One Core Fit All: Towards Merging block ciphers on FPGA

Joao Carlos Resende[1], Shivam Bhasin[2], Francesco Regazzoni[3], Ricardo Chaves[1]

[1]INESC-ID, IST, Universidade de Lisboa, Lisbon,
Portugal.joaocresende@tecnico.ulisboa.pt, ricardo.chaves@inesc-id.pt
[2]Temasek Labs@NTU, 21 Nanyang Link, 637371, Singapore.sbhasin@ntu.edu.sg
[3]ALaRI - USI, via Buffi 13, 6900 Lugano, Switzerland.regazzoni@alari.ch

Abstract. The future Internet of Things (IoT) will be populated by a number of devices all connected to inter-operate. Each device will be designed having a specific goal in mind and to meet specific constraints. As a result, in a realistic scenario, different devices will implement different cryptographic algorithms. To facilitate their interoperability, central devices acting as hubs will need to support multiple encryption algorithms. Towards this, we explore a scenario where multiple cryptographic functions co-exist on the hub. In this context, we propose a design that supports a range of different block ciphers realized on top of a common base architecture. Our results demonstrate that, by exploiting the structures of novel FPGAs and by correctly scheduling the resources, it is possible to derive a compact and efficient structure, capable of achieving a throughput in the gigabit range.