PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Domenico Argenziano

XXX Cycle

Training and Research Activities Report – First Year

Tutor: Alessandro Cilardo

1. Information

Domenico Argenziano - Laurea Magistrale in Ingegneria Informatica - Università degli studi di Napoli "Federico II"

XXX Cycle- ITEE – Università di Napoli Federico II

No fellowship

Tutor: Alessandro Cilardo

2. Study and training

I attended the following MSc Courses:

- Metodi Algebrici per la crittografia (6 CFU)
- Calcolabilità e complessità (6 CFU)

These I attended to gain fundamental knowledge in order to deal with algebraic and complexity aspects of my research line, which focus around security and cryptography.

A large part of study anyway was self-study, given the need to deepen the knowledge of a complex subject such cryptography. For example, many advanced algebra topic are hard to find in common courses and are dealt with in very specialized books.

I also attended:

- Sistemi Real-Time (6 CFU)
- Elaborazione numerica dei segnali (6 CFU)

In order to integrate my background in embedded systems.

Seminars attended:

- *Modelli matematici e calcolo scientifico nell'ingegneria e nell'innovazione tecnologica.* (Lecturer: prof. Alfio Quarteroni) (0.6 CFU)
- *Memory technologies and tracing techniques in Android* (lecturer: Luca Porzio from Micron SRL) (0.4 CFU)
- *Play with connectome – Challenges and opportunities from in-vivo imaging of brain function and structure.* (lecturer: dr. Marco Aiello) (0.2 CFU)

3. Research activity

My research work in the first year of I dealt with topics in the security field, both for server/cloud computing systems and for embedded systems. Firstly, I focused around a new exciting topic in cryptography: homomorphic encryption, which allows a machine to perform arithmetic operations directly on ciphertexts, with no call for decryption. This allows a user to delegate computation on sensitive data to a third untrusted party, such as a cloud server, in encrypted form, ensuring this way confidentiality.

Homomorphic encryption, though, suffers from a very high computational cost, which makes it still unsuitable for real life applications. Anyway, remarkable progresses in the mathematics field have lead to new alternative homomorphic schemes, with lower computational complexity. Besides, homomorphic encryption can benefit from the design of ad hoc acceleration solutions and since my research line is in Computer Architecture and Reprogrammable Hardware, my tutor and I aimed to give our contribution on this second perspective.

In order to deal with such a complex matter, I had to extend my knowledge in the algebra and number theory field, and study aspects of computational complexity theory topics. I acquired such training by attending suitable classes and by extensive self-study.

Accelerating homomorphic encryption required also studying the best algorithms for the underlying operations, which are mostly modular arithmetic operations on very long operands.

So I concentrated on developing an FPGA-based accelerator to be used in an heterogeneous server to accelerate cryptographic primitives and I started, of course, by studying the state-of-the-art in homomorphic encryption acceleration in order to devise my own contribution.

A first important step was the design and development of an FPGA-based Integer FFT unit to be used in the Stonhage-Strassen algorithm implementation. Our design improved over existing solutions with respect to area usage and performance. In this context, I followed and keep following the work thesis of the M.Sc. student Stefano Marano, which contributed with the development of part of the accelerator and its testing.

Another thesis work I'm currently following is that of Antonio Crispino, who is working on an FPGA-optimized solution for long size addition.

Currently my tutor and I are working on a project proposal which aims to integrate homomorphic encryption together with Information Flow Control techniques. This would allow to mix computing on encrypted and plain-text data while preserving confidentiality and preventing information leakage.

In July I won a fellowship for a research work to do in the project WISCH, by prof. Clemente Galdi. The activity focuses on security in embedded and in particular mobile devices and the objective is to develop a cryptographic filesystem which runs in a Trusted Execution Environment and is able to enforce security policies. After an initial study of underlying platform and current standards, we have designed an overall architecture and worked out some of the problems that arised.

4. Products

We presented our homorphic accelerator solution to the Altera's "Innovate Europe Design Contest 2015" and our project won the *Best project in SoC design* award.

With my tutor, I wrote two articles, one for the "10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing" and the other for "3rd International Workshop on Cloud and Distributed System Applications (CADSA-15)". Both articles have been accepted.

Another article has been written and submitted for the "Design Automation and Test in Europe (DATE16)" conference.

5. Conference and seminars

In May I hold an internal seminar for my research group, which focused around the explanation of algebraic and implementation aspects of homomorphic encryption.

7. Tutorship

Support to the thesis work of MSc student Stefano Marano on an FPGA accelerator for Number Theoretic DFT and its testbed (33 Hours).

Support to the thesis work of MSc student Antonio Crispino on an FPGA optimized adder for very long operands (4 Hours).

Assistence to my tutor during a final exam of Calcolatori Elettronici I (3 hours).