Pairings on Edward's Curves

Michael Naehrig

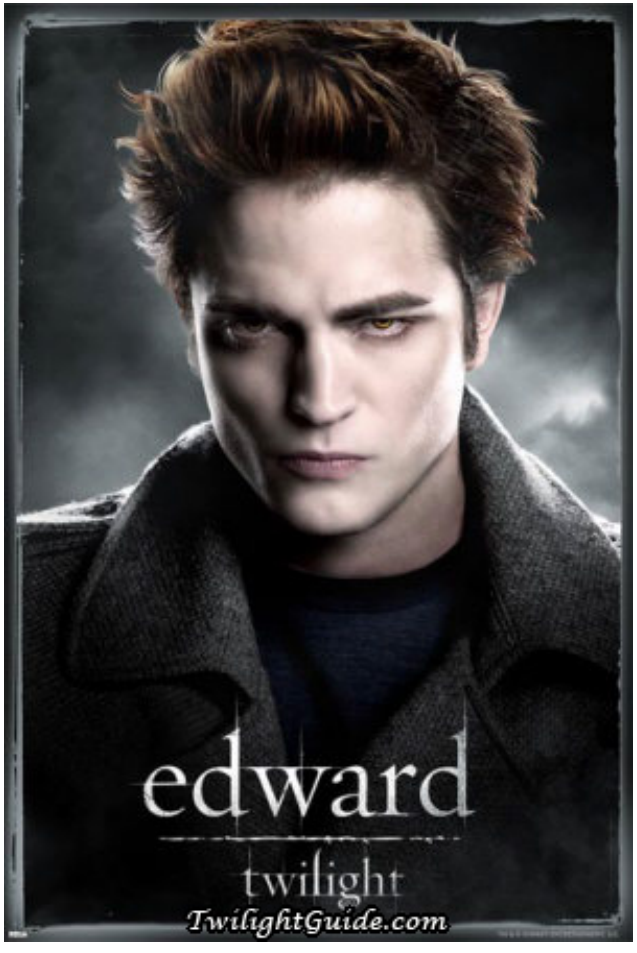
Technische Universiteit Eindhoven
michael@cryptojedi.org

