THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Multi-Layer Electromagnetic Side Chanel Attack Prevention Design for IoT

Adil Gokturk

April 21, 2023

Agenda

- **Intro: EM SCA**
  - **Background**
  - **Mind Map**
  - **Proposed Influence Diagram**
  - **Operational View / Activity Diagram**

Background

What is Side Channel Attack?

- The Side-channel attack—SCA is a security exploitation technique that adversaries use to extract secret information/data from a chip/hardware/system by measuring or analyzing various physical parameters like power supply current, chip execution time, and electromagnetic radiation.
- The SCAs pose significant threats with the extensive and emerging use of the Internet of Things—IoTs in users' private lives and almost every industry with different priorities and complex connectivity-generated vulnerabilities.

Why is this research?

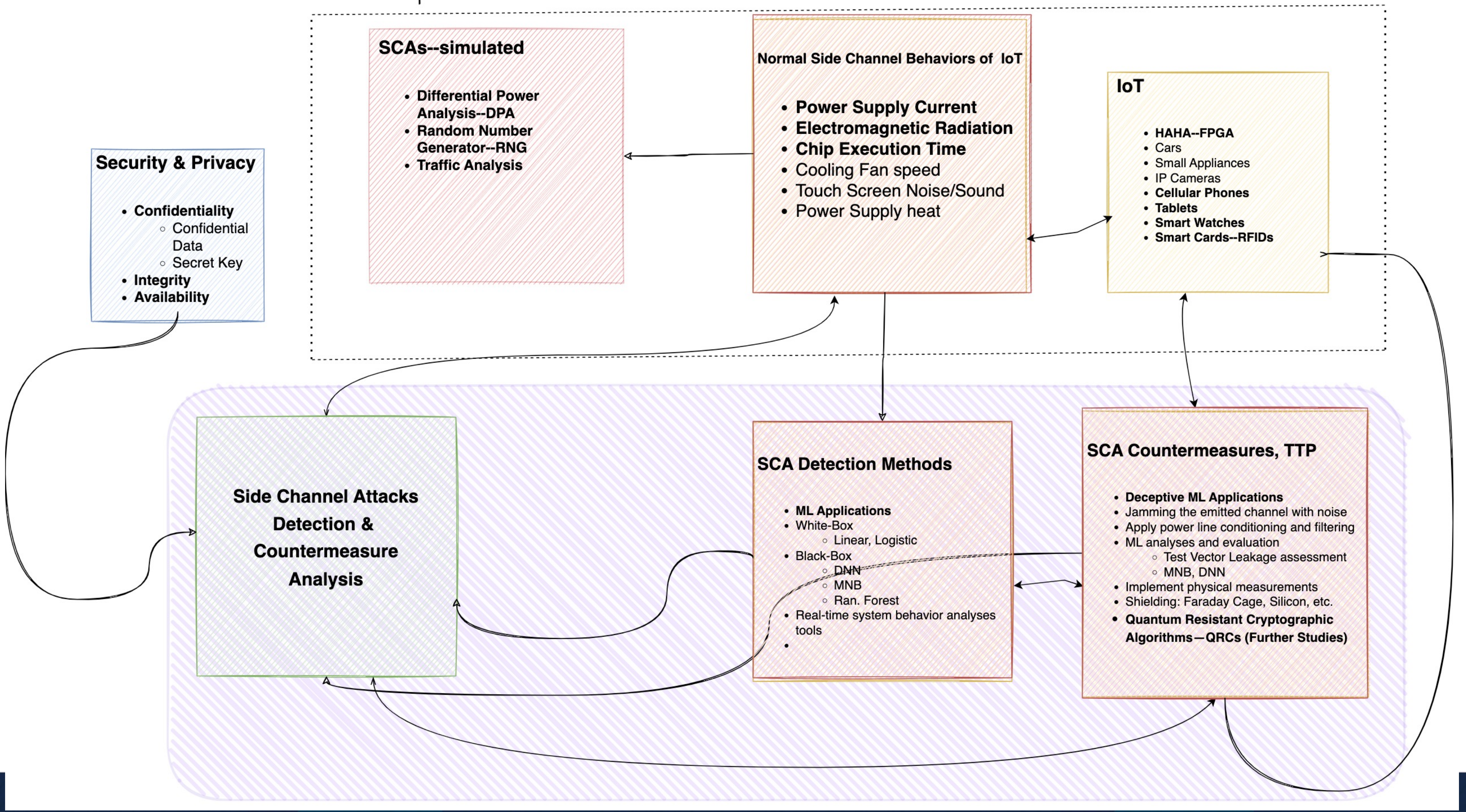
- According to Gartner, the connected IoTs will rise to **75 billion by 2025** (Hodgdon, 2021). The convenience of IoTs comes with a price: falsely underestimated the vulnerability of almost any electronic device hardware against side-channel attacks.
- SCA causes multi-billion dollar incidents: In 2018, Spectre and Meltdown exploited speculative execution on a CPU to snoop on another and steal cryptographic keys, which caused to force redesign of all superscalar SPUs from 2020 to 2025 (Anderson, 2021).
- It is only possible to provide information security by securing the system's hardware (Bhunia & Tehranipoor, 2019).

