NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

pace Physical Analysis and Cryptographic Engineering

Mind The Portability

A Warriors Guide through Realistic Profiled Side-channel Analysis

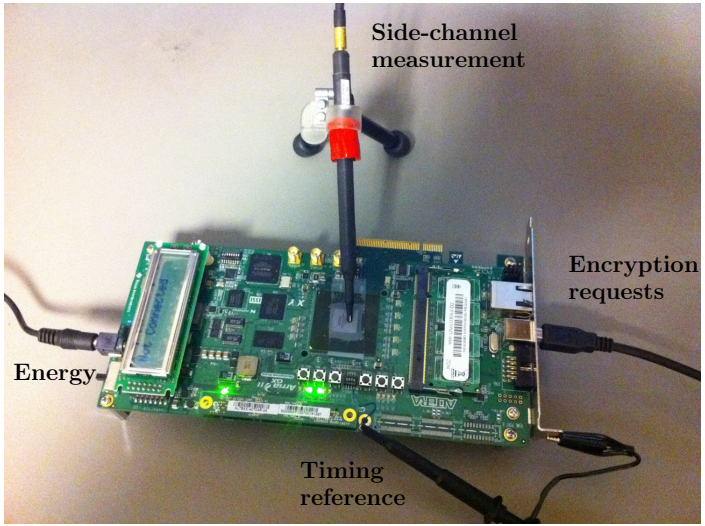
Shivam Bhasin[1], Dirmanto Jap[1], Anupam Chattopadhyay[1], Stjepan Picek[2], Annelie Heuser[3], and Ritu Ranjan Shrivastwa[4]

[1]NTU, Singapore
[2]TU Delft, Netherlands
[3]IRISA, France
[4]Secure-IC France

NDSS 2020, San Diego
23-26 February 2020

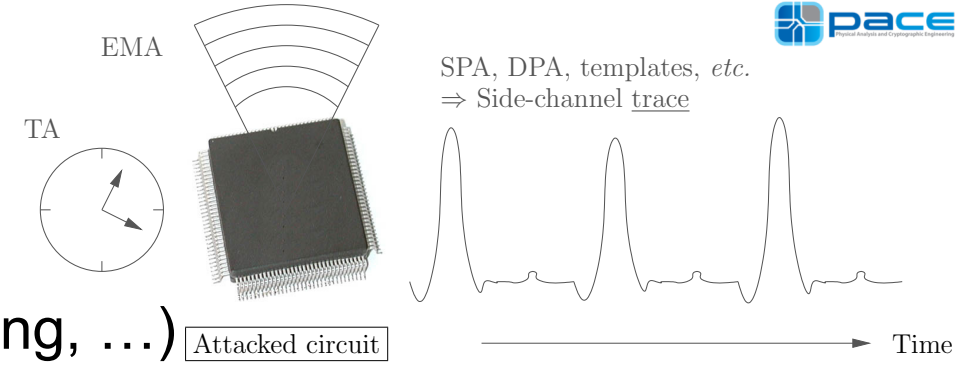
Side-Channel Analysis (SCA)

THEN



NOW

What is SCA?



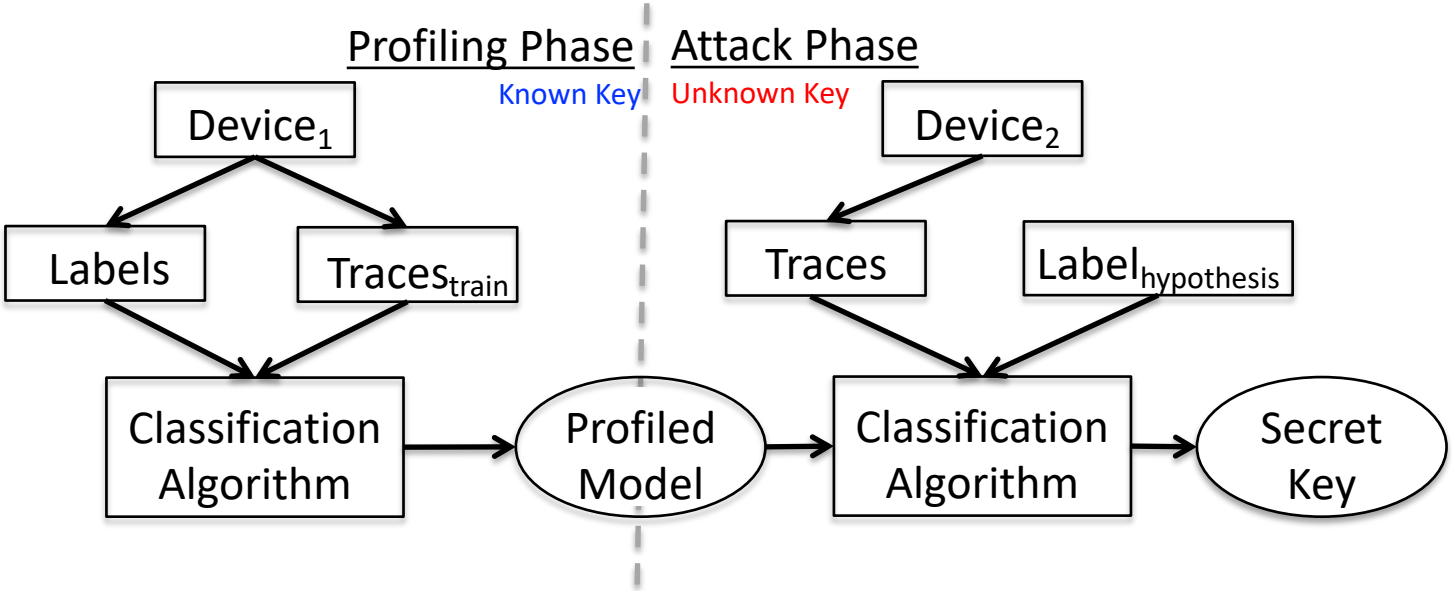
- Non-invasive (power, EM, timing, …)
- Powerful & practical. Ex:
  - *Keeloq*
  - *FPGA Bitstream encryption*
  - *Bitcoin wallets*
  - *…*
- Applications: Secret key recovery and more …
- Serious threat to embedded systems

