A Very Lightweight Reconfigurable Elliptic Curve Crypto-Processor

Michal Varchola
Technical University of Kosice, Slovakia

Abstract

In this paper we present a novel and very compact FPGA-based architecture for 256-bit elliptic curve cryptography over prime fields. Although quite a few ECC implementations have been proposed so far (such as the design by Vliegen et al. presented on ASAP 2010), our architecture differs in two main points. First, we heavily optimized the use of memories and registers and second, we use elliptic curves based on standardized NIST primes. Our MicroECC implementation finally achieves a throughput of 67 full 256-bit point multiplications per second using only 615 slices, 3 BRAMs and a single hardware multiplier on a Xilinx Virtex-2 Pro. According to this performance data, our design provides an increased performance by a factor of 5.5 compared to the work by Vliegen et al.