ECC 2009 Rump Session
Calgary, 2009-08-24

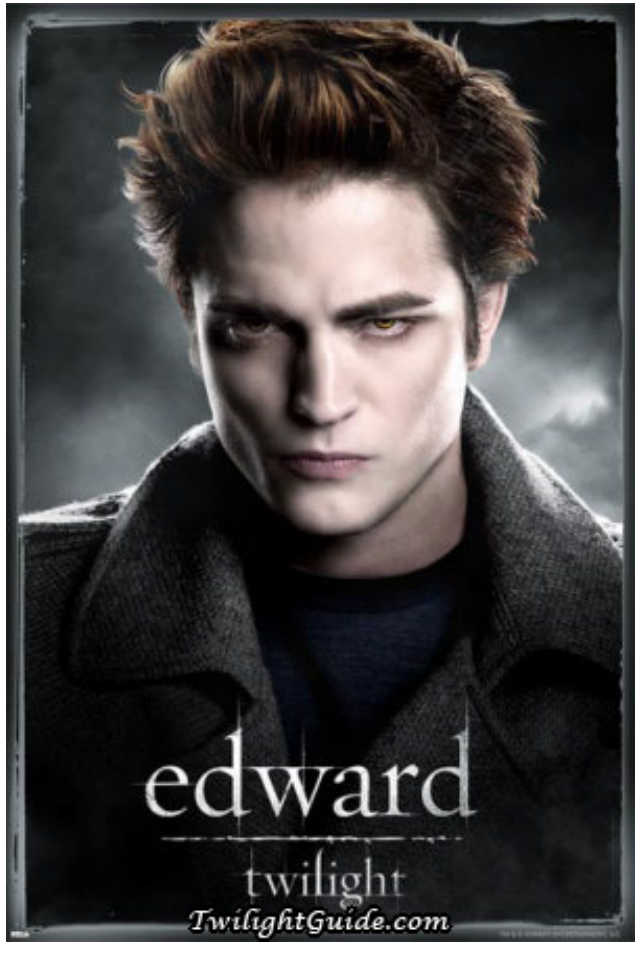
Pairings on Edwards curves

Pairings on Edward’s curves

Edward's curves

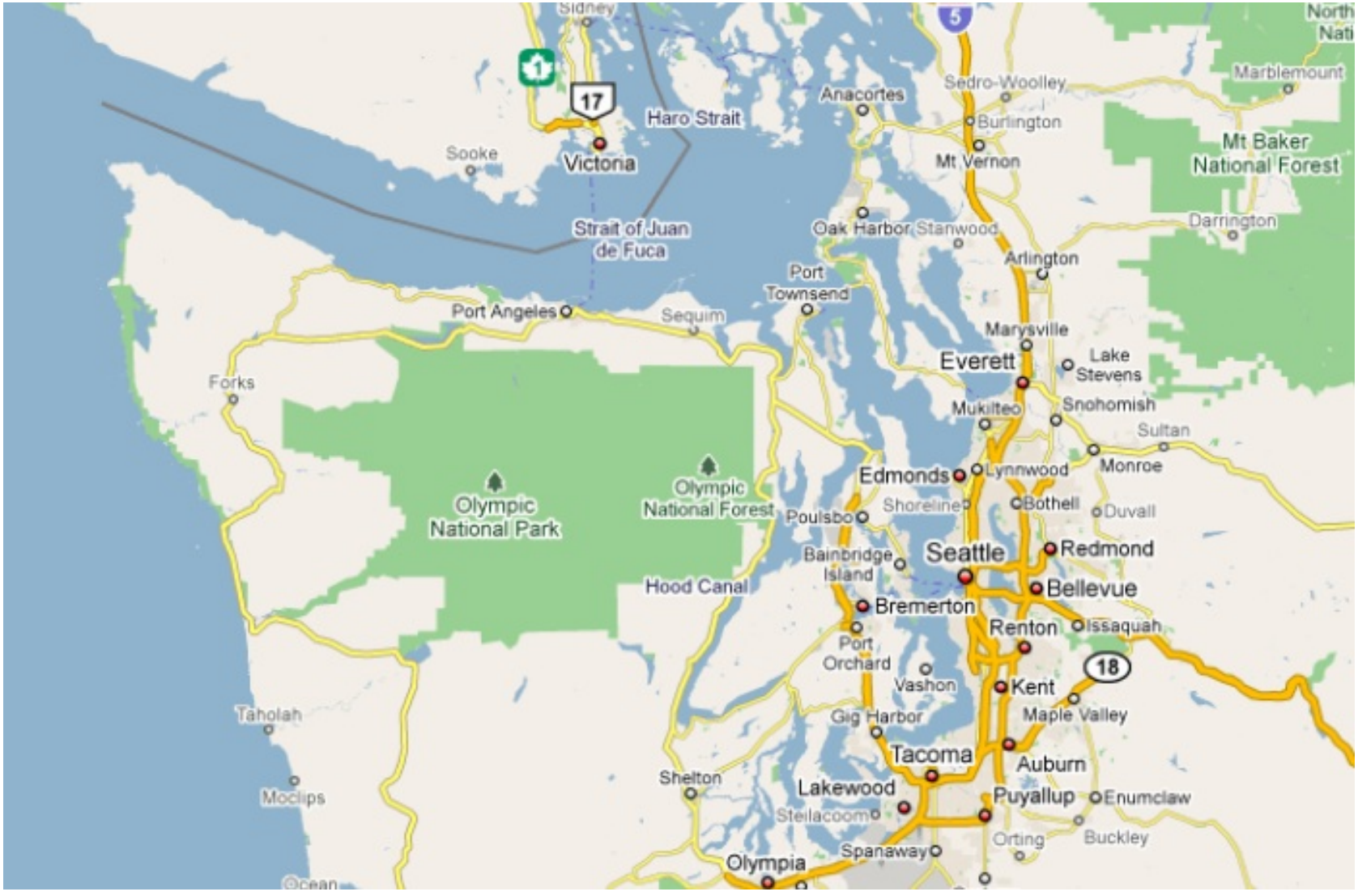


