Università degli Studi di Napoli Federico II

itee PhD information technology electrical engineering

DIETI UNINA

PON Ricerca e Innovazione 2014 - 2020

MUR

REACT EU SOSTENIAMO LA RIPRESA

Francesco Caputo

Machine learning based Side-Channel Attacks

Tutor: Pasquale Arpaia

Cycle: 37 Year: 2023

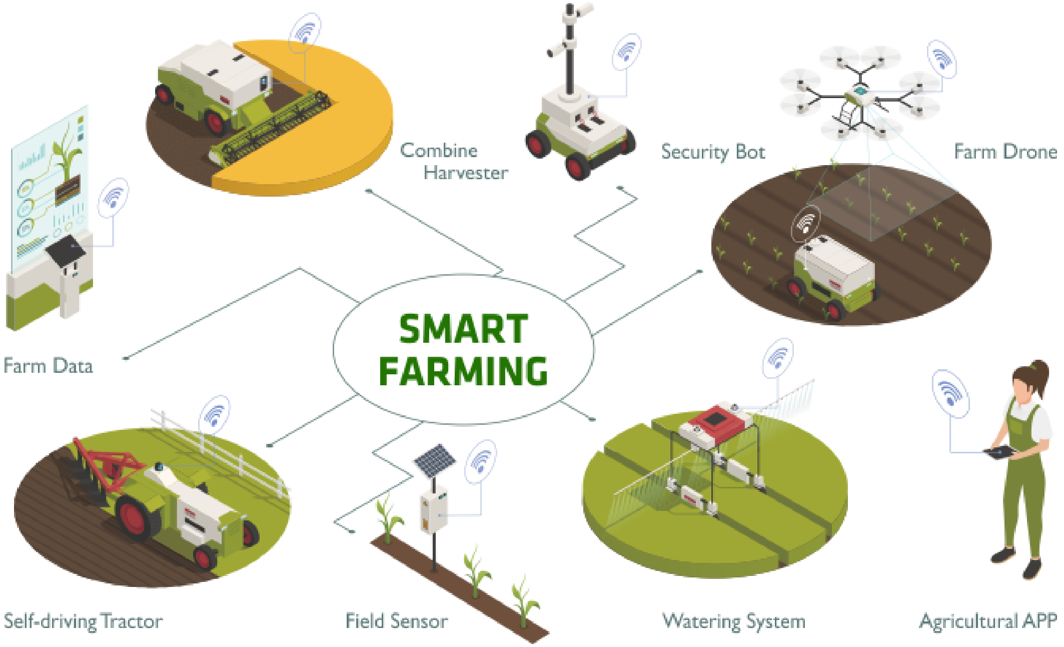
itee PhD information technology electrical engineering

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
- Industry period: 12 / 12 months
- Abroad period: 0 / 6 months

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

A **Secure Element** is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities

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

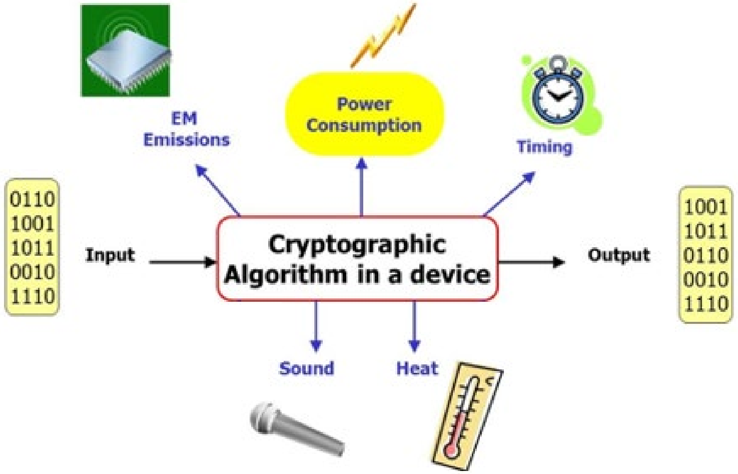
A **Side-Channel Attack** is a non-invasive attack aimed at extracting information that a particular system can exhibit