Types of SCA

- Simple SCA (ex. Visual inspection)
- Non Profiled SCA (ex. DPA, CPA, other on the fly statistical attacks)
- **Profiled SCA (ex. Templates, Machine-Learning based attacks)**

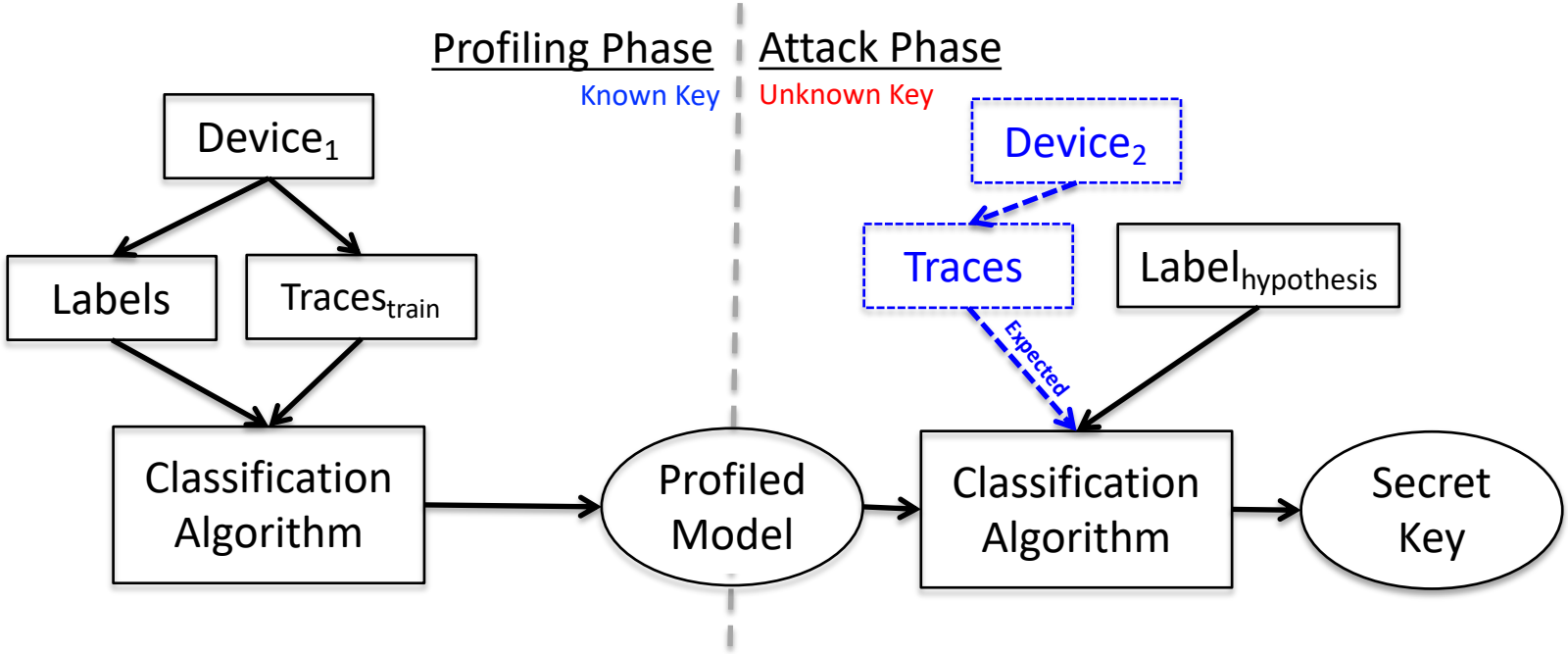
In the following, we focus on profiled power/EM attacks on embedded devices targeting encryption algorithms for secret key recovery

