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

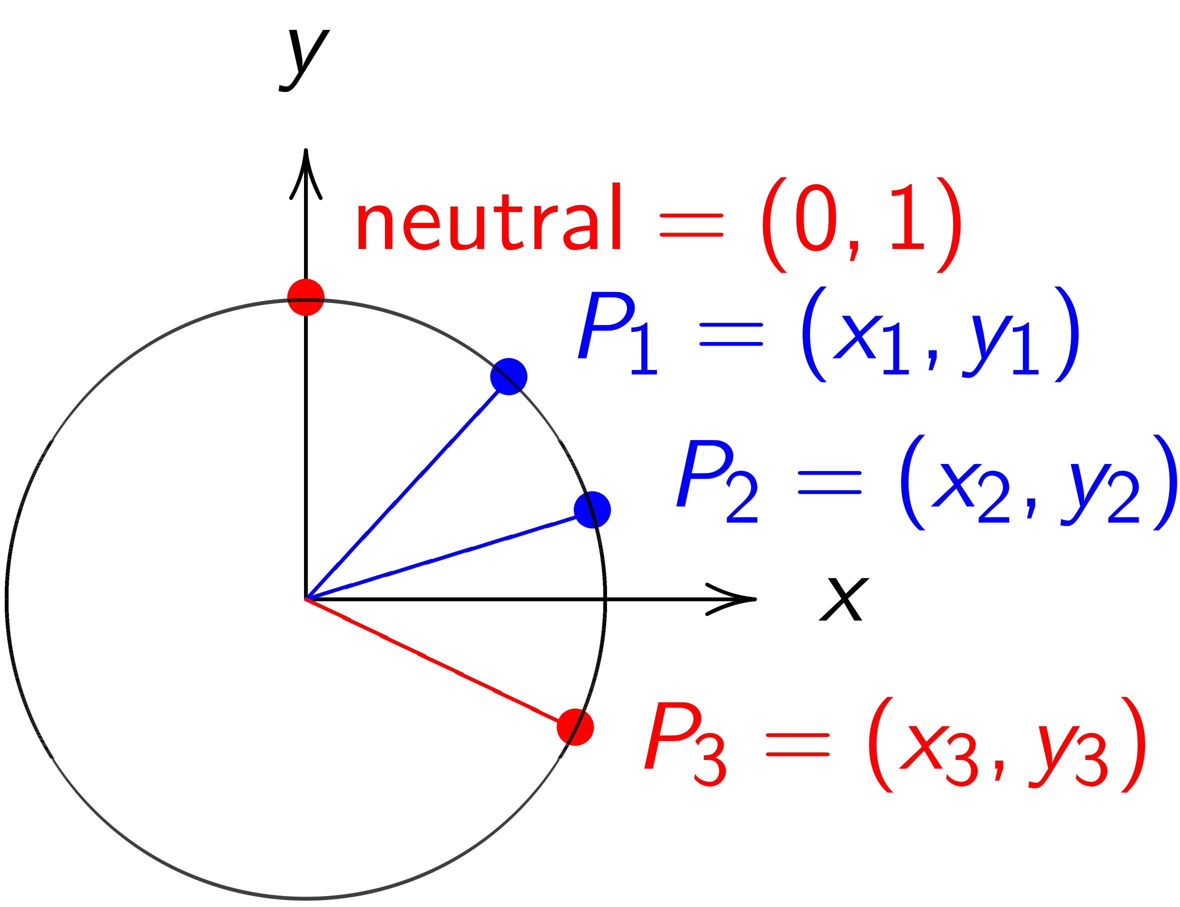
cr.yp.to/papers.html#hyperand

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

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

"−": $(x, y) \mapsto (-x, y)$;

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



More clock perspectives:

"A parametrized clock":

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

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

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

More clock perspectives:

"A parametrized clock":

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

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

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

"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

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

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":

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

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

"2-dimensional rotations":

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

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

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.