Edward's curves



Vampire
Virtual Application and Implementation Research Lab

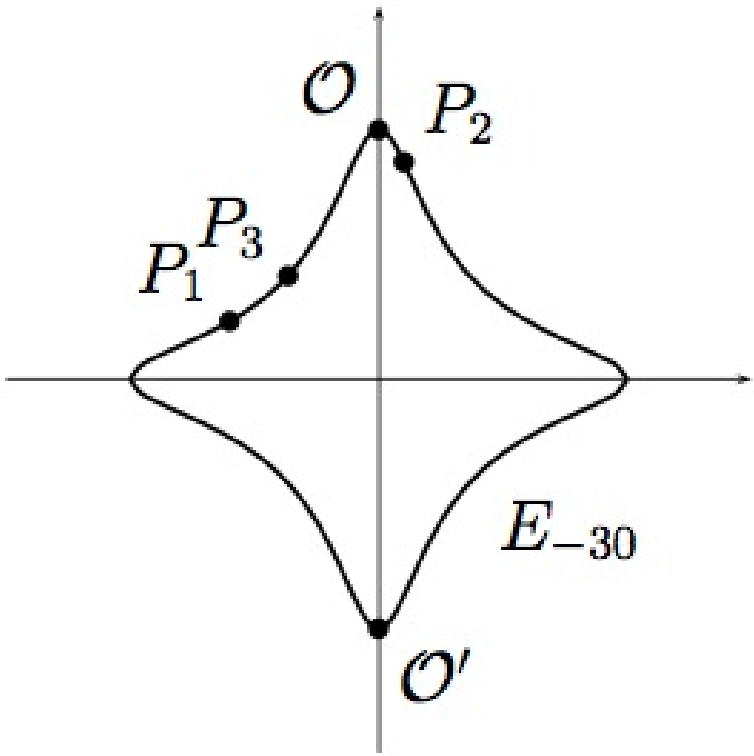
Edward's curves

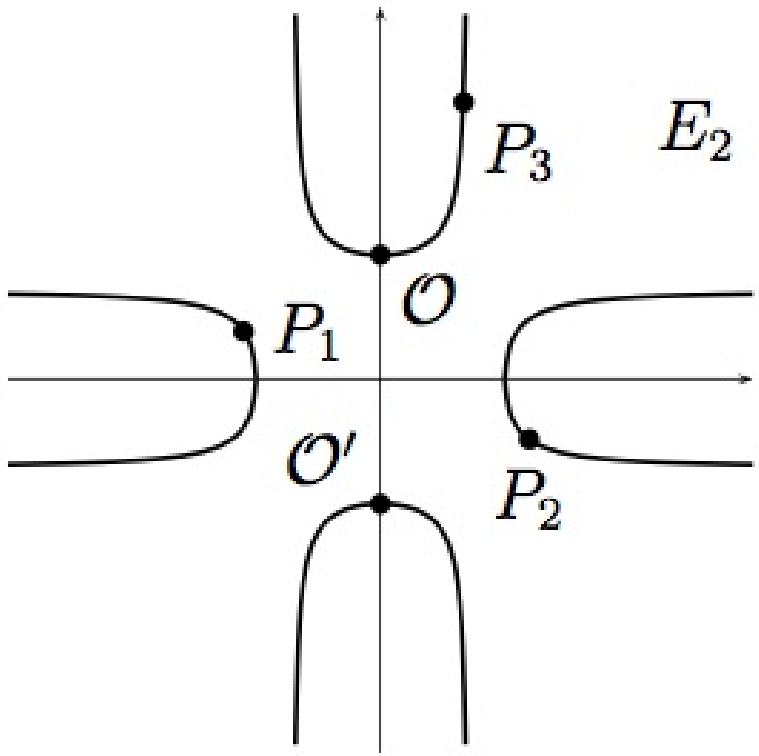


Edward's curves