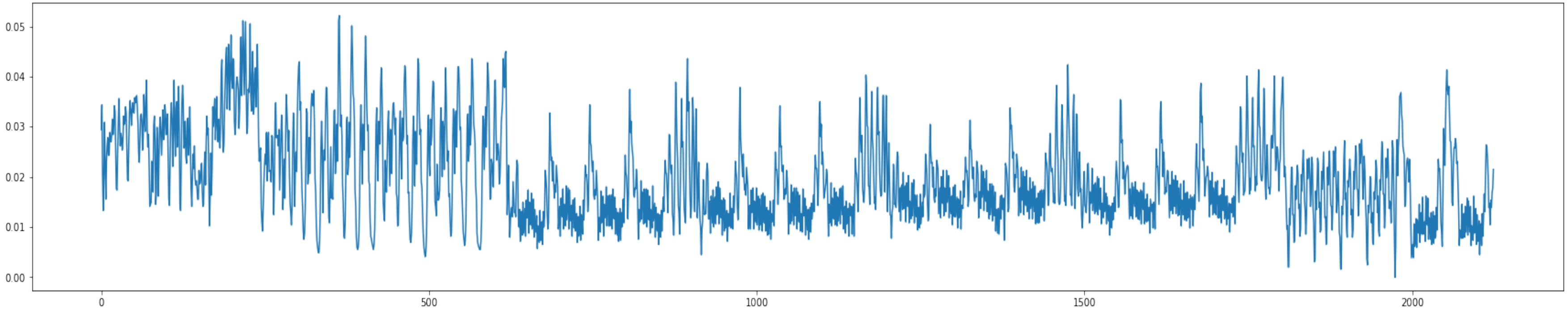
Summary of study activities

- Study of Attack/Anomaly detection using machine learning models.
- Study of sustainability of Data Centers
- Study of embedding machine learning model on microcontrollers
- Attended Ad hoc PhD courses of “Using Deep Learning Properly” and STMicroelectronics Course “The Deep Edge” Attended Seminars on focused on Cybersecurity and Machine Learning
- Attended 2023 IEEE International Conference On Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering in Milan, presenting a demo about Side-Channel Attacks using Machine Learning models.

