Antonella Cioffi

Tutor: Pasquale Arpaia –
co-Tutor: Francesco Bonavolontà

XXXIV Cycle - I year presentation

Phenomenological Approach to Cyber Security based on Electronic Measurements

Università degli Studi di Napoli
Federico II

Content

- My background
- Problem
- Research activity
- Products
- Next years

Background

Graduation:

- B.Sc. degree cum laude in Electronic Engineering from the University of Naples "Federico II" on October 27, 2016.
  Thesis: "Diagnostica di dispositivi elettronici attraverso l'uso di campi elettromagnetici"
- M.Sc. degree cum laude in Electronic Engineering from the University of Naples "Federico II" on October 25, 2018.
  Thesis: "Metrological characterization of AR-BCI based instrumentation for maintenance in Industry 4.0"

Fellowship:

- PhD Student of XXXIV cycle in Information Technology and Electrical Engineering (ITEE).
  Theme: "Phenomenological Approach to Cyber Security based on Electronic Measurements"
- My fellowship is financed by ST Microelectronics.

Cooperation

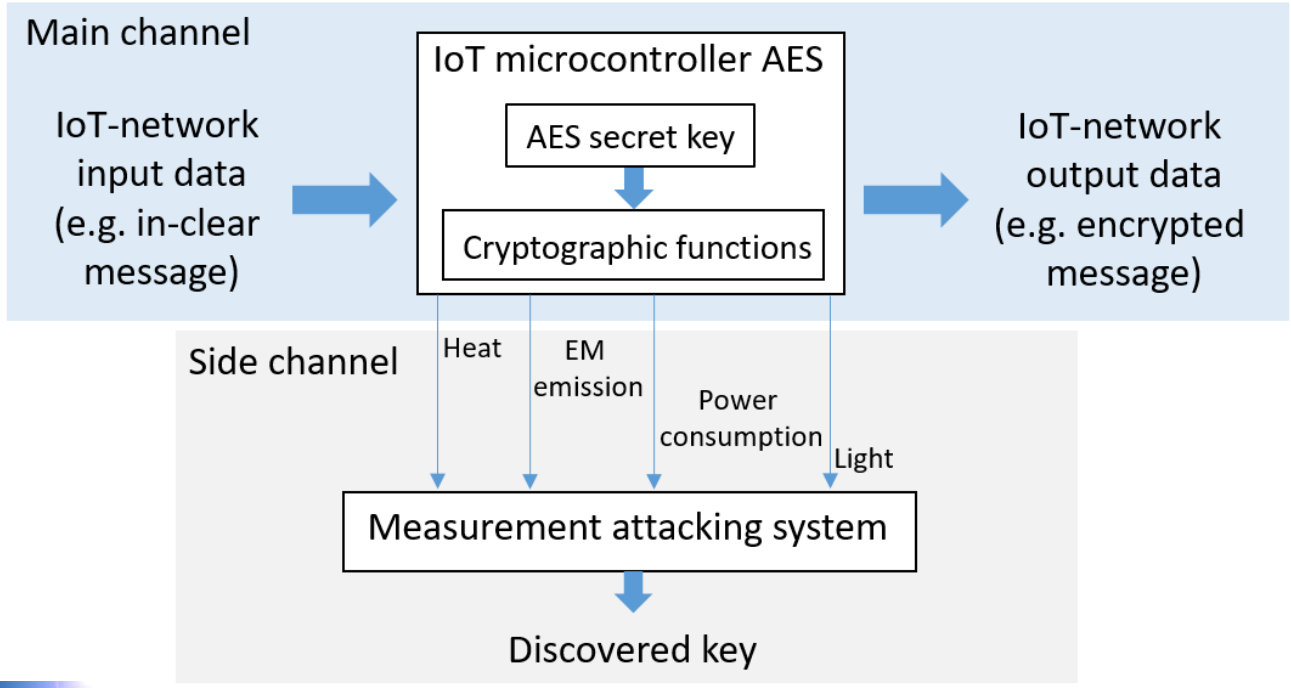
- Research Group: Prof. Pasquale Arpaia (tutor), Francesco Bonavolontà (co-tutor)
- Cooperation: ST Microelectronics in Marcianise

Problem

- Informatic systems security is the primary requirement to guarantee confidentiality and integrity of data.
- Cryptographic algorithms are typically implemented to ensure the information security.
- For embedded devices, the security is undermined also by physical attacks, known as side-channel attacks.

Problem

- Side-channel attacks consist in measuring unintended effects of the cryptographic algorithm computation from an embedded device, as power consumption, electromagnetic radiations, time and heat, to extract sensitive information, as the secret key.



