Cryptology ePrint Archive: Report 2011/176

A FPGA pairing implementation using the Residue Number System

Sylvain Duquesne and Nicolas Guillermin

Abstract: Recently, a lot of progresses have been made in software implementations of pairings at the 128-bit security level in large characteristic. In this work, we obtain analogous progresses for hardware implementations. For this, we use the RNS representation of numbers which is especially well suited for pairing computation in a hardware context. A FPGA implementation is proposed, based on an adaptation of Guillermin's architecture which computes a pairing in 1.07 ms. It is 2 times faster than all previous hardware implementations (including ASIC and small characteristic implementations) and almost as fast as best software implementations.

Category / Keywords: public-key cryptography /

Date: received 5 Apr 2011, last revised 6 Apr 2011

Contact author: sylvain duquesne at univ-rennes1 fr