Cryptology ePrint Archive: Report 2011/243

Affine Pairings on ARM

Tolga Acar and Kristin Lauter and Michael Naehrig and Daniel Shumow

Abstract: Pairings on elliptic curves are being used in an increasing number of cryptographic applications on many different devices and platforms, but few performance numbers for cryptographic pairings have been reported on embedded and mobile devices.

In this paper we give performance numbers for affine and projective pairings on a dual-core Cortex A9 ARM processor and compare performance of the same implementation across three platforms: x86, x86-64 and ARM. Using a fast inversion in the base field and doing inversion in extension fields by using the norm map to reduce to inversions in smaller fields, we find a very low ratio of inversion-to-multiplication costs. In our implementation, this favors using affine coordinates on all three platforms, even for the current 128-bit minimum security level specified by NIST. We use Barreto-Naehrig (BN) curves and report on the performance of an optimal ate pairing for curves covering security levels roughly between 128 and 192 bits. We compare with other reported performance numbers for pairing computation on ARM processors.

Category / Keywords: implementation / Pairing computation, affine coordinates, optimal ate pairing, pairing cost, ARM architecture.

Date: received 16 May 2011, last revised 26 Jul 2011

Contact author: michael at cryptojedi org