The focus of Research?

This research will explore commonly existing vulnerabilities in IoT devices. It will improve SCA detection accuracy and speed to provide countermeasures by using ML models and simulations against Electromagnetic—EM Side-channel Attacks.

Mind Map

Side Channel Attacks--SCA Mind Map



SCAs--simulated

- Differential Power Analysis--DPA
- Random Number Generator--RNG
- Traffic Analysis

Normal Side Channel Behaviors of IoT

- **Power Supply Current**
- **Electromagnetic Radiation**
- **Chip Execution Time**
- Cooling Fan speed
- Touch Screen Noise/Sound
- Power Supply heat

IoT

- **HAHA--FPGA**
- Cars
- Small Appliances
- IP Cameras
- **Cellular Phones**
- **Tablets**
- **Smart Watches**
- **Smart Cards--RFIDs**

Security & Privacy

- **Confidentiality**
  - Confidential Data
  - Secret Key
- **Integrity**
- **Availability**

Side Channel Attacks Detection & Countermeasure Analysis

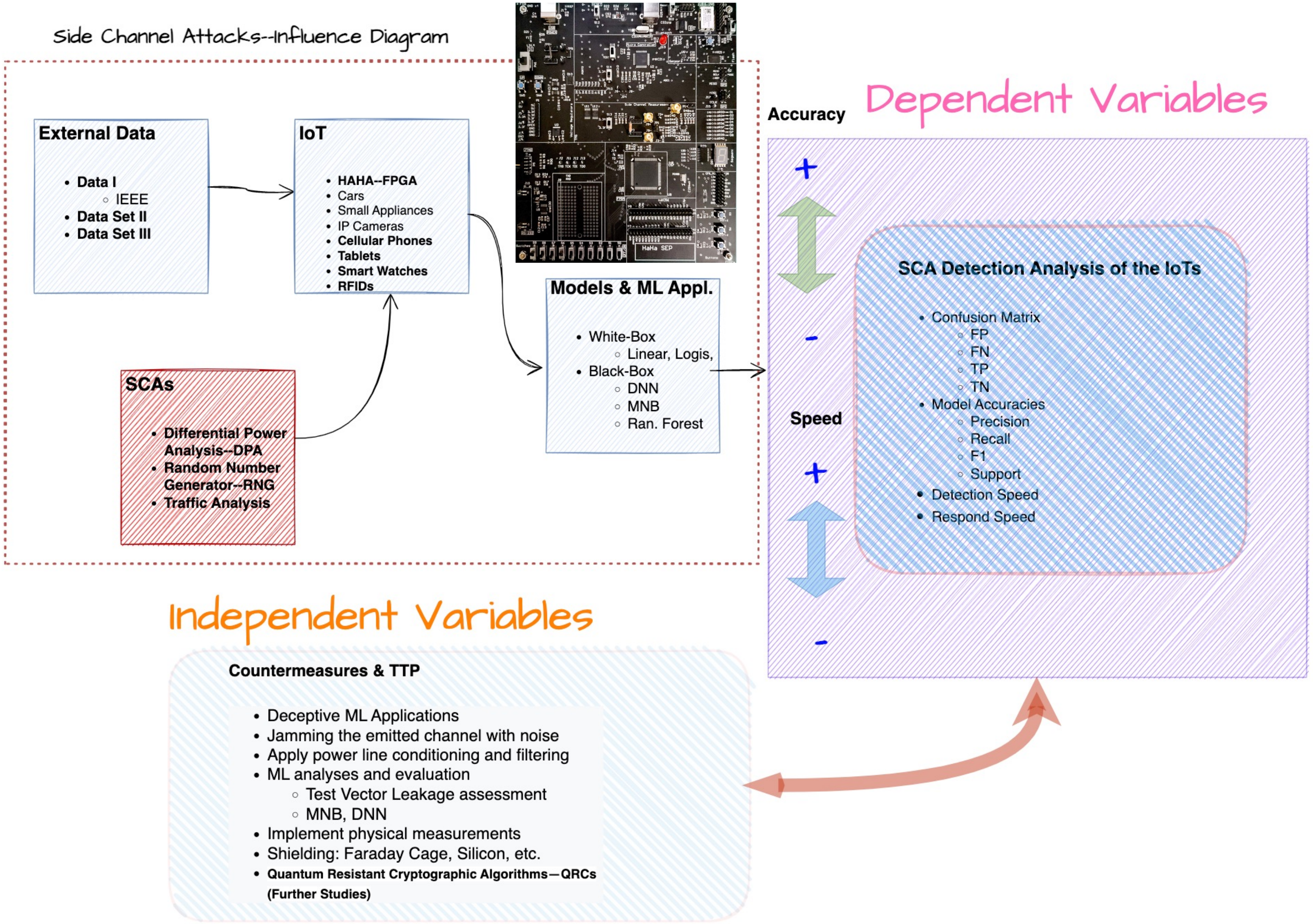
SCA Detection Methods

- **ML Applications**
- White-Box
  - Linear, Logistic
- Black-Box
  - DNN
  - MNB
  - Ran. Forest
