PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Raffaele Martino

XXXII Cycle

Training and Research Activities Report – Third Year

Tutor: prof. Alessandro Cilardo

Table of Contents

1. Information

Raffaele Martino

- Master's Degree in Computer Engineering, magna cum laude, awarded by University of Naples Federico II in 2016
- Ph.D. student of the XXXII Cycle of the ITEE Course, at the University of Naples Federico II
- No Fellowship
- Tutor: prof. Alessandro Cilardo
- Collaboration from March 2018 with the Department of Agriculture of the University of Naples Federico II under subsequent grants from the Regione Campania programme "URCoFi – Unità Regionale di Coordinamento Fitosanitario"

2. Study and Training Activities

Credits Summary

	Credits year 3							
		1	2	3	4	5	6	
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary
Modules	**0**	1.2	6	0	0	0	0	**7.2**
Seminars	**0**	0	0.3	0	0	0	0	**0.3**
Research	**60**	8.8	3.7	10	10	10	10	**52.5**
	60	10	10	10	10	10	10	**60**

Courses

- "Data Science and Optimization", **ad hoc module** held by Prof.Manlio Gaudioso, Prof. Laura Palagi and Prof. Enza Messina, February 2019: 1.2 ECTS acquired on 07/02/2019
- "Strategic Orientation for STEM Research & Writing", **improvement research skills module** held by Dr. Chie Shin Fraser, March - April 2019: 6 ECTS acquired on 08/04/2019

Seminars

- "IEEEXplore Training and Authorship Workshop", **seminar** held by Dr. Eszter Lukacs on 04/04/2019: 0.3 ECTS

3. Research Activity

Exploring the SHA-2 Design Space

Cryptographic hash functions underlie many aspects of our everyday life today. Thanks to their properties, they are the cornerstone of many security applications and protocols where tampering with either the content of the messages, or the identity of the sender, or both, is to be avoided. With the phasing out of once-popular hash algorithms such as MD5 and SHA-1 due to security vulnerabilities, SHA-2 is the most commonly used hash function nowadays.

Traditionally, their application domain has been network security, usually over the Internet. In this context, client devices can be safely assumed to be sufficiently powerful to perform the relatively limited number of hash computations required by the security protocols, while servers can possibly benefit from hardware acceleration of the hash operation. The hardware accelerator is designed to deliver the maximum possible throughput, typically at the cost of increased area and power consumption.

However, in recent years the peculiar properties of cryptographic hash functions have made them the essential ingredient for emerging innovative applications, like blockchains and distributed ledgers, involving a wide range of platforms from high-end servers down to resource-constrained Internet of Things (IoT) devices. The Bitcoin mining process, which heavily relies on the SHA-2 hash function, is extremely demanding in terms of energy efficiency, even making its profitability uncertain from the miner's standpoint. Additionally, the development of new domains such as IoT, with its low-cost, battery-powered devices needing to communicate securely, has also contributed to an increased demand for area-efficient and energy-efficient accelerators to be paired with the resource-constrained main processor.

Driven by the diverse stets of requirements posed by emerging applications, a number of different design techniques have been introduced, targeting the optimisation of area, energy or power consumption of the resulting SHA-2 accelerator. Many of these techniques still deliver an increased throughput, but without excessive area or power penalties. Nevertheless, there are also optimisation techniques. which are keen to sacrifice throughput in order to achieve significant area or power savings. One of the contributions of the research activity is to provide a classification of the design techniques which have been proposed for the design of the SHA-2 accelerator, and a systematic, evidence-supported analysis of the impact of each technique on the application requirements. These findings can be useful for the designer who is confronted with the task of designing a SHA-2 hardware accelerator under a given set of performance, area, energy and power requirements.

The choice of the best design alternative to meet a specific set of requirements is influenced also by the specific technological features of the hardware which will be used to physically realise the accelerator, the impact of which is often difficult if not impossible to estimate on paper. One of the reasons for this is that many low-level characteristics of the target technology are not made known by the manufacturer, but are only available to the algorithms used by vendor-specific Computer-Aided Design (CAD) and Integrated Development Environment (IDE) tools used to translate the Hardware Description Language (HDL) description of the architecture into a physical circuit. Therefore, the fulfilment of strict requirements may force the designer to implement a number of alternatives in order to compare their actual performance.