Edward's curves

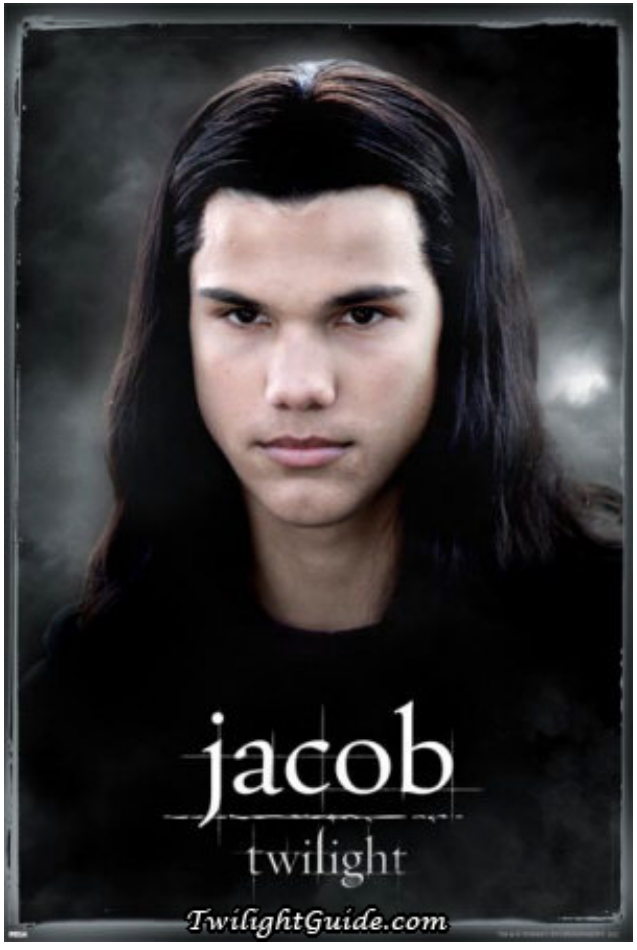
Edward's curves



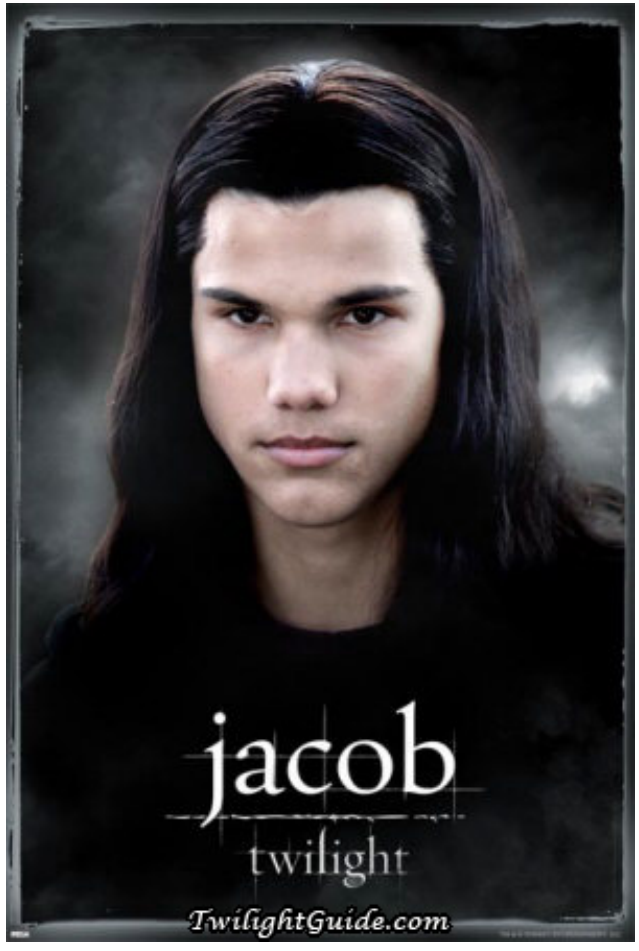


$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

Jacob's curves



