Power Management for IoT Security: *Power, EM & ML* Side-Channel Attacks & Defenses

Shreyas Sen

Director, SPARC Lab

Assistant Professor, ECE, Purdue University

Jan 04, 2020

VLSI Design, Bangalore

References: Our Recent Work on Hardware Security

- **Best Paper Awards @ HOST – three years in a row**
  - Best Student Paper Award **HOST 2017**: ASNI **[1]**, TCAS1 **[2]**
  - Best Poster Award **HOST 2018**: RF-PUF **[3]**, JIoT **[4]**
  - Best Student Paper Award **HOST 2019**: STELLAR **[5]**
- **Top Picks in Hardware Security**
  - Our work ASNI has been selected as a "Top Pick" in the field of embedded and hardware security as one of the top 10 papers in the field over the span of last 6 years, including but not limited to DAC, DATE, ICCAD, HOST, VLSI Design, CHES, ETS, VTS, ITC, IEEE S&P, Euro S&P, Usenix Security, ASIA CCS, NDSS, ISCA, HASP, MICRO, ASPLOS, HPCA, ACSAC and ACM CCS**.**
- Hardware Security IC in **ISSCC 2020**, **showing >1B MTD for both EM and Power Attack [6]**
- **CICC 2020 paper will show protection to Deep-Learning Attack** [7]
- X-DeepSCA: **DAC 2019 [8]**, TVLSI 2019 **[9]** demonstrated Cross-device Deep-Learning SCA Attack
- SNIFFER **[10]** shows new EM-SCA attack with automated localization.

[1] Das, D., Maity, S., Nasir, S. B., Ghosh, S., Raychowdhury, A., & Sen, S. (2017, May). High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 62-67). IEEE.
[2] Das, D., Maity, S., Nasir, S. B., Ghosh, S., Raychowdhury, A., & Sen, S. (2018). ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity. IEEE Transactions on Circuits and Systems I: Regular Papers, 65(10), 3300-3311.
[3] Chatterjee, B., Das, D., & Sen, S. (2018, April). RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. In 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 205-208). IEEE.
[4] Chatterjee, B., Das, D., Maity, S., & Sen, S. (2018). RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. IEEE Internet of Things Journal, 6(1), 388-398.
[5] Das, D., Nath, M., Chatterjee, B., Ghosh, S., & Sen, S. (2019, March). STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis. In Proc. 2019 IEEE Int. Symp. Hardw. Oriented Security Trust.
[6] D. Das et al., "EM and Power SCA-resilient AES-256 in 65nm CMOS through >350x Current Domain Signature Attenuation," in IEEE International Solid-State Circuits Conference (ISSCC) 2020.
[7] D. Das et al., "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," in IEEE Custom Integrated Circuits Conference (CICC) 2020
[8] Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., & Sen, S. (2019, June). X-DeepSCA: Cross-device deep learning side channel attack. In Proceedings of the 56th Annual Design Automation Conference 2019 (p. 134). ACM.
[9] Golder, A., Das, D., Danial, J., Ghosh, S., Sen, S., & Raychowdhury, A. (2019). Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 27(12), 2720-2733.
[10] Danial, J., Das, D., Ghosh, S., Raychowdhury, A., & Sen, S. (2019). SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing. arXiv preprint arXiv:1908.09407.

SparcLab @ ECE, Purdue

PI: Shreyas Sen

Assistant Professor, ECE, Purdue University

MIT Technology Review INNOVATORS UNDER 35 INDIA

TEDx Indianapolis

14+ years research experience @ **Purdue, Georgia Tech, Intel Labs, Qualcomm, Rambus**

ECE PURDUE UNIVERSITY

GT

Intel Labs

QUALCOMM

Rambus

SPARC Lab: Sensing, Processing, Analytics & Radio Communication

SparcLab May 2019

NSF

DARPA

Lilly

Google

intel

SRC Semiconductor Research Corporation

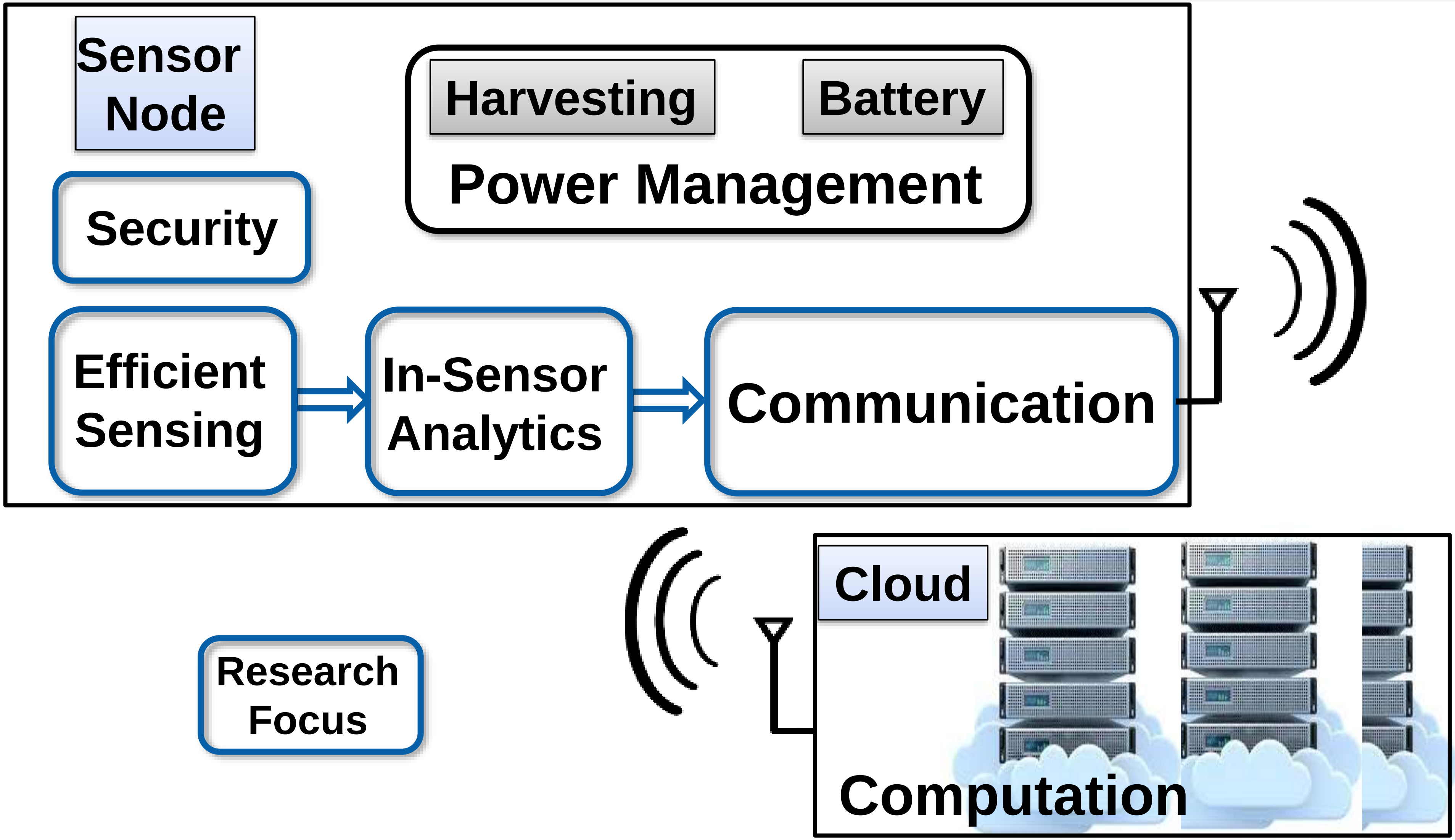
PRINTING SMART FILMS

INDIANA CTSI Clinical and Translational Sciences Institute

LANDAUER

SPARC Lab

SparcLab Research Focus



Sensor Node

Harvesting

Battery

Power Management

Security

Efficient Sensing

In-Sensor Analytics

Communication

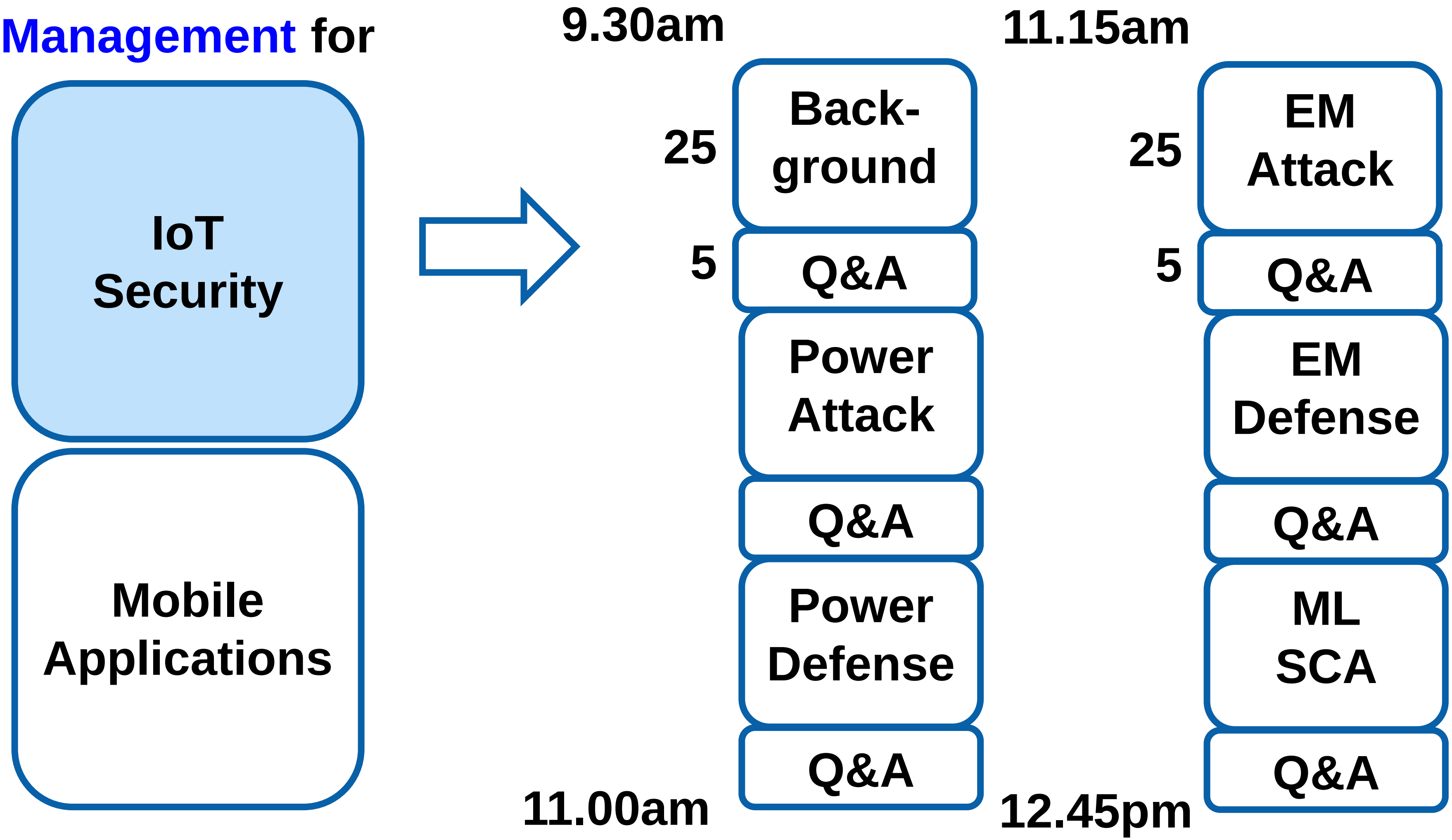
Cloud

Computation

Research Focus

Tutorial Overview

Advances in **Power Management** for



IoT Security

Mobile Applications

9.30am

25 Back-ground

5 Q&A

Power Attack

Q&A

Power Defense

Q&A

11.00am

11.15am

25 EM Attack

5 Q&A

EM Defense

Q&A

ML SCA

Q&A

12.45pm

Acknowledgements

- Debayan Das
- Josef Danial
- Shovan Maity

- Collaborator: Prof. Arijit Raychowdhury (Georgia Tech) and his students

- Intel Labs (Dr. Santosh Ghosh, Emerging Security Lab and others)

Outline

Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

Overview: New Attacks and Defenses

Attack

SCNIFFER: Automated EM leakage point detection

arxiv 2019

X-DeepSCA: Cross-Device Deep-Learning SCA

DAC 2019, TVLSI 2019

Power & Electro-Magnetic Side-Channel

Defense

ASNI: Attenuated Signature Noise Injection

HOST 2017, TCAS-1 2018

White-Box Root-Cause Analysis

HOST 2019

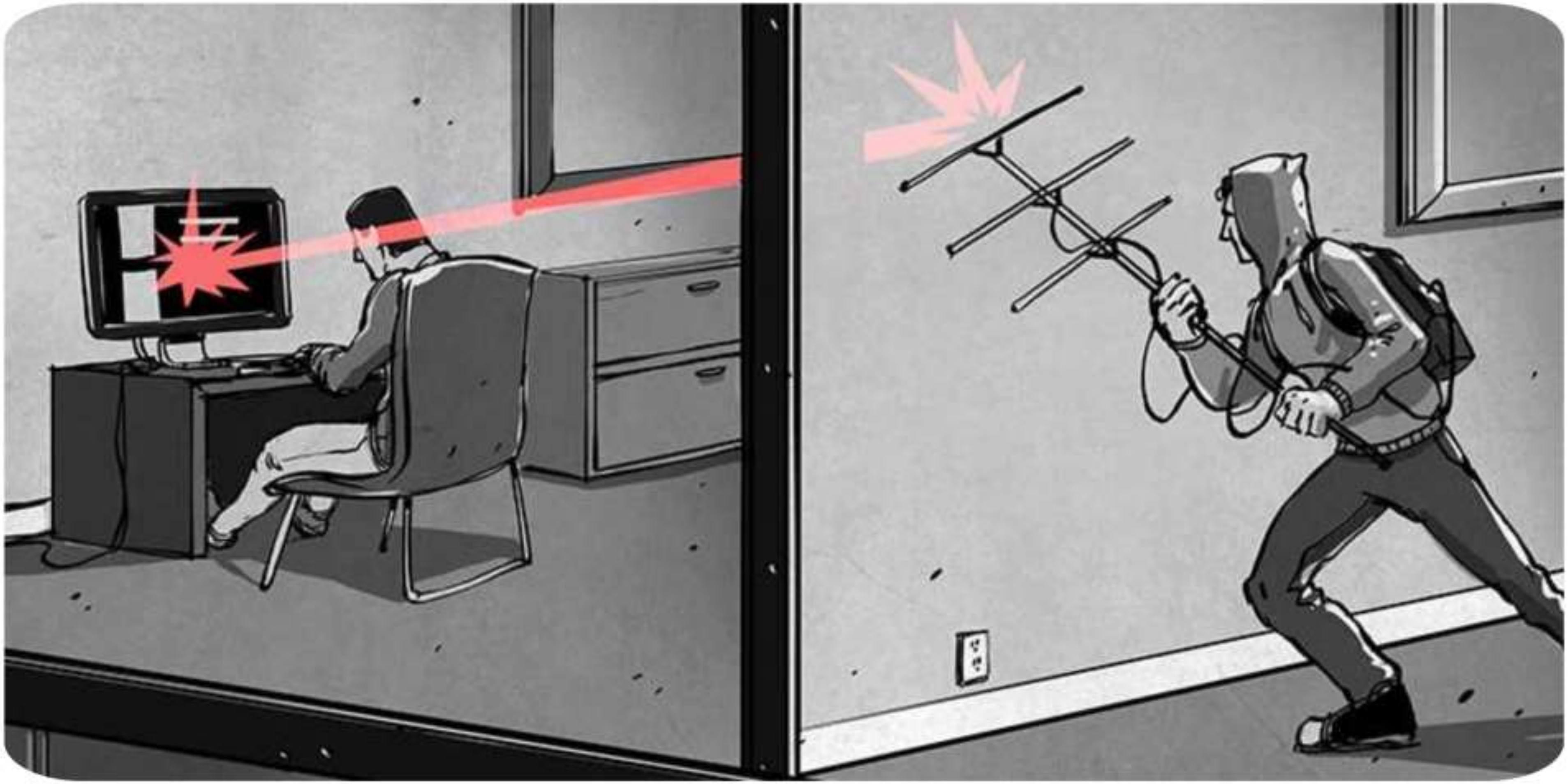
STELLAR: Generic EM SCA Tolerance

ISSCC 2020

Outline

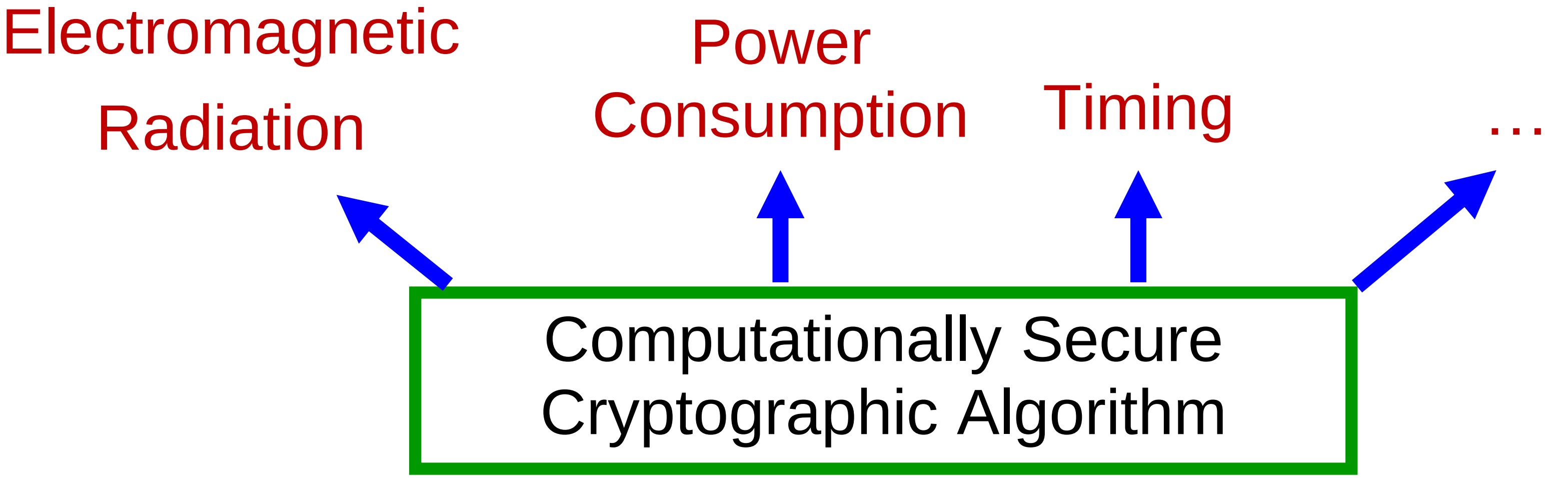
Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

Stealing Secret from Distance



Reference: *https://www.fox-it.com/nl/wp-content/uploads/sites/12/Tempest_attacks_against_AES.pdf*

Physical Side-Channel Attacks



Electromagnetic Radiation

Power Consumption

Timing

…

Computationally Secure Cryptographic Algorithm

Introduction

- Classical Cryptography treats security using ***mathematical abstractions***
- Classic cryptanalysis has had a huge success and promise
  - Analysis and quantification of crypto algorithm shows high resilience against brute-force attacks
- Over the last two decades, many of the security protocols have been attacked using ***physical attacks***
  - Take advantage of the underlying physical implementation to recover secret parameters

Power Side-Channel Basics

- Physical Implementations of crypto algorithms leak intermediate data
- Data-dependent power leaks due to the switching activity of the transistors
- Why so powerful?