Profiled SCA

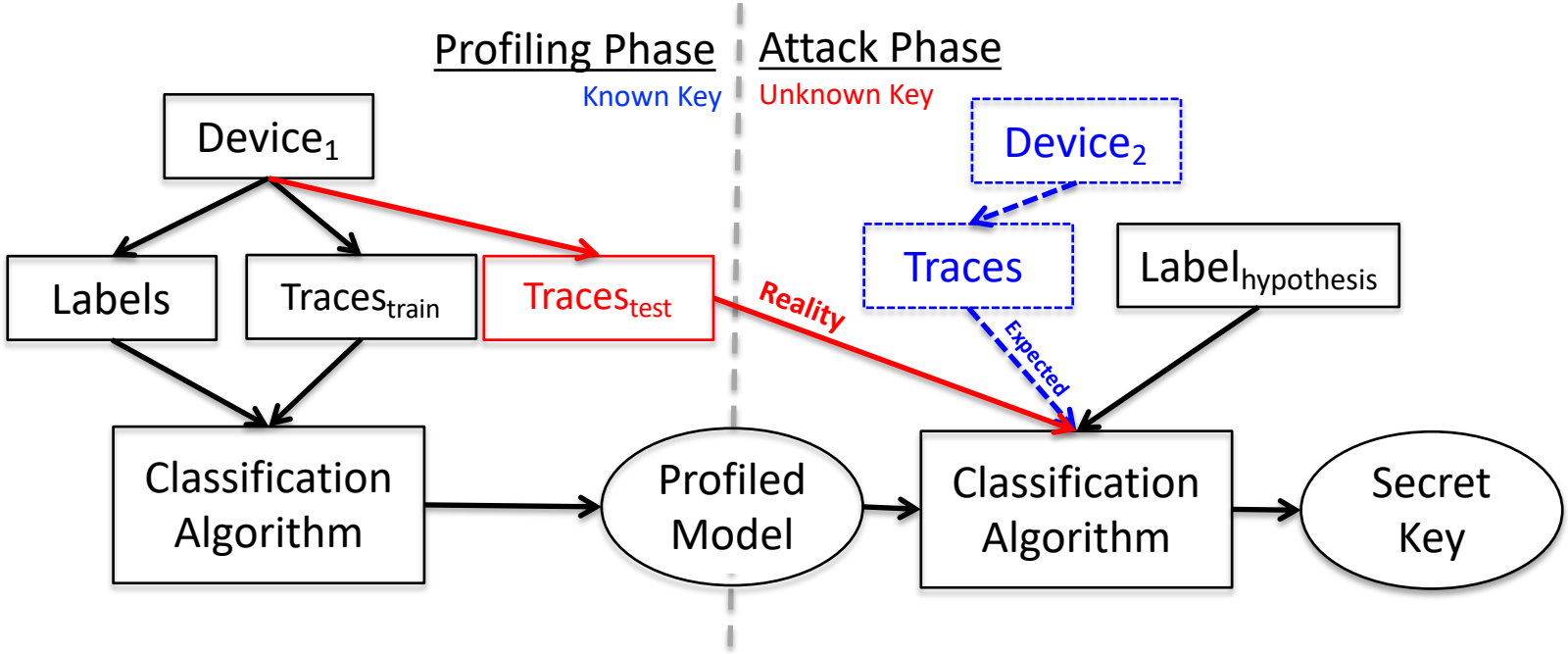


- Target exploitation in few traces, **ideally single trace**
- **Classification Algorithm:** Template Attacks (TA) vs Machine Learning (ML)
- **Deep Learning** has shown great success with protected implementations
- Recent work with deep learning report successful attack in 100X less traces (500 vs 5).

Expectations vs Reality



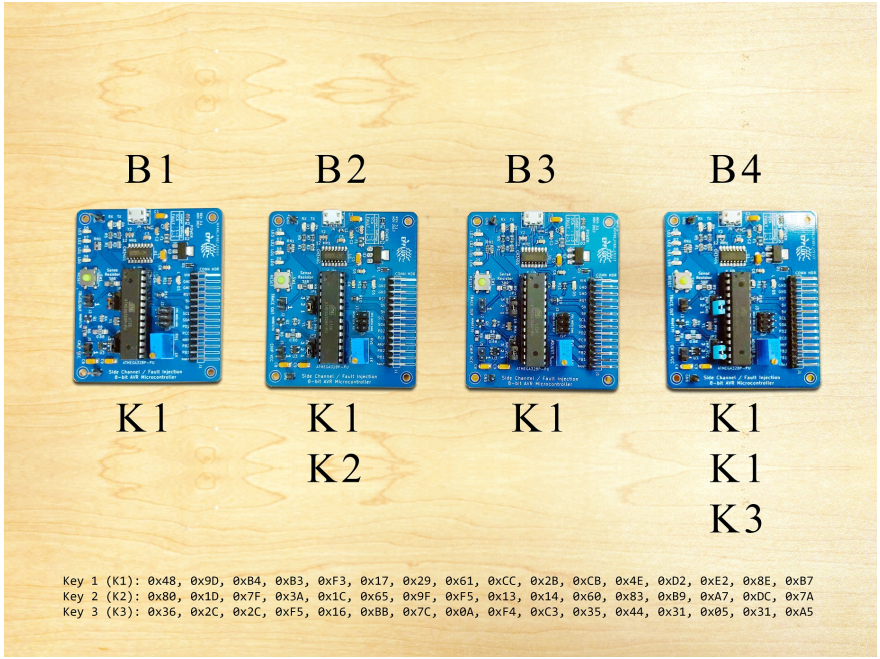
Expectations vs Reality

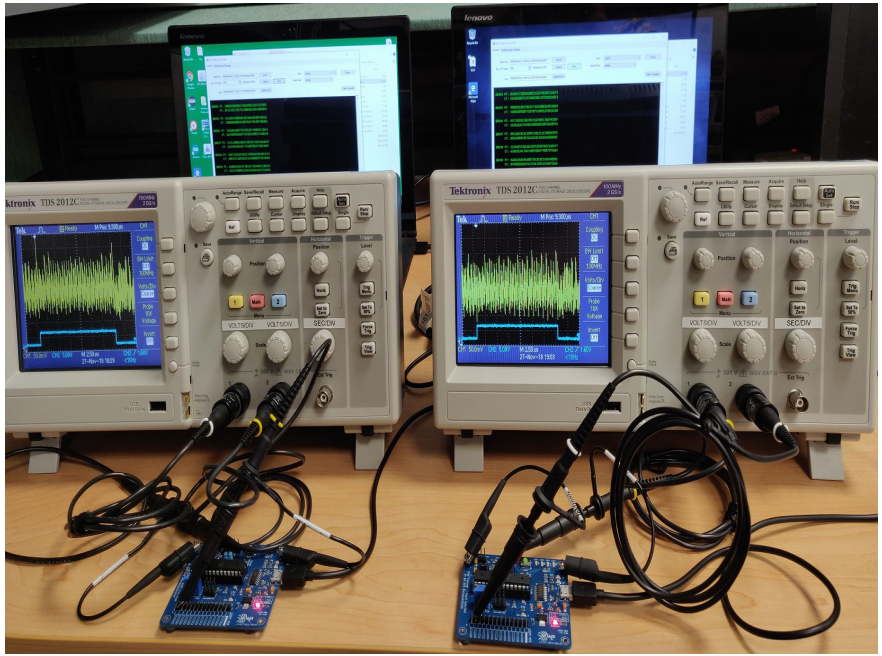


Portability

- B and B’ are two copies of same device
- Differences between B and B’ are due to uncontrolled variations in process, measurement setup, or other stochastic factors
- *Portability* denotes all settings in which an attacker can conduct the training on the measurement data obtained from a clone device B’ and import the learned knowledge $L_{B'}$ to model the actual device B, under similar parameter setup

