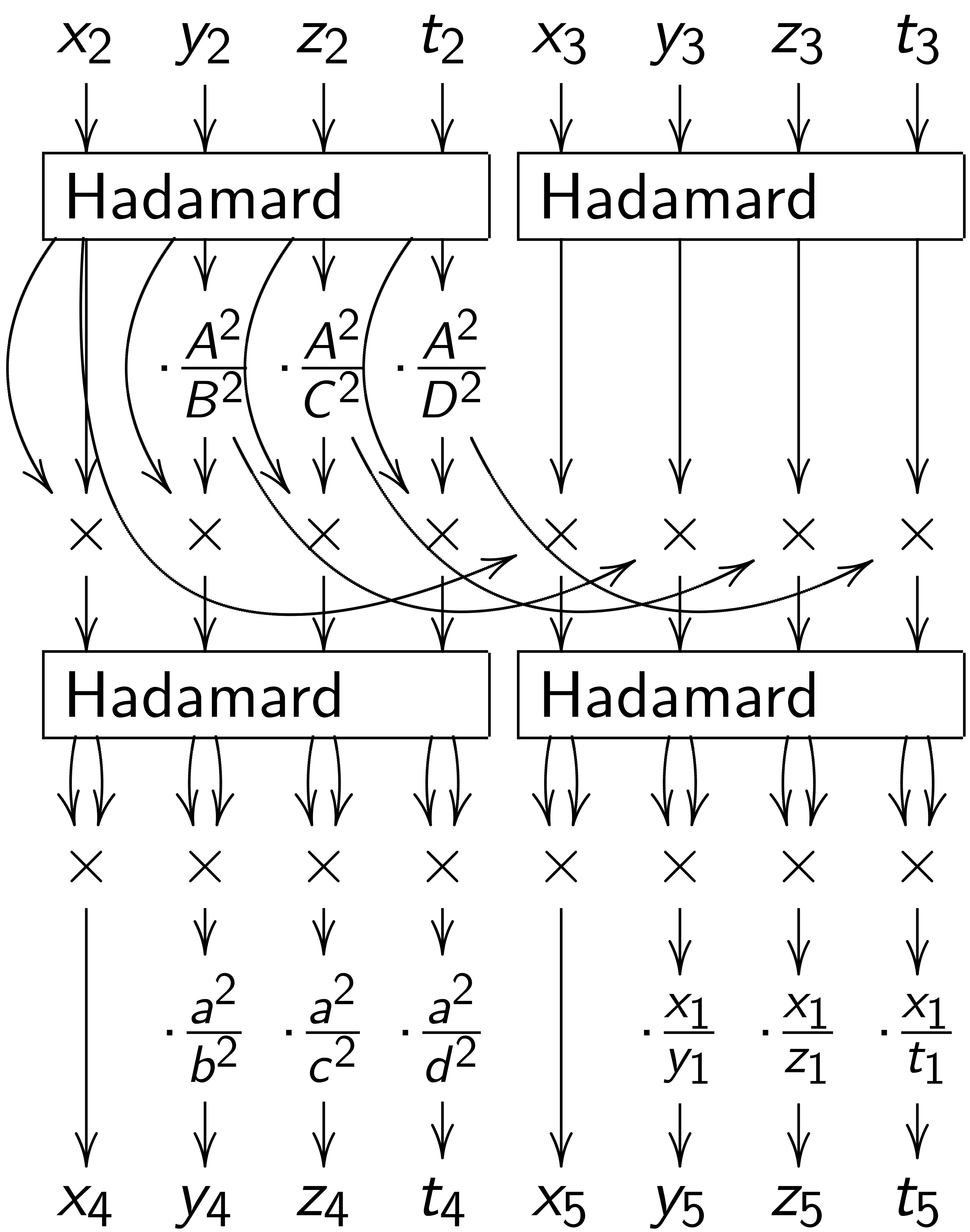
: t)
ation
$2P_2$
$P_3 - P_2$.
vsky,

$v_0 v_1$:
u_1 −
u_0 −
many
;