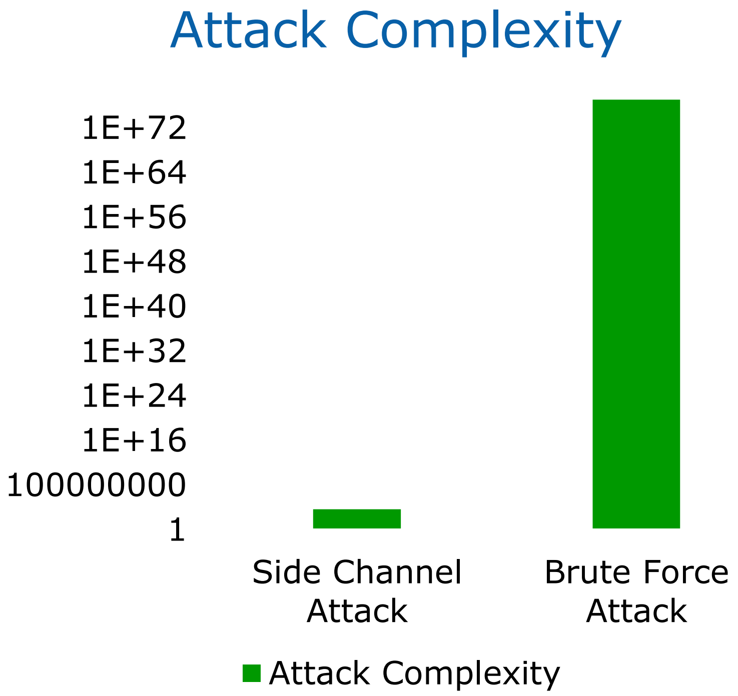
Complexity of breaking AES-128 reduced from 2^{128} to 2^{12}.

Divide and conquer approach:

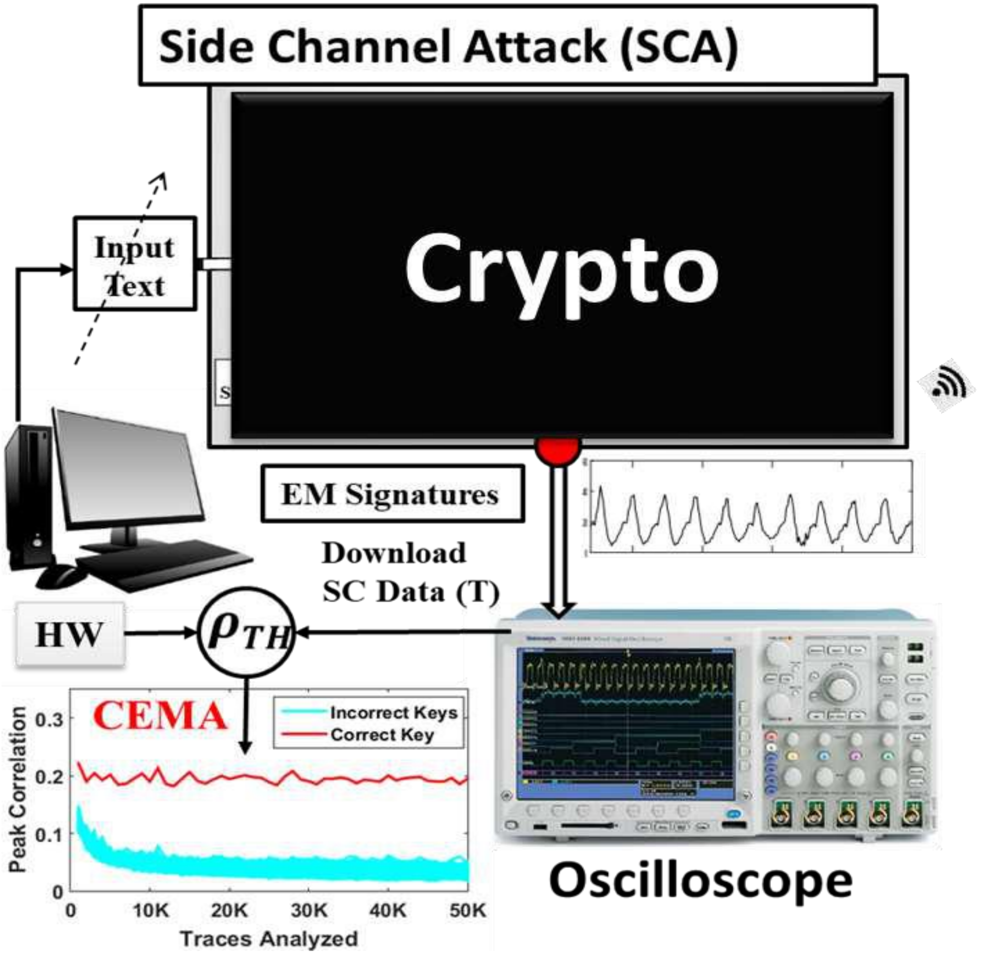
Byte-wise attack, 2^8 Combinations for each byte, and 16 key bytes.

128 Key = 16 x 8-bit key

Byte-wise Attack Complexity: $16 \times 2^8 = 2^{12}$

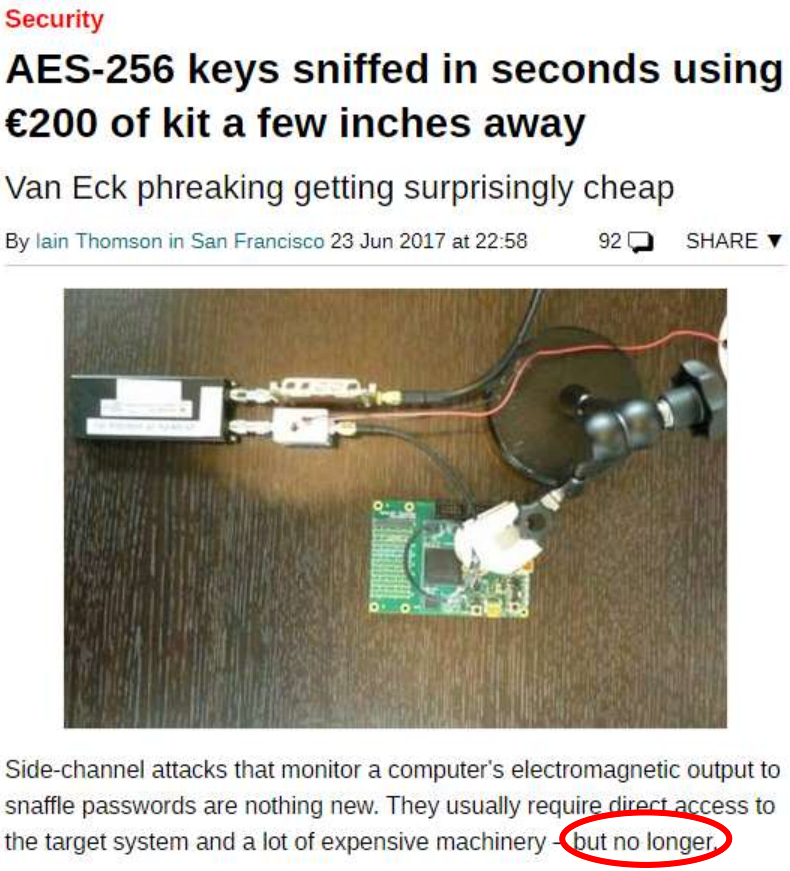


Power/EM Side-Channel Basics



- Power Consumption /Electromagnetic radiations emanating from ICs performing crypto operations can be picked up.
- Using statistical analyses, the secret key operating in the hardware can be revealed.
- Most attackers treat these EM emanations as a Black Box!

AES-256 is not enough!



Security

AES-256 keys sniffed in seconds using €200 of kit a few inches away

Van Eck phreaking getting surprisingly cheap

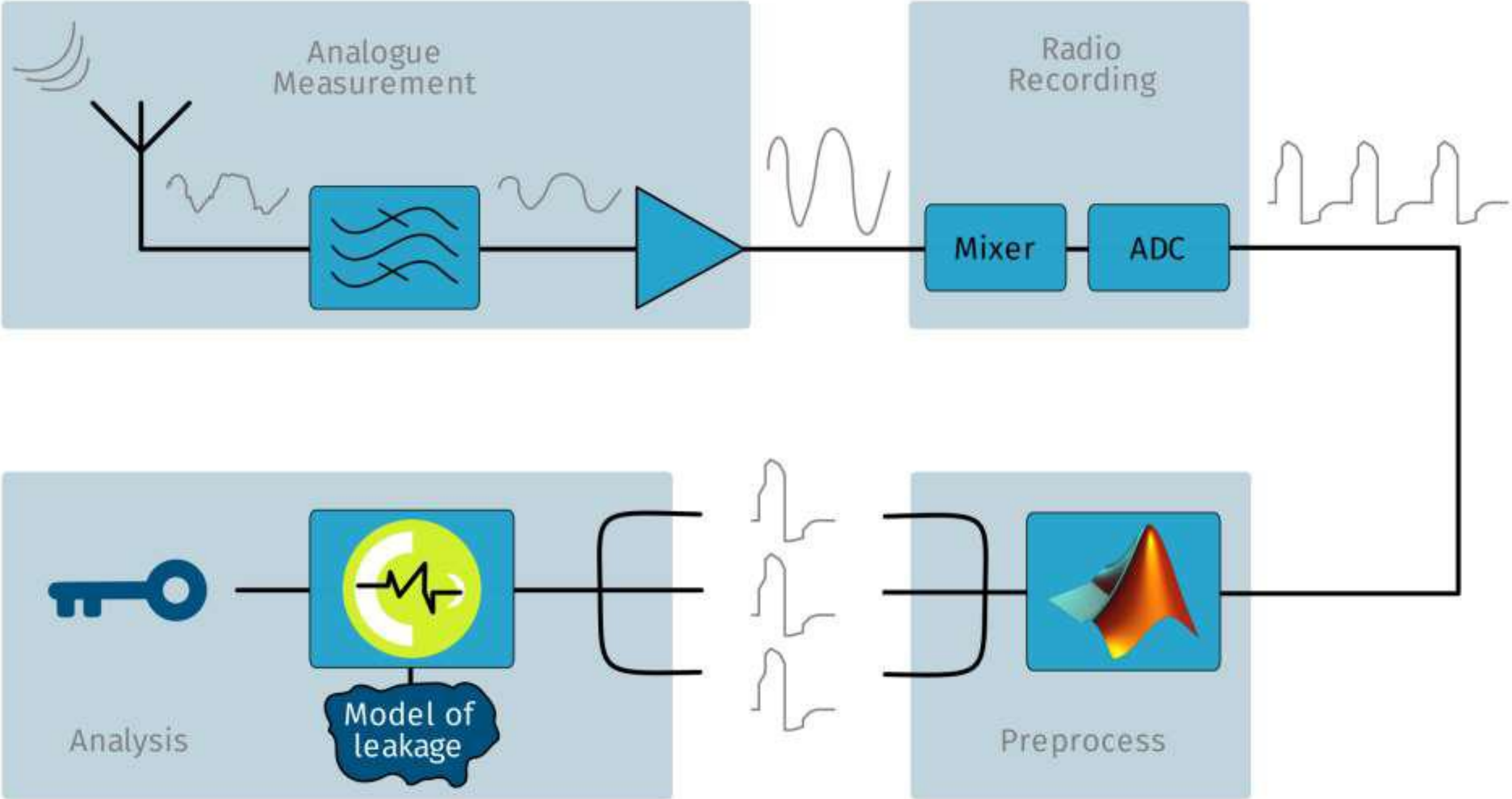
By Iain Thomson in San Francisco 23 Jun 2017 at 22:58 92 SHARE ▼

Side-channel attacks that monitor a computer's electromagnetic output to snaffle passwords are nothing new. They usually require direct access to the target system and a lot of expensive machinery – but no longer.

- AES-256 key recovered in just 5 minutes from a 1 meter distance
- Complexity of breaking AES-256 reduced from 2^{256} to 2^{13}
- From AES-128 to AES-256, SCA resistance increases linearly (2x)

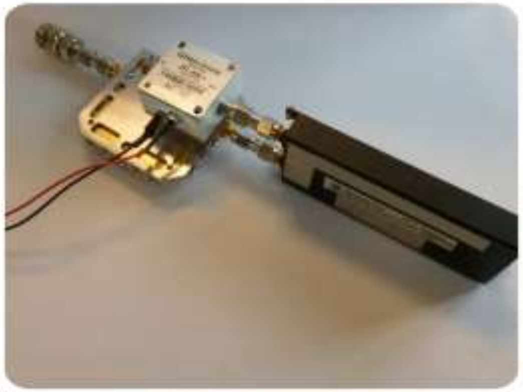
Reference: *https://www.fox-it.com/nl/wp-content/uploads/sites/12/Tempest_attacks_against_AES.pdf*

Attack Setup: Overview

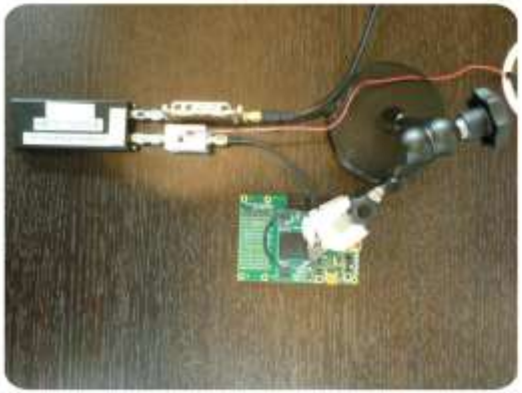


Recording Hardware

Loop antenna



External amplifier and bandpass filters



Example attack setup

SR-7100 Data Recorder

High-end
€200k
500 MHz (max BW)
1.3 GB/s (max data rate)

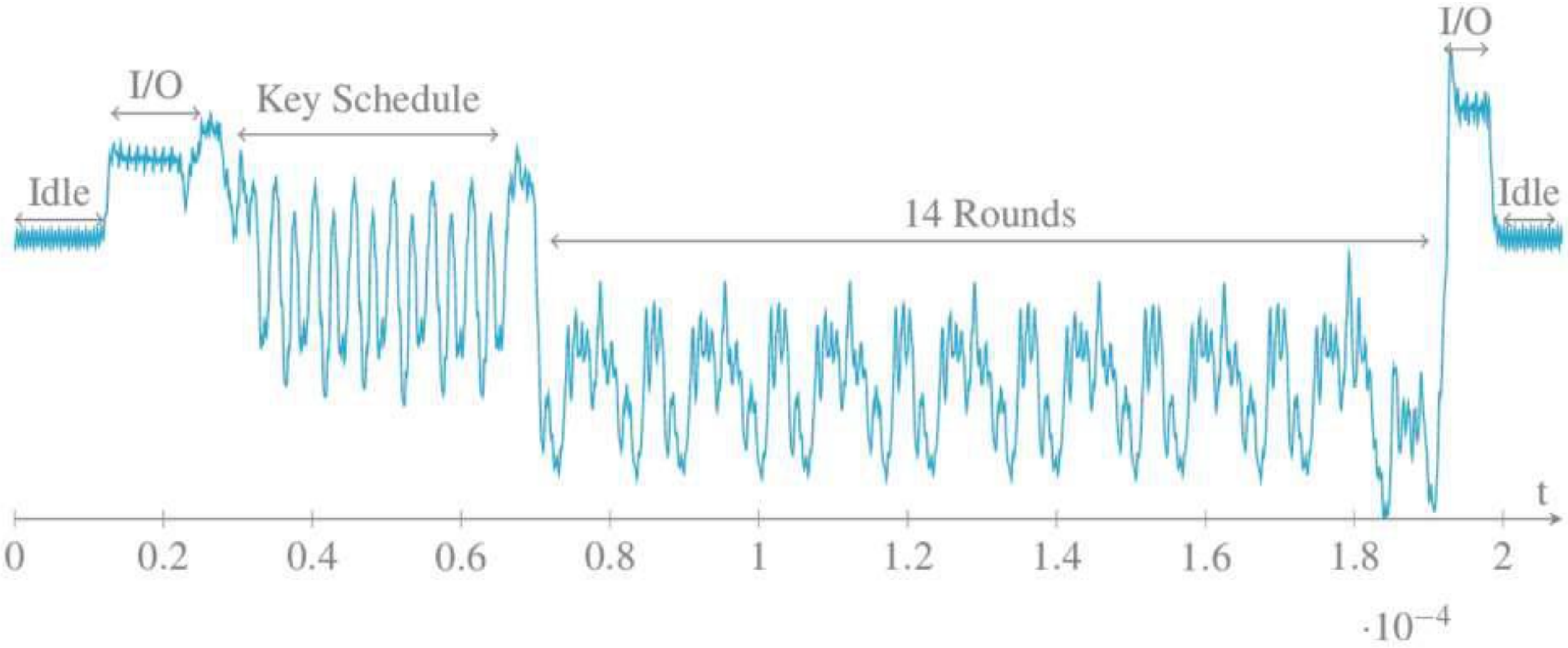
USRP B200

Low-end
€755
56 MHz
184 MB/s

RTLSDR

Budget
€20
2.4 MHz
5.2 MB/s

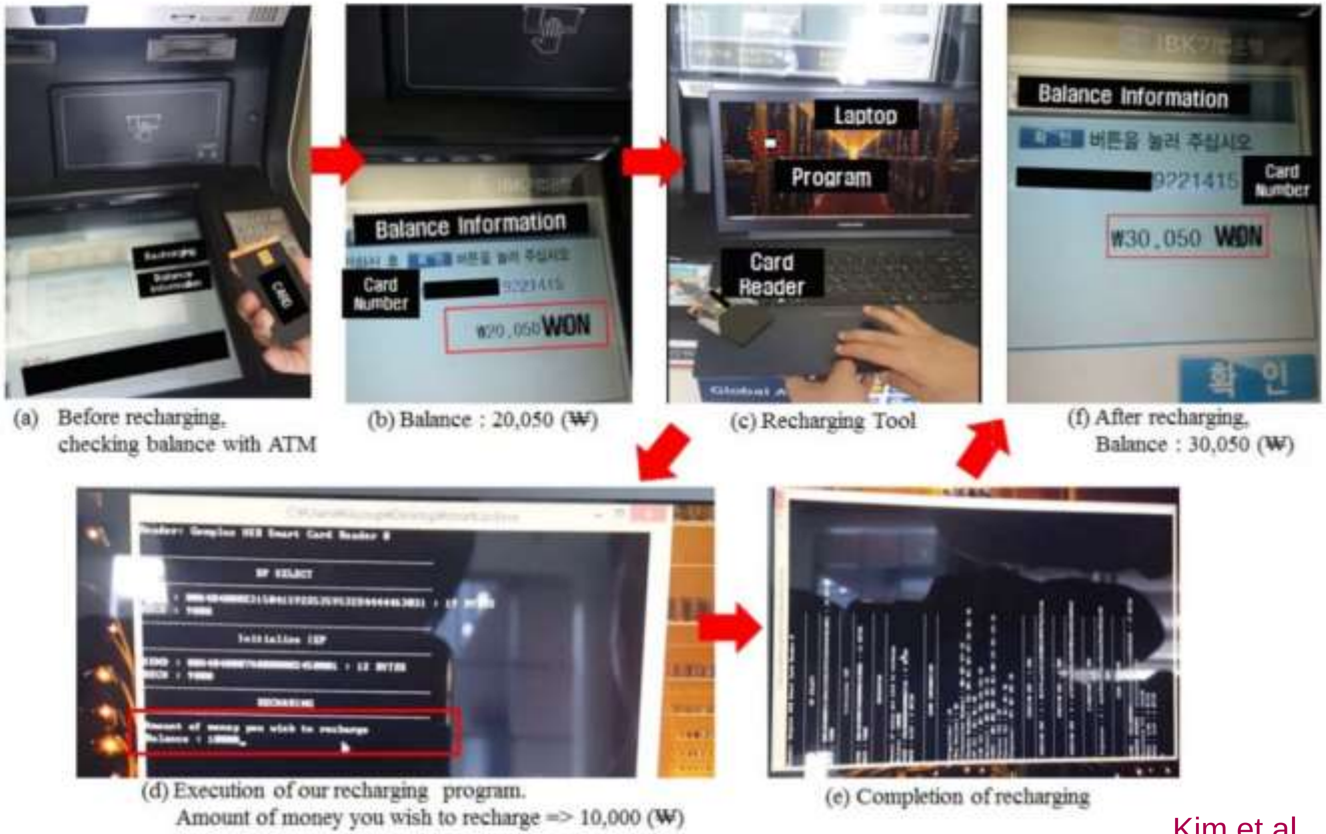
Simple Power Analysis: AES-256



Overview trace showing pattern dependent on AES algorithm

Practical Power/EM Analysis Attacks

- Smart Cards – credit cards, etc. are vulnerable to these attacks
- IoT devices – 8/16-bit microcontrollers can be attacked
- Counterfeiting of e-cigarettes to gain market share