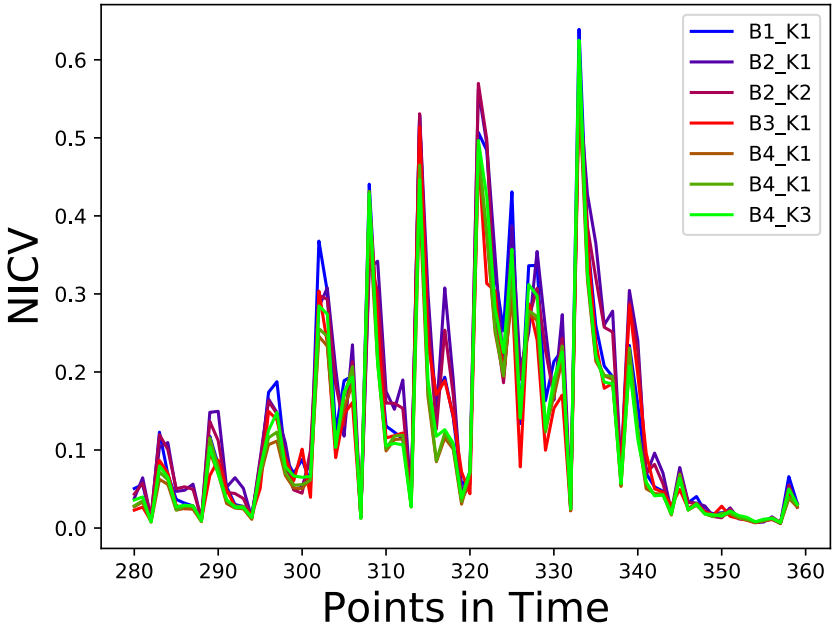
Practical Study of Portability

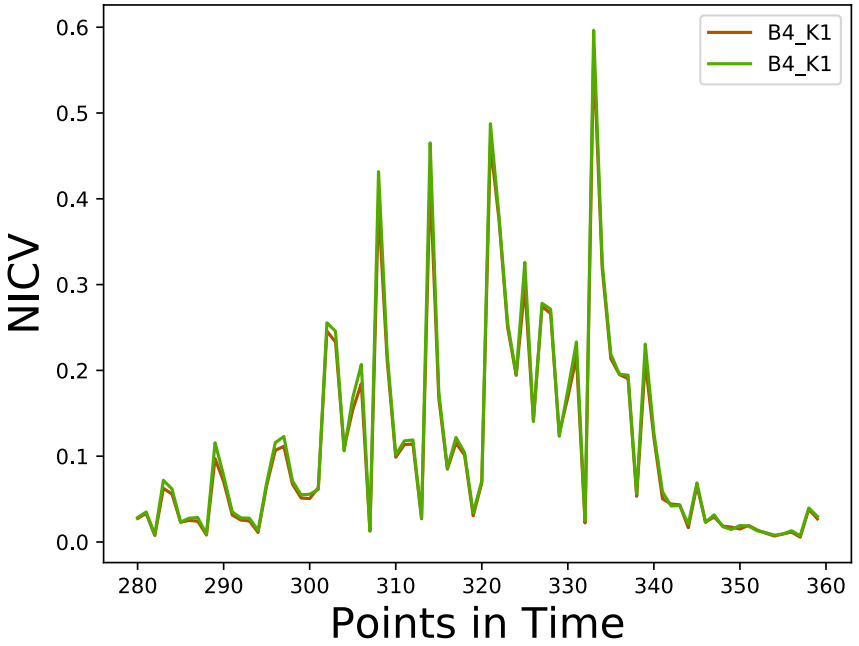




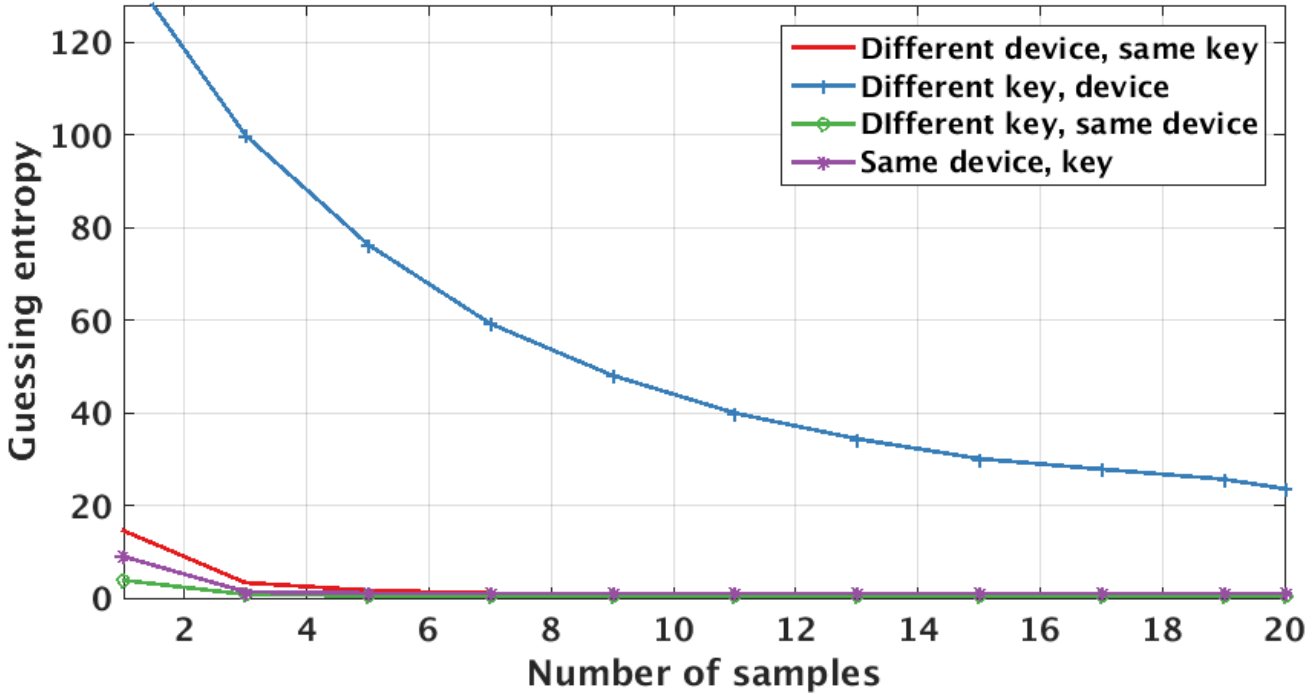
Different Sources Of Portability: Process variation (chip, wires, PCB components, connectors), environmental factors, ...

