Antonella Cioffi

Tutor: Pasquale Arpaia – co-Tutor: Francesco Bonavolontà

XXXIV Cycle - II year presentation

Security countermeasures in IoT devices: effectiveness and performance

RESEARCH ACTIVITY CONTEXT

The wide diffusion of Internet of Things technology opens the doors to several security challenges. Connected devices, located in the environment, are the target of various hardware attacks, as ***side-channel attacks*** and ***fault injection***. The formers are able to discover the secret key of cryptographic algorithms exploiting quantities as timimg, power consumption or electromagnetic emission, while the latter is able to bypass sensitive operations injecting faults into the device. Suitable countermeasures have been developed in literature to guarantee the security of all IoT devices.

MAIN RESEARCH ACTIVITIES OF THE YEAR

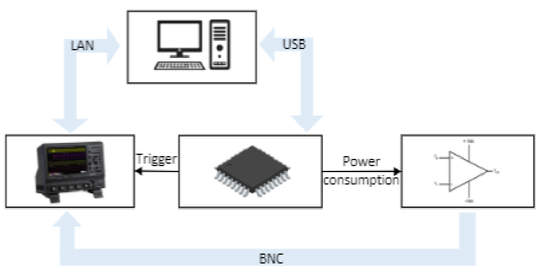
The main objective of the year is to evaluate the effectiveness and performances of countermeasures against power attacks and fault injections.

METHOD

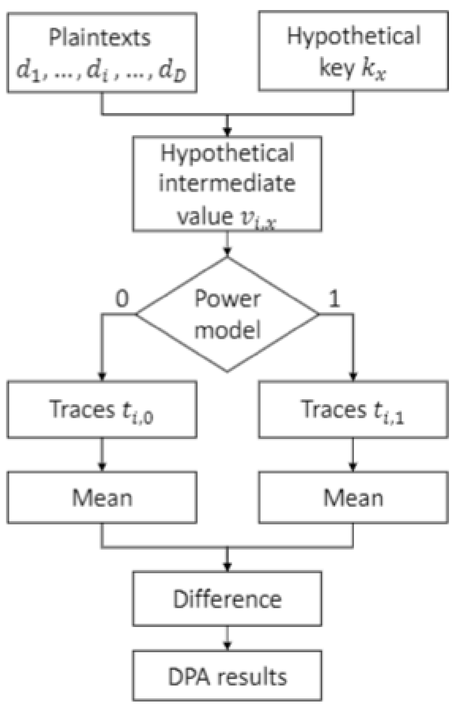
The evaluation of countermeasures effectivness against power attacks is made by comparing the number of traces needed to discover the secret key of a software implementation of AES-128 when the countermeasures are activated versus their absence. The countermeasures evaluated are random delay, random SBox, and masking, while the power attacks implemented are DPA, CPA, and scatter.

The implementation of each power attack consists of an acquisition phase (Fig. a) and a statistical one.

The Fig. b shows a flow diagram of the DPA.



(a)

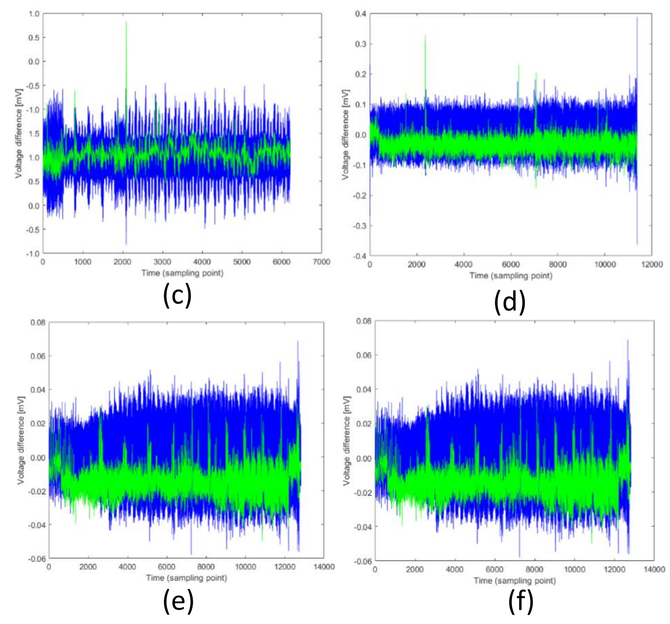


(b)

RESULTS

The attacks adopt a *divide and conquer* strategy, discovering separately the bytes of the secret key. For each key byte, a number of patterns coinciding with all the possible values of the key byte is obtained. The results of the DPA for the first key byte are shown for absence of countermeasures (c), for the random delay (d), for the random SBox (e), and for the masking (f).

The correct key byte is obtained only in absence of counter-measures and with random delay, where the peaks in the relative pattern (green) are evident. The Table, that shows the number of power traces needed to discover the secret key, highlights that random S-Box and masking give a major level of security.



(c) (d) (e) (f)

Countermeasure	DPA	CPA	scatter
None	200	200	30000
Random delay	400	400	> 30000
Random SBox	> 15000	15000	> 30000
Masking	> 30000	> 30000	> 30000

CONTACTS AND COLLABORATIONS

Email:
antonella.cioffi@unina.it

FUTURE DEVELOPMENTS

- Improving the power attacks by applying statistical methods and techniques.