FPGA IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS AS ASYNCHRONOUS PIPELINE CIRCUITS

Kledermon Garcia (Instituto Tecnológico de Aeronáutica)
Duarte L. Oliveira (Instituto Tecnológico de Aeronáutica)
Gracieth C. Batista (Instituto Tecnológico de Aeronáutica)
Leonardo Romano (Centro Universitário da FEI)

Abstract: Currently, digital systems that are able to meet major security restrictions are increasingly being demanded, both in the military and in commercial areas. Data security can be achieved by cryptographic algorithms, which are subject to attacks, often using the clock signal to reveal the secret data. To deal with this major problem, the asynchronous paradigm presents interesting features, due to the lack of the clock signal, being an option for the project of digital systems. In this paper, we introduce the pipeline style to implement an asynchronous cryptosystem. The cryptographic algorithms was chosen based on its simplicity and are called TEA (Tiny Encryption Algorithm). For its implementations, it was considered FPGAs (Field Programmable Gate Array) devices as target platforms. Comparing the proposed asynchronous pipeline design with synchronous and asynchronous designs, this one in the style AFSM (asynchronous finite state machine) with data-path, the proposal presented a performance (throughput) increase of up to 93 times.