These coordinates
induce coordinates on $J/\{\pm$
so they don't support
rational group operations,
but they do support
rational scalar multiplication

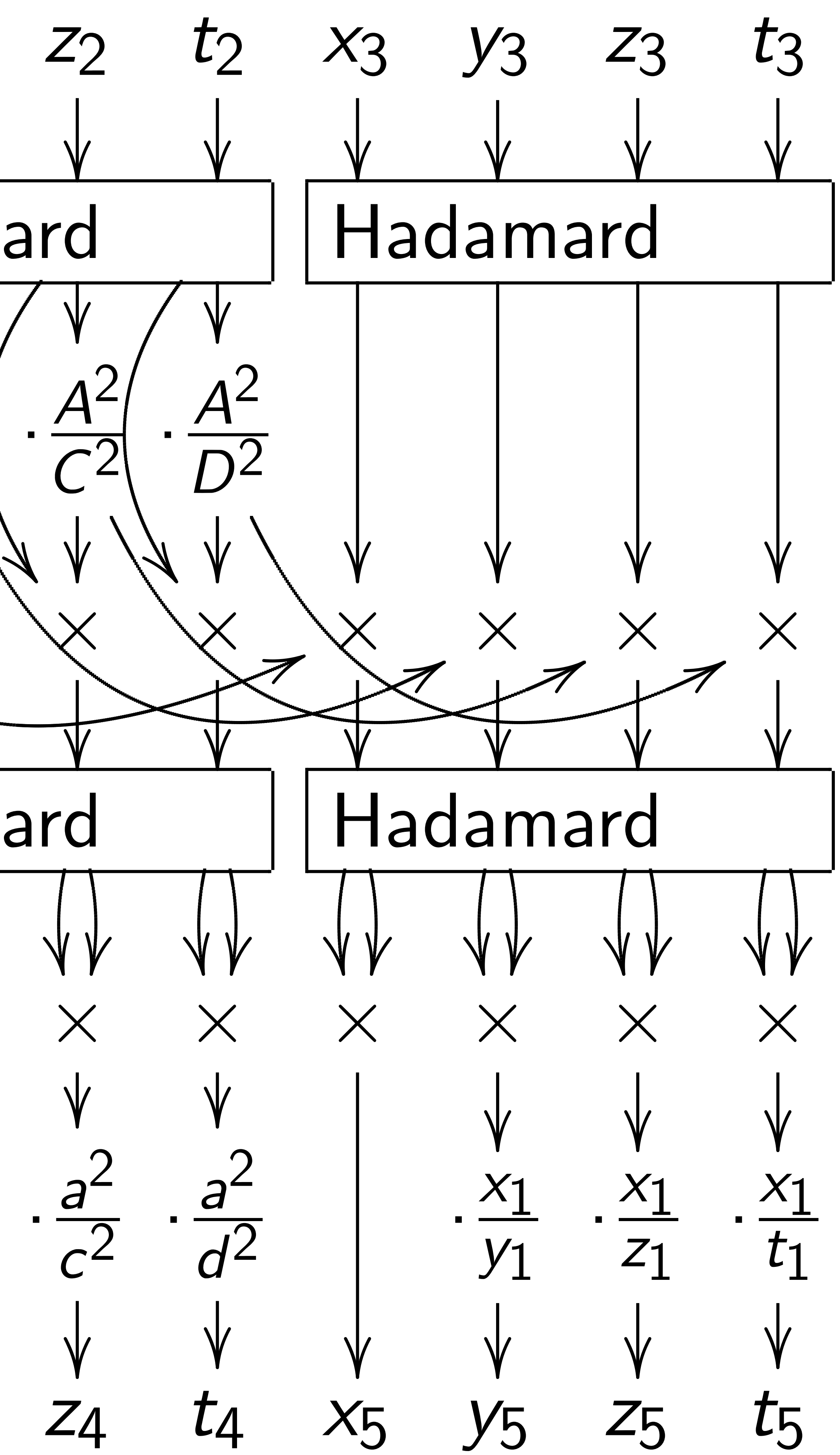
Coefficients in computation
are all small, saving time:
$(a^2 : b^2 : c^2 : d^2)$
$= (20 : 1 : 20 : 40)$,
$(A^2 : B^2 : C^2 : D^2)$
$= (81 : -39 : -1 : 39)$.