(a) Before recharging, checking balance with ATM

(b) Balance : 20,050 (₩)

(c) Recharging Tool

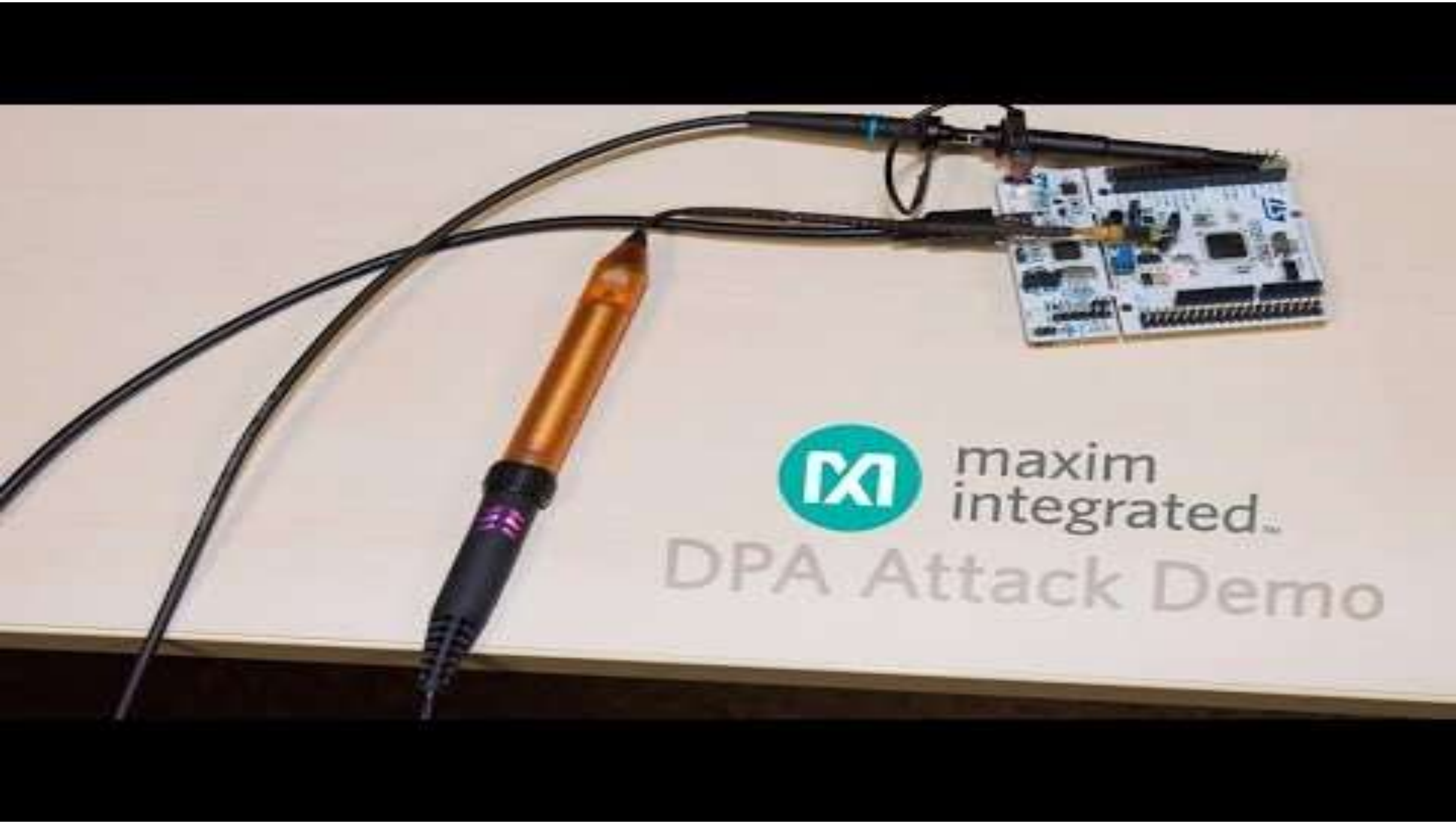
(f) After recharging, Balance : 30,050 (₩)

(d) Execution of our recharging program. Amount of money you wish to recharge => 10,000 (₩)

(e) Completion of recharging

Kim et al., Blackhat Asia 2017

Real Example (Maxim)

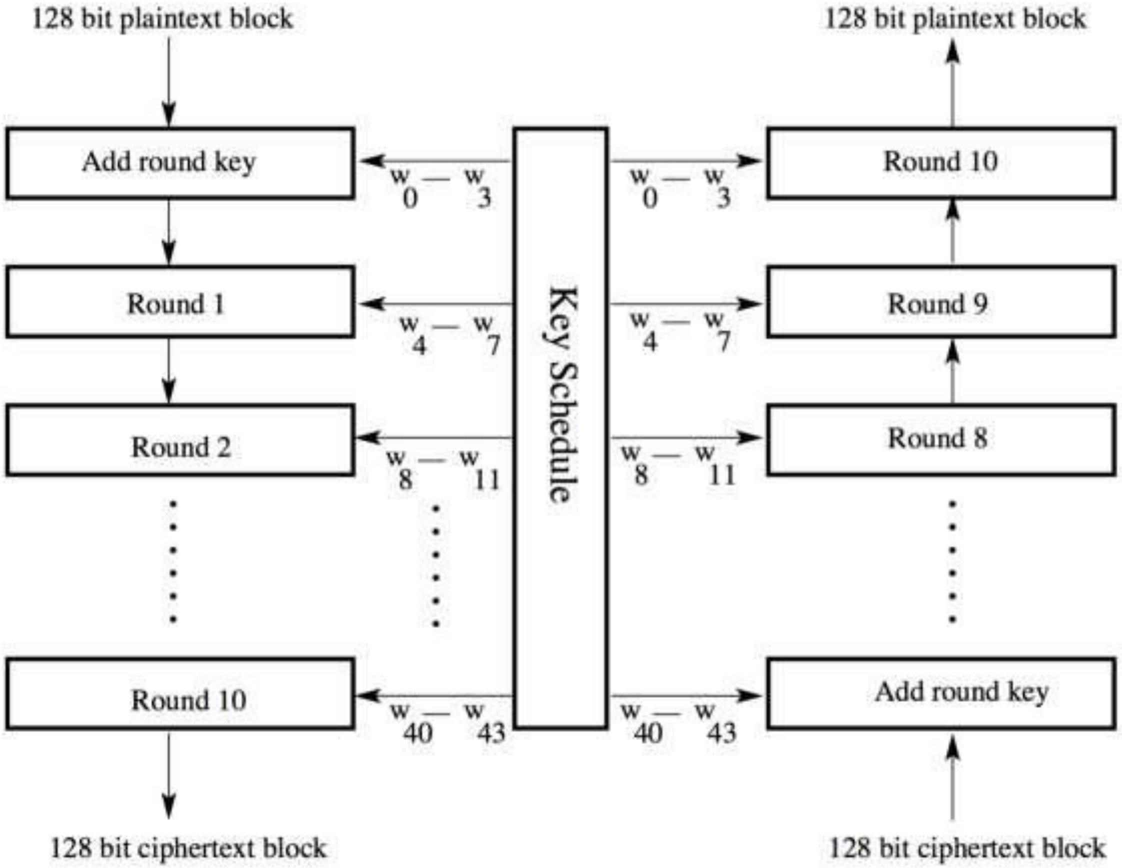


Q&A

Outline

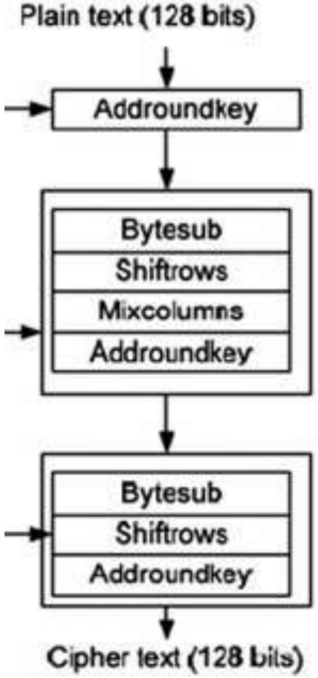
Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

Encryption → AES



AES Encryption

AES Decryption



- Symmetric Key Encryption
- Algorithm Known
- Key Secret

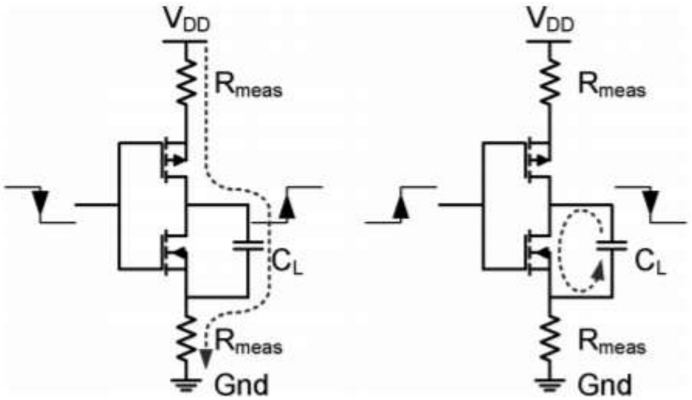
Physical Attacks

- Traditional cryptography revolves around the concepts of one-way and trapdoor functions.
- **One-wayness:** The function is easy to compute, but hard to invert.
- A trapdoor one-way algorithm involves a function which is easily invertible if and only if the secret "key" is available.
- Physical attacks occur in 2 phases:
  - Data collection: The attacker exploits certain physical characteristics (power/EM) of the device under attack.
  - Attack: Run statistical analysis on the gathered traces to recover the secret key.

EM & Power Side-Channel Analysis: Attack Models

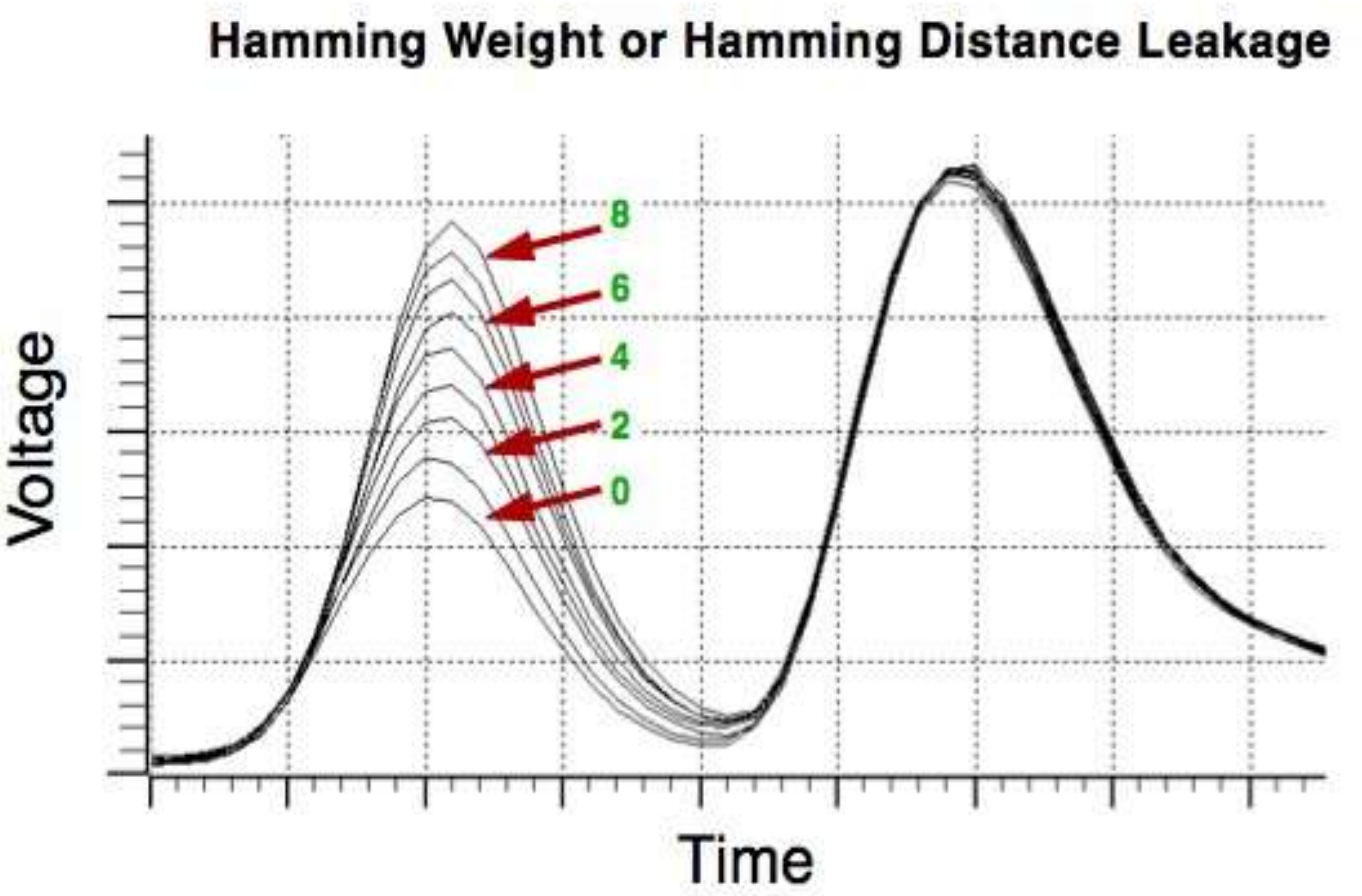
- Power consumption (& EM radiation) proportional to the total **number of bit flips**.
- Hamming Weight (HW) Model: Number of 1's on the data bus
- Hamming Distance (HD) Model: Number of bits switching from previous state to the next.
- HW model is a special case of the HD model.
- Dynamic Power (0->1)

$$P_{dyn} = C_L V_{DD}^2 P_{0\to1} f$$



Cl -> load capacitance
Vdd -> supply voltage
P0->1 -> probability of a 0->1 transition
f -> frequency

Information Leakage

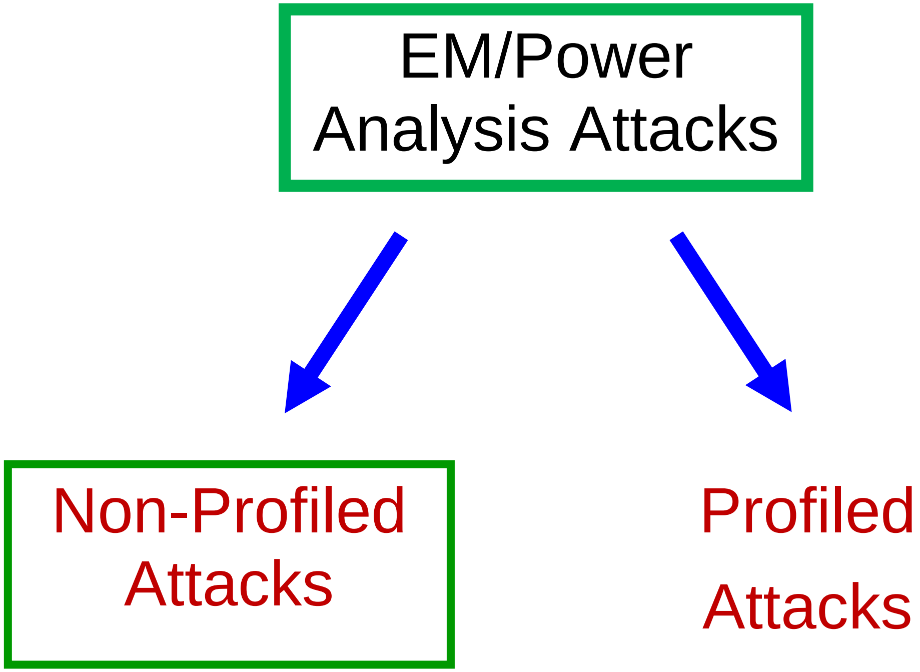


Attack Models: HW vs HD

- Hamming Weight (HW) Model: Crude model, but useful for software implementations in microcontrollers.

- Hamming Distance (HD) Model: Considers both 1-0 and 0-1 transitions equal, useful for hardware implementations where the same register is used to store the updated states.

Non-Profiled and Profiled attacks



EM/Power Analysis Attacks

Non-Profiled Attacks

Profiled Attacks

- Non-Profiled SCA:
  - Direct attack on a target device using HW/HD leakage model.
  - Eg. Differential/Correlational power analysis (DPA/CPA).
- Profiled SCA attack:
  - Build offline template using an identical device
  - Perform attack on a similar device with fewer traces (more powerful attack).
  - Eg. Statistical template attacks, machine learning based attacks.

