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

Abstract: The Micro Edition is of the Java 2 platform (J2ME) provides an application environment specifically designed to address the demands of embedded devices like cell phones, PDAs or set-top boxes. Since the J2ME platform does not include a crypto package, developers are forced to 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 with efficient group arithmetic. More precisely, our implementation uses a pseudo-Mersenne (PM) prime field for fast modular reduction and a Gallant-Lambert-Vanstone (GLV) curve with an efficiently computable endomorphism to speed up the scalar multiplication with random base points. Our 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 about 400 msec.

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

Date: received 31 Dec 2011

Contact author: johann groszschaedl at uni lu