Multi-Purpose Keccak for Modern FPGAs

Panasayya Yalla Ekawat Homsirikamol Jens-Peter Kaps

Abstract

Most widely used security Protocols like Internet Protocol Security (IPSec), Secure Socket Layer (SSL) and Transport Layer Security (TLS) provide cryptographic services which include authentication, confidentiality, integrity, and non-repudiation. A combination of cryptographic primitives such as PRNG, secure hash, symmetric key and asymmetric key crypto-system are involved within these protocols. As a result, multiple cryptographic algorithms are often required. Having a single cryptographic primitive providing most cryptographic services can be very beneficial especially in case of resource constraint devices. In this paper, we are exploring the Keccak f-function on which the new secure hash standard SHA-3 and two candidates of the cryptographic competition Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) Ketja and Keyak are built. We are presenting two hardware implementations of a muli-purpose Keccak core, one targeting high-speed, the other low-area, which can provide Authenticated Encryption, Message Authentication Code (MAC), generate pseudo-random numbers, and produce the hash of a message. We are comparing the results with our implementation of similar multi-purpose AES cores.