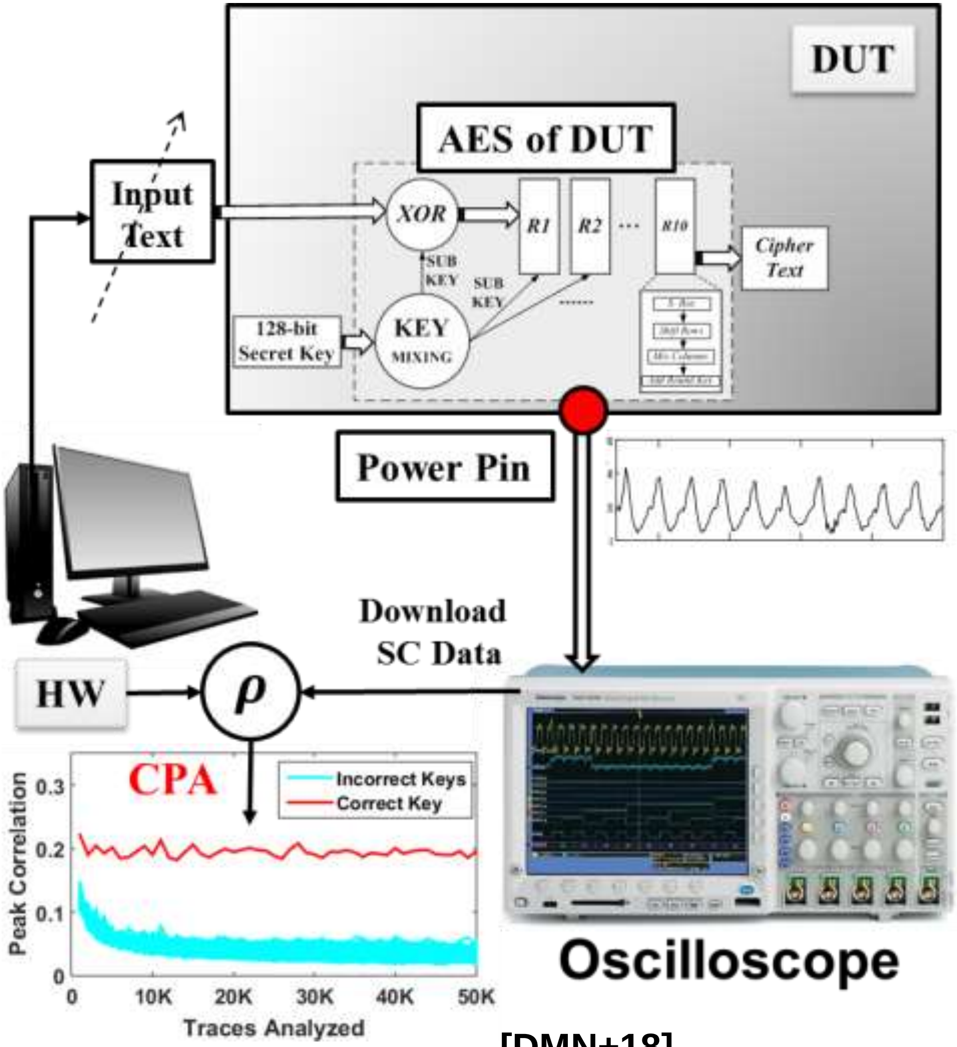
Attack Modalities

- Chosen Plaintext Attack: Assumes that the attacker has full control on the device and can collect power/EM traces for different input plaintexts.
  - Easy attack on microcontrollers, useful to test countermeasures on software implementations
- Known Ciphertext Attack: Practical attack, assumes the attacker can collect power/EM traces corresponding to each ciphertext.
  - Useful to attack well-designed hardware crypto implementations with HD models

Non-Profiled SCA: CPA (and CEMA)

- Correlational Power Analysis (CPA) Attack:
  - Step 1: Identify point of attack – usually 1st round S-box output for AES-128/256 with chosen PT attack (or, the last round HD attack based on CT).
  - Step 2: Choose HW or HD model depending on the platform for attack. Eg. HW model for software AES.
  - Step 3: Make a guess for key byte. Repeat for all 256 key guesses (0 to 255 for each key byte).
  - Step 4: Compute HW of data transition for each PT value.
  - Step 5: Compute correlation coefficient between the HW matrix and the power traces.
  - Step 6: Repeat for all 16 key bytes to recover the AES-128 key

Non-Profiled SCA: CPA (and CEMA)



[DMN+18]

- Collect power traces (T).
- Build a power hypothesis (H).
- Correlate the measured & expected traces.

$$\rho_{TH} = \frac{Cov\,(T,H)}{\sigma_T * \sigma_H}$$

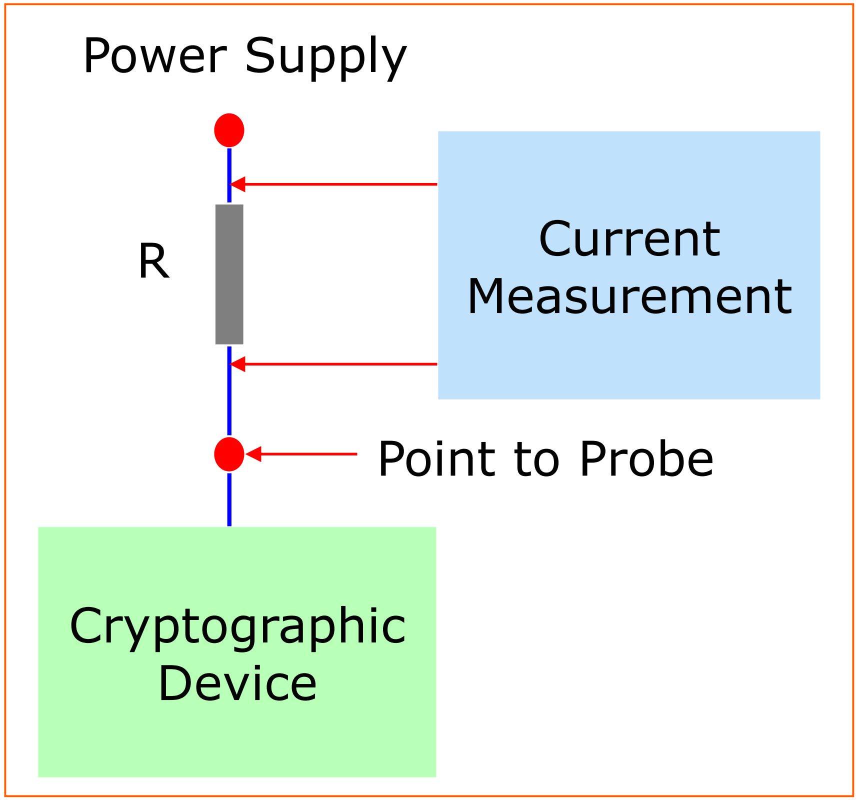
ρ: Correlation co-efficien

σ: Standard Deviation

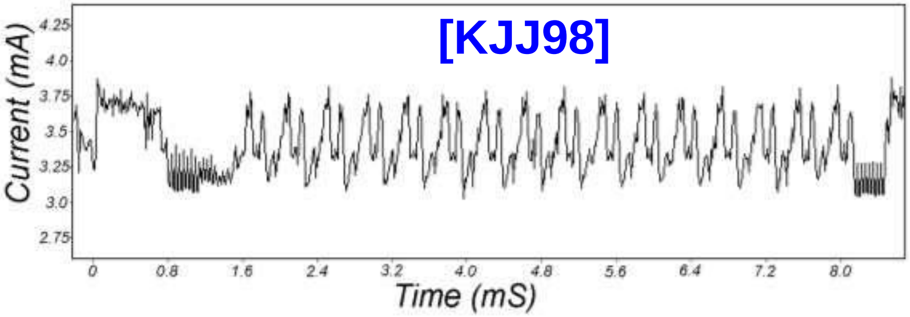
Cov: Covariance

- More Traces -> Better chance of finding key

Power Analysis Attacks



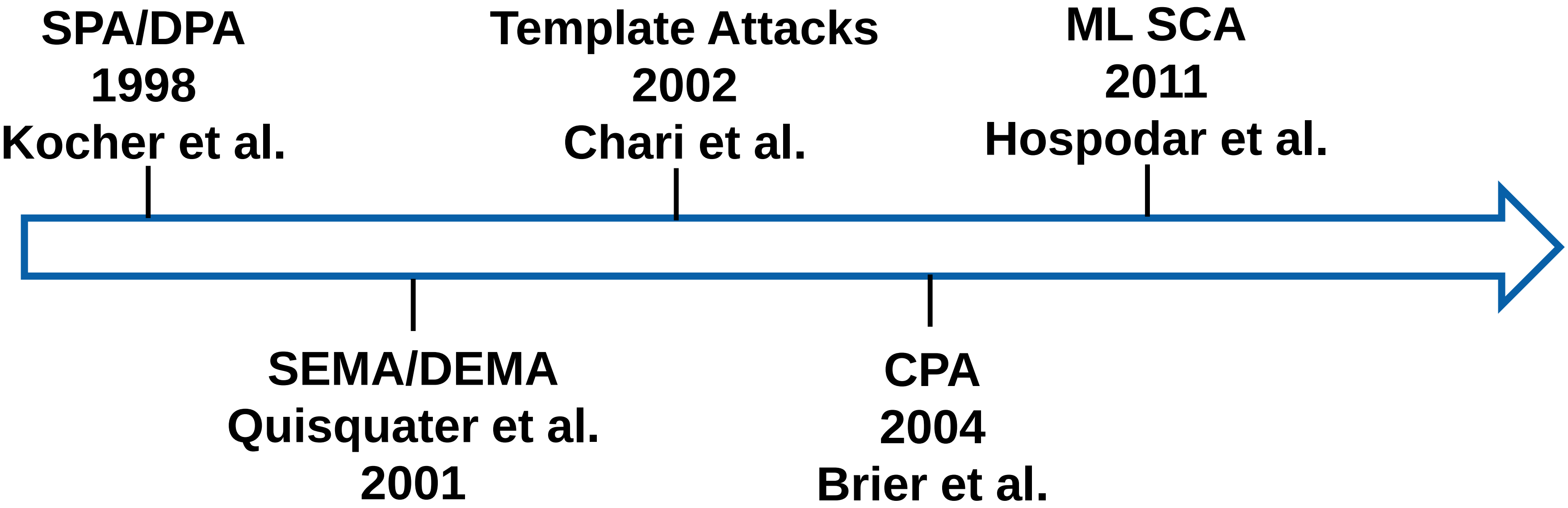
- First attack demonstrated by Kocher et al. in 1998.
- Simple Power Analysis (SPA) and Differential Power Analysis (DPA) used to break DES.



[KJJ98]

Figure 1: SPA trace showing an entire DES operation.

Power and EM SCA Attacks: History



SPA/DPA
1998
Kocher et al.

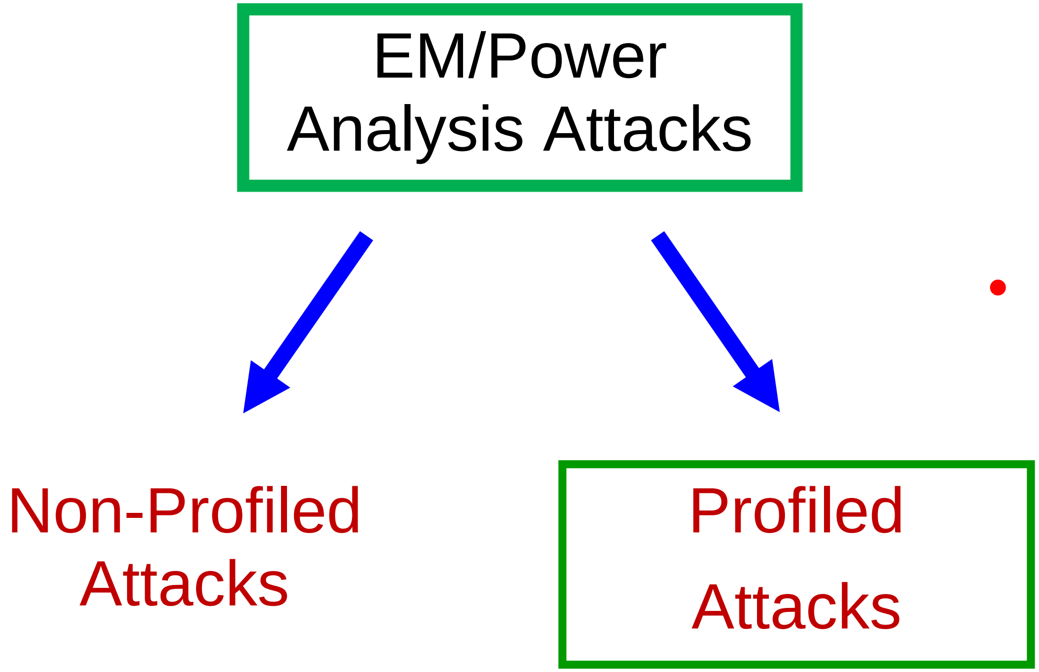
SEMA/DEMA
Quisquater et al.
2001

Template Attacks
2002
Chari et al.

CPA
2004
Brier et al.

ML SCA
2011
Hospodar et al.

Non-Profiled and Profiled attacks



EM/Power Analysis Attacks

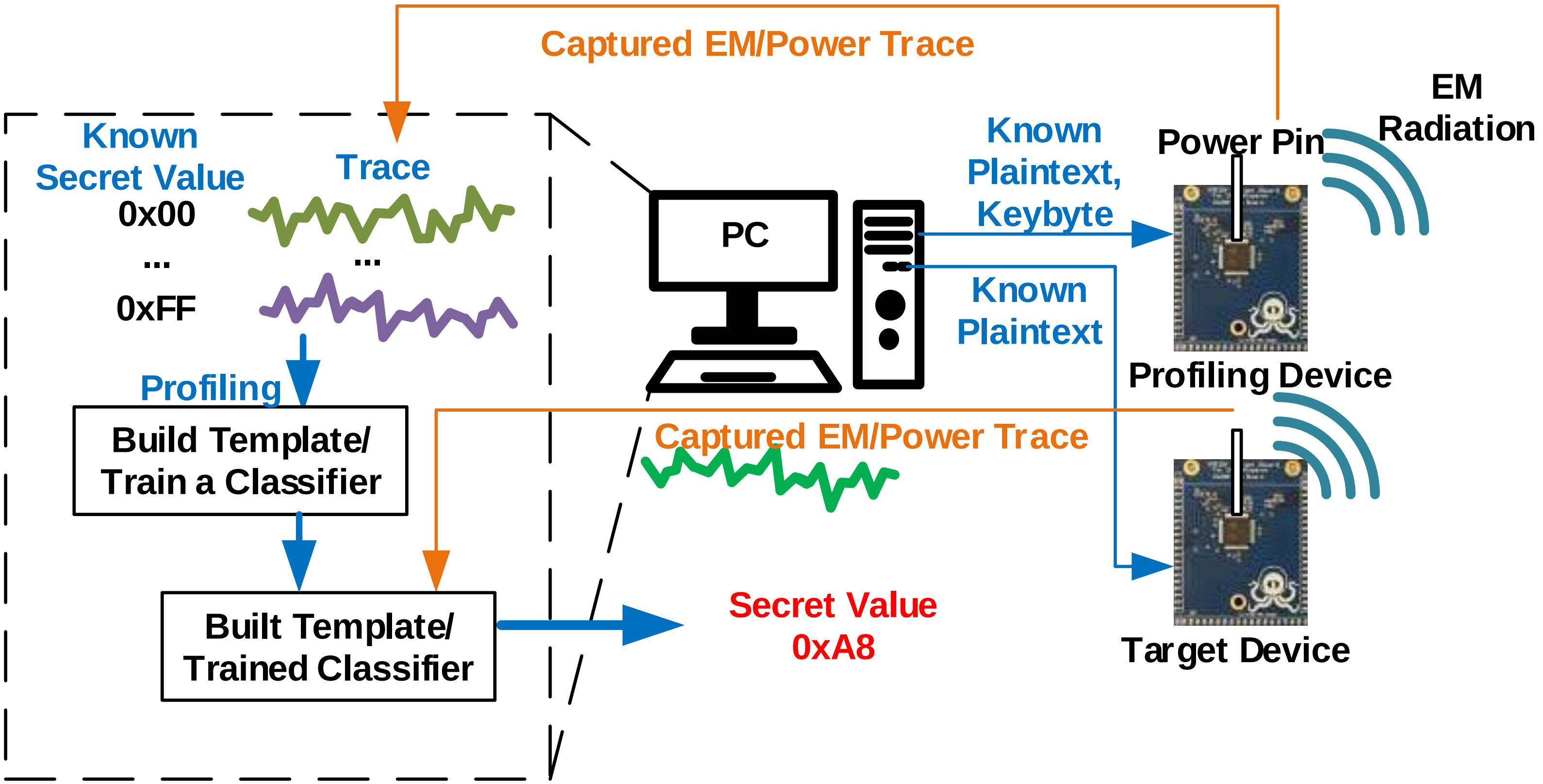
Non-Profiled Attacks

Profiled Attacks

- Non-Profiled SCA:
  - Direct attack on a target device using HW/HD leakage model.
  - Eg. Differential/Correlational power analysis (DPA/CPA).

- Profiled SCA attack:
  - Build offline template using an identical device
  - Perform attack on a similar device with fewer traces (more powerful attack).
  - Eg. Statistical template attacks, machine learning based attacks.

Profiled attack



Literature Review of Profiled Attacks

Profiled Attack Scenario	Method	Corresponding Articles
Same-device Attack	Gaussian Template Attack	[CRR02], [RO04], [OM07]
	Support Vector Machine	[BL12], [HZ12], [LBM14], [LBM15]
	Random Forest	[LBM14]
	Neural Networks	[MHM13], [GHO15], [MPP16], [MDM16], [CDP17], [BPS+18]
Cross-device Attack	Gaussian Template Attack	[RSV+11], [MBT+13], [HOT+14], [OK18]
	Neural Networks	[DGD+19],[CCC+19], [GDD+19]

Gaussian Distribution based Template Attack

- First elaborated in [CRR02]
- During profiling phase, leakage vectors (traces) are recorded
- Sample mean vector ($\overline{\mathbf{x}_k}$) and sample covariance matrix ($\mathbf{S}_k$) for each possible intermediate (secret) value (k) can estimate true mean and true covariance for sufficient number of leakage vectors.
- As side-channel leakage traces can generally be modeled well by a multivariate normal distribution, sample mean and sample covariance matrix completely define underlying probability distribution of leakage vector $\mathbf{x}$ by:

$$f(\mathbf{x} \mid k) = \frac{1}{\sqrt{(2\pi)^m |\mathbf{S}_k|}} \cdot e^{-\frac{1}{2}(\mathbf{x}-\bar{\mathbf{x}}_k)' \mathbf{S}_k^{-1} (\mathbf{x}-\bar{\mathbf{x}}_k)}$$

- In the attack phase, using each recorded trace, $\mathbf{x}_i$,a discriminant score, $D(k|\mathbf{x}_i\mathbf{)}$ is computed for each possible *k* (derived from Bayes' rule), where $P(k)$ = a-priori probability of the secret value, *k*:

$$D(k \mid \mathbf{x}_i) = f(\mathbf{x}_i \mid k) P(k)$$

- By ordering the discriminant scores for each *k*, we find the correct secret value.

Numerical Problems in Template based Attack and Solutions

- Number of leakage traces per candidate value should be greater than the number of dimensions per trace so that sample covariance matrix is non-singular [OK18], due to some samples being highly correlated.

- Using pooled Covariance matrix [OK18] instead of separate covariance matrices for each candidate value provides a better estimate and satisfies the above criteria easily

- Selection of Samples (Points of Interest – PoI) by Difference of Means (DOM), Sum of Squared Differences (SOSD), Signal-to-Noise ratio (SNR) helps reduce the number of samples per trace

- Reducing the number of dimensions using Principal Component Analysis (PCA) or Fisher’s Linear Discriminant Analysis (LDA) also improves the performance of template attack

Q&A

Outline

Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

SCA Countermeasures

Logical

- SABL
- WDDL
- Gate-level Masking

Architectural

- Random Insertion of operations
- Shuffling of Operations
- Software Masking

Physical

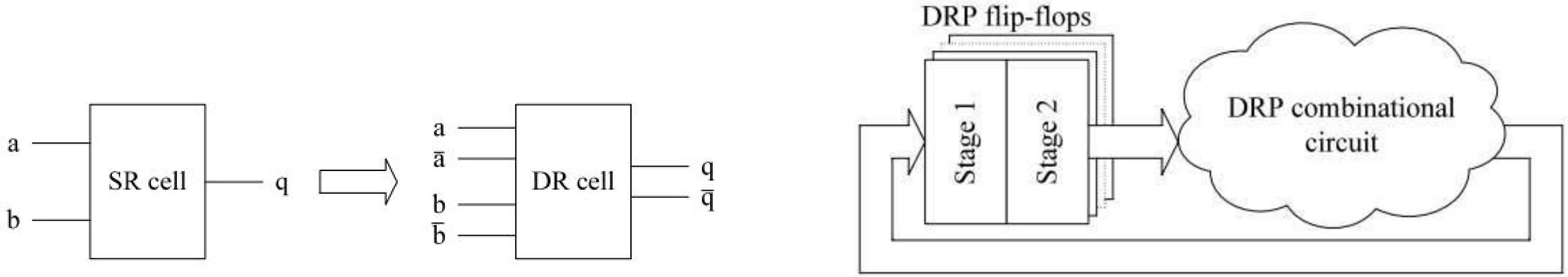
- Noise Injection
- Switched Capacitor
- IVR
- ASNI

Logic Level Countermeasures

- Sticking to the same architecture, the focus is on designing DPA resistant logic styles which consume equal power in each clock cycle.
- **Two approaches:**
  - Designing entirely new dual-rail logic cells (due to high customizability), or
  - Using single-rail cells available in Standard Cell libraries (due to reduced design effort).

