Master's Thesis Engineering Technology

2020-2021

Embedded FPGA for cryptography

Biesmans Jelle

Master of Electronics and ICT Engineering Technology

Dekeyser Matthias

Master of Electronics and ICT Engineering Technology

Security is important

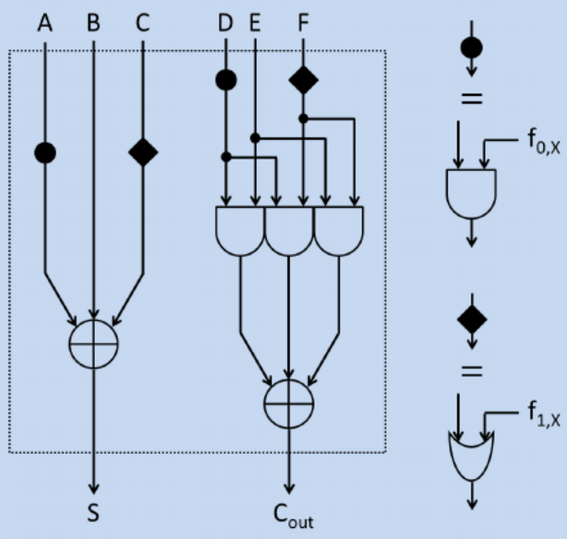
Encryption is an important feature in modern devices, especially in the Internet of Things (IoT). When a deployed encryption algorithm is not considered secure anymore, billions of IoT devices are immediately vulnerable.

Embedded FPGA

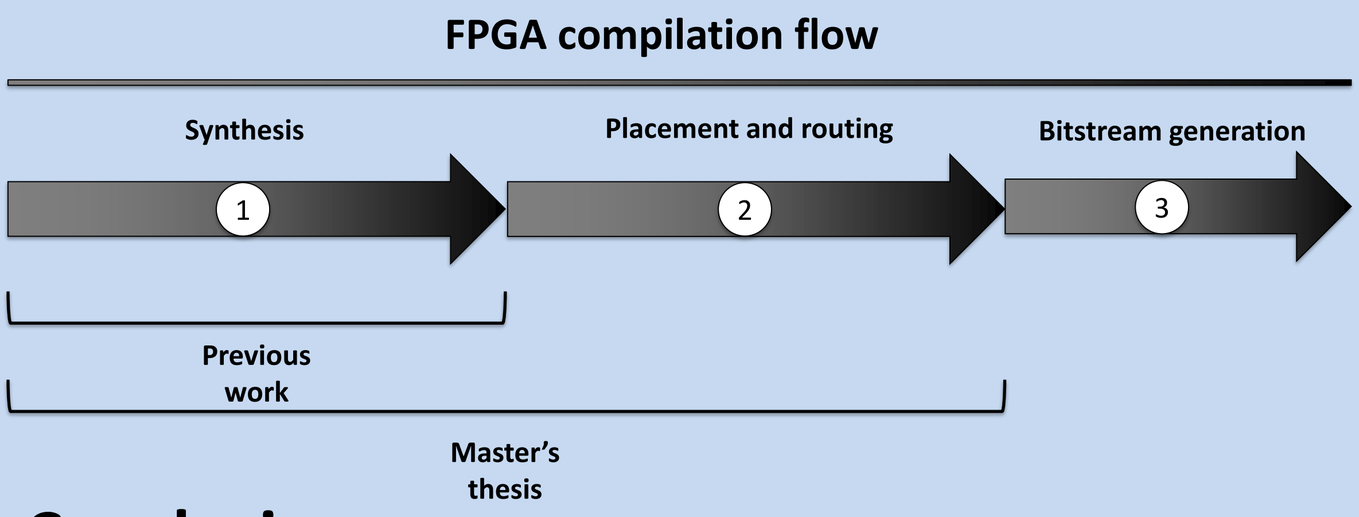
In 2018, Mentens et al. proposed to use a small embedded FPGA (eFPGA) dedicated to cryptography. The eFPGA, by its nature, allows to update the hardware implementation of the cryptographic algorithm. Ultimately, an eFPGA for security should be more efficient than general purpose ones.

Proposed cFA cell

Mentens et al. proposed to use a new type of logic element called the configurable Full Adder (cFA) [1] to replace the Lookup Tables (LUT) inside the eFPGA. The cFA is optimized for cryptographic operations which results in a significant reduction in area usage. These results were based on post-synthesis information not including the routing.



The cFA cell proposed by Mentens et al. [1]



Toolchain

A toolchain was created with open-source tools to compile Verilog or VHDL code for a traditional LUT based FPGA and the new cFA based FPGA. Using this toolchain, different encryption algorithms were compiled for each of the FPGAs to compare the area usage, timings and configuration bitstream length.

Results

Results show that the full implementation of a cFA based FPGA is 130% to 310% the size of a classical LUT based FPGA. The cFA based FPGA achieves 30% to 90% of the frequency of a LUT based FPGA. The configuration bitstream length can be up to 10% smaller for the cFA based FPGA.

Conclusion

Results show that the cFA based FPGA requires less logic area but a larger routing area than the LUT based FPGA. For all tested algorithms, the additional routing usage was bigger than the logic area reduction. One reason is that the cFA, which consists of two independent parts, uses routing for both parts even if one is unused. This can be improved if the synthesis tool would support an equal usage of both parts of the cFA cell.

A modified cell or a brand new cell that can be better supported by the design tools has the potential to outperform LUT based FPGAs.

References

[1] N. Mentens, E. Charbon, and F. Regazzoni, "Rethinking secure fpgas: Towards a cryptography-friendly configurable cell architecture and its automated design flow," International Symposium on Field-Programmable Custom Computing Machines (FCCM), IEEE Computer Society, 2018.

Supervisors / Co-supervisors / Advisors

Prof. Dr. Ir. Mentens Nele

Dr. Regazzoni Francesco

Università della Svizzera italiana

UHASSELT

KU LEUVEN