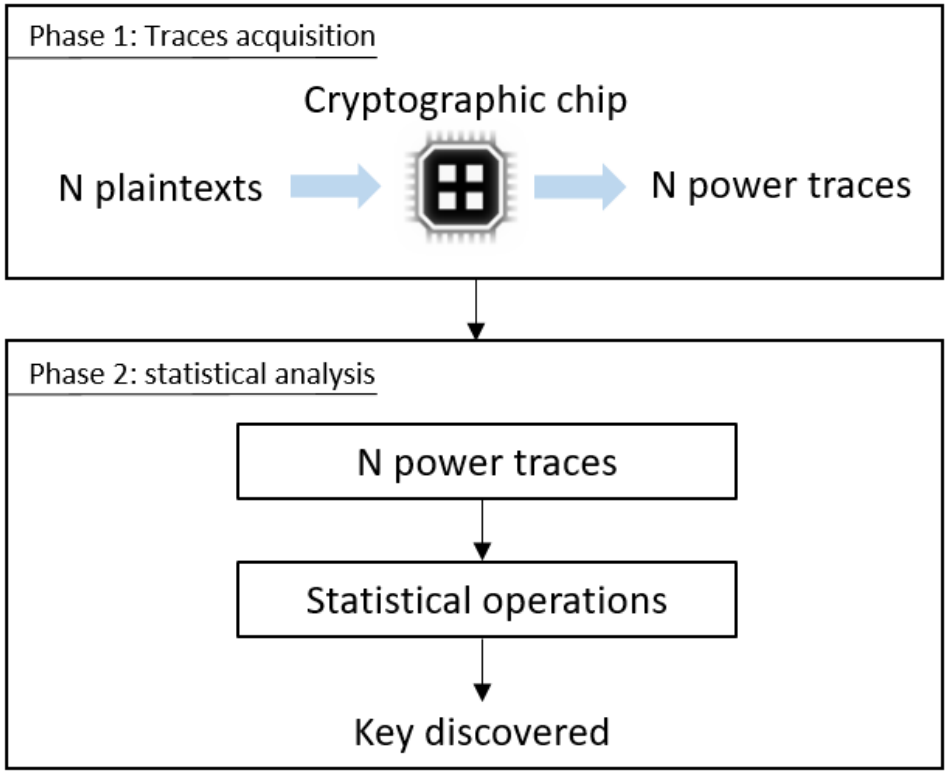
Research activity

- Prove experimentally the security vulnerability of the most used cryptographic algorithm in Internet of Things sensor networks, the Advanced Encryption Standard (AES).
- The AES was implemented on an microcontroller.
- The side-channel attack implemented was the scatter.

Research activity

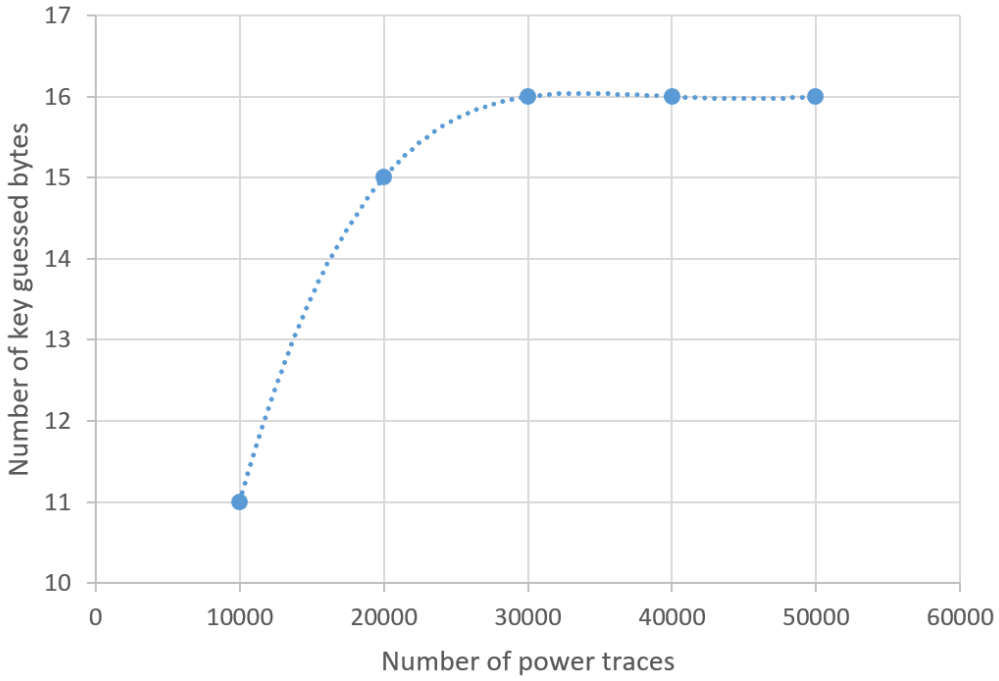
- The activity was divided in two phases:

1. Power traces acquisition
2. Statistical analysis



Research activity

- With at least 30,000 power traces, the attack is able to recover the secret key.



1st year production

- Pasquale Arpaia, Francesco Bonavolontà, Antonella Cioffi, **"Problems of the Advanced Encryption Standard in protecting Internet of Things sensor networks"** (to submit to a journal)

Next year

Research activity:

- Make the vulnerability analysis on EC-DSA (Elliptic Curve Digital Signature Algorithm) through a Timing Attack based on Lattice.

Conferences and PhD Schools:

- I2mtc conference, Dubrovonik, Croatia, May 25^{th} – 28^{th} 2020
- Italo Gorini PhD School, Reggia Calabria, Italy, September 2020

Credit Summury:

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									
	Estimated	1 bimonth	2 bimonth	3 bimonth	4 bimonth	5 bimonth	6 bimonth	Summary	Estimated	1 bimonth	2 bimonth	3 bimonth	4 bimonth	5 bimonth	6 bimonth	Summary	Estimated	1 bimonth	2 bimonth	3 bimonth	4 bimonth	5 bimonth	6 bimonth	Summary	Total	Check
Modules	20	1,2	1,2	3	11	0	4	20,4	10							0	0							0	20,4	30-70
Seminars	5	0	0	1,9	1	0	0,6	3,5	4							0	3							0	3,5	10-30
Research	35	5	5	5	7	7	8	37,0	45							0	40							0	37	80-140
	60	6,2	6,2	9,9	19	7	13	60,9	59	0	0	0	0	0	0	0	43	0	0	0	0	0	0	0	61	180

Thank you for your kind attention