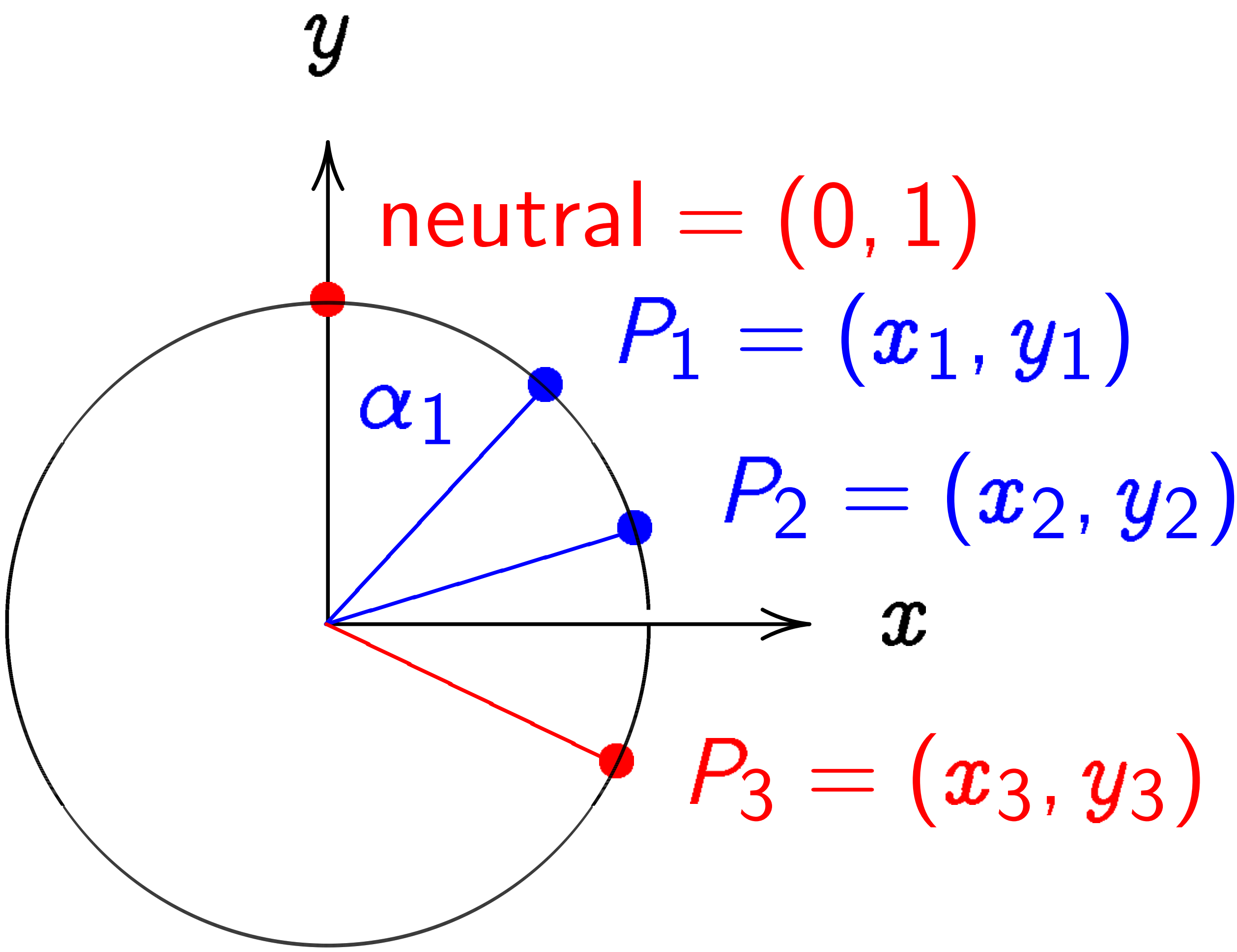
Twisted Edwards curves

D. J. Bernstein (`uic.edu`)
Peter Birkner (`tue.nl`)
Marc Joye (`thomson.net`)
Tanja Lange (`tue.nl`)
Christiane Peters (`tue.nl`)

Thanks to:
NSF ITR–0716498
IST–2002–507932 ECRYPT
INRIA Lorraine, LORIA

Today's speaker: DJB.