In order to simplify this activity, an evaluation framework has been proposed, which allows to obtain different architectures of the SHA-2 core simply by reconfiguring a number of parameters. This framework is particularly useful when the designer wants to evaluate a design originally proposed for a different application. In such a case, the design may take advantage of hypotheses specific to the original application, which are no longer valid in the context at hand. The proposed framework allows to evaluate each design without taking into account such assumptions.

A greater degree of control over the impact of the target technology over the implementation results can be obtained by working at a level lower than the Register Transfer Level (RTL). This makes it possible to take advantage of specific features of the target technology in order to achieve further gains in the optimisation objective. Therefore, one of the contributions of the research activity is the proposal of an architecture of the SHA-2 accelerator for the Xilinx 7-series Field Programmable Gate Array (FPGA) family, capable of achieving the best area efficiency reported in the literature. This architecture has been designed at the level of the structural components of the 7-series FPGA.

An Integrated Platform for Agricultural Metereology Management and Planning

Collaboration with the Department of Agriculture of the University of Naples Federico II under subsequent grants from the Regione Campania programme "URCoFi – Unità Regionale di Coordinamento Fitosanitario"

The increasing diffusion of Precision Agriculture methodologies requires the timely availability of relevant weather data for supporting decisions about farm management. For instance, the decision about whether, when and how much to use a given pesticide can be tailored to the expected diffusion of the insect, which can be estimated from knowledge of the conditions which favours its development. A simulation model, based on such knowledge, can forecast the diffusion of the insect in an area of interest in response to a given weather trend provided as input.

Local authorities typically develop their own web-based platforms for providing agricultural metereology data, which are updated by technicians who manually collect data from the monitoring networks, check them for quality and make the data available. On the other end, simulation models which have been implemented in software requires manual intervention to be fed with relevant data in the proper format. To date, there is no single integrated platform capable of managing the whole life cycle of the agricultural metereological data, and of supporting agricultural decisions, according to the technical literature. The development of such a Spatial Decision Support System (SDSS) is the ultimate goal of the URCoFi research programme.

The overall planned architecture for the system is shown in Figure 1. One feature of the proposed system is the capability of integrating data from different sources, both from "institutional" monitoring network and from low-cost stations, which have been developed within the URCoFi programme with the aim of improving monitoring coverage. This data integration in a single data base is performed by the main engine of the system, called *WeatherProg*, which performs also quality controls and data reconstruction where appropriate.

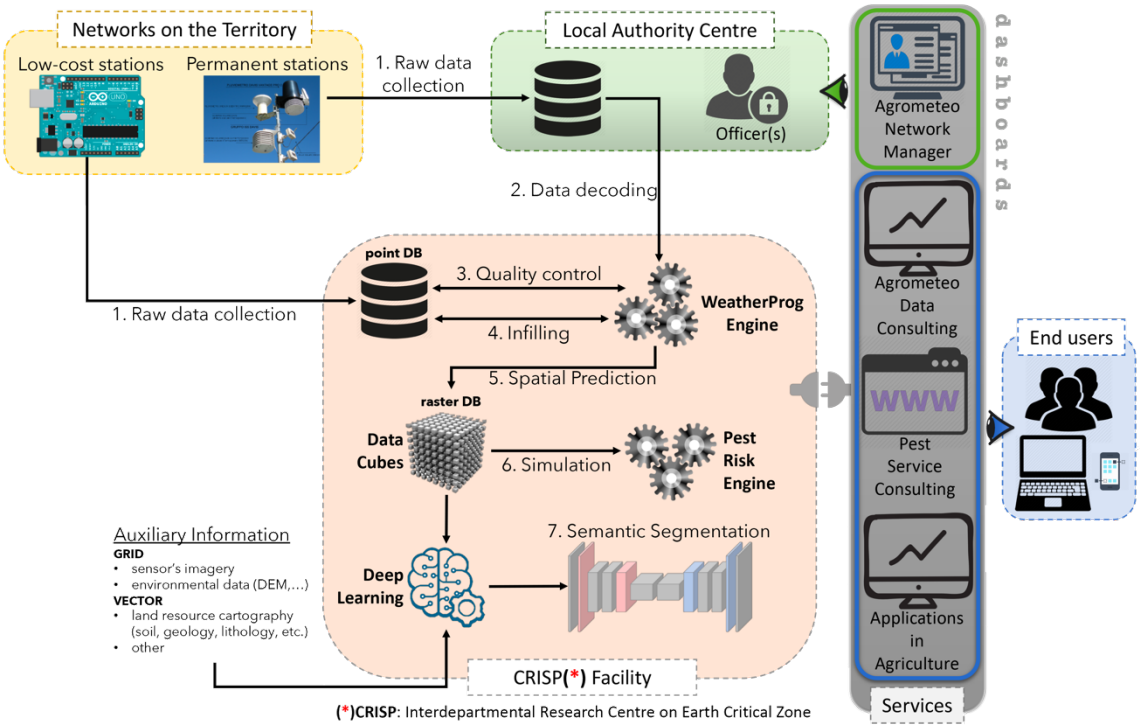

Figure 1: Overall planned architecture for the proposed Spatial Decision Support System