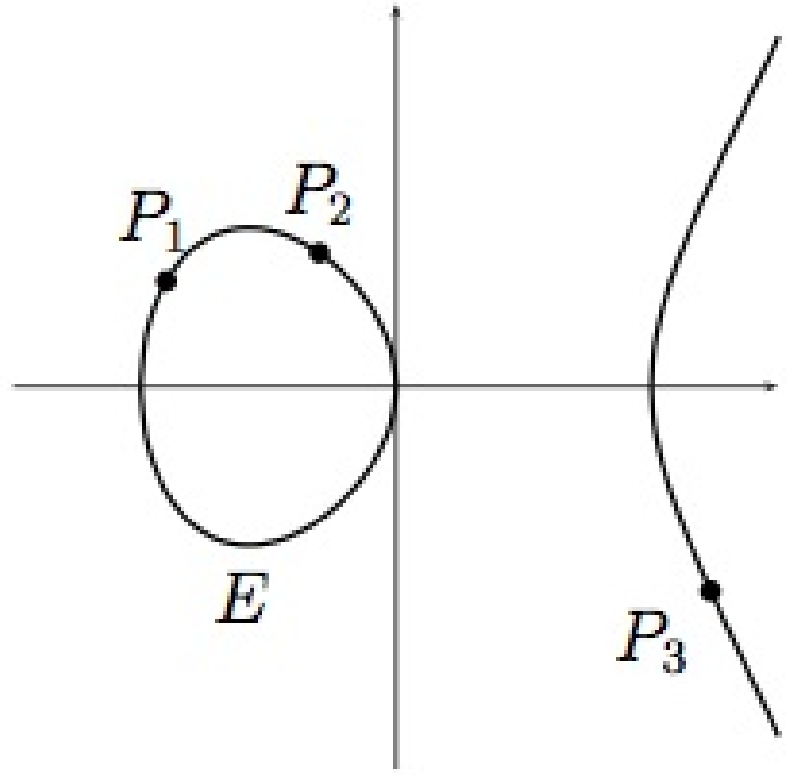
Jacob's curves



Weierstrass Werewolf

Jacob’s curves

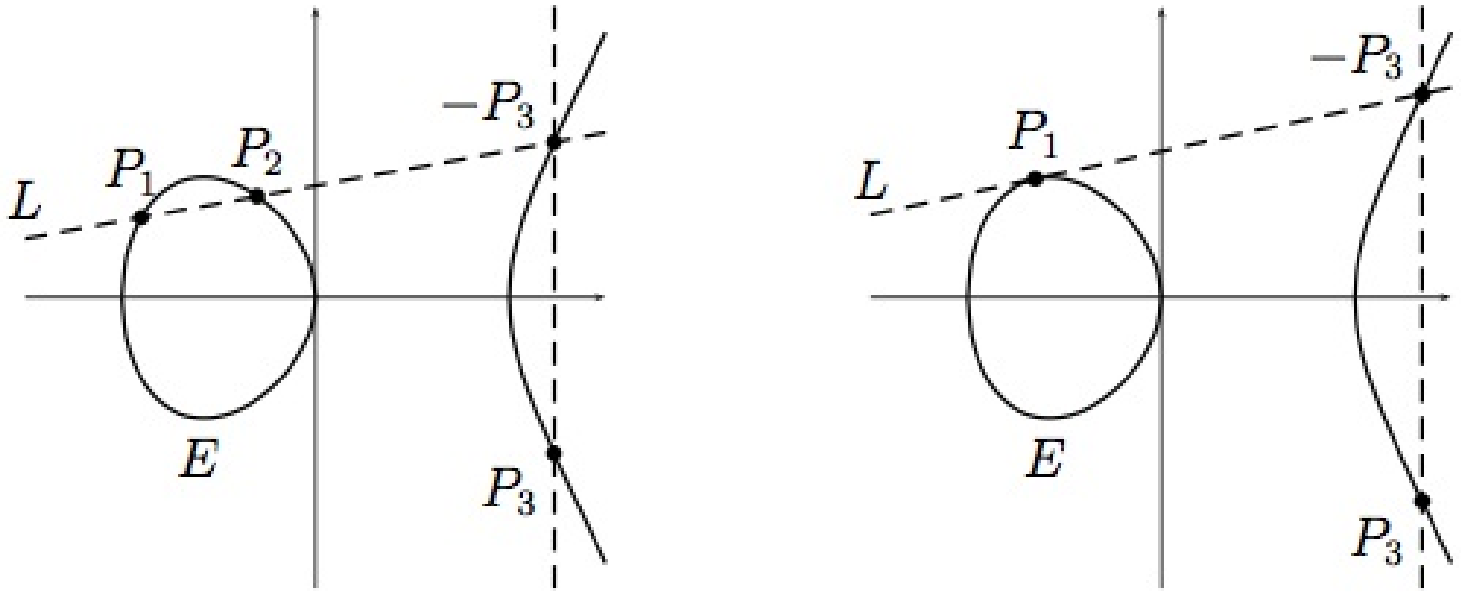
Jacob's curves



$$E : y^2 = x^3 + ax^2 + b$$

Group law on Jacob's curves