Basics of Logic Level Countermeasure: Dual Rail Precharge (DRP) Logic Style

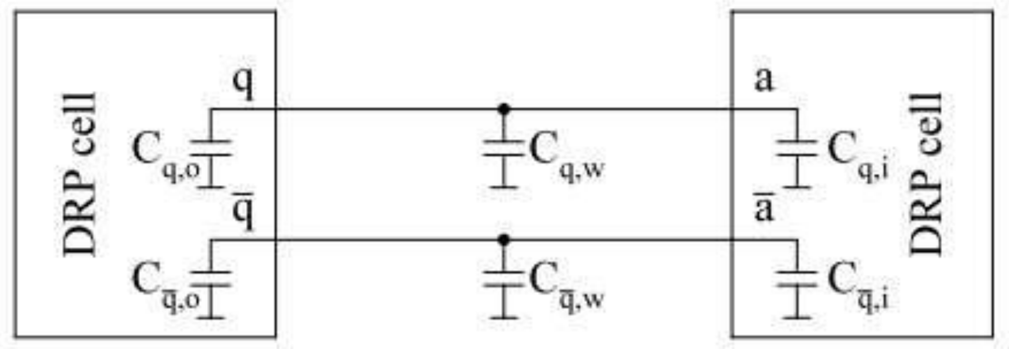
- Combination of *Dual Rail Logic* (input and output signals are carried on complimentary wires) and *Precharge Logic* (signals set to a predefined precharge value before evaluation)
- In DRP cells, always one of the outputs (either original output or its complemented version) transitions, making power consumption of the cells constant.
- DRP flip-flops consist of two stages, so as to provide stored values in Stage 2 to combinational DRP cells during precharge phase of Stage 1, and to store outputs of combinational values in Stage 1 before precharge phase of Stage 2, thus preventing data loss.



DRP Logic style [MOP07]

DRP Logic Style: Tricks to ensure constant power consumption

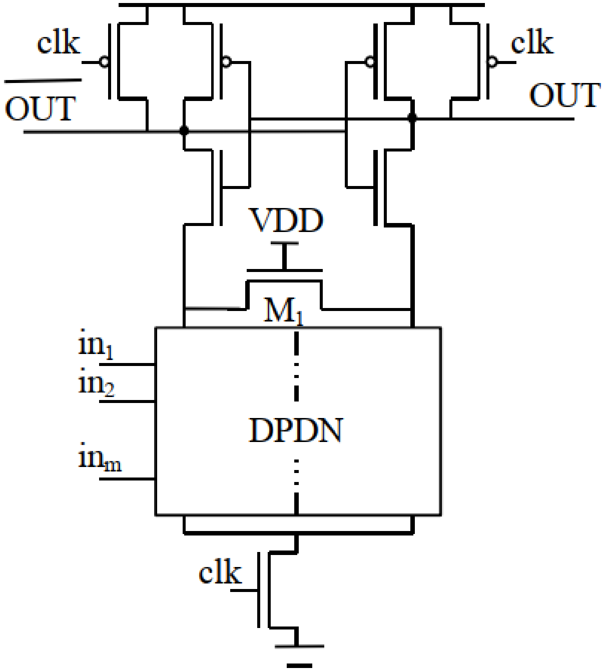
- Need to balance the capacitances at the complimentary outputs of a DRP cell
- **Balancing the complimentary outputs:** Dominating factor in modern process technologies is the interconnect capacitance (than input or output capacitance of cells) which should be done during place and route.
- **Balancing the internal power consumption:** Internal power consumption of DRP cells should be made constant by charging or discharging all internal nodes in each clock cycle.



Balancing the complimentary outputs [MOP07]

Logic Level Hiding: Sense Amplifier Based Logic (SABL)

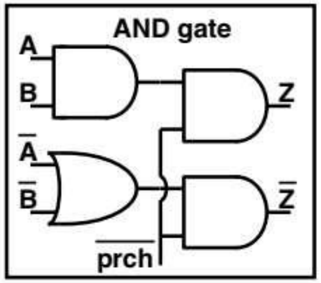
- SABL achieves uniform power consumption by:
  - Employing a Dynamic and Differential Logic style and therefore having exactly one switching event per cycle
  - Making Time of Evaluation data independent (cells evaluate after all signals are set to complementary values)
  - Making the four output transitions (0-0, 0-1, 1-0, 1-1) equal by charging/discharging constant load capacitance: one of the balanced output load capacitances together with the sum of all internal node capacitances.
- Requires design and characterization of complete new standard cell library.
- Area requirement doubles compared to CMOS counterpart.



Sense Amplifier Based Logic (SABL) [TAV02]

Logic Level Hiding: Wave Dynamic Differential Logic (WDDL)

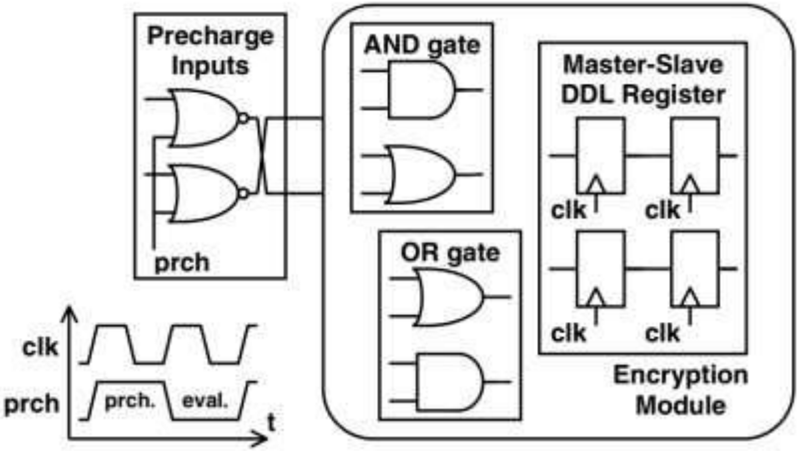
- Built based on Single Rail AND and OR cells (used to implement original and complemented version of a logic function) which can be found in Standard Cell Library
- Combinational WDDL gates do not pre-charge simultaneously. The pre-charged 0’s ripple through the combinational logic, therefore there is a pre-charge wave (hence the name).
- Under the assumption that the differential signals travel in the same environment, the interconnect capacitance are equivalent, which ensures the total capacitance to be charged is of constant value.
- Can be realized in FPGAs.



$(A.B).\overline{prch} \leftrightarrow (\overline{A}+\overline{B}).\overline{prch}$

A	B	$\overline{A}$	$\overline{B}$	prch	Z	$\overline{Z}$
0	0	1	1	0	0	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	0	0	0	1	0
X	X	X	X	1	0	0

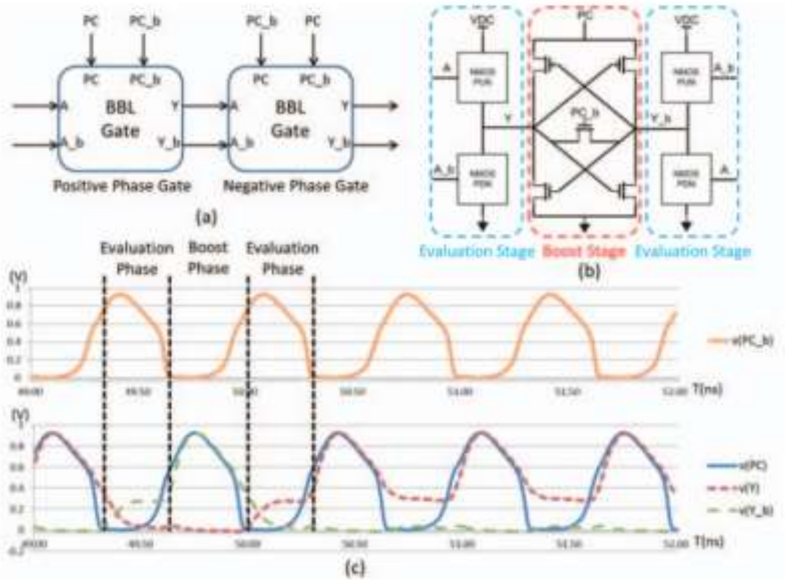
Simple Dynamic Differential Logic (SDDL) [TV04]



Wave Dynamic Differential Logic (WDDL) [TV04]

Logic Level Hiding: Bridge Boost Logic (BBL)

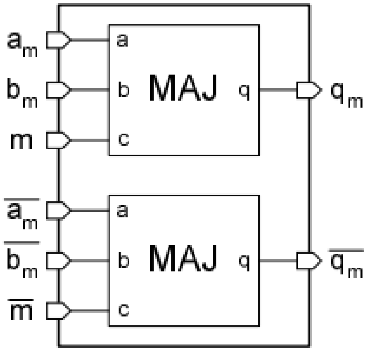
- A logic style which uses a bridge transistor to equalize currents in the evaluation stage.
- Bridge transistor shorts the PUN and PDN on the opposite sides of the evaluation stage to conduct the same current regardless of the previous state.
- At the end of evaluation phase, the bridging transistor makes sure that the voltage difference between the complementary outputs is always the same, enabling Boost stage to boost it up to the same level of the clock signal.

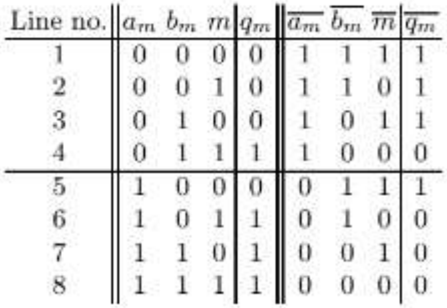


Bridge Boost Logic (BBL) [LZP15]

Logic Level Masking: Masked Dual-Rail Pre-charge Logic (MDPL)

- Uses masking at the gate level
- Avoids glitches in the circuit by Dual-Rail Pre-charge
- Can be built from Standard Cell Libraries as outputs of MDPL AND Gate can be calculated by Majority (MAJ) gate (available in Standard Cell Libraries), and all other combinational MDPL gates are based on this one
- Every signal is masked with the same mask
- Pre-charge wave is similar to WDDL





Line no.	a_m	b_m	m	q_m	$\overline{a_m}$	$\overline{b_m}$	$\overline{m}$	$\overline{q_m}$
1	0	0	0	0	1	1	1	1
2	0	0	1	0	1	1	0	1
3	0	1	0	0	1	0	1	1
4	0	1	1	1	1	0	0	0
5	1	0	0	0	0	1	1	1
6	1	0	1	1	0	1	0	0
7	1	1	0	1	0	0	1	0
8	1	1	1	1	0	0	0	0

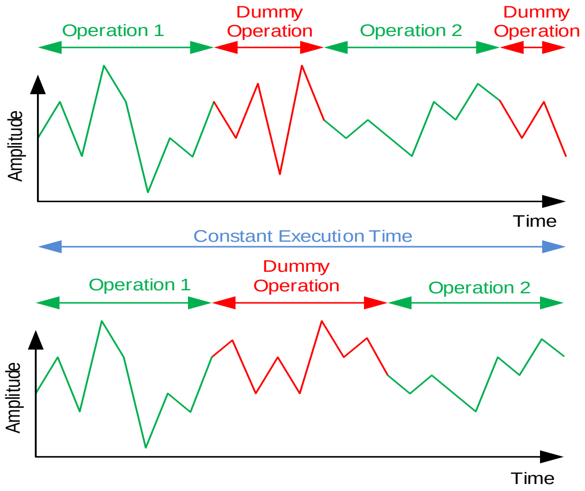
Masked Dual-Rail Pre-Charge Logic (MDPL) AND Gate [PM05], [PKZ+07]

Architecture Level Hiding Countermeasure for Software Implementations

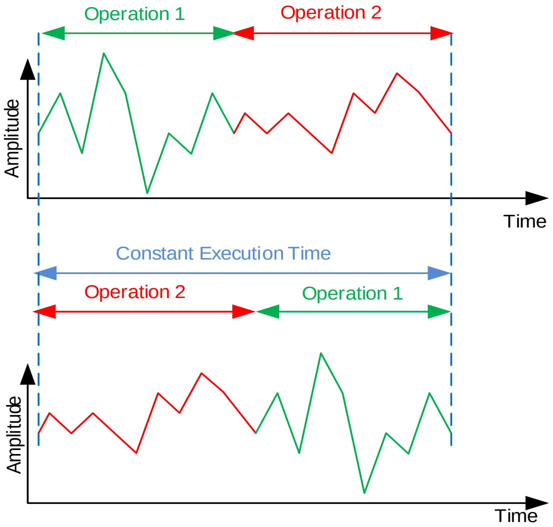
- The power consumption characteristics is defined by the underlying hardware
- Introducing Time Distortion:
  - Can be done only by random insertion of dummy operations or by shuffling of operations
  - Does not provide high level of protection
- Introducing Amplitude Distortion:
  - By choosing instructions with lowest leakage, avoiding conditional jumps or usage of memory addresses depending on key, and thus reducing amplitude of leakage
  - By performing activities parallel to the execution of cryptographic algorithm

Architectural Countermeasure: Time Distortion

- **Random Insertion of Dummy Operations:**
  - Dummy operations (not present in actual algorithm) are performed at random times, keeping the total execution time constant.
  - Affects the throughput.

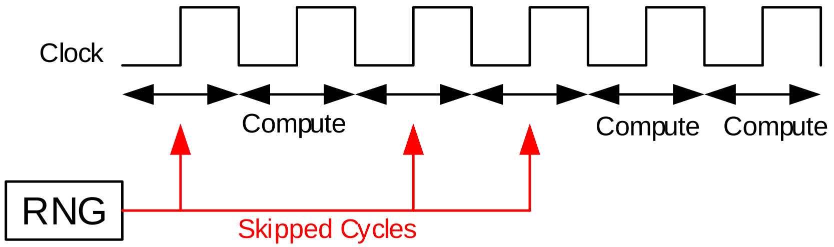


- **Shuffling of Operations:**
  - Independent operations such as, 16 AES S-box lookups for AES-128 can be performed in arbitrary order.
  - Does not affect throughput as much.
  - Number of operations that can be shuffled are limited depending on the algorithm and the architecture of the.

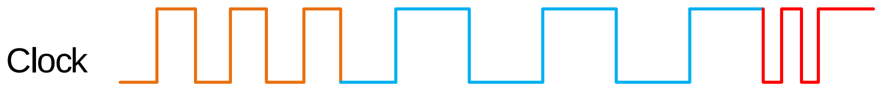


Architectural Countermeasure: Time Distortion

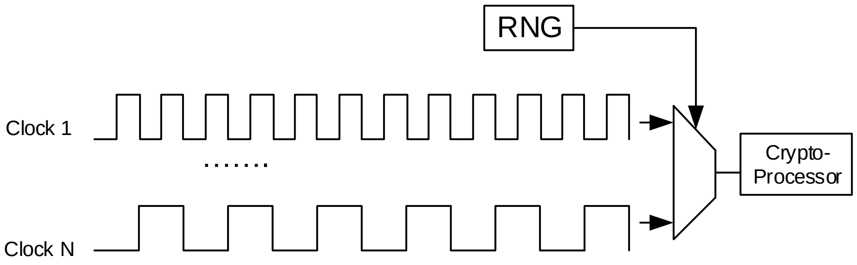
- **Skipping of Clock Pulses:**
  - RNGs are used to randomly skip clock pulses



- **Randomly Changing Clock Frequency:**
  - Internal oscillator based on RNG controls the operating frequency of the clock signal

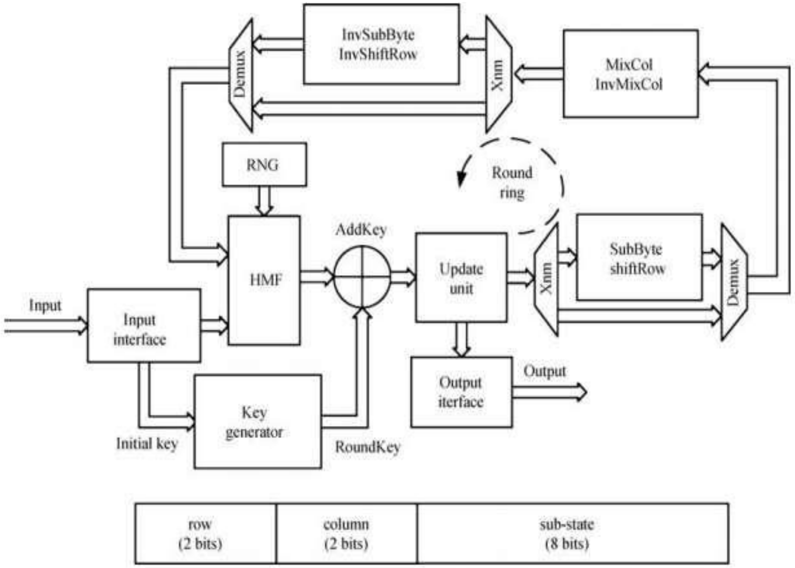


- **Multiple Clock Domains:**
  - Randomly switching between several clock signals generated on the device



Architecture Level Hiding: Random Order Execution

- AddRoundKey, SubBytes and ShiftRows are performed at byte level
- 16 bytes of a state can be independently processed by these operations
- Although MixColumns involves linear multiplications between columns of a state and a constant matrix, it can be decomposed into a set of independent byte-grained multiplication and additions
- 16-byte grained operations can be executed in any order.



Random Order Execution [BXC+12]

Architecture Level Masking: for Software Implementations

- Boolean Masking for linear operations:
  - Intermediate values can easily be masked, and masks can be removed at the end of computation
- Masking Table Look-Ups for non-linear operations:
  - Block ciphers allow implementing non-linear operations as table look-ups
  - Look-Up Tables need to store masked values of actual intermediate value for masked intermediate values, such that the mask can be removed by an exclusive-OR operation later on.
- Random Pre-charging:
  - To prevent Hamming Distance (HD)-based leakage, loading or storing a random value before the actual intermediate value changes leakage profile

Architecture Level Masking: for Hardware Implementations

- Boolean Masking
- Masking Multipliers
- Random Pre-charging:
  - By using duplicate registers (by doubling original number of registers) such that on each clock cycle one set of registers contain random values
- Masking Buses:
  - By using duplicate registers (by doubling original number of registers) such that on each clock cycle one set of registers contain random values

Physical Countermeasures

- Noise Injection: High power/area overheads.
- Switched Capacitor Current Equalizer: Supply Current Equalization [4]; 2x performance degradation.
- Supply regulation-based: LDO-based - security by obfuscating the performance parameters [5], buck converter-based [6] – embedded passives.
- An ideal LDO-based implementation is inherently insecure.
- IVR: High area overheads, may not be suited for IoT devices or microcontrollers.
- STELLAR: Generic low-overhead technique to prevent both power and EM SCA attacks

State-of-the-art HW schemes for SCA resistance

Power Balancing

- Dual rail logic, WDDL
- Equalizes power for rising/falling clock edges.
- WDDL 1st in-silicon circuit validation with MTD~21K [1].
- Incurs 4x power overhead, 3x area, 4x performance degradation

[1] D. D. Hwang et al., "AES-Based Security Coprocessor IC in 0.18- CMOS with Resistance to Differential Power Analysis Side-Channel Attacks", JSSC 2006.