These coordinates induce coordinates on $J/\{\pm 1\}$, so they don't support rational group operations, but they do support rational scalar multiplication.

Coefficients in computation are all small, saving time:

$(a^2 : b^2 : c^2 : d^2)$
$\quad = (20 : 1 : 20 : 40)$,
$(A^2 : B^2 : C^2 : D^2)$
$\quad = (81 : -39 : -1 : 39)$.

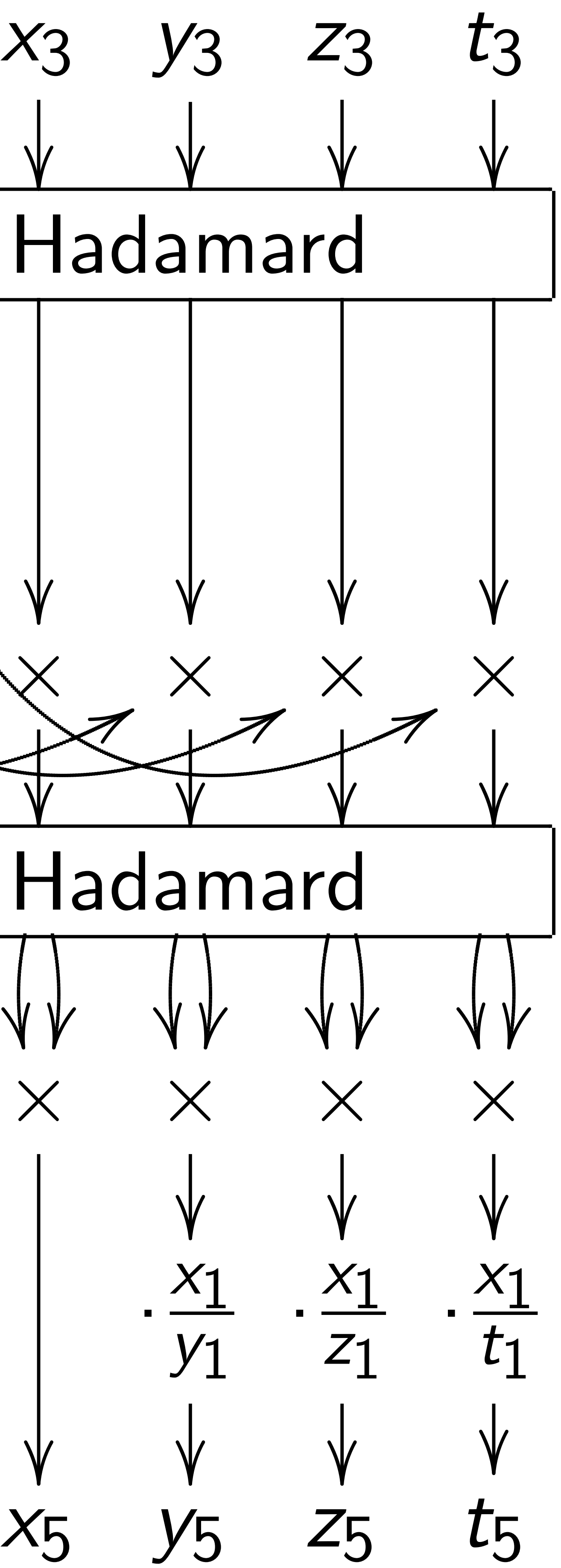


These coordinates
induce coordinates on $J/\{\pm 1\}$,
so they don't support
rational group operations,
but they do support
rational scalar multiplication.

Coefficients in computation
are all small, saving time:
$(a^2 : b^2 : c^2 : d^2)$
$= (20 : 1 : 20 : 40)$,
$(A^2 : B^2 : C^2 : D^2)$
$= (81 : -39 : -1 : 39)$.