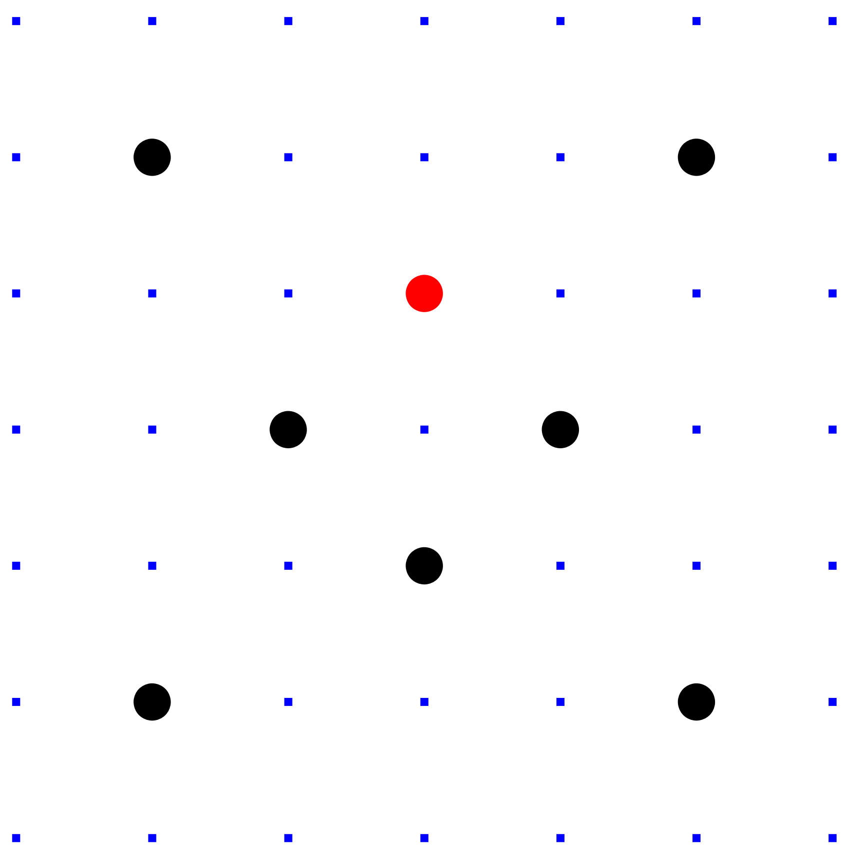


Diagram plots $\mathbf{F}_7$ as
$-3, -2, -1, 0, 1, 2, 3.$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $(n+1)P$.

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?