- Real-time system behavior analyses tools
-

SCA Countermeasures, TTP

- **Deceptive ML Applications**
- Jamming the emitted channel with noise
- Apply power line conditioning and filtering
- ML analyses and evaluation
  - Test Vector Leakage assessment
  - MNB, DNN
- Implement physical measurements
- Shielding: Faraday Cage, Silicon, etc.
- **Quantum Resistant Cryptographic Algorithms—QRCs (Further Studies)**

Proposed Influence Diagram



Side Channel Attacks--Influence Diagram

External Data

- **Data I**
  - IEEE
- **Data Set II**
- **Data Set III**

IoT

- **HAHA--FPGA**
- Cars
- Small Appliances
- IP Cameras
- **Cellular Phones**
- **Tablets**
- **Smart Watches**
- **RFIDs**

SCAs

- **Differential Power Analysis--DPA**
- **Random Number Generator--RNG**
- **Traffic Analysis**

Models & ML Appl.

- White-Box
  - Linear, Logis,
- Black-Box
  - DNN
  - MNB
  - Ran. Forest

Dependent Variables

Accuracy

+

-

Speed

+

-

SCA Detection Analysis of the IoTs

- Confusion Matrix
  - FP
  - FN
  - TP
  - TN
- Model Accuracies
  - Precision
  - Recall
  - F1
  - Support
- Detection Speed
- Respond Speed

