Low-power Elliptic Curve Crypto Processor in 130nm technology

Vladimir Rožić, Yong Ki Lee, Junfeng Fan, Miroslav Knežević, Duško Karaklajić, Roel Maes, Lejla Batina, and Ingrid Verbauwhede

COSIC, Katholieke Universiteit Leuven, Belgium

Abstract. In Radio Frequency Identification (RFID) systems, public key cryptography (PKC) is used to provide security features such as unclonability and untracebility. Given that public-key algorithms are in general very computationally intensive, it is a challenging task to provide a hardware implementation of a PKC which meets strict area and power requirements of the RFID devices. Due to small operand sizes, elliptic curve cryptography can be used to answer the imposed challenges.
In this talk we present a processor for elliptic curve cryptography over $GF(2^{163})$. The proposed processor can perform elliptic curve point multiplication as well as general modular operations which are used in authentication protocols.
The chip is fabricated using UMC 130nm 1P8M process. The core size is $0.54mm^2$ and energy consumption for performing one point multiplication is below $5\mu J$.
In this presentation we will discuss processor architecture, FPGA prototype, testing strategy and the ASIC measurement results.