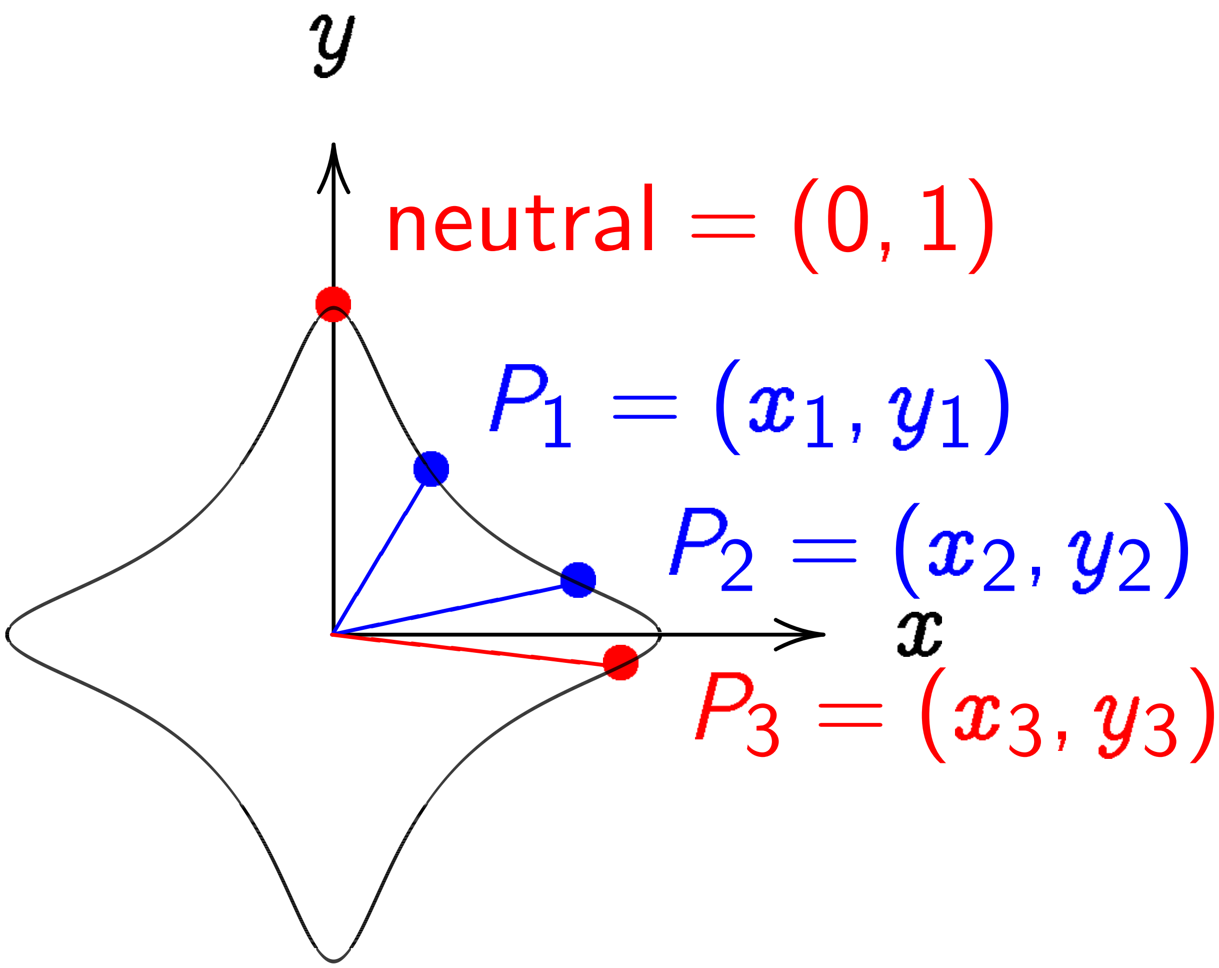
Addition on a clock



$x^2 + y^2 = 1$, parametrized by
$x = \sin\alpha, \quad y = \cos\alpha$.
Sum of (x_1, y_1) and (x_2, y_2) is
$(x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$.

Fast but not elliptic; low security.