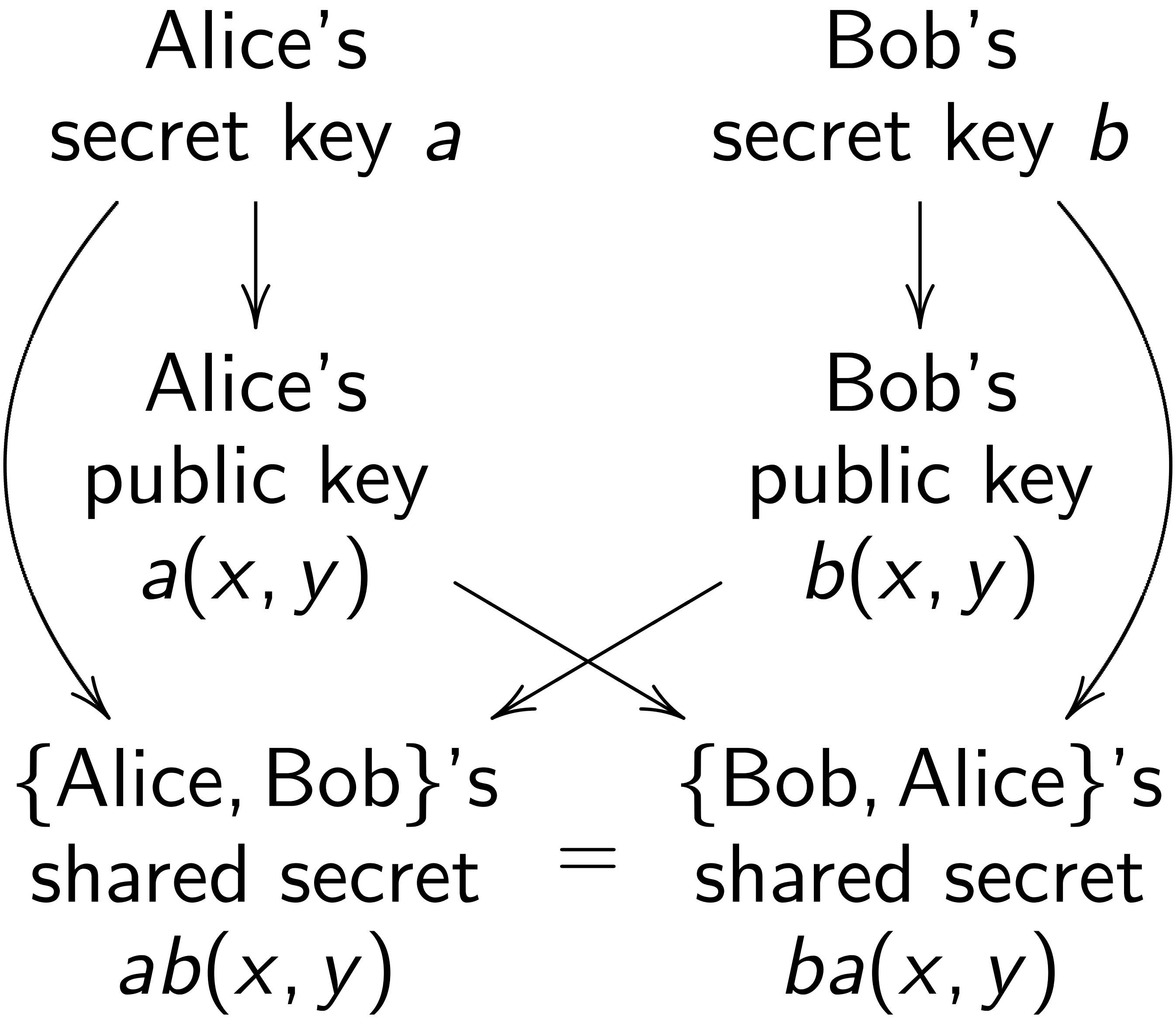
Clock cryptography

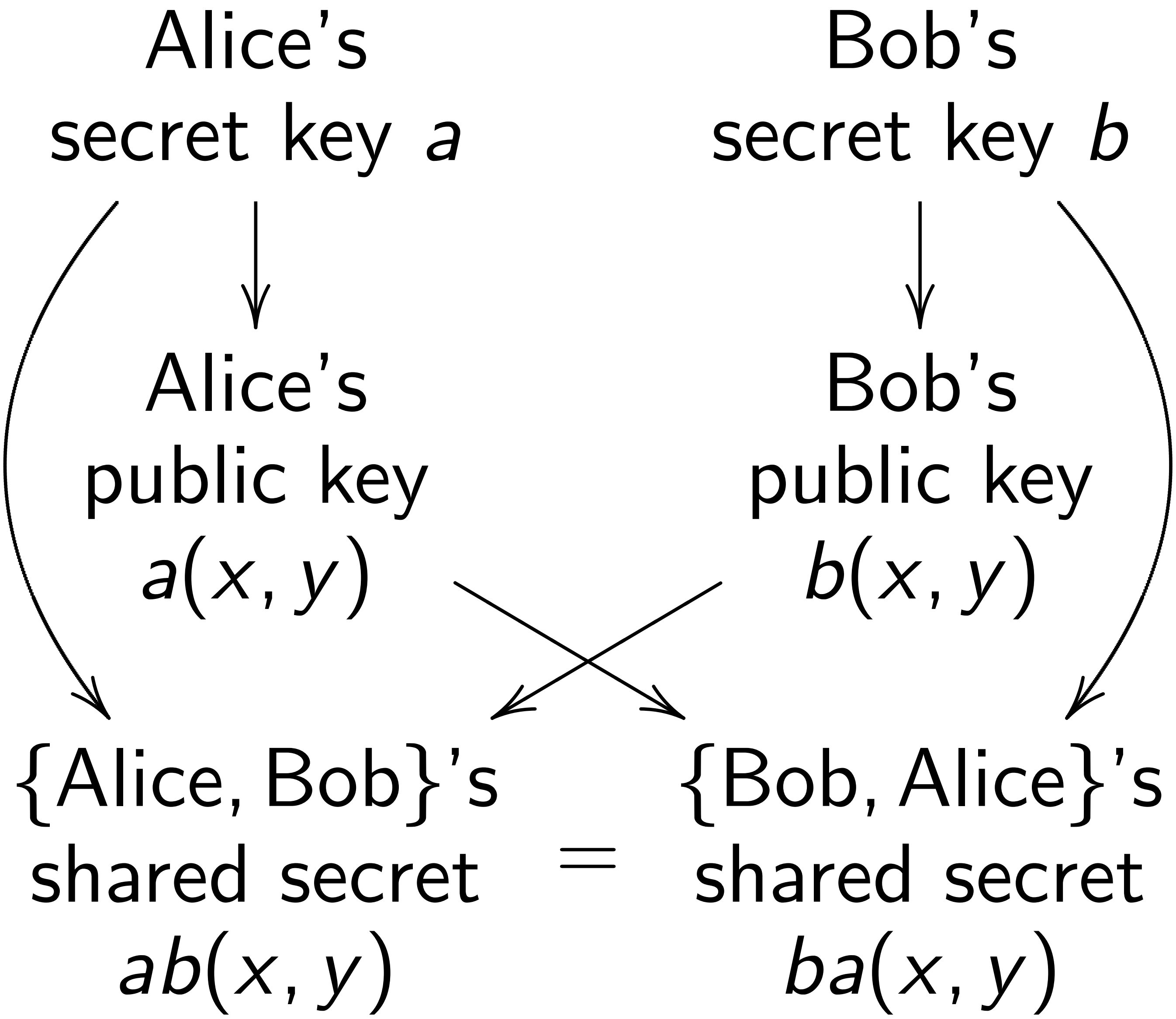
Standardize odd prime power q
and $(x, y) \in \text{Clock}(\mathbf{F}_q)$
of large prime order.

