Cryptology ePrint Archive: Report 2011/712

Efficient Java Implementation of Elliptic Curve Cryptography for J2ME-Enabled Mobile Devices

Johann Gro{\ss}sch{\"a}dl and Dan Page and Stefan Tillich

Abstract: The Micro Edition of the Java 2 platform (J2ME) provides an application environment specifically designed to address the demands
embedded devices like cell phones, PDAs or set-top boxes. Since the J2ME platform does not include a crypto package, developers are force
use third-party classes or to implement all cryptographic primitives from scratch. However, most existing implementations of elliptic curve (EC)
cryptography for J2ME do not perform well on resource-restricted devices, in most cases due to poor efficiency of the underlying arithmetic
operations. In this paper we present an optimized Java implementation of EC scalar multiplication that combines efficient finite-field arithmetic wi
efficient group arithmetic. More precisely, our implementation uses a pseudo-Mersenne (PM) prime field for fast modular reduction and a Gallar
Lambert-Vanstone (GLV) curve with an efficiently computable endomorphism to speed up the scalar multiplication with random base points. Ou
experimental results show that a conventional mobile phone without Java acceleration, such as the Nokia 6610, is capable to execute a 174-bit
scalar multiplication in roughly 400 msec, which is more than 45 times faster than the widely-used Bouncy Castle Lightweight Crypto API for J2

Category / Keywords: implementation / Elliptic Curve Cryptography, Prime-Field Arithmetic, Endomorphism

Publication Info: To be published in the Proceedings of WISTP 2012

Date: received 31 Dec 2011, last revised 28 Aug 2012

Contact author: johann groszschaedl at uni lu

Available formats: PDF | BibTeX Citation

Version: 20120828:202404 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]