Addition on an Edwards curve



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

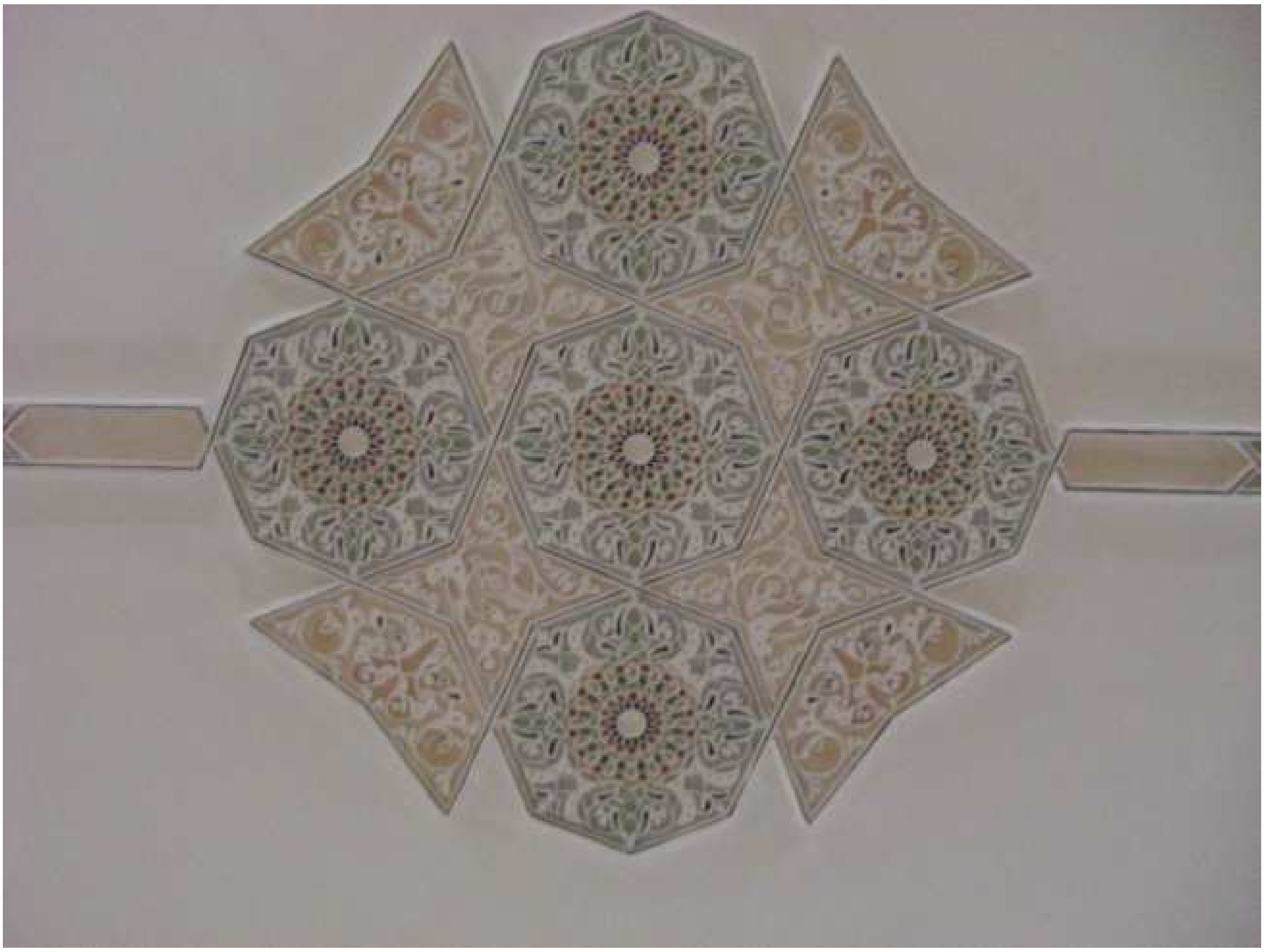
Sum of (x_1, y_1) and (x_2, y_2) is

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

New elliptic-curve speed records!

Edwards curves in Casablanca

Photographed 10 June 2008
in Casablanca mosque:



Montgomery curves

1987 Montgomery:
Use curves $Bv^2 = u^3 + Au^2 + u$.
$5\mathbf{M} + 4\mathbf{S} + 1\mathbf{A}$ for each bit of n
to compute $n, P \mapsto nP$. Warning:
$n, n', P, P' \mapsto nP+n'P'$ is harder.

Often used in ECC etc.

Example: 2005 Bernstein,
"Curve25519: new
Diffie–Hellman speed records."
Very fast software for secure
twist-secure Montgomery curve
$v^2 = u^3 + 486662u^2 + u$
over $\mathbf{F}_p$ where $p = 2^{255} - 19$.

Some statistics

Counting elliptic curves
over $\mathbf{F}_p$ if $p \equiv 1 \pmod 4$:

$\approx 2p$ elliptic curves.
$\approx 5p/6$ curves with order $\in 4\mathbf{Z}$.
$\approx 5p/6$ Montgomery curves.
$\approx 2p/3$ Edwards curves.
$\approx p/2$ complete Edwards curves.
$\approx p/24$ original Edwards curves.

(Many more statistics in paper:
e.g., complete Edwards curves
with group order $8 \cdot$ odd.)