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

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

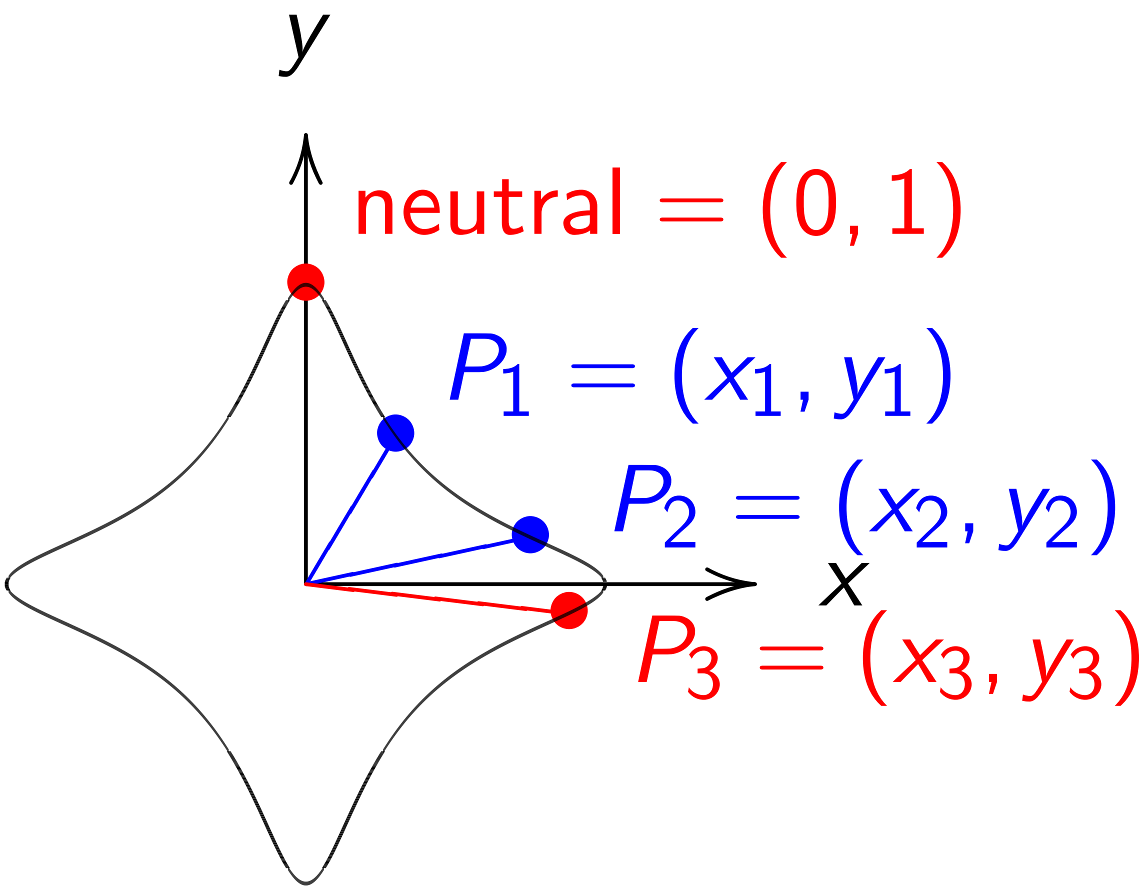
Alice computes $a(b(x, y))$.
Bob computes $b(a(x, y))$.
They use this shared secret
to encrypt with "AES-GCM" etc.