A Kumm

If $y^2 =$
$\delta t(t - 1$
then
$(y(z+2$
$(z$ -
where z



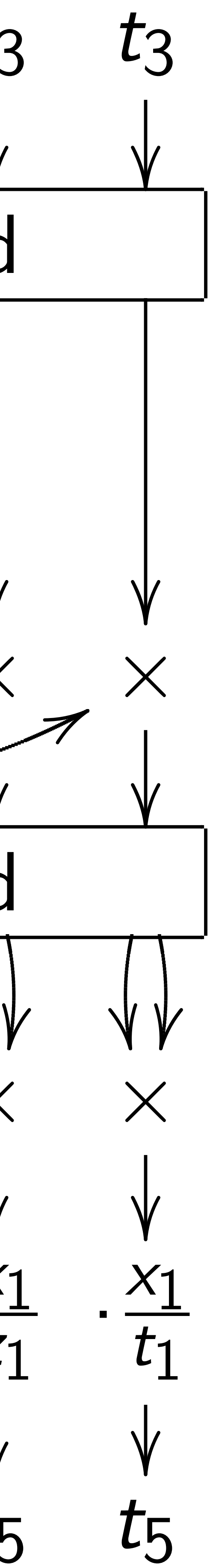
These coordinates
induce coordinates on $J/\{\pm 1\}$,
so they don't support
rational group operations,
but they do support
rational scalar multiplication.

Coefficients in computation
are all small, saving time:

$(a^2 : b^2 : c^2 : d^2)$
$\quad = (20 : 1 : 20 : 40)$,
$(A^2 : B^2 : C^2 : D^2)$
$\quad = (81 : -39 : -1 : 39)$.

A Kummer-friendl

If $y^2 =$
$\delta t(t-1)(t-10)($
then
$(y(z+2)^3)^2 = (z$
$\quad (z-1/2)(z+$
where $z = (5-2t$



These coordinates induce coordinates on $J/\{\pm 1\}$, so they don't support rational group operations, but they do support rational scalar multiplication.

Coefficients in computation are all small, saving time:

$(a^2 : b^2 : c^2 : d^2)$
$\quad = (20 : 1 : 20 : 40)$,
$(A^2 : B^2 : C^2 : D^2)$
$\quad = (81 : -39 : -1 : 39)$.

A Kummer-friendly Scholten

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t$
then
$(y(z+2)^3)^2 = (z-1)(z+1)$
$\quad (z-1/2)(z+3/2)(z-$
where $z = (5-2t)/(5+t)$.

These coordinates induce coordinates on $J/\{\pm 1\}$, so they don't support rational group operations, but they do support rational scalar multiplication.

Coefficients in computation are all small, saving time:

$$(a^2 : b^2 : c^2 : d^2) = (20 : 1 : 20 : 40),$$

$$(A^2 : B^2 : C^2 : D^2) = (81 : -39 : -1 : 39).$$

A Kummer-friendly Scholten curve

If $y^2 = \delta t(t-1)(t-10)(t-5/8)(t-25)$ then

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

where $z = (5-2t)/(5+t)$.

These coordinates induce coordinates on $J/\{\pm 1\}$, so they don't support rational group operations, but they do support rational scalar multiplication.

Coefficients in computation are all small, saving time:

$$(a^2 : b^2 : c^2 : d^2) = (20 : 1 : 20 : 40),$$

$$(A^2 : B^2 : C^2 : D^2) = (81 : -39 : -1 : 39).$$

A Kummer-friendly Scholten curve

If $y^2 =$

$\delta t(t-1)(t-10)(t-5/8)(t-25)$

then

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

where $z = (5-2t)/(5+t)$.

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

These coordinates induce coordinates on $J/\{\pm 1\}$, so they don't support rational group operations, but they do support rational scalar multiplication.

Coefficients in computation are all small, saving time:

$$(a^2 : b^2 : c^2 : d^2) = (20 : 1 : 20 : 40),$$

$$(A^2 : B^2 : C^2 : D^2) = (81 : -39 : -1 : 39).$$

A Kummer-friendly Scholten curve

If $y^2 = \delta t(t-1)(t-10)(t-5/8)(t-25)$ then

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

where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$ where $x = (1+iz)^2/(1-iz)^2$.

oordinates

oordinates on $J/\{\pm 1\}$,

don't support

group operations,

do support

scalar multiplication.

ents in computation

mall, saving time:

$: c^2 : d^2)$

$0 : 1 : 20 : 40)$,

$: C^2 : D^2)$

$1 : -39 : -1 : 39)$.