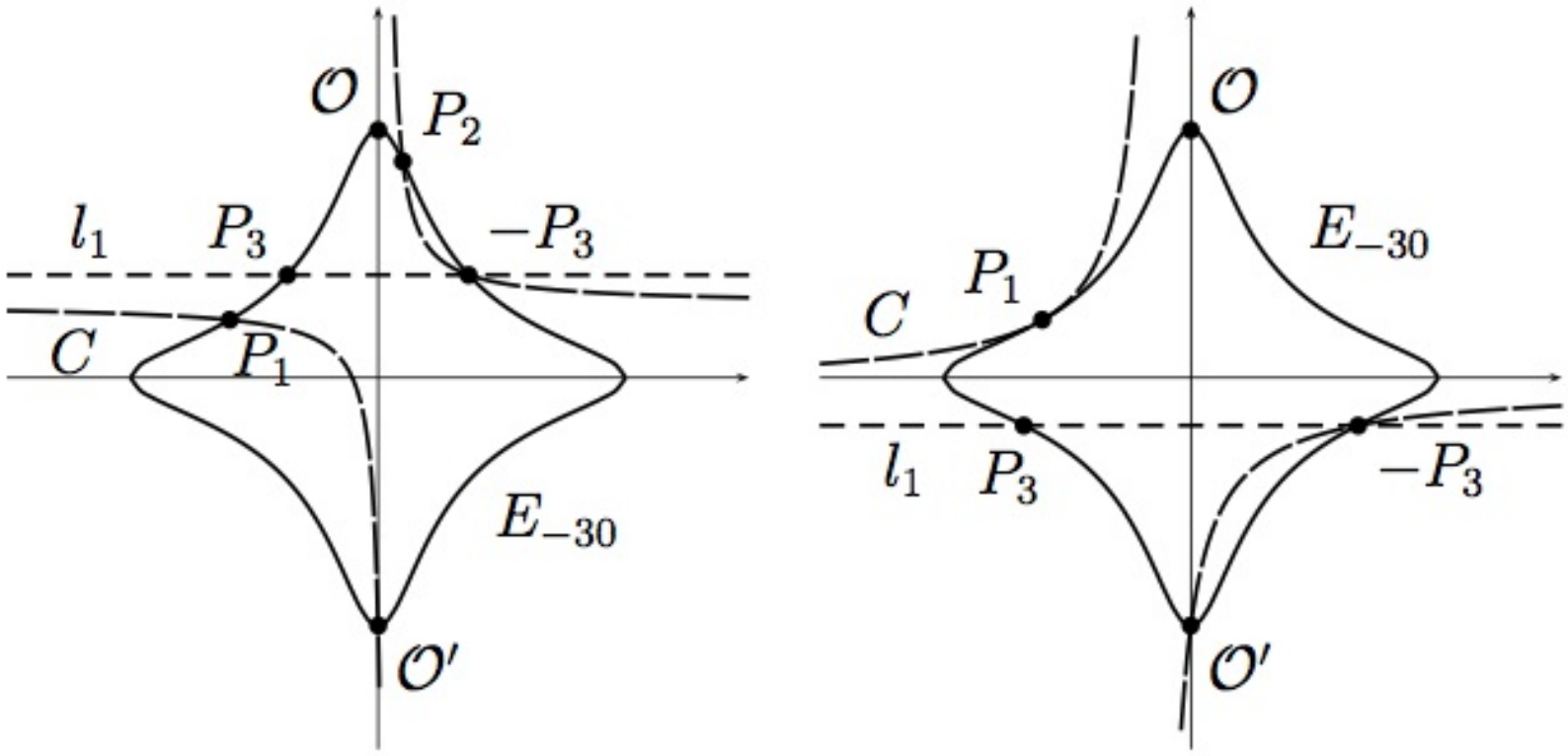
Does not work at full moon...



$$E : y^2 = x^3 + ax^2 + b$$

Group law on Edward's curves

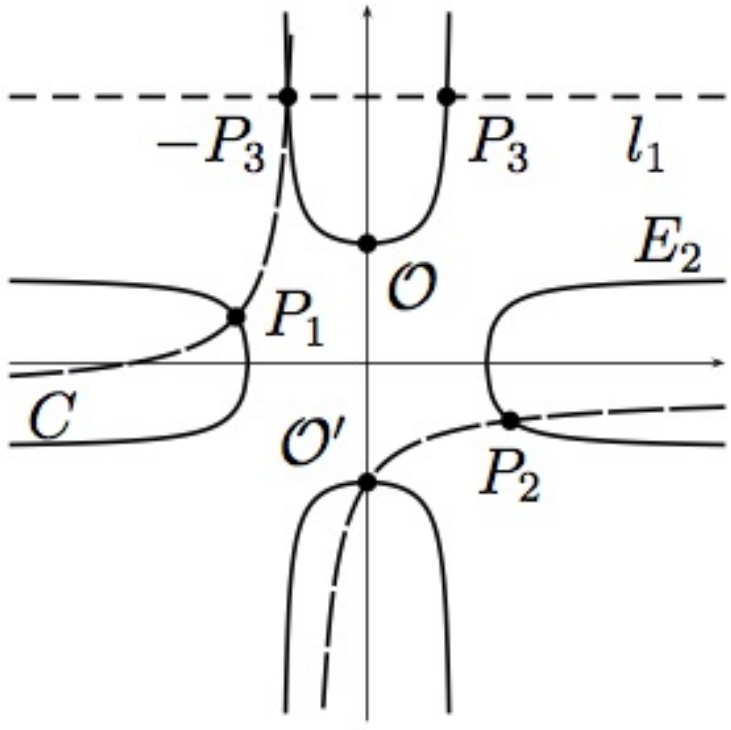
Works only at night...

