UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD information technology electrical engineering

DIETI UNINA

Francesco Caputo

Power measurements attacks

Tutor: Pasquale Arpaia

Cycle: 37 Year: 2022

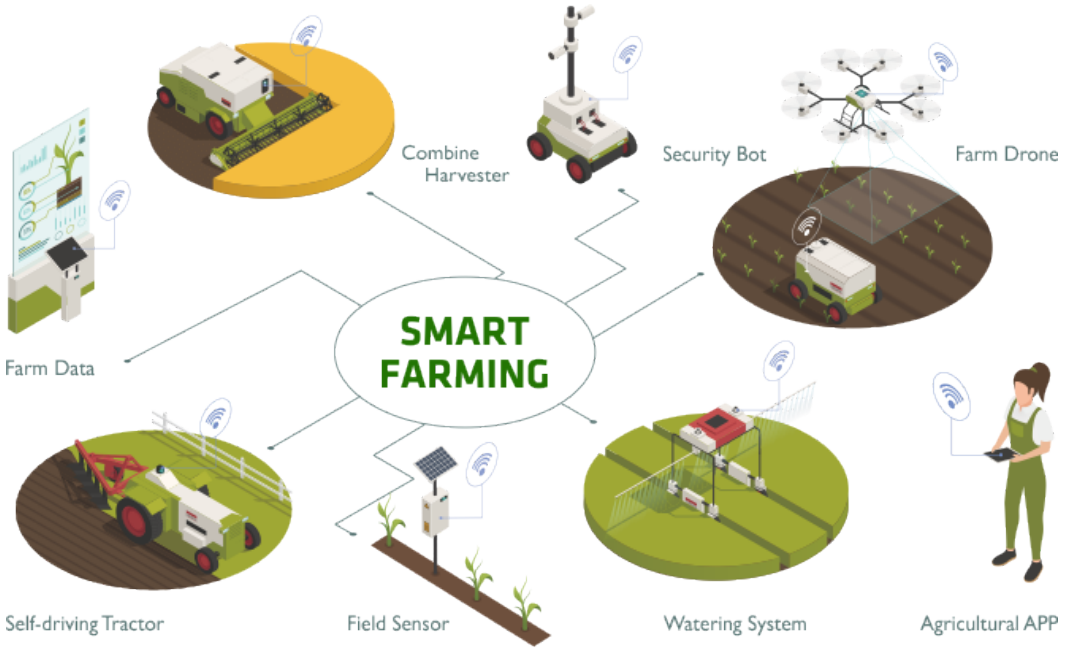
itee PhD information technology electrical engineering

My background

- MSc degree: Electronic Engineering (University of Naples “Federico II”)
- Research group/laboratory: ARHeMLab
- PhD start date: 01/01/2022
- Scholarship type: MUR PON

Research field of interest

- In the agrifood field, smart farms are increasingly used. Smart farms use connected smart sensors (IoAT) to
  - Collect data on field
  - Analyze data for decision making
  - Control actuators



Research field of interest

An **attack** is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission

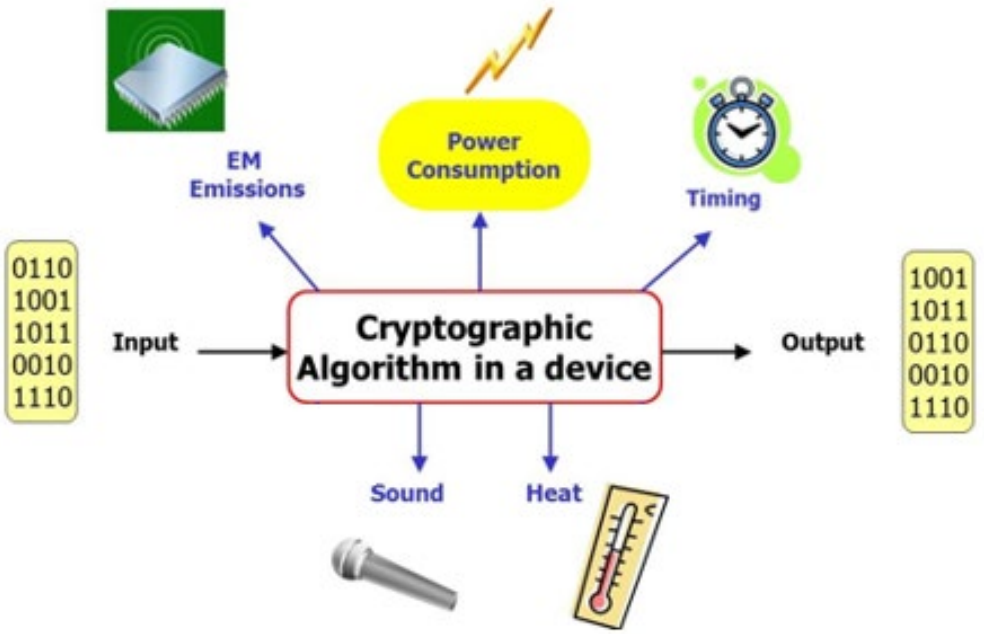
A **Side-Channel Attack** is a non-invasive attack aimed at extracting information that a particular system can exhibit