A Kummer-friendly Scholten curve

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
then
$$(y(z+2)^3)^2 = (z-1)(z+1)(z+2)(z-1/2)(z+3/2)(z-2/3)$$
where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2$
$= rx^3 + sx^2 + \bar{s}x + \bar{r}$
where $x = (1+iz)^2/(1-iz)^2$.

Map $(x,$

to an Ed

by chain

s on $J/\{\pm 1\}$,
port
erations,
rt
ltiplication.

nputation
g time:

40),
)
−1 : 39).

A Kummer-friendly Scholten curve

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
then

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

where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2$
$= rx^3 + sx^2 + \bar{s}x + \bar{r}$
where $x = (1+iz)^2/(1-iz)^2$.

Map $(x, \omega y(z+2)$
to an Edwards cur
by chain of “2-isog

1},

.

A Kummer-friendly Scholten curve

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
then
$$(y(z+2)^3)^2 = (z-1)(z+1)(z+2)$$
$$(z-1/2)(z+3/2)(z-2/3)$$
where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2$
$= rx^3 + sx^2 + \bar{s}x + \bar{r}$
where $x = (1+iz)^2/(1-iz)^2$.

Map $(x, \omega y(z+2)^3/(1-iz$
to an Edwards curve E over
by chain of "2-isogenies".

A Kummer-friendly Scholten curve

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
then
$(y(z+2)^3)^2 = (z-1)(z+1)(z+2)$
$(z-1/2)(z+3/2)(z-2/3)$
where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2$
$= rx^3 + sx^2 + \bar{s}x + \bar{r}$
where $x = (1+iz)^2/(1-iz)^2$.

Map $(x, \omega y(z+2)^3/(1-iz)^3)$
to an Edwards curve E over $\mathbf{F}_{p^2}$
by chain of "2-isogenies".

A Kummer-friendly Scholten curve

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
then
$(y(z+2)^3)^2 = (z-1)(z+1)(z+2)$
$\quad (z-1/2)(z+3/2)(z-2/3)$
where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2$
$= rx^3 + sx^2 + \bar{s}x + \bar{r}$
where $x = (1+iz)^2/(1-iz)^2$.

Map $(x, \omega y(z+2)^3/(1-iz)^3)$
to an Edwards curve E over $\mathbf{F}_{p^2}$
by chain of "2-isogenies".

View two coordinates over $\mathbf{F}_{p^2}$
as four coordinates over $\mathbf{F}_p$;
view curve E as surface W.
Have now mapped C rationally
to this Abelian variety W.

A Kummer-friendly Scholten curve

If $y^2 =$
$\delta t(t-1)(t-10)(t-5/8)(t-25)$
then
$(y(z+2)^3)^2 = (z-1)(z+1)(z+2)$
$(z-1/2)(z+3/2)(z-2/3)$
where $z = (5-2t)/(5+t)$.

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

Then $(\omega y(z+2)^3/(1-iz)^3)^2$
$= rx^3 + sx^2 + \overline{s}x + \overline{r}$
where $x = (1+iz)^2/(1-iz)^2$.

Map $(x, \omega y(z+2)^3/(1-iz)^3)$
to an Edwards curve E over $\mathbf{F}_{p^2}$
by chain of "2-isogenies".

View two coordinates over $\mathbf{F}_{p^2}$
as four coordinates over $\mathbf{F}_p$;
view curve E as surface W.
Have now mapped C rationally
to this Abelian variety W.

Compute formulas for
the unique map $J \to W$
of C-Abelian varieties
and a "dual isogeny" $W \to J$.
Composition has small kernel.

ner-friendly Scholten curve

)$(t-10)(t-5/8)(t-25)$

$)^3)^2 = (z-1)(z+1)(z+2)$
$-1/2)(z+3/2)(z-2/3)$
$= (5-2t)/(5+t)$.