Hardware Gate level masking

- Versatile technique
- Modifies the logic gates to consume symmetric power for both 0 and 1 logic operations [2].
- High Area & power overhead

[2] J. Balasch et al., DPA, Bitslicing and Masking at 1 GHz, CHES-2015

Noise Injection

- Active suppression, reducing SNR.
- High power overhead [3]

[3] T. Güneysu et.al. "Generic Side-Channel Countermeasures for Reconfigurable Devices," CHES, 2011
[4] C. Tokunaga et.al. "Securing Encryption Systems with a Switched Capacitor Current Equalizer," IEEE JSSC, 2010

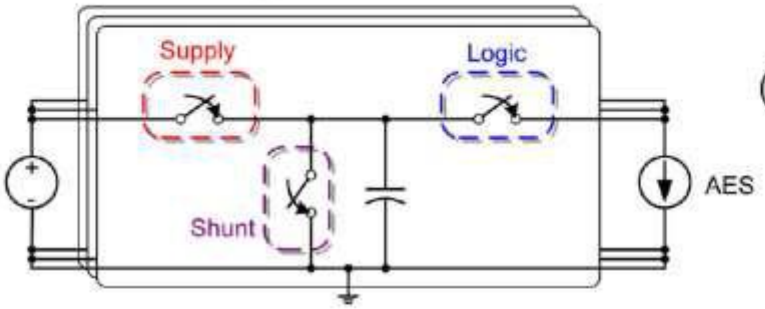
Supply Isolation

- Switched capacitors: Supply Current Equalization [4]; 2x performance degradation.
- Supply regulation-based: LDO-based [5], buck converter-based [6] – embedded passives.
- An ideal LDO-based implementation is inherently insecure.

[5] A. Singh et al. "Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines," *HOST*, 2016.
[6] M. Kar et al. "Improved Power-Side-Channel-Attack Resistance of an AES-128 Core via a Security-Aware Integrated Buck Voltage Regulator", ISSCC 2017.

Switch Capacitor Equalizer

Current Equalizer Block
3 Switching Capacitor Modules

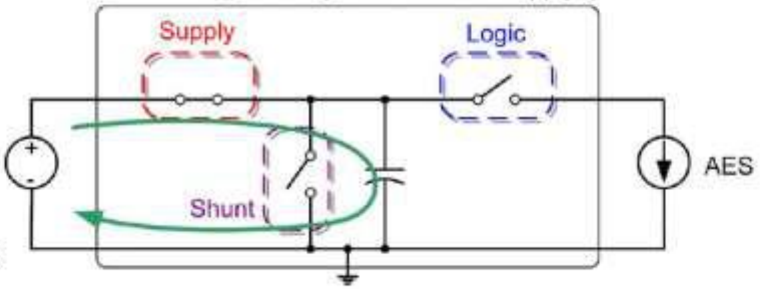


Staggered switching pattern

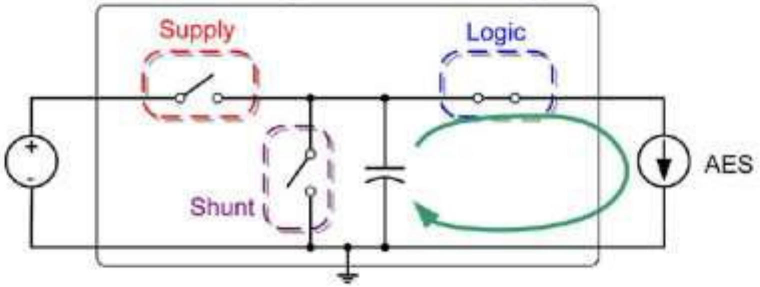
SC Module	Sequence	t_0	t_1	t_2
1	S1	🟥		
	S2		🟦	
	S3			🟪
2	S1		🟥	
	S2			🟦
	S3	🟪		
3	S1			🟥
	S2	🟦		
	S3		🟪	

3 switching states: S1, S2, S3

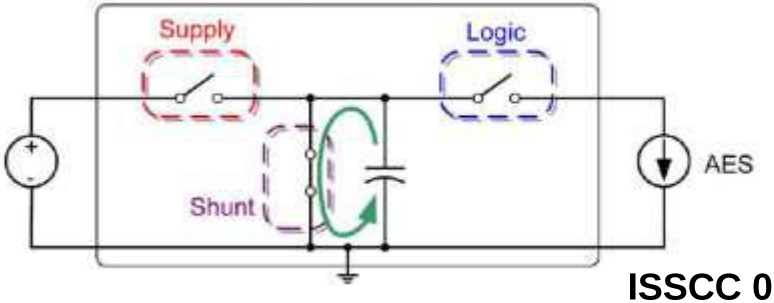
S1: Charge the capacitor from the supply



S2: Provide charge to the core for encryption



S3: Discharge the capacitor to a pre-defined value

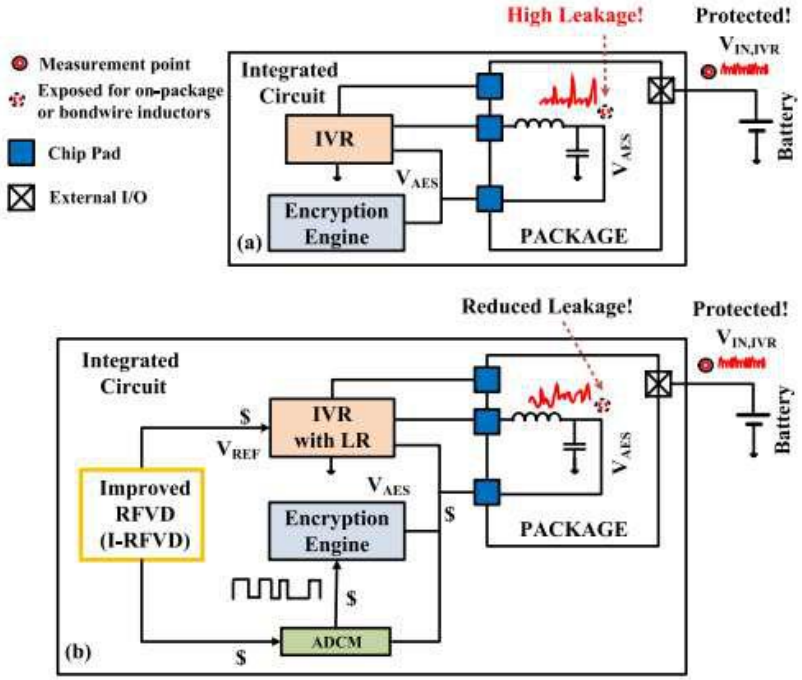


ISSCC 09, JSSC 10

Physical Countermeasure: Random Fast Voltage Dithering (RFVD)

- High-frequency, high-bandwidth IVR (Integrated Voltage Regulator) is used to dither the voltage around the target level by randomly assign a different voltage for each encryption (Amplitude distortion)

- ADCM (All-Digital Clock Modulation) circuit transforms voltage variations to dithering of the clock edges to ensure correct operation while creating timing randomness (Time distortion)



Random Fast Voltage Dithering [SKM+18]

Overview: New Attacks and Defenses

Attack

SCNIFFER: Automated EM leakage point detection

X-DeepSCA: Cross-Device Deep-Learning SCA

Power & Electro-Magnetic Side-Channel

Defense

ASNI: Attenuated Signature Noise Injection

White-Box Root-Cause Analysis

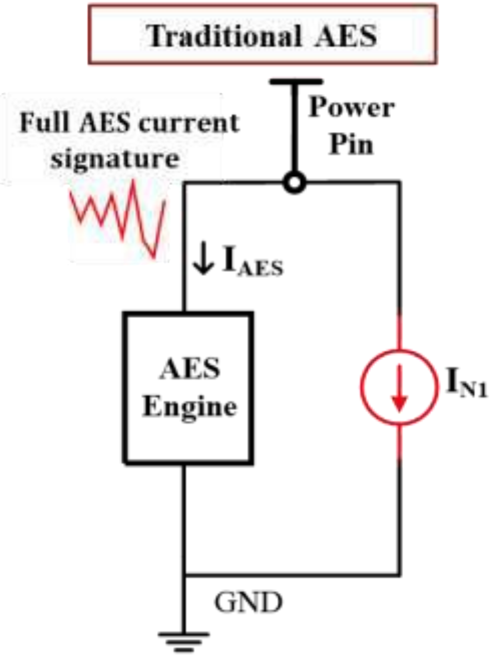
STELLAR: Generic EM SCA Tolerance

High-Efficiency Power SCA Immunity

- Need a low-overhead & generic technique, with no performance degradation.

- Suppress the Crypto current signature in the supply traces.

ASNI: Signature Suppression

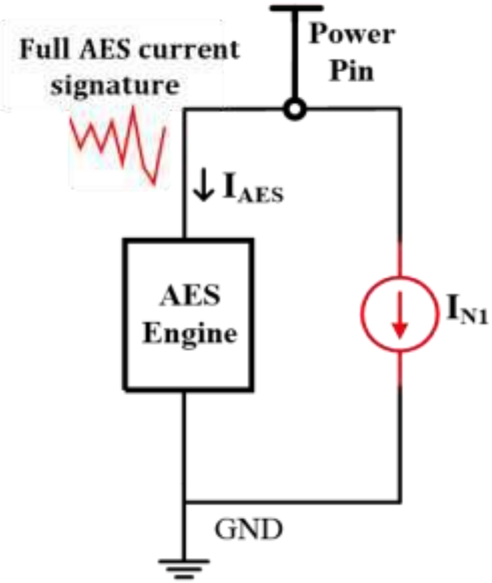


$$I_{Ov1} = I_{N1}$$

$$\rho_{T'H_1} = \frac{Cov(T,H)}{\sqrt{\sigma_T^2 + \sigma_{N_1}^2} * \sigma_H}$$

ASNI: Signature Suppression

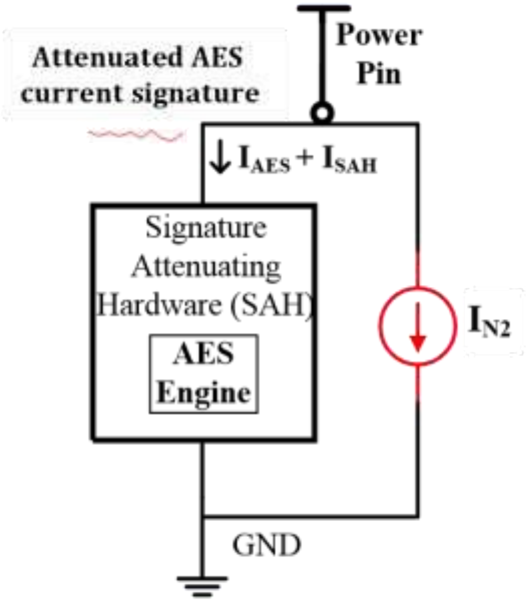
Traditional AES



$$I_{Ov1} = I_{N1}$$

$$\rho_{T'H_1} = \frac{Cov(T,H)}{\sqrt{\sigma_T^2 + \sigma_{N_1}^2} * \sigma_H}$$

ASNI-AES


Attenuated AES current signature
Power Pin
$\downarrow I_{AES} + I_{SAH}$
Signature Attenuating Hardware (SAH)
AES Engine
I_{N2}
GND

$$I_{Ov2} = I_{N2} + I_{SAH}$$

$$\rho_{T'H_2} = \frac{\frac{1}{AT} * Cov(T,H)}{\sqrt{\frac{1}{AT^2} * \sigma_T^2 + \sigma_{N_2}^2} * \sigma_H}$$

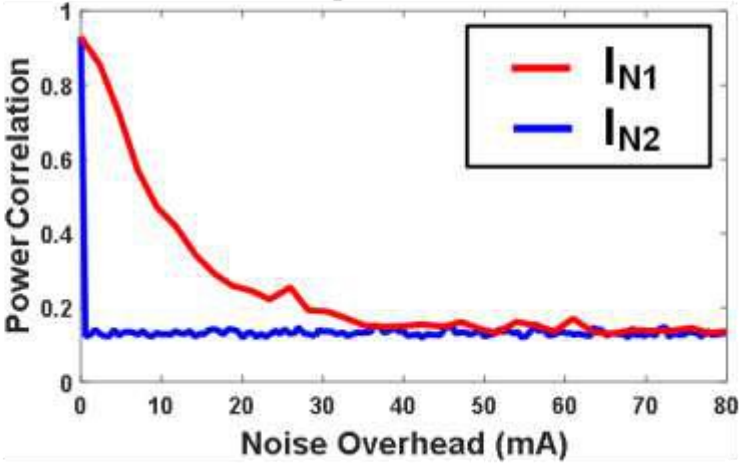
Overhead Comparison

$$\sigma_{N_2}^2 = AT^2 * \sigma_{N_1}^2$$

$$I_{N2} = \frac{I_{N1}}{AT} \ll I_{N1}$$

$$I_{Ov_2} \sim \frac{I_{Ov_1}}{AT} \ll I_{Ov_1}$$

$$I_{AES_{avg}} = 18.89\ mA$$



*HOST Best Student Paper 2017, TCAS-1 2018

Concept

$$\text{MTD} \propto \frac{1}{SNR^2}$$

$$\text{MTD} \propto \frac{1}{SNR^2} * AT^2$$

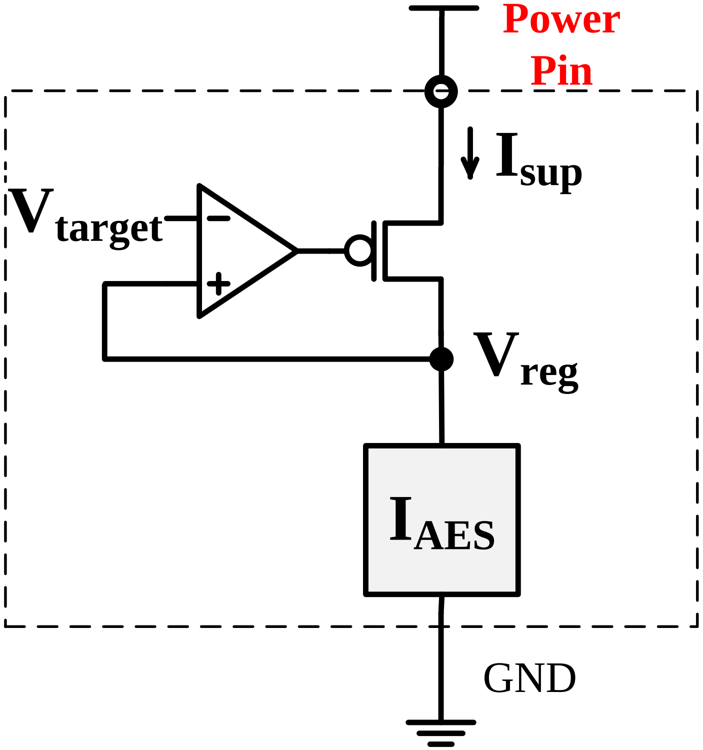
Signature Attenuation

Baseline

- Low dropout regulator (LDO) is used to regulate the output voltage.
- In an ideal series LDO operation, $\mathrm{I}_{\mathrm{sup}} = I_{AES}$.
- Modify the encryption hardware module, such that, power consumption of the chip is independent of the AES transitions, without degradation in performance.
- $\boldsymbol{I_{supply} \neq f(I_{AES})}$,

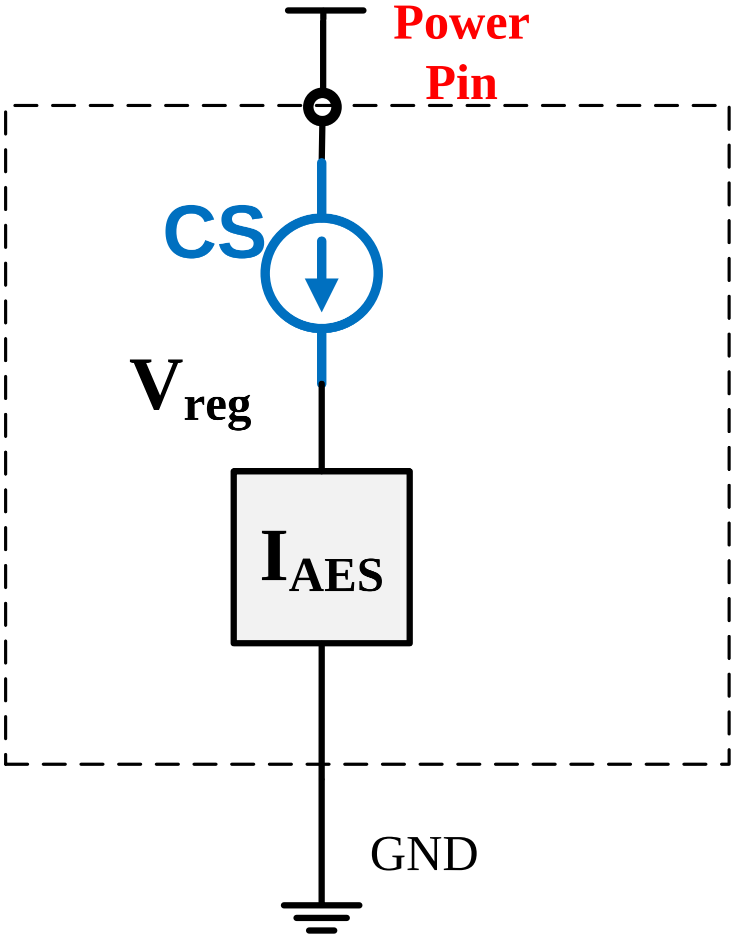
  Full suppression $(\boldsymbol{AT} = \infty)$

Traditional LDO


Power Pin
$\mathrm{I}_{\mathrm{sup}}$
$\mathrm{V}_{\mathrm{target}}$
−
+
$\mathrm{V}_{\mathrm{reg}}$
$\mathrm{I}_{\mathrm{AES}}$
GND

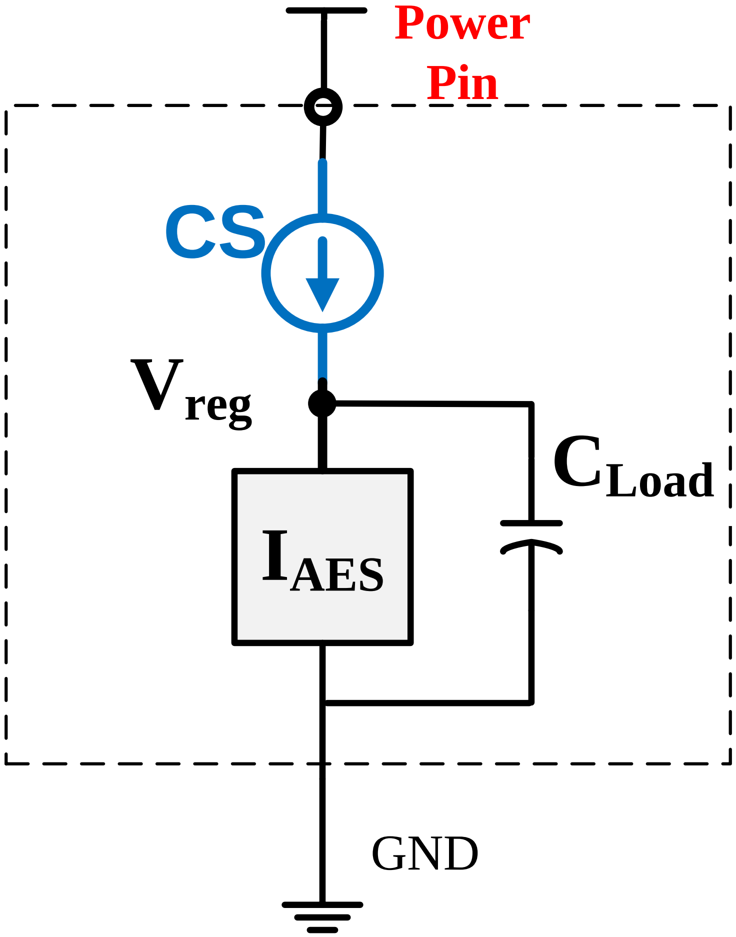
How can we achieve a supply current independent of the AES current??