Summary of study activities

- Study of smart farm's IoT devices ecosystem and study on the state of the art concerning "side-channel attacks" using "machine learning" models.
- Period in the STMicroelectronics: functional and vulnerability tests of embedded "secure elements".
- Attended Ad hoc PhD courses of "Machine Learning" and "Statistical data analysis for science and engineering research"
- "Laboratorio di programmazione" course borrowed from MSc curricula for Python programming language used for Machine Learning
- Attended Seminars on focused on Cybersecurity

Research activity: Overview

Problem



Research activity: Overview

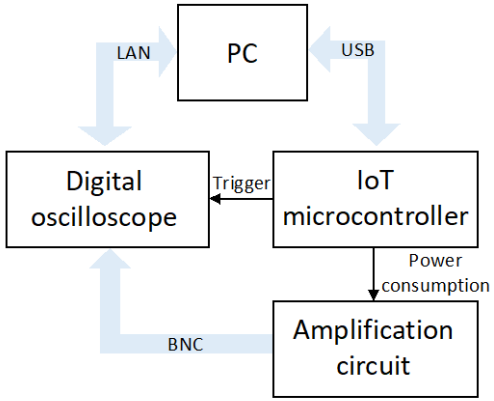
Objective

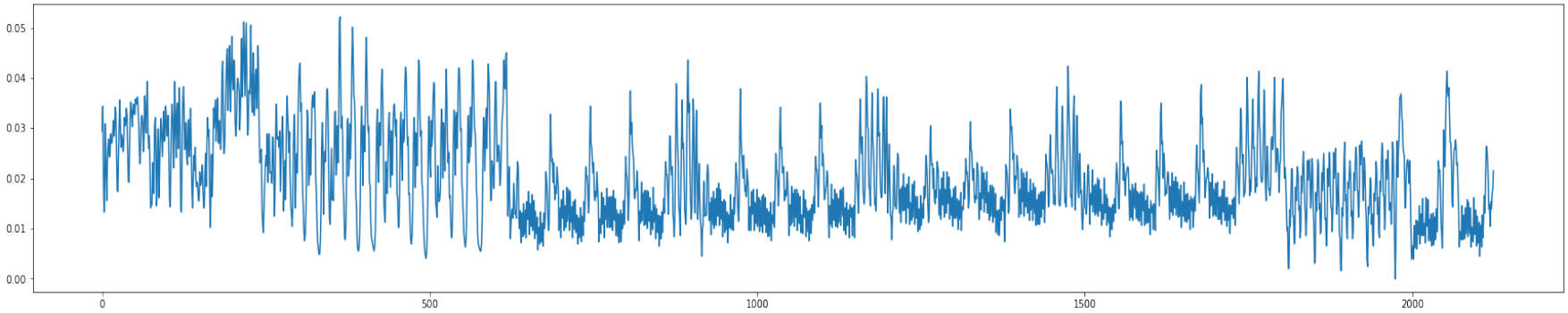
- Analyze leakages of a device power consumption
- Train a model to attack the device and discover the cryptographic key
- Assess the performance of a model for side-channel attacks. Among them, a widely used metric is the *guessing entropy*, which quantifies the number of guesses needed on average to recover the right (sub-) key in an enhanced brute force attack
- Assess the associated uncertainty for profiling side-channel attacks

Research activity: Overview

Metodology

A custom dataset was made using an automatic acquiring station

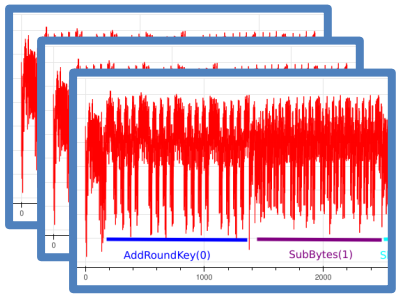


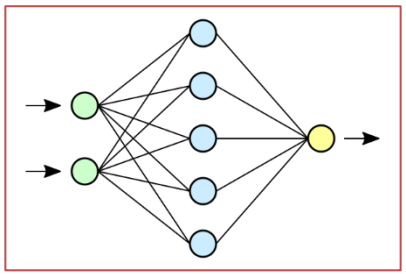


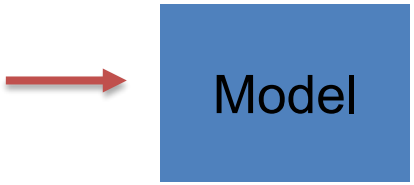
Research activity: Overview

Metodology

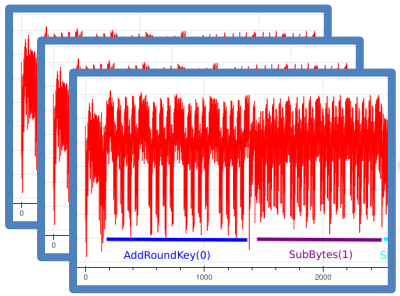
Traces are pre processed and used to Train the attack model