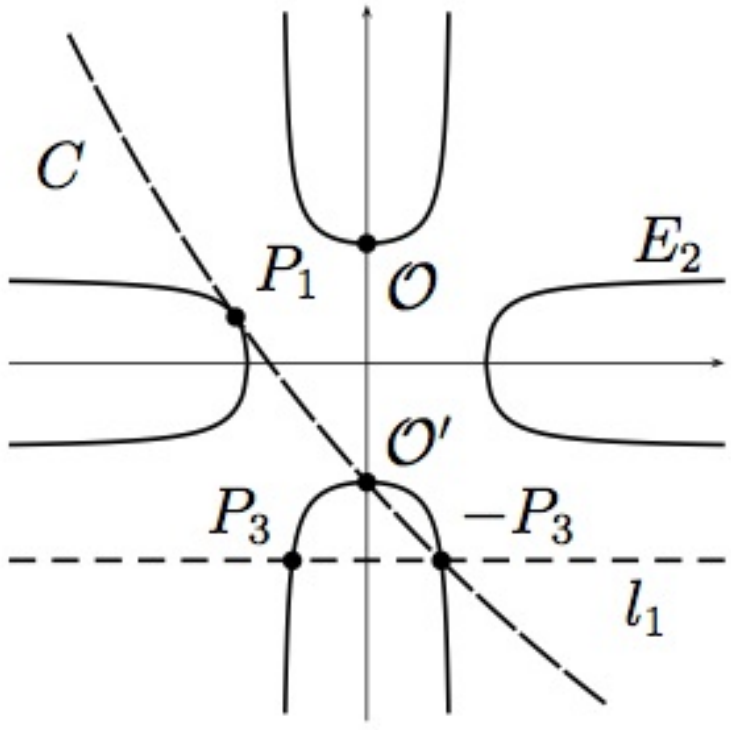


$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

Group law on Edward's curves

Works only at night...