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

$y(z+2)^3/(1-iz)^3)^2$
$sx^2 + \bar{s}x + \bar{r}$
$= (1+iz)^2/(1-iz)^2$.

Map $(x, \omega y(z+2)^3/(1-iz)^3)$ to an Edwards curve E over $\mathbf{F}_{p^2}$ by chain of "2-isogenies".

View two coordinates over $\mathbf{F}_{p^2}$ as four coordinates over $\mathbf{F}_p$; view curve E as surface W. Have now mapped C rationally to this Abelian variety W.

Compute formulas for the unique map $J \to W$ of C-Abelian varieties and a "dual isogeny" $W \to J$. Composition has small kernel.

Cryptogr

Speed re
$a \mapsto aP$

Speed re
$a, P \mapsto a$
for Jaco
with sma

"Hyper-a
groups s
and sup
with sma
3 indepe
on 2 deg
but ever

y Scholten curve

$t - 5/8)(t - 25)$

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

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

$)/(5 + t)$.

$]/(i^2 + 1)$;

$3 + 56i$;

$= \sqrt{-384}$.

$/(1 - iz)^3)^2$

$+ \bar{r}$

$)^2/(1 - iz)^2$.

Map $(x, \omega y(z + 2)^3/(1 - iz)^3)$ to an Edwards curve E over $\mathbf{F}_{p^2}$ by chain of "2-isogenies".

View two coordinates over $\mathbf{F}_{p^2}$ as four coordinates over $\mathbf{F}_p$; view curve E as surface W. Have now mapped C rationally to this Abelian variety W.

Compute formulas for the unique map $J \to W$ of C-Abelian varieties and a "dual isogeny" $W \to J$. Composition has small kernel.

Cryptographic con

Speed records for
$a \mapsto aP$ use Edwa

Speed records for
$a, P \mapsto aP$ use Ku
for Jacobians of g
with small Kumme

"Hyper-and-ellipti
groups support Ed
and support Kum
with small coeffici
3 independent con
on 2 degrees of fr
but everything lift

n curve

t − 25)

(z+2)
- 2/3)

;

.

3)²

z)².

Map $(x, \omega y(z+2)^3/(1-iz)^3)$ to an Edwards curve E over $\mathbf{F}_{p^2}$ by chain of "2-isogenies".

View two coordinates over $\mathbf{F}_{p^2}$ as four coordinates over $\mathbf{F}_p$; view curve E as surface W. Have now mapped C rationally to this Abelian variety W.

Compute formulas for the unique map $J \to W$ of C-Abelian varieties and a "dual isogeny" $W \to J$. Composition has small kernel.

Cryptographic consequences

Speed records for high-secur
$a \mapsto aP$ use Edwards coords

Speed records for high-secur
$a, P \mapsto aP$ use Kummer coo
for Jacobians of genus-2 cur
with small Kummer coefficie

"Hyper-and-elliptic-curve" groups support Edwards coo *and* support Kummer coords with small coefficients. 3 independent constraints on 2 degrees of freedom, but everything lifts to $\mathbf{Q}$.

Map $(x, \omega y(z+2)^3/(1-iz)^3)$ to an Edwards curve E over $\mathbf{F}_{p^2}$ by chain of "2-isogenies".

View two coordinates over $\mathbf{F}_{p^2}$ as four coordinates over $\mathbf{F}_p$; view curve E as surface W. Have now mapped C rationally to this Abelian variety W.

Compute formulas for the unique map $J \to W$ of C-Abelian varieties and a "dual isogeny" $W \to J$. Composition has small kernel.

Cryptographic consequences

Speed records for high-security $a \mapsto aP$ use Edwards coords.

Speed records for high-security $a, P \mapsto aP$ use Kummer coords for Jacobians of genus-2 curves with small Kummer coefficients.

"Hyper-and-elliptic-curve" groups support Edwards coords *and* support Kummer coords with small coefficients. 3 independent constraints on 2 degrees of freedom, but everything lifts to $\mathbf{Q}$.