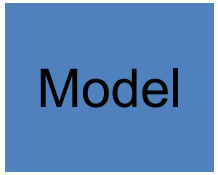


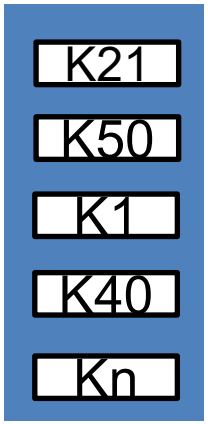


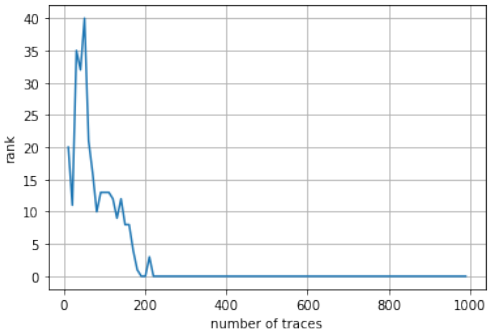


The model is used to attack the device and a rank was estimated





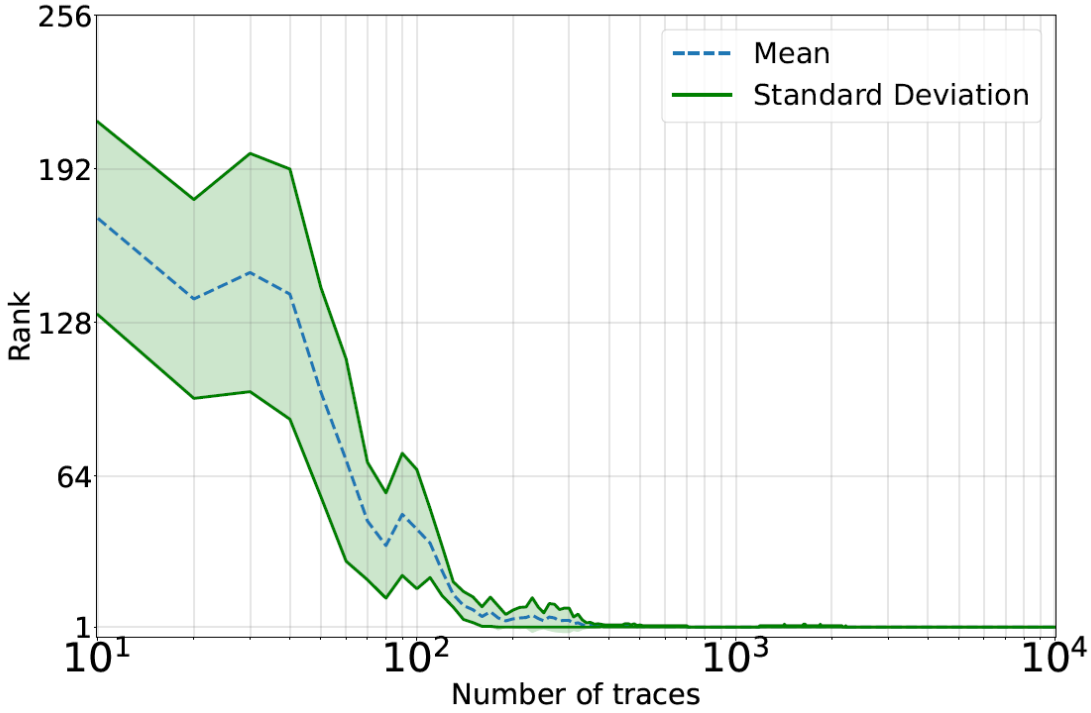




Research activity: Overview

Metodology

Multiple attacks are guessed to assess the attack uncertainty



Products (if any, otherwise remove)

[P1]	*Pasquale Arpaia, Francesco Caputo, Antonella Cioffi, Antonio Esposito, Francesco Isgrò, Uncertainty analysis in cryptographic key recovery for machine learning-based power measurements attacks, IEEE Transactions for Instrumentation and Measurements (submitted)*

Next Year

- Build a smart sensor network
- Study authentication of devices in a smart network
- Find unauthorized devices in the network by means of Machine Learning