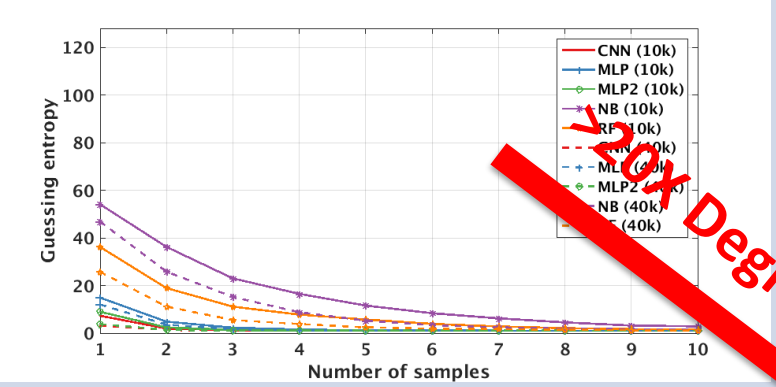
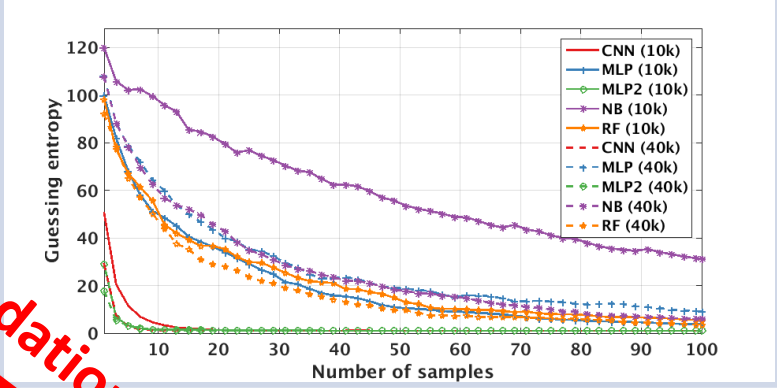
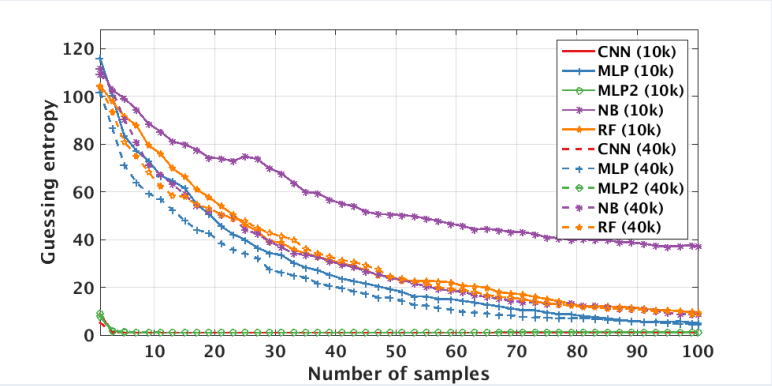
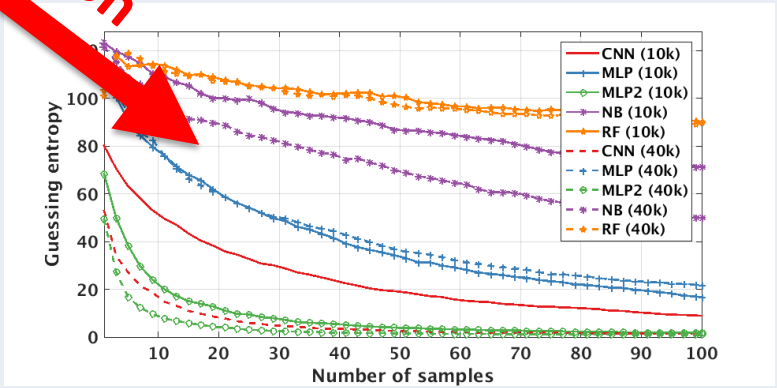
Comparing Signal Quality