Alice's secret key a
Bob's secret key b
Alice's public key $a(x, y)$
Bob's public key $b(x, y)$
{Alice, Bob}'s shared secret $ab(x, y)$
=
{Bob, Alice}'s shared secret $ba(x, y)$



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

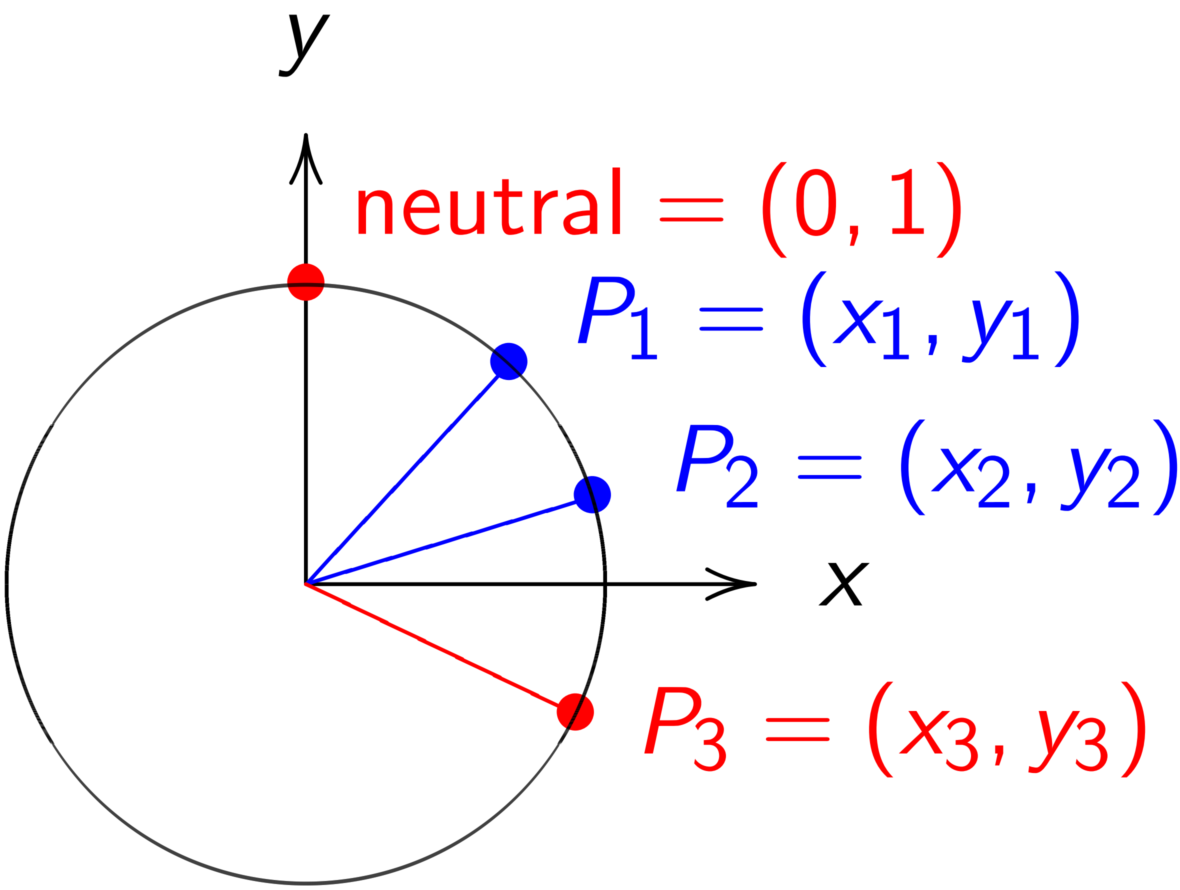


$x^2 + y^2 = 1 - 30x^2y^2$.

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

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

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

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

“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.

“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 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)

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

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.

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 $\mathbf{F}_q$.

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 "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".

