Ph.D. in Information Technology
Thesis Defense

March 21, 2023
at 10:00
Room PT1

Andrea GALIMBERTI – XXXV Cycle

Design and implementation of a QC-MDPC code-based post-quantum KEM targeting FPGAs

Supervisor: Prof. **William Fornaciari**

Abstract:

Quantum computing is expected to break traditional public-key cryptography in the upcoming decades, making it paramount to design new security solutions that can also resist attacks carried out by quantum computers. Post-quantum cryptography aims to design cryptosystems that can be deployed on traditional computers and resist both traditional and quantum attacks. Providing effective hardware support for such cryptosystems is one of the requirements set by NIST within its ongoing post-quantum cryptography standardization process, and it is particularly crucial to ensuring a wide adoption of post-quantum security solutions across embedded devices at the edge. This thesis delivers a configurable FPGA-based hardware architecture to support BIKE, a post-quantum QC-MDPC code-based KEM. The proposed architecture aims to improve performance over the existing state-of-the-art software and hardware solutions, and it is configurable through a set of architectural and code parameters, which make it efficient, providing good performance while using the resources available on FPGAs effectively, flexible, allowing to support different large QC-MDPC codes defined from the designers of the cryptosystem, and scalable, targeting the whole Xilinx Artix-7 FPGA family. The hardware components implementing QC-MDPC bit-flipping decoding, binary polynomial inversion, and binary polynomial multiplication, i.e., the three most complex operations employed within BIKE, are designed in a parametric way to exploit parallelism as desired according to performance requirements and area constraints. Two separate modules target the cryptographic functionality of the client and server nodes of the quantum-resistant key exchange, respectively. This thesis delivers a preliminary definition of a methodology to identify the best parameterization of the configurable hardware components implemented within the BIKE client and server cores. The methodology uses a complexity-based heuristic that leverages the knowledge of the time and space complexity of such parametric components to steer the design space exploration.

The proposed architecture's client- and server-side instances outperform the state-of-the-art reference software, exploiting the Intel AVX2 extension and running on a desktop-class CPU, by up to 1.91 and 1.83 times, respectively. Moreover, compared to the fastest state-of-the-art reference hardware architecture, which targets the same Artix-7 FPGA family, the architecture described in this thesis provides a performance speedup of up to six times.

Andrea GUSSONI – XXXIV Cycle

Control-Flow Analysis and Manipulation Techniques for Effective Binary Translation and Decompilation

Supervisor: Prof. **Giovanni Agosta**

Abstract:

Reverse engineering is an important branch of the computer security landscape, and its purpose is to extract information about the internals, or more in general the behavior, of a piece of software (and/or hardware).
In this context, decompilers are fundamental tools to perform security assessments of third-party software, that try to undo the work of the compiler.
A decompiler is a tool that allows to extract a source code-like representation starting from binary programs, and can be of great help to understand the behavior of such software.
In this thesis, we tackle a specific problem of the decompilation field, the recovery of high-level control constructs.
To do this, we design novel control-flow restructuring techniques, and implement an entire decompiler tool on top of the rev.ng binary analysis framework. rev.ng is a binary translator tool, that is able to extract a raw representation for a binary, exploiting the LLVM and QEMU frameworks (in particular, a representation in terms of LLVM IR).
As output, we obtain C pseudocode in which we are able to emit high-level control-flow construct typical of the C programming language.
In the thesis, we perform extensive comparison of the produced output by our tool against the major decompiler solutions available on the market.
In addition to this, we also improve the translation capability of the rev.ng framework, a key feature that enable us to also produce binaries, in which the transformations applied by our decompiler stage are reflected in the executable form. This in turn, enable us to prove that the restructuring techniques, that we apply in order to emit the C pseudocode, preserve the functionality in the binary, thus suggesting their correctness

PhD Committee

Prof. **Alessandro Barenghi, DEIB -** Politecnico di Milano
Prof. **Biagio Cosenza**, Universita' degli Studi di Salerno
Prof. **Francesco Regazzoni**, University of Amsterdam