Cryptology ePrint Archive: Report 2013/005

Efficient Multiplier for pairings over Barreto-Naehrig Curves on Virtex-6 FPGA

Riadh Brinci , Walid Khmiriy, Mefteh Mbarekz, Abdellatif Ben Rabaˆa, Ammar Bouallegue and Faouzi Chekir

Abstract: This paper is devoted to the design of a 258- bit multiplier for computing pairings over Barreto-Naehrig (BN) curves at 128-bit security level. The proposed design is optimized for Xilinx field programmable gate array (FPGA). Each 258-bit integer is represented as a polynomial with five,65 bit signed integer, coefficients . Exploiting this splitting we designed a pipelined 65-bit multiplier based on new Karatsuba-Ofman variant using non-standard splitting to fit to the Xilinx embedded digital signal processor (DSP) blocks. Our architecture is able to compute 258-bit multiplication suitable for BN curves using only 11 in-built DSP blocks available on Virtex-6 Xilinx FPGA devices. It is the least DSP blocks consumption in the known literature. This work can be extended to efficiently compute pairings at higher security levels.

Category / Keywords: Modular Multiplication, Modular Reduction, Cryptography, Pairing-Friendly Curves, Non-Standard Splitting, Field Programmable Gate Array(FPGA).

Date: received 5 Jan 2013

Contact author: wkhmiri at yahoo fr