Research activity: Overview

Problem





Research activity: Overview

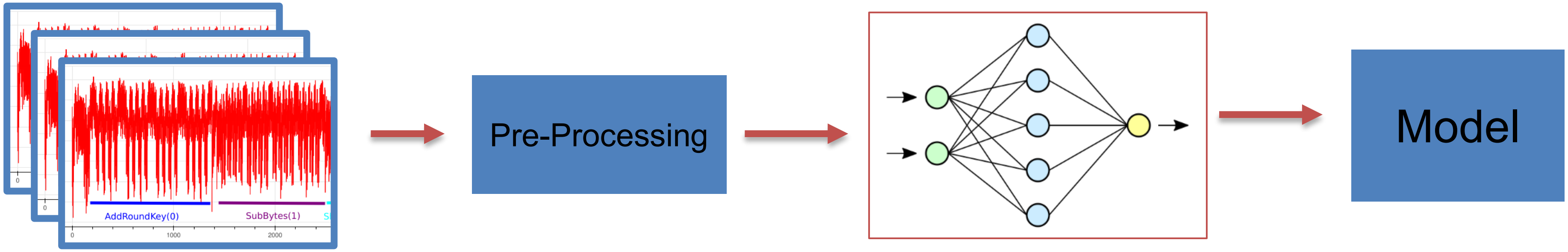
Objective

- Last Year:
  - 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

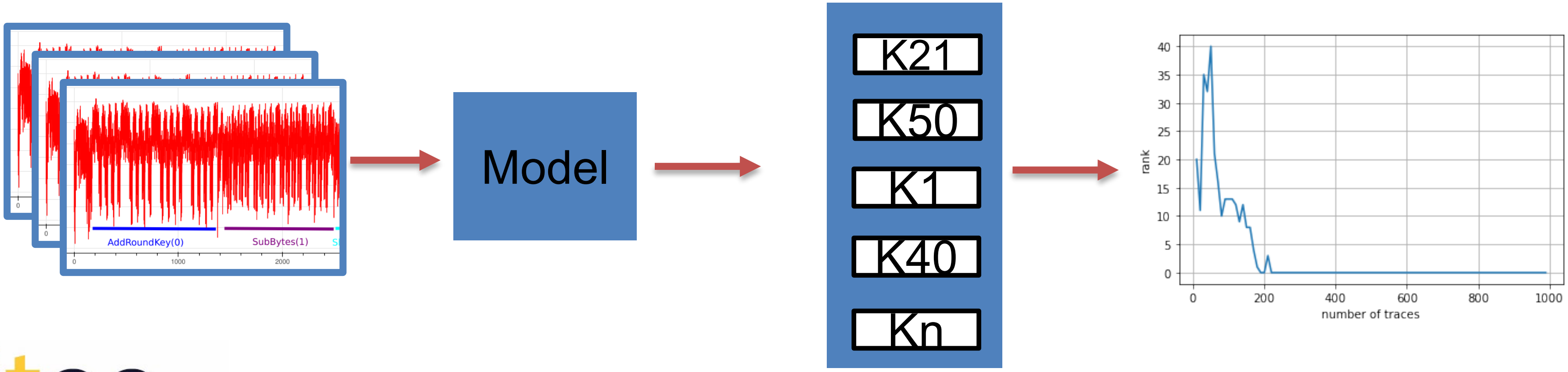
Research activity: Overview

Methodology

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

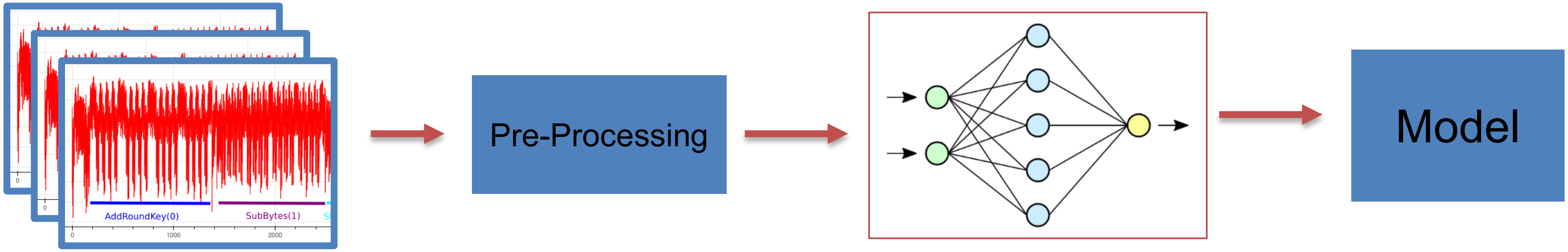
Objective

- This Year:
  - Use a machine learning model for anomaly detection using the power consumption as chip signature
  - Embed machine learning model into tiny device (for a better sustainability)
  - Assess performaces of machine learning models embedded into tiny devices in terms of:
    - Power Consumption
    - Inference Time

Research activity: Overview

Methodology

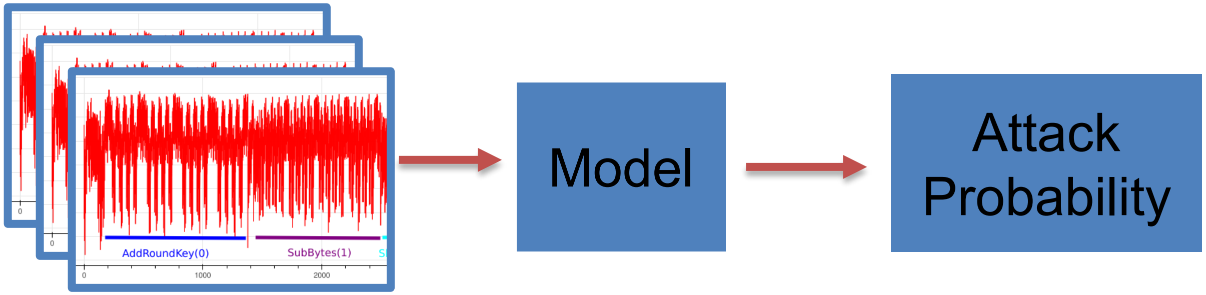
Traces are pre-processed and used to Train the attack model



Pre-Processing

Model

The model is used to detect an attack



Model

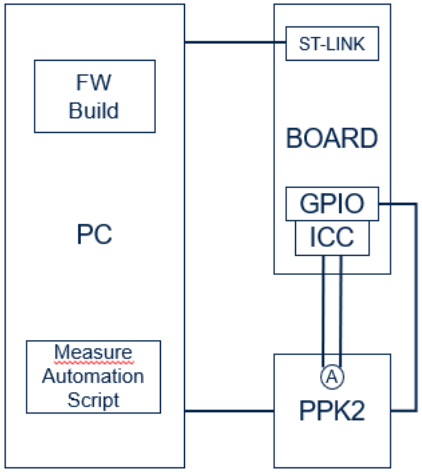
Attack Probability

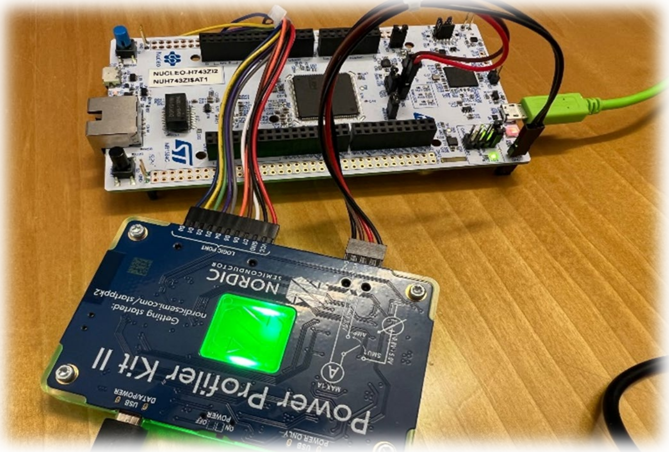
Research activity: Overview

Methodology

Where put the model?

- Data Center
  - Pros: Online update, “unlimited” resources
  - Cons: Denial Of Service, Authentication, Sustainability
- On Chip
  - Pros: Internet not needed, Sustainability
  - Cons: limited resources
    - Time Performance
    - Power Consumption





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)*
[P2]	*2023 IEEE International Conference On Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering in Milan, presenting a demo about Side-Channel Attacks using Machine Learning models*

Next Year

- Study anomaly/intrusion detection based on machine learning
- Build a model that can be used as countermeasure
- Find unauthorized devices in the network by means of Machine Learning