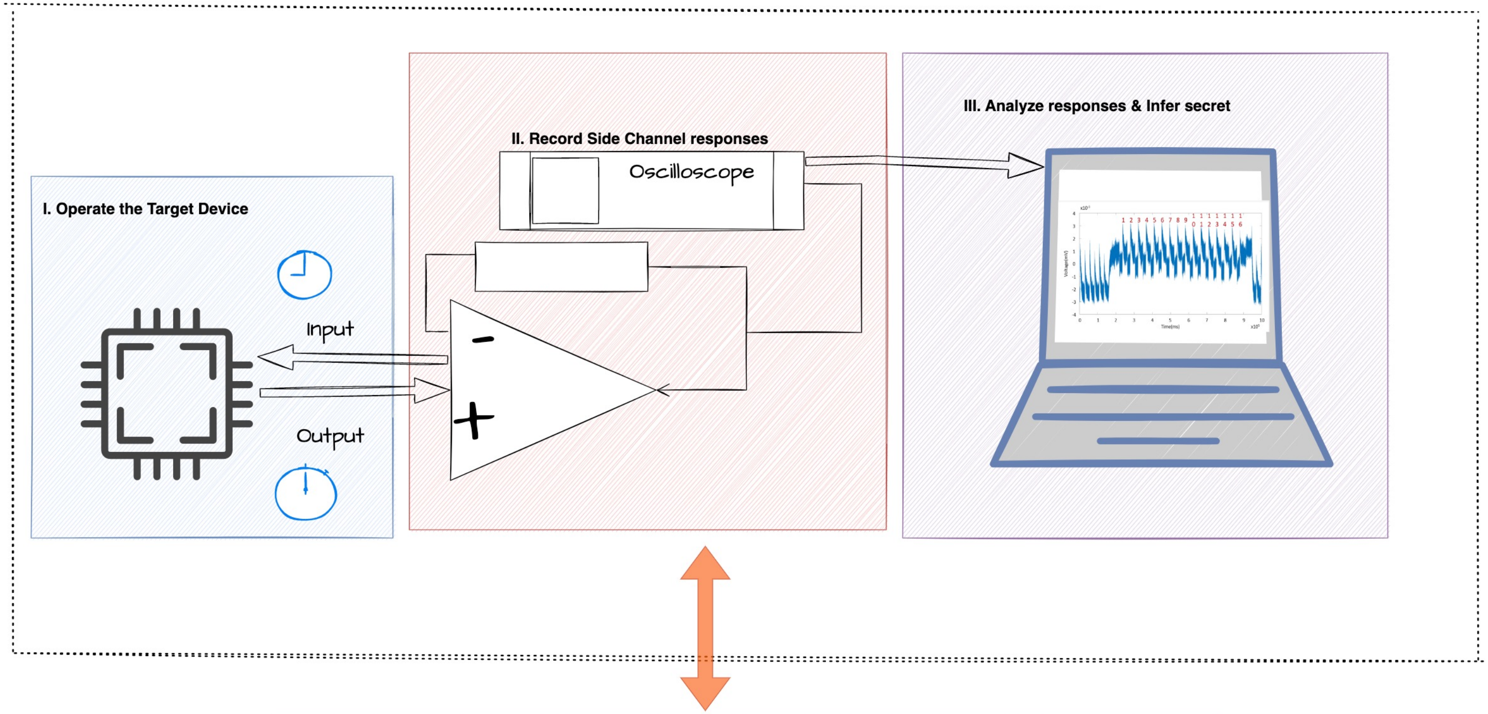
Independent Variables

Countermeasures & TTP

- Deceptive ML Applications
- Jamming the emitted channel with noise
- Apply power line conditioning and filtering
- ML analyses and evaluation
  - Test Vector Leakage assessment
  - MNB, DNN
- Implement physical measurements
- Shielding: Faraday Cage, Silicon, etc.
- **Quantum Resistant Cryptographic Algorithms—QRCs (Further Studies)**

Operational View/Activity Diagram

Side Channel Attacks--Operational View/Activity Diagram



I. Operate the Target Device

II. Record Side Channel responses

III. Analyze responses & Infer secret

IV. Back propagate, Detect & Apply Countermeasures

Countermeasures & TTP

- Deceptive ML Applications
- Jamming the emitted channel with noise
- Apply power line conditioning and filtering
- ML analyses and evaluation
  - Test Vector Leakage assessment
  - MNB, DNN
- Implement physical measurements
- Shielding: Faraday Cage, Silicon, etc.
- **Quantum Resistant Cryptographic Algorithms—QRCs (Further Studies)**