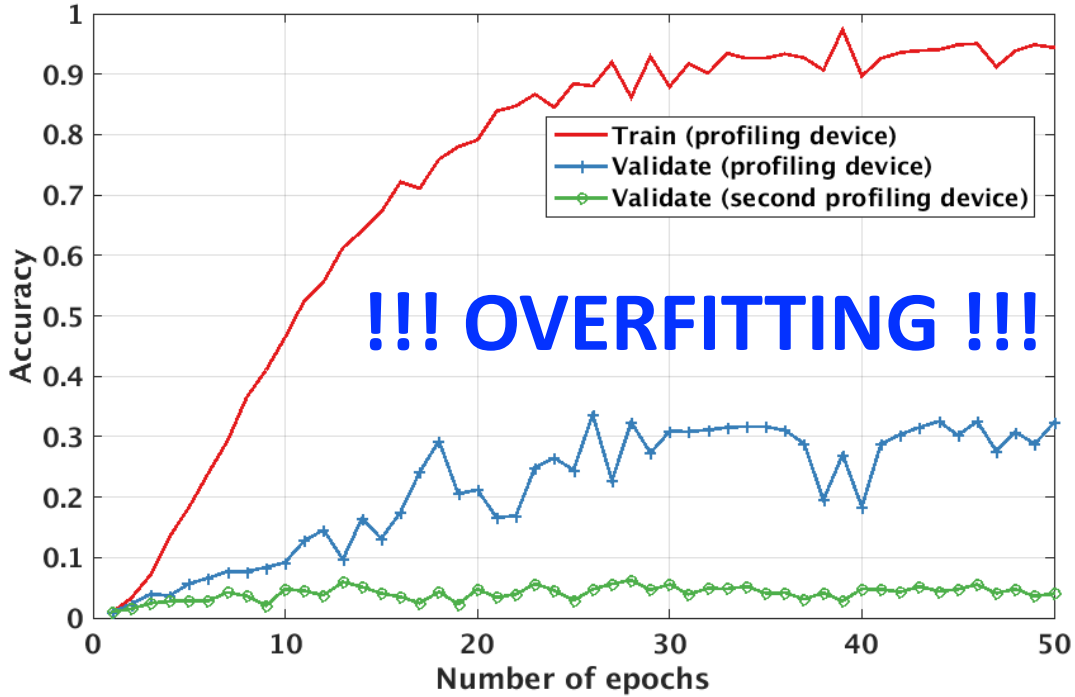


Comparing SCA Vulnerability

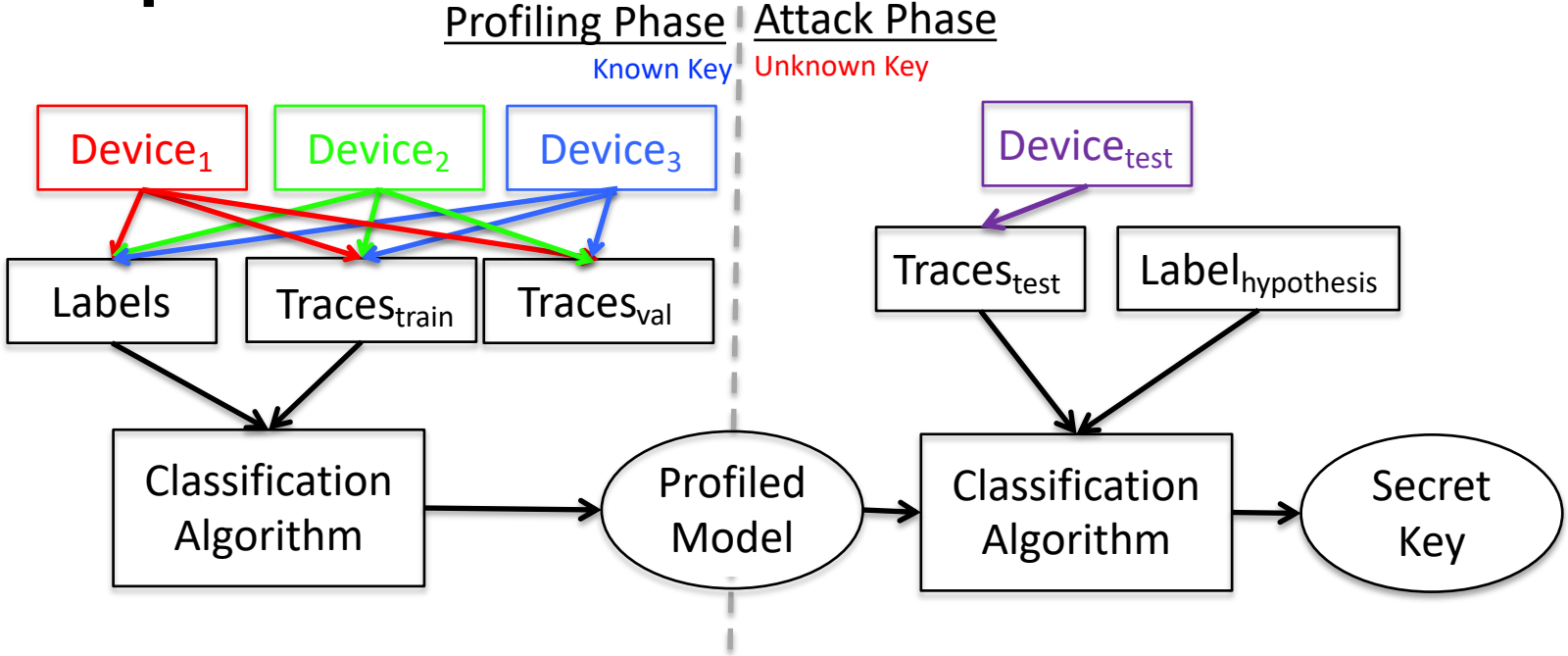


	Same Device	Different Device
Same Key		
Different Key		

Why Does It Happen?