Counting elliptic curves
over $\mathbf{F}_p$ if $p \equiv 3 \pmod 4$:

$\approx 2p$ elliptic curves.
$\approx 5p/6$ curves with order $\in 4\mathbf{Z}$.
$\approx 3p/4$ Montgomery curves.
$\approx 3p/4$ Edwards curves.
$\approx p/2$ complete Edwards curves.
$\approx p/4$ original Edwards curves.

Can we achieve Edwards-like
speeds for more curves?

Main results of this paper

1. Can add very quickly on **twisted Edwards curves** $ax^2 + y^2 = 1 + dx^2y^2$.

2. Some Edwards curves are sped up by twists.

3. All Montgomery curves can be written as twisted Edwards curves.

4. Can use isogenies to achieve similar speeds for all curves where 4 divides group order.

5. Improving previous proofs: All curves with points of order 4 can be written as Edwards curves.

Twisted Edwards curves

This paper introduces curves
$ax^2 + y^2 = 1 + dx^2y^2$ where
$a \neq 0$, $d \neq 0$, $a \neq d$, $2 \neq 0$.

Generalization of . . .

. . . "Edwards curves": $a = 1$.
(see 2007 Bernstein–Lange)

. . . "complete Edwards curves":
$a = 1$; d not a square.
(see 2007 Bernstein–Lange)

. . . "original Edwards curves":
$a = 1$; $d =$ fourth power.
(see 2007 Edwards)

Sum of (x_1, y_1) and (x_2, y_2) on a twisted Edwards curve is
$((x_1 y_2 + \ y_1 x_2)/(1+d x_1 x_2 y_1 y_2),$
$\ (y_1 y_2 - a x_1 x_2)/(1-d x_1 x_2 y_1 y_2)).$

Speed in projective coordinates:
ADD $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{A} + 1\mathbf{D}$;
i.e., 10 mults, 1 squaring,
1 mult by a, 1 mult by d.
DBL $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{A}$.

Speed in inverted coordinates:
ADD $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{A} + 1\mathbf{D}$.
DBL $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{A} + 1\mathbf{D}$.

(See paper for more options.)

Montgomery and twisted Edwards

$Bv^2 = u^3 + Au^2 + u$
is equivalent to
a twisted Edwards curve.

Simple, fast computation: define
$a = (A+2)/B$; $d = (A-2)/B$;
$x = u/v$; $y = (u-1)/(u+1)$.
Then $ax^2 + y^2 = 1 + dx^2y^2$.

(What about divisions by 0?
Easy to handle; see paper.)

So can use fast twisted-Edwards formulas to compute on any Montgomery curve.

Often can translate to Edwards, avoiding twists. Example (2007 Bernstein–Lange): Curve25519 can be expressed as $x^2 + y^2 = 1 + (121665/121666)x^2y^2$.

However, in many cases, twists are faster! Example (this paper): Curve25519 can be expressed as $121666x^2 + y^2 = 1 + 121665x^2y^2$.

Mults by 121665 and 121666 are much faster than mult by $121665/121666 =$

20800338683988658368647408995589388737092878452977063003340006470870624536394.

2×2 and twisted Edwards

All Montgomery curves over $\mathbf{F}_p$ have group order $\in 4\mathbf{Z}$.

Can a curve with order $\in 4\mathbf{Z}$ be written as a Montgomery curve? Not necessarily!

Can nevertheless achieve twisted-Edwards speeds for all curves with order $\in 4\mathbf{Z}$.

Central idea: The missing curves are 2-isogenous to twisted Edwards curves.

The missing curves
can be written in the form
$v^2 = u^3 - (a + d)u^2 + (ad)u$.

Starting from (u, v) define
$x = 2v/(ad - u^2)$; $\quad y =$
$(v^2 - (a - d)u^2)/(v^2 + (a - d)u^2)$.
Then $ax^2 + y^2 = 1 + dx^2y^2$.

Compatible with addition.
Also, can work backwards
from (x, y) to $2(u, v)$.

So can compute $2n(u, v)$,
$2n(u, v) + 2n'(u', v')$, etc. via
$n(x, y)$, $n(x, y) + n'(x', y')$, etc.

Recent news

Bernstein–Lange:
`http://hyperelliptic.org/EFD`.

B.–L.–Rezaeian Farashahi, CHES 2008, “Binary Edwards curves”: Edwards-like curve shape for all ordinary elliptic curves over fields $\mathbf{F}_{2^n}$ if $n \geq 3$.

B.–Birkner–L.–Peters, “ECM using Edwards curves”: Better curves for ECM; and twisted-Edwards ECM software, faster than state-of-the-art GMP-ECM Montgomery software.