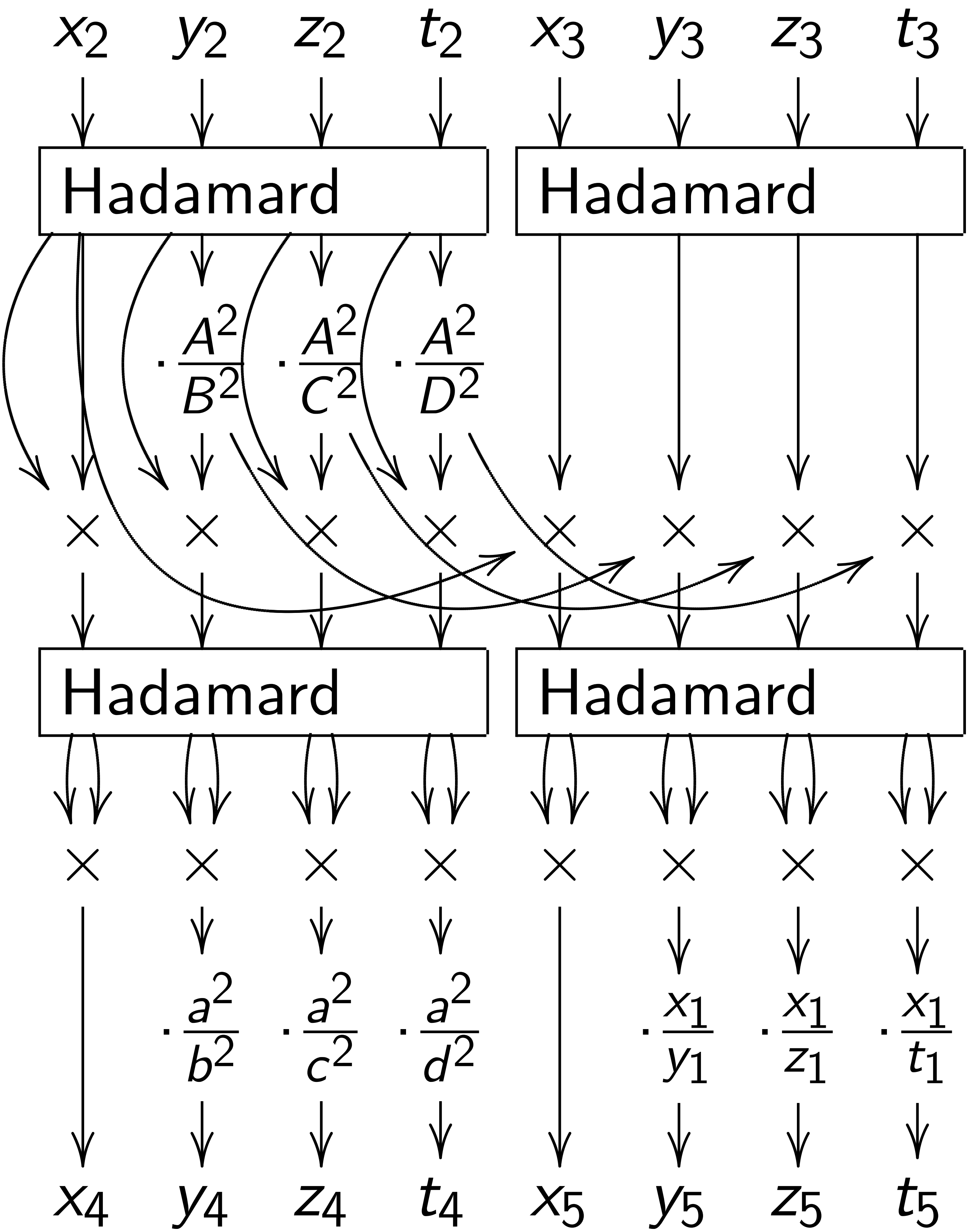
Rationally map C to J,
taking ∞ to 0.
J is a "C-Abelian variety".

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

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 $1, u_0, u_1, u_0^2, u_0 u_1, u_1^2, u_0 u_1^2, v_0 v_1$: $x = 16u_0u_1^2 - 8u_0^2 + 573u_0u_1 - 5u_1^2 - 1215000v_0v_1 + 2460u_0 - 175u_1 - 1250$, etc. Warning: many wrong formulas in literature; always use a computer!



x_2 y_2 z_2 t_2 x_3 y_3 z_3 t_3
Hadamard
Hadamard
$\cdot \frac{A^2}{B^2}$ $\cdot \frac{A^2}{C^2}$ $\cdot \frac{A^2}{D^2}$
Hadamard
Hadamard
$\cdot \frac{a^2}{b^2}$ $\cdot \frac{a^2}{c^2}$ $\cdot \frac{a^2}{d^2}$ $\cdot \frac{x_1}{y_1}$ $\cdot \frac{x_1}{z_1}$ $\cdot \frac{x_1}{t_1}$
x_4 y_4 z_4 t_4 x_5 y_5 z_5 t_5

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

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

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".

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.

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 $\mathbf{Q}$.