
**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 – First 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 first year of PhD program, I attended the following seminars and courses:

a. Modules
- Author Seminar: How to publish a scientific paper (26/11/2018), Aliaksndr Birukou and Elisa Magistrelli, 0.4 CFU
- Ciberconflitti, sicurezza informatica, difesa, stabilità internazionale e diritto umanitario (28/11/2018), Gian Piero Siroli, Francesco Vestito, Simon Pietro Romano, Daniele Amoroso, 0.8 CFU
- Advanced techniques for software robustness and security testing (01/2019 – 04/2019), Roberto Natella, 3 CFU
- Data Science and Optimization (05-06-06/02/2019), Manlio Gaudioso, Laura Palagi, Enza Messina, 1.2 CFU
- Machine Learning e applicazioni (03/2019 – 06/2019), Roberto Prevete, 6 CFU
- Machine Learning (05/2019), Anna Corazza, Francesco Isgrò, Stefano Olivieri, Roberto Prevete, Carlo Sansone, 5 CFU
- Instrumentation and measurement Ph.D. School "Italo Gorini 2019", 4 CFU

b. Seminars
- Matlab and Embedded System (28/03/2019), Stefano Marrone, 0.4 CFU
- Wireless communications and sensor (10/04/2019), Filippo Colaianni – ST Microelectronics, 0.7 CFU
- Microcontrollers and artificial intelligence (10/04/2019), Danilo Pau – ST Microelectronics, 0.8 CFU
- Simscape for design (21/05/2019), Francesco Alderisio, 0.6 CFU
- In-network Machine Learning for Networks (14/06/2019), Roberto Bifulco, 0.4 CFU
- Ethics, science & society in Brain Computer Interface (18/10/2019), Pim Haselagerv, 0.6 CFU

c. External courses
During the $1^{th}$ year I didn't attend external courses.

| | Credits year 1 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | |
| | Estimated | bimonth | bimonth | bimonth | bimonth | bimonth | bimonth | Summary |
| **Modules** | 20 | 1,2 | 1,2 | 3 | 11 | 0 | 4 | **20,4** |
| **Seminars** | 5 | 0 | 0 | 1,9 | 1 | 0 | 0,6 | **3,5** |
| **Research** | 35 | 5 | 5 | 5 | 7 | 7 | 8 | **37,0** |
| | 60 | 6,2 | 6,2 | 9,9 | 19 | 7 | 13 | **60,9** |

3. Research activity

My research activity is about "Phenomenological Approach to Cyber Security based on Electronic Measurements".

Today's society is witnessing growth of intelligent objects that collect and share information to improve the quality of life [1]. Informatic system security is the primary requirement to guarantee confidentiality and integrity of data. Typically, cryptographic algorithms are used for this purpose.

Two categories of cryptografic algorithms exists: (i) symmetric algorithms that use the same key to encrypt and decrypt the data and (ii) asymmetric algorithms that use a private key to sign a message and a public key to verify that the message was created by someone possessing the corresponding private key.

In the context of embedded devices, physic attacks undermine the security [2]. These attacks, known as side-channel attacks, exploit the leakage information, as power consumption electromagnetic radiations, time and noise, to break system's security. Power analysis attack [3] is one of the most popular and volatile side-channel attack. For this kind, the power consumed by the system to execute its operations is used to identify the cryptographic technique implemented and the secret key.

My reaserch activity takes care to analize the security of embedded devices that implement symmetric and asymmetric cryptographic algorithms from side-channel attacks. In my first work the security of the Advanced Encryption Standard [4] was examined. Power traces were collected through an active circuit with low-noise and high bandwidth analogue components and then analyzed with statistical operations proper to a side-channel attack known as scatter attack [5].

Collaborations

ST Microelectronics in Marcianise

References:

[1] J.Deogirikar and A. Vidhate, "Security attack in iot: A survey", in *2017 International Conference on I-SMAC (IoT in Social , Mobile, Analytics and Cloud), IEEE, 2017, pp. 32-37.*

[2] M. Navir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks", in 2016 3rd International Conference on Electronic Design (ICED). IEEE, 2016, pp. 321-326.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", in *Annual International Cryptology Conference. Springer, 1999, pp. 338-397*.

[4] L. Daemen and V.Rijimen, "Aes proposal: Rijndael", 1999.

[5] H. Thiebeauld, G. Gagnerot, A. Wurcher, and C. Clavier, "Scatter: A new dimension in side channel attack", in *International Workshop on Constructive Side-Channel Analysis and Secure Design. Springer, 2018, pp. 135-152.*

4. **Products**
    a. Publications in preparation
        - Pasquale Arpaia, Francesco Bonavolontà, Antonella Cioffi, "Problems of the Advanced Encryption Standard in protecting Internet of Things sensor networks"

5. **Conferences and Seminars**
During my $1^{th}$ PhD year I didn't partecipate to conference.

6. **Activity abroad**
During my $1^{th}$ PhD year I didn't spend time aboard.

7. **Tutorship**
During my $1^{th}$ PhD year I didn't make tutorship activity.