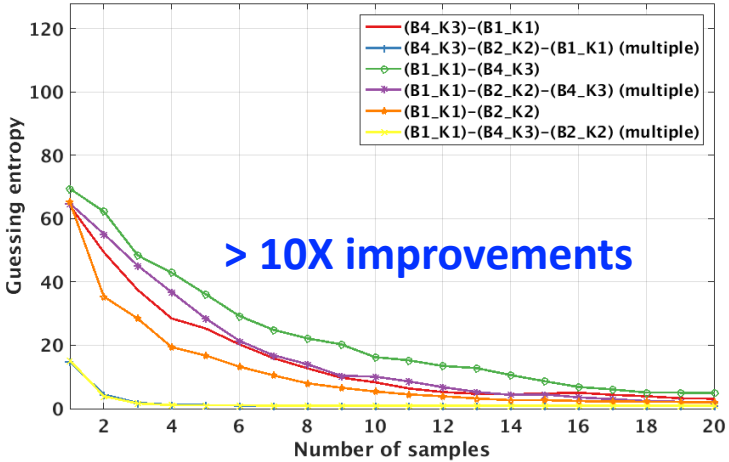


Proposed Multi-Device Model



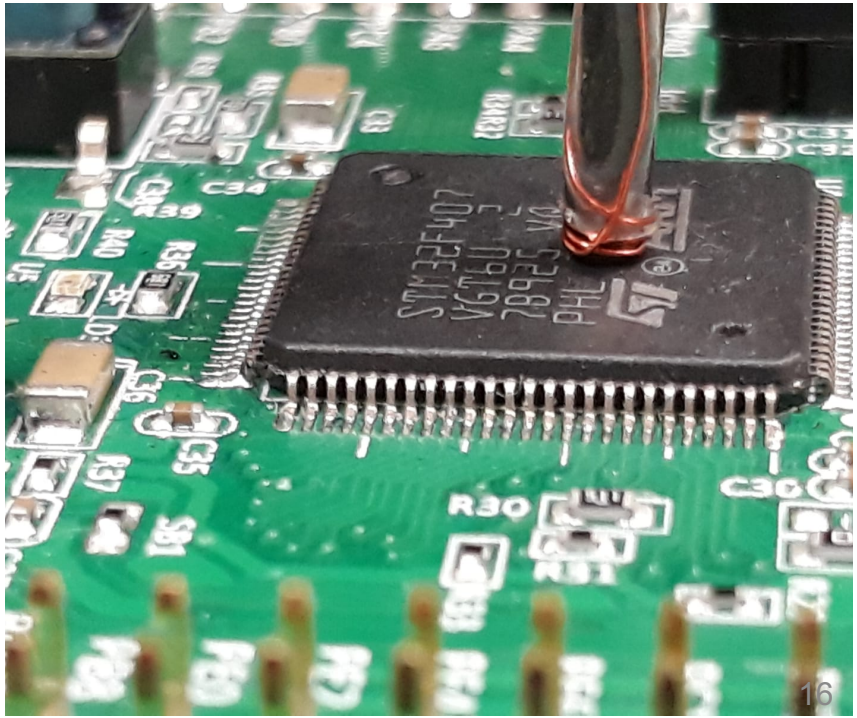
Proposed Multi-Device Model

- *Multiple Device Model (MDM)* denotes all settings where attacker can conduct the training on measurement data from a number of similar devices (≥ 2), $B' = \{B_0', \ldots, B_{n-1}'\}$ and import the learned knowledge $L_{B'}$ to model the actual device B, under similar but uncontrolled parameter setup



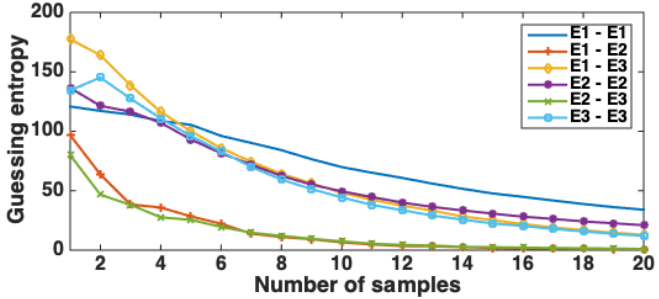
Overcoming Human Error

- Electromagnetic measurements often preferred over power measurements
  - Easy access
  - High SNR
  - Localized Leakage capture
  - …
- Extremely sensitive to probe position *(position, distance, and orientation)*
- Error comes naturally when measuring on multiple devices
- We call this human error of placement
- **A classical case of Portability**

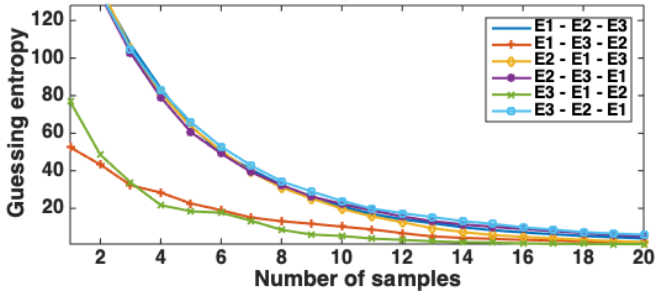


Overcoming Human Error

- Electromagnetic measurements often preferred over power measurements
  - Easy access
  - High SNR
  - Localized Leakage capture
  - …
- Extremely sensitive to probe position *(position, distance, and orientation)*
- Error comes naturally when measuring on multiple devices
- We call this human error of placement
- **A classical case of Portability**



