

Edwards curves for ECC

(Bernstein, Lange):

faster than Jacobian etc.

cr.yp.to/newelliptic.html

Edwards curves for ECM

(Bernstein, Birkner, Lange,

Peters), in progress:

current predictions are

faster than Montgomery.