High-Throughput Implementation of AES-Based Lightweight Authenticated Encryption - ALE

Francesco Regazzoni

Abstract

For a large number of applications, encryption is not sufficient. What is really needed is authenticated encryption (AE). Fostered by the NIST financed project CAESAR, it can be foreseen that authenticated encryption, which is a fundamental security functionality allowing to encrypt and authenticate data at the same time, will be subject of extensive research efforts in future.

In the view of this relevant problem, in this talk, we present a high throughput implementation of AES-Based Lightweight Authenticated Encryption - ALE - which has recently been proposed at FSE 2013. Our design is evaluated on ASIC using different technological libraries, as well as state-of-the-art FPGAs in terms of performance, area, power, and energy consumption.