A Scalable ECC Processor Implementation for High-Speed and Light-Weight

Ahmad Salman, Ahmed Ferozpuri, Ekawat Homsirikamol, Panasayya Yalla, Jens-Peter Kaps, and Kris Gaj

Geroge Mason University

ABSTRACT

The performance of Public Key Cryptosystems (PKC) based on elliptic curves is mostly dependent on the performance of the underlying field arithmetic. In this work, we present high-speed and lightweight implementations of a fully scalable architecture of an Elliptic Curve Cryptography (ECC) scalar multiplier processor. The processor supports operations over GF(p) for arbitrary values of p, and field sizes up to 521 bits. The implementations perform modular multiplication operations using fully scalable Montgomery multiplier architectures, one tailored for high-speed and one for lightweight. Point addition and point doubling operations are performed over modified Jacobian projective coordinates instead of affine coordinates to avoid costly division operations. Circuits used to convert from affine to modified Jacobian coordinates and back are included in the core. In addition to having dedicated high-speed and lightweight architectures, both also support different bus widths to increase flexibility and allow for a wide range of applications.

We have implemented the design on FPGA and All Programmable System on Chip platforms from different vendors as well as using a standard-cell ASIC library in order to provide comprehensive results We also analyzed power and energy consumptions for each implemented design to determine the relation between area/throughput trade-off and power and energy consumptions. We have evaluated our designs based on NIST recommended field lengths - 192, 224, 256, 384 and 521 bits - using several arbitrary values of prime p.