Abstract

THE PRIMARY CHALLENGE in modern day cryptographic hardware development lies in coping with progressively strong physical attacks commonly referred to as side-channel analysis. This research deals with practical implementations and analysis of physical security of pairing based cryptographic operations on prime fields. Pairing computation and elliptic curve scalar multiplication are two major operations in pairing based cryptography. These operations in turn rely on arithmetic in finite fields − prime fields ($\mathbb{F}_p$). Hence, this work first designs a portable and compact architecture for $\mathbb{F}_p$ arithmetic. Subsequently, the work proposes an efficient dual-core cryptoprocessor for elliptic curve scalar multiplication based on the above compact $\mathbb{F}_p$ core. Field Programmable Gate Array (FPGA) is a relevant platform which provides various in-built features for optimizing arithmetic operations. A configurable core on FPGA device has been developed for $\mathbb{F}_{p^k}$ arithmetic based on the above optimized $\mathbb{F}_p$ primitive. Two such configurable cores are utilized for developing a pairing cryptoprocessor which computes pairing over Barreto-Naehrig curve. Security of pairing computations against fault and power attacks are subsequently addressed in this work. The work further studies existing as well as new vulnerabilities of pairing computations against fault and power attacks. Suitable countermeasures are also proposed to resist those attacks.

Keywords: Pairing based cryptography, Elliptic curve cryptography, Field programmable gate array, Prime field, Side-channel attacks.