Fast arithmetic on hyperelliptic Koblitz curves

Tanja Lange
lange@exp-math.uni-essen.de
IEM
University of Essen
Germany

Nov 17, 2000
MAGiC, Urbana-Champaign

Outline

- Motivation
- Introduction to hyperelliptic curves
- Koblitz Curves
  - Counting points
  - Fast arithmetic
  - "Disadvantages"
  - Outlook