The contribution to the system has been manifold. First, the whole data management strategy has been overhauled, starting from a complete redesign of the climatic data base and the data collection server for the low-cost station. An appropriate API has been defined for WeatherProg to properly access data with policies put in place to minimise risks of data corruption. Also, the end-user interface has been redesigned from scratch, taking into account the needs and instances brought forward by intended users. Another area of activity has been the low-cost station, data from which has been analysed for validation purposes. The comparison with nearby-located institutional station has been quite satisfactorily, apart from some discrepancies which can be put down to deployment imperfections.

Furthermore, work has been done towards the acceleration of spatial interpolation algorithms on GPUs. Since they operate on a raster map, and their output for each point of the raster depends on climatic values in neighbouring points, these algorithms are particularly well-suited for GPU acceleration. One example is PRISM (Parameter-Elevation Regression on Independent Slopes Model), an algorithm for computing digital climatic maps from point-based data, i.e. measurements from climatic stations. Initial implementation results show the potential for real-time digital climatic maps production at the hourly time scale at the national level.

4. Products

International Conference papers

- R. Martino, A. Cilardo, "A Configurable Implementation of the SHA-256 Hash Function'", *Proceedings of the 14th International Conference on P2P, Parallel, Grid, Cloud and Internet*

Computing (3PGCIC 2019), in Advances on P2P, Parallel, Grid, Cloud and Internet Computing, in Lecture Notes in Networks and Systems, vol. 96, 2020, pp. 558-567, DOI: 10.1007/978-3-030-33509-0_52.

- **R. Martino**, M. Nicolazzo, M. Crimaldi, G. Langella, "A low-cost movable station for fast and effective agroclimatic monitoring". *Proceedings of the 2nd International Workshop on Metrology for Agriculture and Forestry (METROAGRIFOR 2019)*, Portici, Italy, Oct. 24-26, 2019, DOI: 10.1109/MetroAgriFor.2019.8909248.
- **R. Martino**, M. Nicolazzo, G. Langella, "Towards efficient production of digital climatic maps for the Campania Region". *Proceedings of the 2nd International Workshop on Metrology for Agriculture and Forestry (METROAGRIFOR 2019)*, Portici, Italy, Oct. 24-26, 2019, DOI: 10.1109/MetroAgriFor.2019.8909232.
- **R. Martino**, M. Nicolazzo, G. Langella, "A full integrated system for agroclimatic and pest monitoring at farm and landscape scales in Campania Region", *Proceedings of the 1st International Workshop on Metrology for Agriculture and Forestry (METROAGRIFOR 2018)*, in IOP Conference Series: Earth and Environmental Science, 2019, vol. 275, nº 12007, DOI: 10.1088/1755-1315/275/1/012007.

International Journal papers

- **R. Martino**, A. Cilardo, "SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey". *IEEE Access* (accepted for publication), DOI: 10.1109/ACCESS.2020.2972265.
- **R. Martino**, A. Cilardo, "A Flexible Framework for Exploring, Evaluating, and Comparing SHA-2 Designs", *IEEE Access*, vol. 7, 2019, DOI: 10.1109/ACCESS.2019.2920089.

5. Conferences and Seminars

METROAGRIFOR 2019

2nd IEEE International Workshop on Metrology for Agriculture and Forestry

- Venue: Reggia di Portici, Portici, Italy
- Date: 24-26/10/2019
- Presented papers:
  - "Towards efficient production of digital climatic maps for the Campania Region"
  - "A full integrated system for agroclimatic and pest monitoring at farm and landscape scales in Campania Region"

6. Tutorship

Tutorship activities grant from the University

- Grants from the University of Naples "Federico II" to perform tutorship activities for students attending the 1st year of the B.Sc. for the academic years 2018/2019 and 2019/2020:
- Provided tutorship to students of the course of "Fondamenti di Informatica"
- 7 hours under the 2018/2019 grant
- 41 hours under the 2019/2020 grant