Signature Suppression



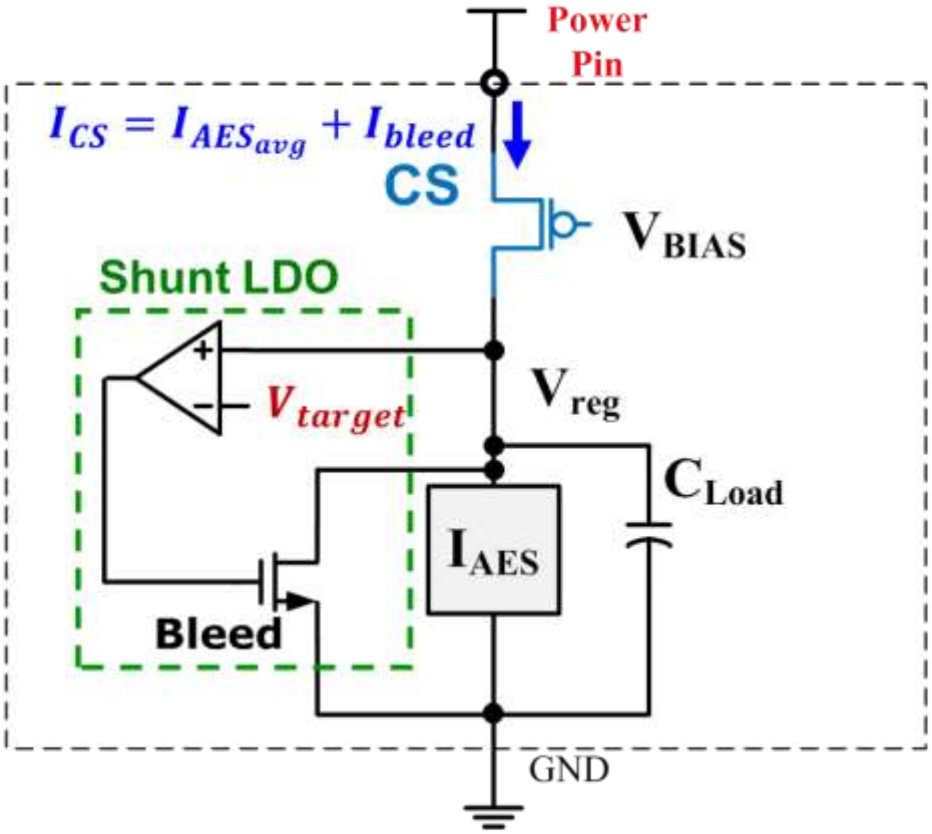
- A constant current cannot drive a fluctuating load current.
- Need an element to draw the extra current, and replenish the excess requirement.

Signature Suppression



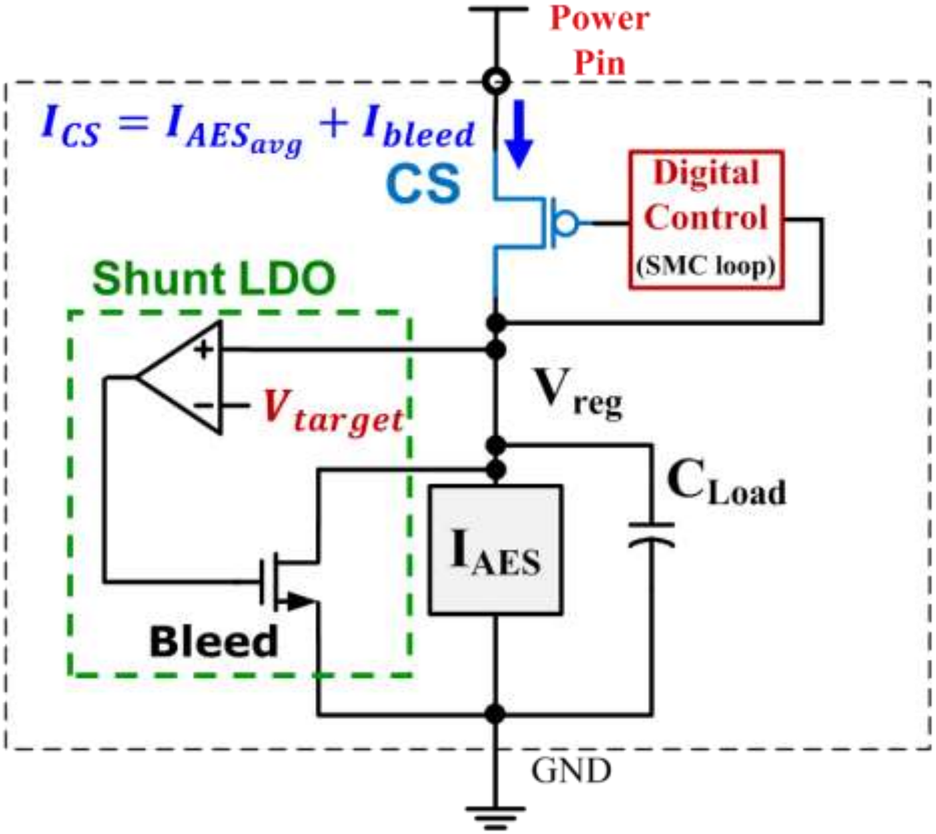
- V_{reg} fluctuations.
- Performance hit.
- Need for LDO regulator inherently satisfying $I_{supply} \neq f(I_{AES})$

SAH: Signature Attenuation Hardware



- Practical CS: biased PMOS.
- Shunt LDO loop with the NMOS bleed regulates V_{reg}.

SAH: Variation-tolerance



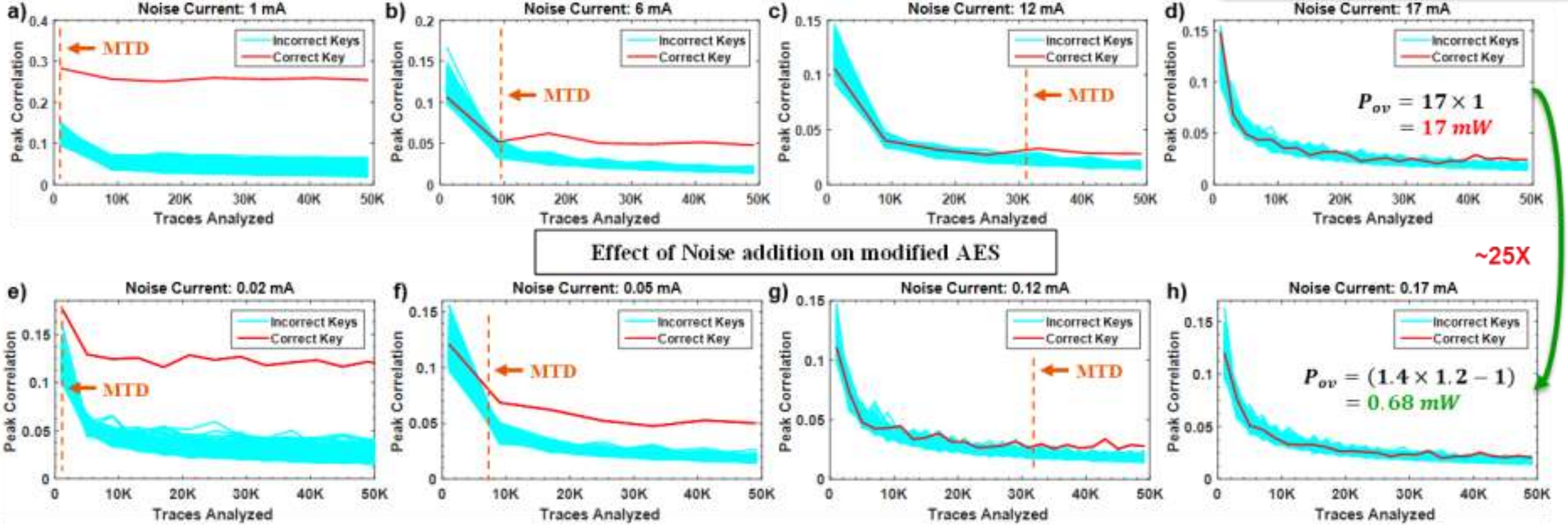
- Digital (SMC) loop engages to compensate any slow variations like frequency, T, process.

- Normal Operation: Only the shunt LDO regulates.

MTD Analysis

~25X improvement in power overhead for SCA immunity

Effect of Only Noise addition on traditional AES

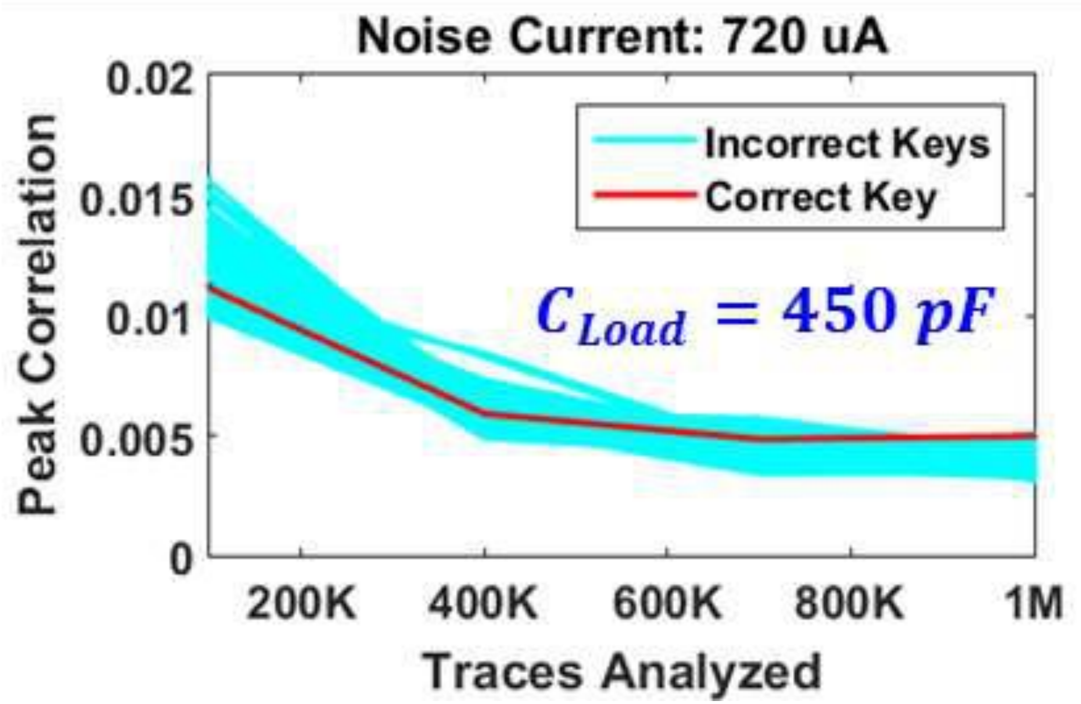


$$P_{ov} = 17 \times 1 = 17\ mW$$

Effect of Noise addition on modified AES

$$P_{ov} = (1.4 \times 1.2 - 1) = 0.68\ mW$$

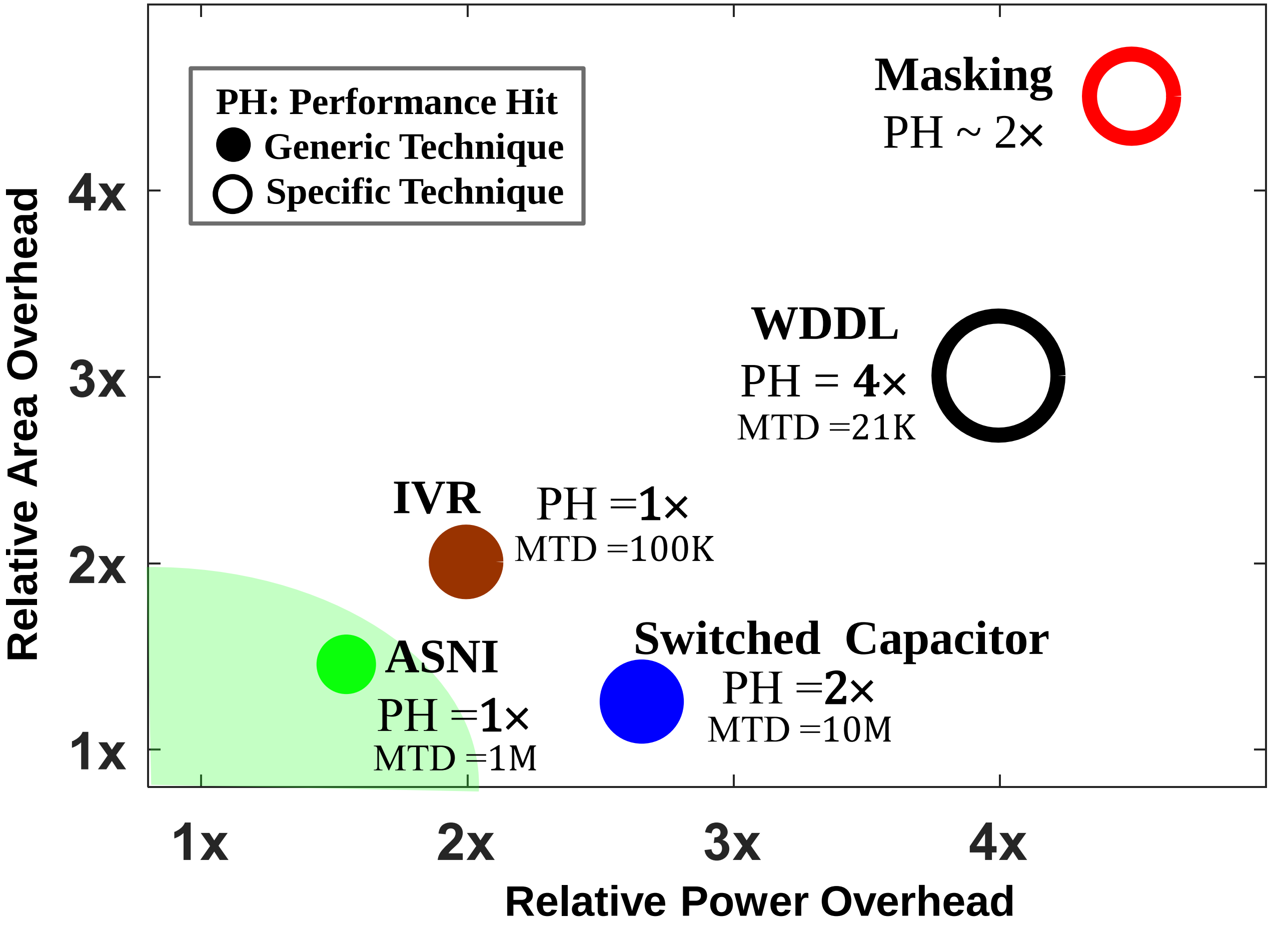
ASNI: MTD > 1M



- Power efficiency $\eta = \frac{1\ mA*1V}{1.4mA*1.2V} \sim 60\%$ to achieve MTD > 1M.
- Capacitance for 40MHz operation. Higher f will lower C

ASNI: Comparison with State-of-the-Art

State-of-the-Art Power SCA Countermeasures:
Overhead Comparison with ASNI



Q&A

Outline

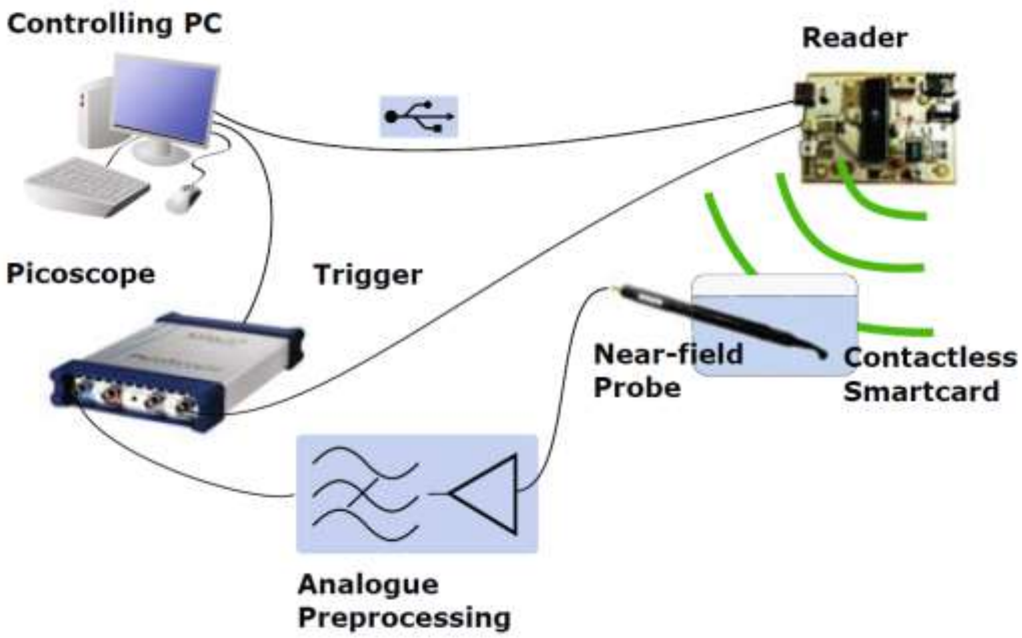
Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

Coffee Break

Outline

Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

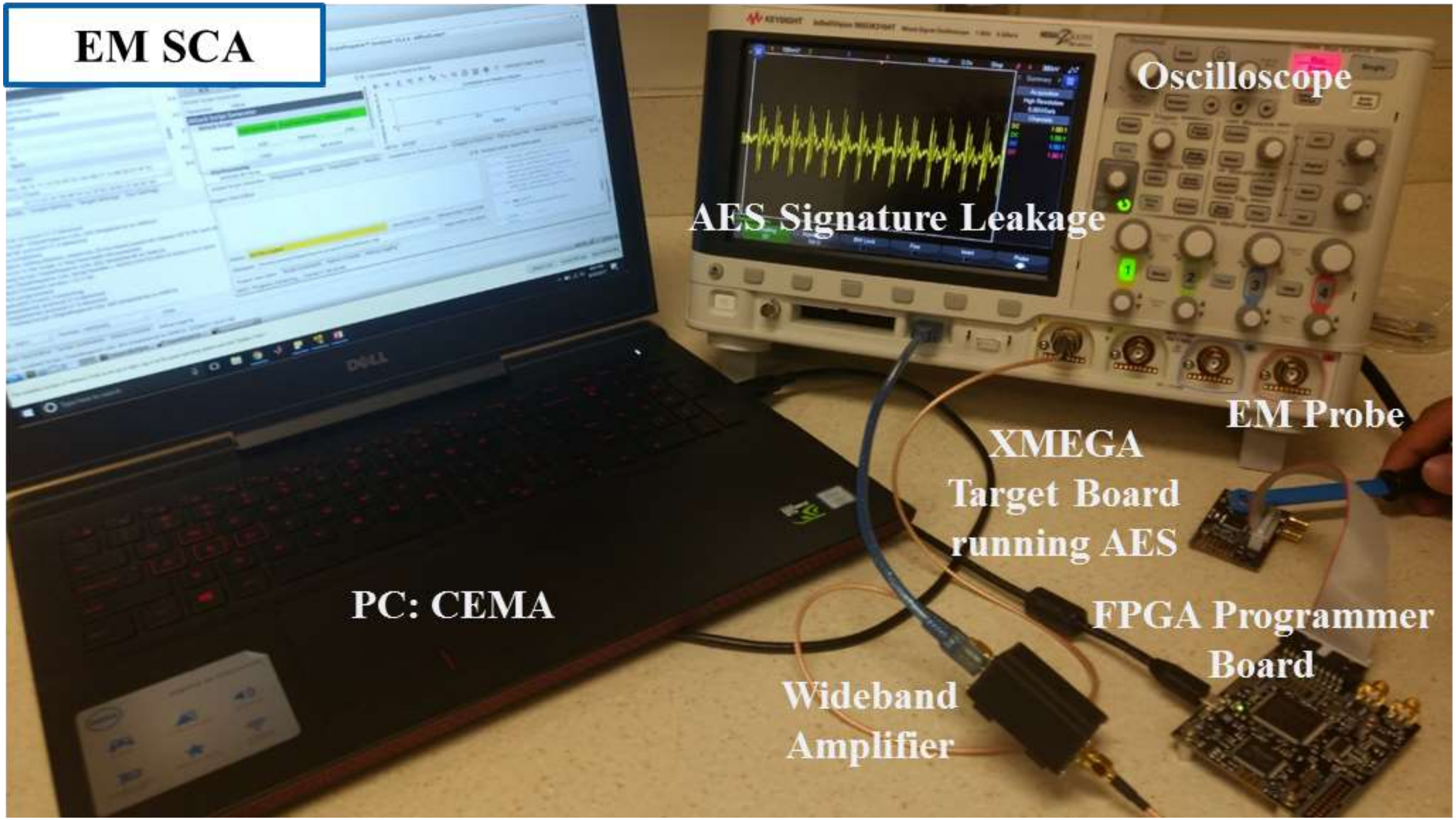
Electromagnetic Analysis Attacks



[KOP09]

