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 – Third Year

Tutor: Prof. Pasquale Arpaia

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

a. Modules
- Statistical data analysis for science and engineering research (02/2021 – 03/2021), Roberto Pietrantuono, 4 CFU

b. Seminars
- The Ohta-Kawasaki model for diblock copolymers: stability and minimality of critical points (26/11/2020), Nicola Fusco, 0.2 CFU
- Patent Searching Best Practices with IEEE Xplore (21/11/2020), Eszter Lukacs (IEEE), 0.2 CFU
- Force and Visual Control for Safe Human–Robot Interaction (03/12/2020), Bruno Siciliano, 0.4 CFU
- 5G: l'architettura, le applicazioni e la rete di accesso radio (08/06/2021), Francesco Mollica, 0.4 CFU
- PhD School Italo Gorini 2021 (06-10/09/2021), 3.6 CFU

c. External courses

During the 3^{rd} year I didn't attend external courses.

Student: Antonella Cioffi									Tutor: Pasquale Arpaia								Cycle XXXIV									
antonella.cioffi@unina.it									pasquale.arpaia@unina.it																	
	Credits year 1								Credits year 2								Credits year 3									
		1	2	3	4	5	6			1	2	3	4	5	6			1	2	3	4	5	6			
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Total	Check
Modules	20	1,2	1,2	3	11	0	4	20,4	10	1,5	0	9	0	0	0	11	0	0	0	4	0	0	0	4	34,9	30-70
Seminars	5	0	0	1,9	1	0	0,6	3,5	5	0,2	0,2	1,4	0,3	0	3,6	5,7	3	0,8	0	0	0,4	0	3,6	4,8	14	10-30
Research	35	5	5	5	7	7	7	36,0	45	9	7	7	7	7	7	44	60	8	8	8	9	9	9	51	131	80-140
	60	6,2	6,2	9,9	19	7	12	60	60	11	7,2	17	7,3	7	11	60	63	8,8	8	12	9,4	9	13	60	180	180

Credit adjustments.

3. Research activity

During the third year of PhD course, my research activity concerned the study and the improvement of power attack efficiency against the Internet of Things devices. The improvement of power attack efficiency is aimed at decreasing the effort and the time needed to find the secret key in a cryptographic algorithm.
To reach this goal, a fractional experimental design was implemented in order to identify the parameter values maximizing the number of correctly discovered key byte with the minimum cost of the attack in terms

of time and resources. The proposed method also contributed to a more detailed description of the attack procedure and to the increase in the repeatability and reproducibility of the Vulnerability Assessment of Internet of Things transducers.
Another task that I faced during the third year of PhD course is the performance characterization of an embedded system.

Collaborations: ST Microelectronics in Marcianise

4. Products

a. Publications as Journal paper

I. Arpaia, P., Bonavolontà, F., **Cioffi, A**., & Moccaldi, N. "Power Measurement-based Vulnerability Assessment of IoT medical devices at varying countermeasures for cybersecurity". *IEEE Transactions on Instrumentation and Measurement*, 2021.

II. Arpaia, P., Bonavolontà, F., **Cioffi, A.,** & Moccaldi. "Reproducibility Enhancement by Optimized Power Analysis Attacks in Vulnerability Assessment of IoT Transducers". *IEEE Transactions on Instrumentation and Measurement*, *2021*.

b. Publications as Conference paper
None

c. Publications in preparation:

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

II. Improving key deciphering with a machine learning-based side-channel attack relying on power trace measurements - P. Arpaia, **A. Cioffi**, & A. Esposito.

5. Conferences and Seminars

None

6. Activity abroad

During my 3^{rd} PhD year I didn't spend time aboard.

7. Tutorship

Supervising one student (for 6 months).