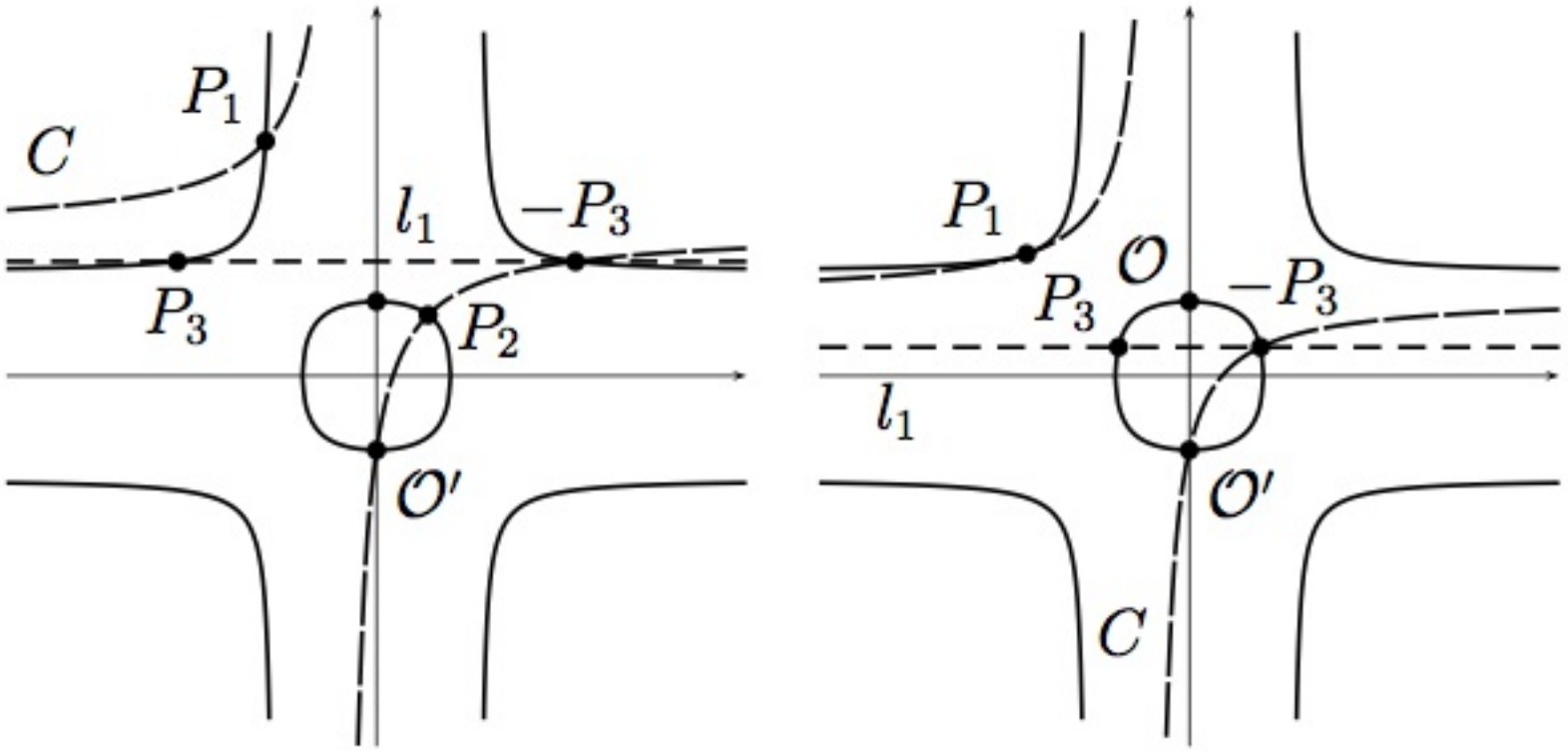




$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

Group law on Edward's curves

Works only at night...



$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

Group law on Edward's curves

Works during the day as well...

Correctly driving through one of Edward's curves over $\mathbb{R}$ for $0 < d < 1$.

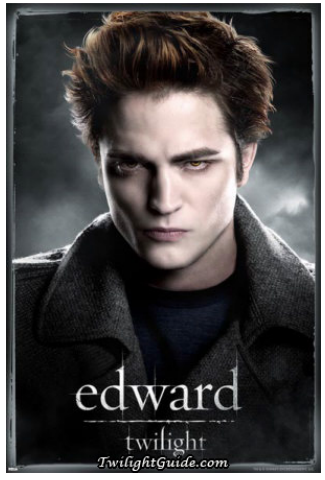
Looking for a good pairing...

Pairings on Jacob's curves

- Jacob uses BN curves,
- Miller's algorithm,
- by using line functions that occur in the group law.
- He can use cool things such as the R-ate pairing.

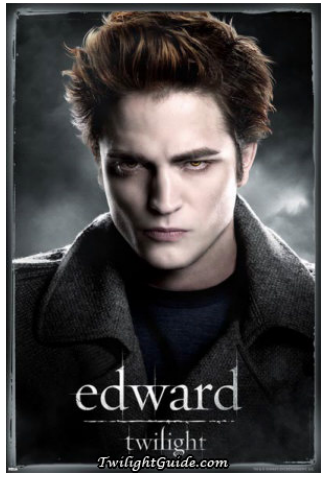
Pairings on Edward's curves

- Edward can't use BN curves,
- he uses other pairing-friendly curves
- (in Edward's projective coordinates).



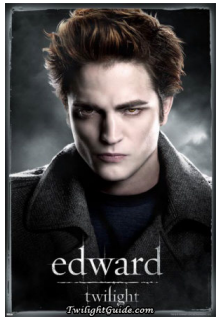
Pairings on Edward's curves

- Edward can't use BN curves,
- he uses other pairing-friendly curves
- (in Edward's projective coordinates).
- But he can use Miller's algorithm,
- by replacing the line functions with the conic section occuring in the group law.
- Many people didn't believe this...



Comparison of operation counts

	DBL	mADD	ADD
Jacob	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_a}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
J. ($a = -3$)	$6\mathbf{m} + 5\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
Jacob (BN)	$3\mathbf{m} + 8\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$15\mathbf{m} + 6\mathbf{s}$
Edward	$6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$	$12\mathbf{m} + 1\mathbf{m_a}$	$14\mathbf{m} + 1\mathbf{m_a}$



For all details, explicit formulas and Edward's curve examples look at preprint

`http://eprint.iacr.org/2009/155`

joint work with Christophe Arène (IML), Tanja Lange (TU/e), Christophe Ritzenthaler (IML), and