Rethinking Secure FPGAs: Towards a Cryptography-friendly Configurable Cell Architecture and its Automated Design Flow

Nele Mentens[1], Edoardo Charbon[2], Francesco Regazzoni[3]

[1]imec-COSIC – KU Leuven, Belgium, email: nele.mentens@kuleuven.be
[2]AQUA – EPFL, Switzerland, email: edoardo.charbon@epfl.ch
[3]ALaRI – USI, Switzerland, email: regazzoni@alari.ch

Cryptography is one of the main applications that are often deployed on FPGAs. Cryptographic primitives, such as block ciphers, public-key algorithms, and hash functions have been successfully implemented as stand-alone designs or as part of a complete system-on-chip. Further, dedicated circuits implementing physically unclonable functions (PUFs) or bitstream decryption blocks have been added to FPGAs by the vendors. Finally, with the advent of side-channel attacks, FPGAs are an attractive platform for implementing protected designs as well as for benchmarking the resistance against power analysis attacks. However, surprisingly, despite such a massive use of reconfigurable hardware for cryptography, to date, the possibility of designing a cryptography-friendly, fine-grained reconfigurable cell has rarely been considered and certainly not explored yet in the right depth.

This work [1] proposes the first fine-grained configurable cell array specifically tailored for cryptographic implementations. The proposed architecture can be added to future FPGAs as an application-specific configurable building block, or to an ASIC as an embedded FPGA (eFPGA). The goal is to map cryptographic ciphers on combinatorial cells that are more efficient than general purpose lookup tables in terms of silicon area, configuration memory and combinatorial delay. As a first step in this research direction, we focus on block ciphers and we derive the most suitable cell structure for mapping state-of-the-art algorithms. We develop the related automated design flow, exploiting the synthesis capabilities of Synopsys Design Compiler and the routing capabilities of Xilinx ISE. Our solution is the first cryptography-oriented fine-grained architecture that can be configured using common hardware description languages.

We evaluate the performance of our solution by mapping a number of well-known block ciphers onto our new cells. The obtained results show that our proposed architecture drastically outperforms commercial FPGAs in terms of silicon area and configuration memory resources, while obtaining a similar throughput.

References

1. N. Mentens, E. Charbon, and F. Regazzoni, "Rethinking secure FPGAs: Towards a cryptography-friendly configurable cell architecture and its automated design flow," in *Field-Programmable Custom Computing Machines (FCCM), 2018 IEEE 26th Annual International Symposium on.* IEEE, 2018.