Cryptology ePrint Archive: Report 2011/354

A coprocessor for secure and high speed modular arithmetic

Nicolas Guillermin

Abstract: We present a coprocessor design for fast arithmetic over large numbers of cryptographic sizes. Our design provides a efficient way to prevent side channel analysis as well as fault analysis targeting modular arithmetic with large prime or composite numbers. These two countermeasure are then suitable both for Elliptic Curve Cryptography over prime fields or RSA using CRT or not. To do so, we use the residue number system (RNS) in an efficient manner to protect from leakage and fault, while keeping its ability to fast execute modular arithmetic with large numbers. We illustrate our countermeasure with a fully protected RSA-CRT implementation using our architecture, and show that it is possible to execute a secure 1024 bit RSA-CRT in less than 0:7 ms on a FPGA.

Category / Keywords: implementation / FPGA, side channel analysis, fault analysis, countermeasure, RNS

Date: received 1 Jul 2011

Contact author: nicolas guillermin at m4x org