New timings for

# SCALAR MULTIPLICATION

## using a new set of coordinates

Thomaz Oliveira, Ph.D student, CINVESTAV-IPN
Francisco Rodríguez-Henríquez, CINVESTAV-IPN
Júlio López, University of Campinas
Diego Aranha, University of Brasília

ECC2012 rump session

An implementation based on the paper "**Analyzing the Galbraith-Lin-Scott Point Multiplication Method for Elliptic Curves over Binary Fields"** [Hankerson, Karabina and Menezes]

---

binary curves over $\mathbb{F}_{2^{254}}$ with approx. 128 bits of security

for Intel Sandy Bridge architecture (AVX, PCLMULQDQ)

half-and-add method

combined with efficiently-computable endomorphisms,

a fast reduction code,

optimization techniques

**and a new set of projective coordinates**

# operations

add-mix 8M + 2S

add-full 11M + 2S

doubling 4M + 1a + 4S

double&add (2P+Q, P in projective, Q in affine)

9M + 1a + 6S

# results: a new speed record

Aranha et al., 2012: 99,000 cc

Longa and Sica, 2012: 91,000 cc

Our work: 75,000 cc

to be improved: parallel processing and more optimization techiniques

# gracias!