MDM

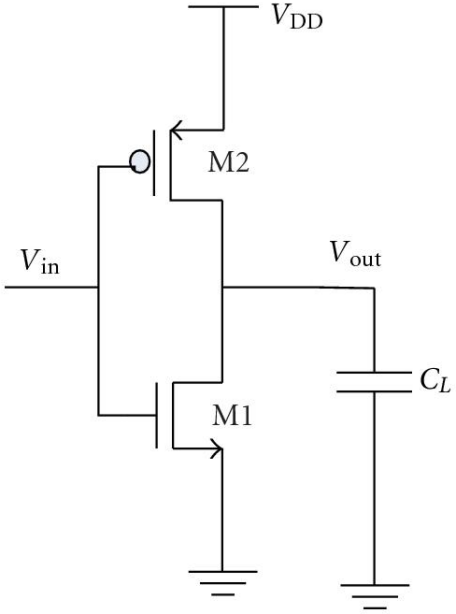


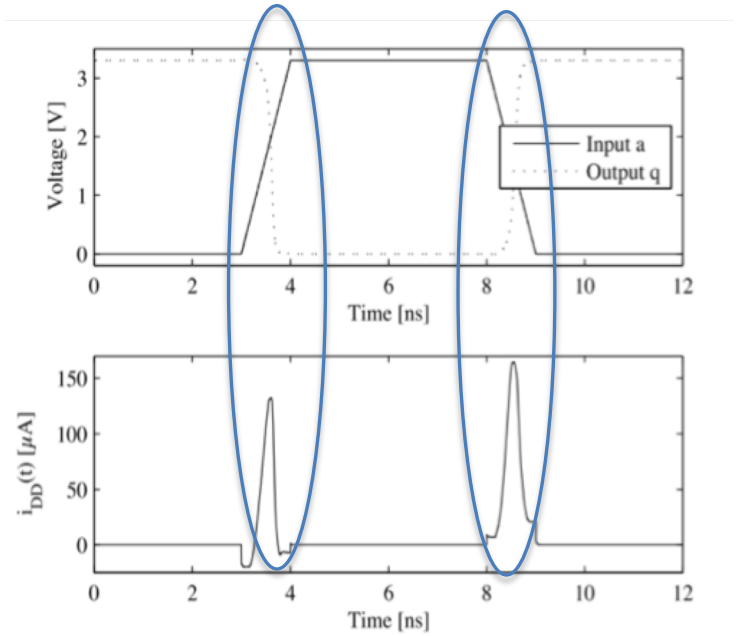
Conclusions

- One must consider portability issues in machine learning based SCA
- We proposed Multiple Device Model (MDM) to overcome portability
- Direct application to EM measurement
- Future Directions:
  - Application to heterogenous devices
  - MDM with one device noise, process-variation models

Thank You !!!

Side-Channel Analysis (SCA)

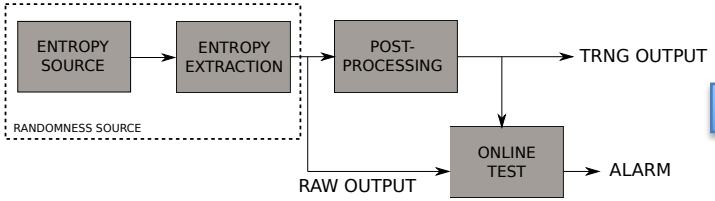


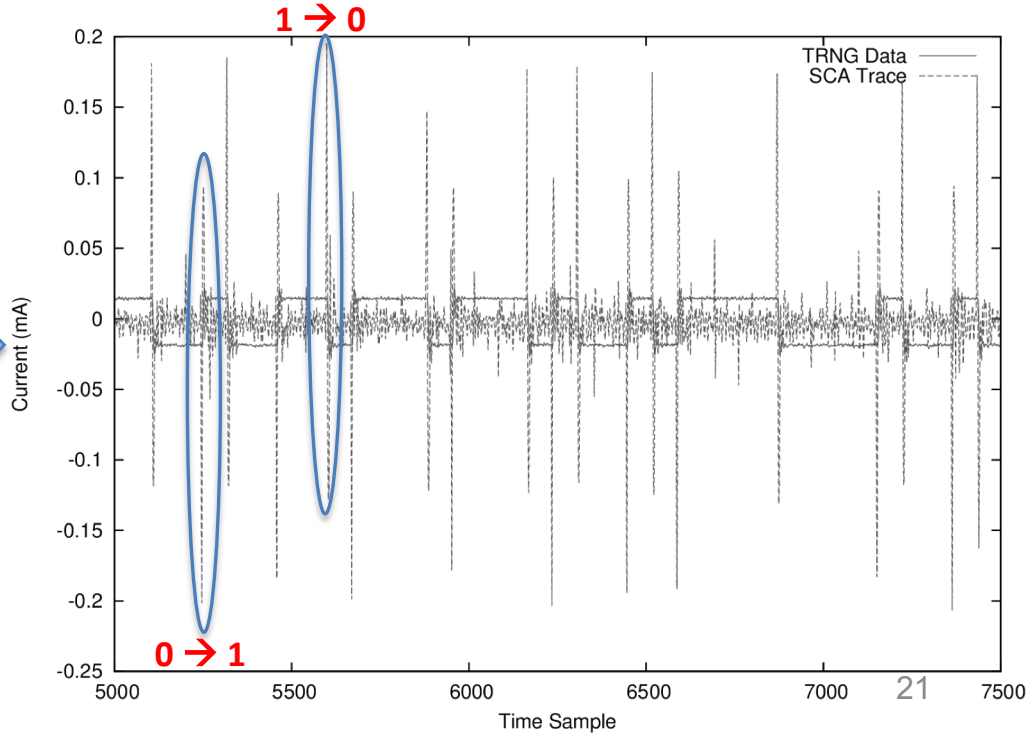


Lets look at a basic CMOS cell

Side-Channel Analysis (SCA)

Random Number Generator





Extending from one cell to a full circuit
Measure by Electromagnetic Probe

Expectations vs Reality

- Profiling and Testing device **MUST** be distinct
- An aspect often **overlooked** in profiled SCA research
- Leads to pessimistic security evaluations
- A common issue for certification labs evaluating security-critical products
- Known as **Portability**