PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Antonella Cioffi

XXXIV Cycle

Training and Research Activities Report – Second Year

Tutor: Prof. Pasquale Arpaia – co-Tutor: Francesco Bonavolontà

1. Information

I received the M.Sc. Degree, cum laude, in Electronic Engineering from University of Napoli 'Federico II' in October 25^{th} 2018 with the thesis "Metrological Characterization of AR/BCI-based instrumentation for maintenance in Industry 4.0".
I belong to XXXIV cycle of Information Technology and Electrical Engineering (ITEE) PhD. My fellowship is financed by ST Microelectronics. My tutor is Prof. Pasquale Arpaia.

2. Study and Training activities

In the second year of PhD program, I attended the following seminars and courses:

a. Modules
- Misure su sistemi wireless (10/2018 – 06/2019), Leopoldo Angrisani, 9 CFU
- Intelligenza Artificiale ed Etica: La ricerca in IA alla prova delle sfide etiche (06/12/2019), Daniele Amoroso, Piero A.Bonatti, José M.Galvan, Riccardo Guidotti, Paola Invernardi, Roberto Prevete, Luciano Serafini, Viola Schiaffonati, 1.5 CFU

b. Seminars
- Introduction to CERN and wakefield measurements at CLEAR (18/11/2019), Antonio Gilardi, 0.2 CFU
- Security attacks and countermeasures to smart card products (28-29/11/2019), Brightsight
- Numerical methods for modeling, simulation and control for soft robots or robots in interaction with deformable environment (14/01/2020), Christian Duriez, 0.2 CFU
- Elettromagnetismo e salute (09/04/20), Rita Massa, 0.4 CFU
- Computational Biology: Large scale data analysis to understand the molecular bases of human diseases (09/04/20), Michele Ceccarelli, 0.2 CFU
- Virtualization technologies and their applications (06-07/04/20), Luigi De Simone, 0.4 CFU
- How to get published with the IEEE? (20/04/20), IEEE, 0.4 CFU
- Non-invasive mapping of electrical properties using MRI (11/06/20), Riccardo Lattanzi, 0.3 CFU
- PhD School Italo Gorini 2020 (04-09/09/20), 2.4 CFU
- Analisi avanzate con l'utilizzo dell'oscilloscopio (12/10/20), Rohde & Schwarz, 0.2 CFU
- Valutazione dei livelli di esposizione e del rispetto dei limiti Antenne e 5G Prof. MD Migliore, Un Cassino e Lazio Meridionale,
  Misure di segnali complessi nell'ambiente: Sistemi 5G, Dr. D. Franci, Arpa Lazio,
  Estrapolazioni su segnali 4G e 5G, Dr. S. Adda, Arpa Piemonte, Dr. S. Pavoncelli Arpa Lazio, (20/10/20), 1 CFU.

c. External courses

During the 2^{th} year I didn't attend external courses.

	Credits year 2							
		1	2	3	4	5	6	
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary
Modules	10	1,5	0	9	0	0	0	**11**
Seminars	5	0,2	0,2	1,4	0,3	0	3,6	**5,7**
Research	45	9	7	8	7	7	8	**46**
	60	11	7,2	18	7,3	7	12	**62**

3. Research activity

During the second year of PhD course, my research activity concerned the study and the evaluation of countermeasures for protecting the Internet of Things devices against the side-channel attacks and fault attacks.

The presence of Internet of Things devices in unsupervised environment makes the cryptographic algorithms inefficient to guarantee the data security. In fact, an attacker can exploit the leakage information, as power consumption, electromagnetic radiation, time, and noise to identify the secret key of the algorithm and discover all the confidential data. For this reason, software and hardware countermeasures were developed. These enforce the robustness of cryptographic algorithms, making it very difficult for an attacker to break the system.

In a first work, I inserted typical countermeasures against power attack in a software implementation of Advanced Encryption Standard algorithm, as delay insertion, shuffling, and masking, and I demonstrated the robustness offered by such countermeasures in terms of power traces needed to discover the secret key of the cryptographic algorithm. Another work involved evaluating of software countermeasures against fault attacks in terms of time and memory coverage. In both these works, a measurement architecture was realized. The first one to acquire power consumption from the cryptographic device, while the second one to measure the time spent by the for the execution of a command, in order to evaluate the increment of time due to the countermeasures.

Collaborations: ST Microelectronics in Marcianise

4. Products

a. Publications as Journal paper

I. P. Arpaia, F. Bonavolontá, & **A. Cioffi**. (2020). Problems of the Advanced Encryption Standard in protecting Internet of Things sensor networks. *Measurement*, 107853.

b. Publications as Conference paper

I. L. Angrisani, P. Arpaia, F. Bonavolontá, & **A. Cioffi**. "Experimental test of ECDSA digital signature robustness from timing-lattice attack". In *2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)* (pp. 1-6). IEEE.

II. P. Arpaia, F. Bonavolontá, & **A. Cioffi**. "Security vulnerability in Internet of Things sensor networks protected by Advanced Encryption Standard". In *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT* (pp. 452-457). IEEE.

c. Publications in preparation:

I. "Measurement and assessment of countermeasures in protecting Internet of Things sensor networks" - P. Arpaia, F. Bonavolontá, & **A. Cioffi**.

II. "Optimization of Power Analysis attack parameters on an Internet of Things device using the Taguchi method" - P. Arpaia, F. Bonavolontá, & **A. Cioffi**.

III. Performances measurement in presence of software countermeasures against fault attacks - P. Arpaia, F. Bonavolontá, & **A. Cioffi**.

5. **Conferences and Seminars**
   IEEE International Instrumentation & Measurement Technology Conference (I2MTC) – online – May 2020 – Paper presented by me as oral

   IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT) – online – June 2020 – Paper presented by me as oral

6. **Activity abroad**
   During my 2^{th} PhD year I didn't spend time aboard.

7. **Tutorship**
   During my 2^{th} PhD year I didn't make tutorship activity.