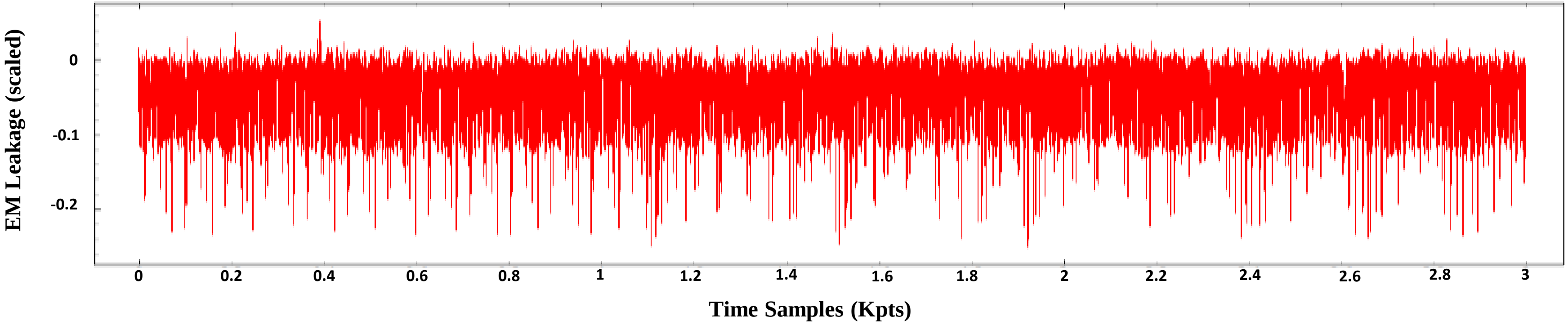
- A magnetic/electric field probe is used to scan the chip and record EM traces.
- For attack, use DEMA/ CEMA to recover the secret key.

Laboratory Set-up for CEMA attack

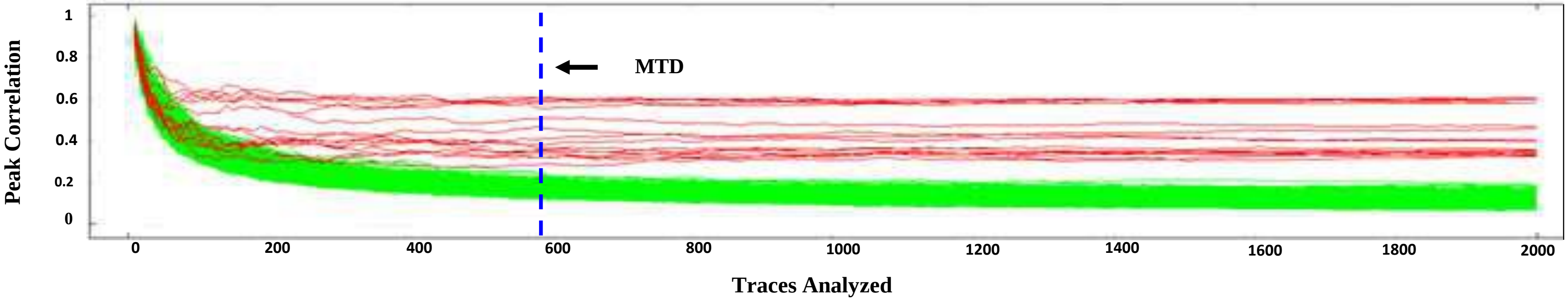


CEMA on AES-128 (8-bit microcontroller)

EM Trace Capture



Minimum Traces to Disclosure: 16 Key Bytes



- EM probe used to break all the 16 key bytes of the software AES running on an Atmega microcontroller within <1K traces (MTD).

Overview: New Attacks and Defenses

Attack

SCNIFFER: Automated EM leakage point detection

X-DeepSCA: Cross-Device Deep-Learning SCA

Power & Electro-Magnetic Side-Channel

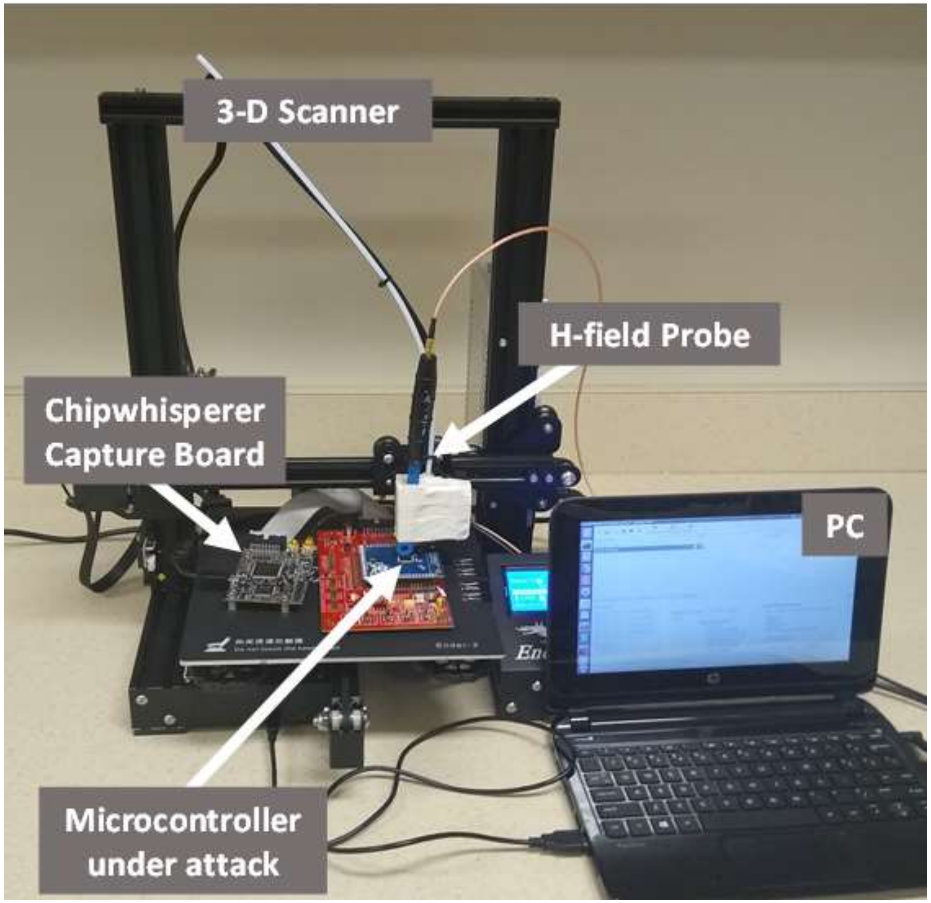
Defense

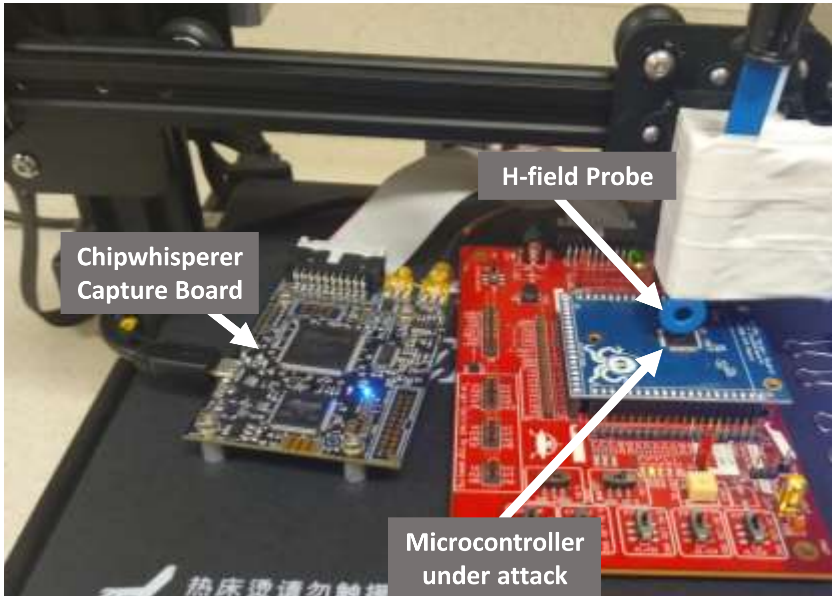
ASNI: Attenuated Signature Noise Injection

White-Box Root-Cause Analysis

STELLAR: Generic EM SCA Tolerance

SCNIFFER: Automated Intelligent EM Sniffing





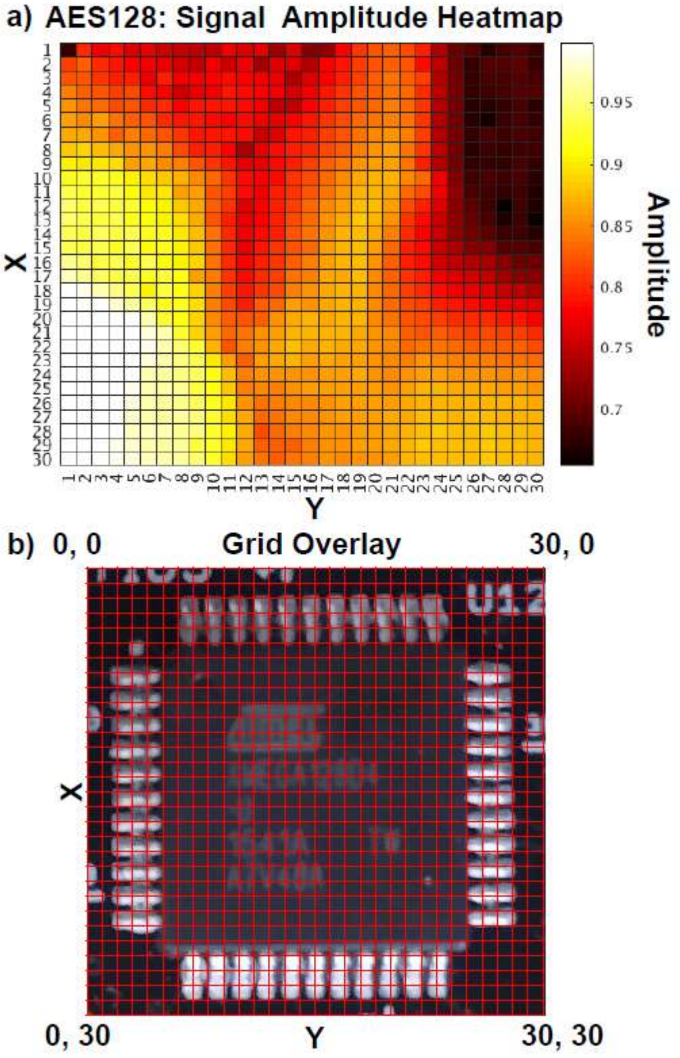
- Automated low-cost end-to-end Framework for efficient EM Side-Channel SNIFFing & Side-Channel Attack

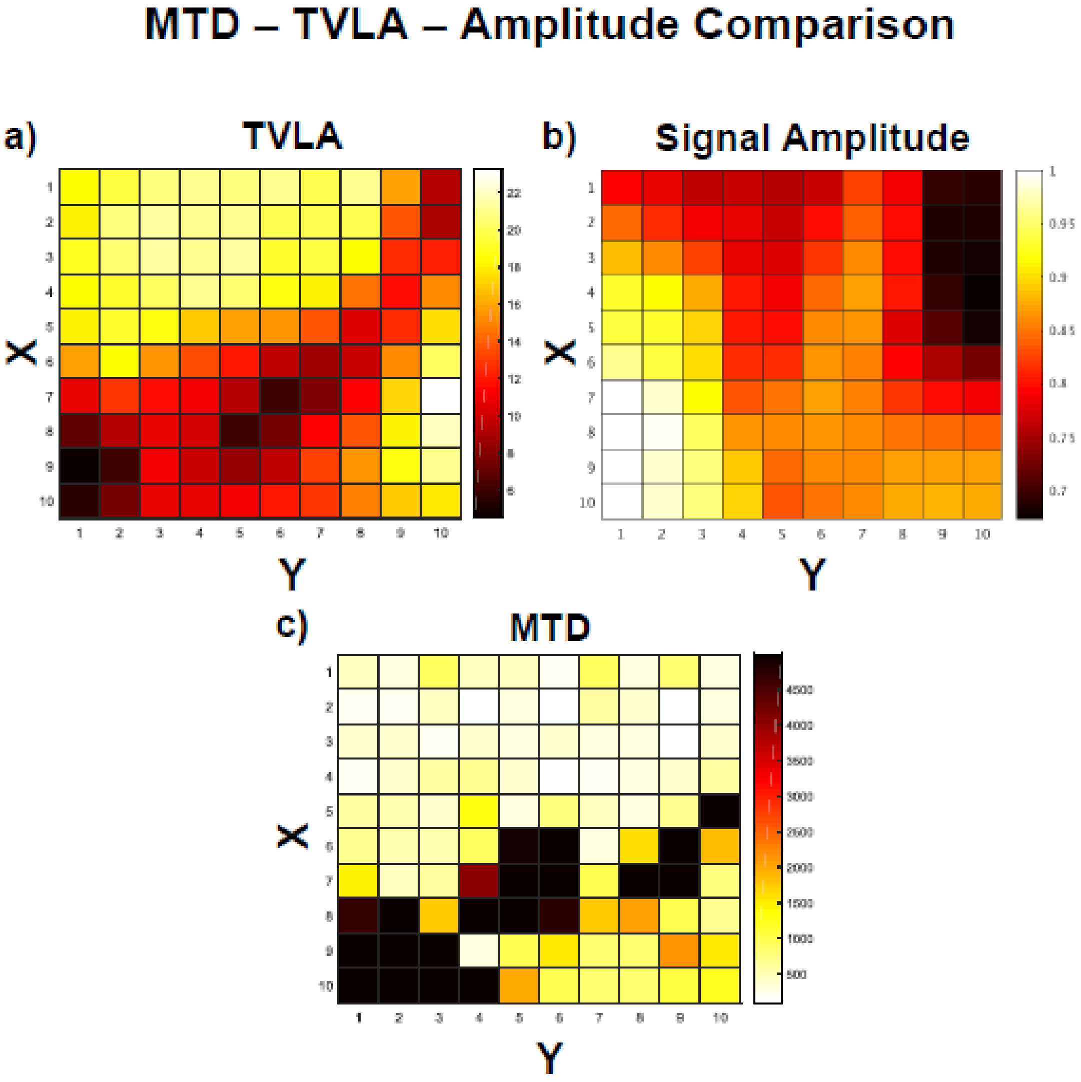
SCNIFFER: Low-cost EM Attack Setup

	Scanner	Amplifier	Probe
Picture			
Cost	$200	$50	$10
SCNIFFER Specifications	100 µm	20dB	16mm^2
Riscure EM Probe Station Specifications	2.5 µm	-	1mm^2

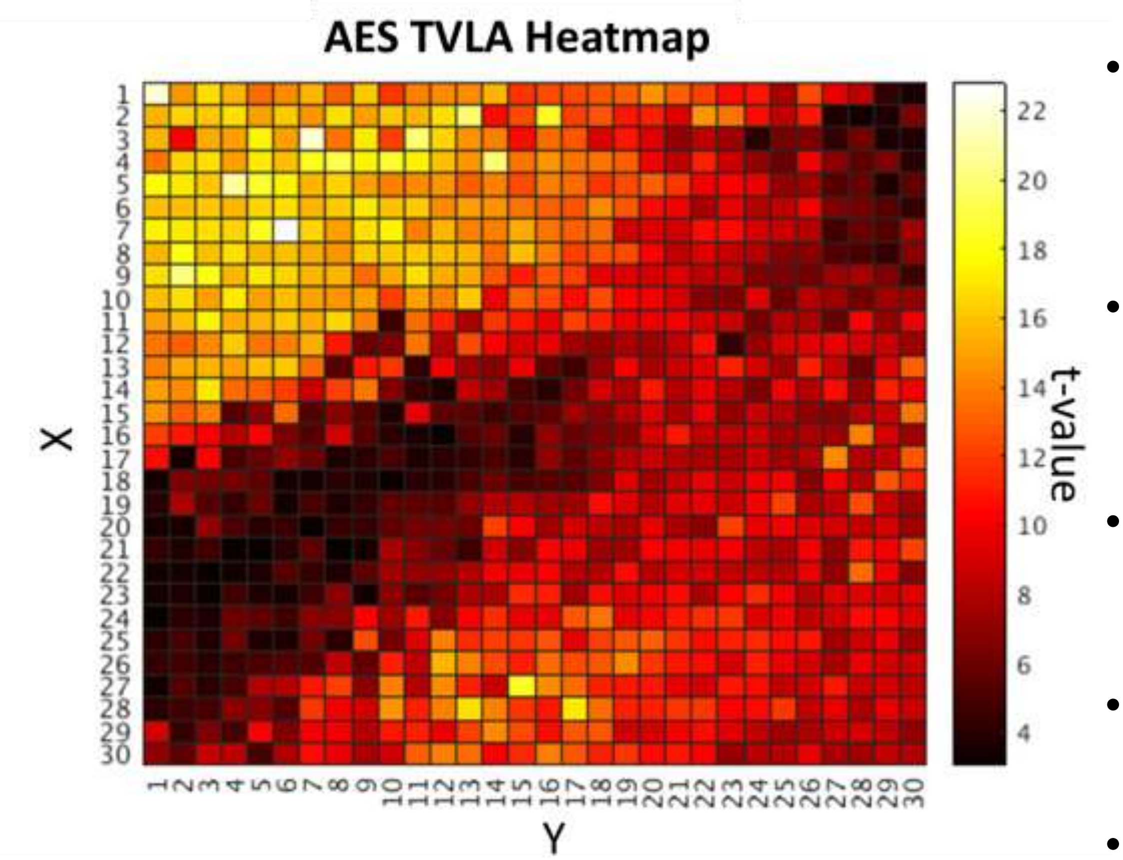
Cost: <$300 compared to ~$50,000

Heat Maps


a) AES128: Signal Amplitude Heatmap
X
Y
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Amplitude
0.95
0.9
0.85
0.8
0.75
0.7
b) 0, 0
Grid Overlay
30, 0
0, 30
30, 30
U12


MTD – TVLA – Amplitude Comparison
a)
TVLA
X
Y
1 2 3 4 5 6 7 8 9 10
22
20
18
16
14
12
10
8
6
b)
Signal Amplitude
1
0.95
0.9
0.85
0.8
0.75
0.7
c)
MTD
4500
4000
3500
3000
2500
2000
1500
1000
500

SCNIFFER: TVLA-Based EM Sniffing

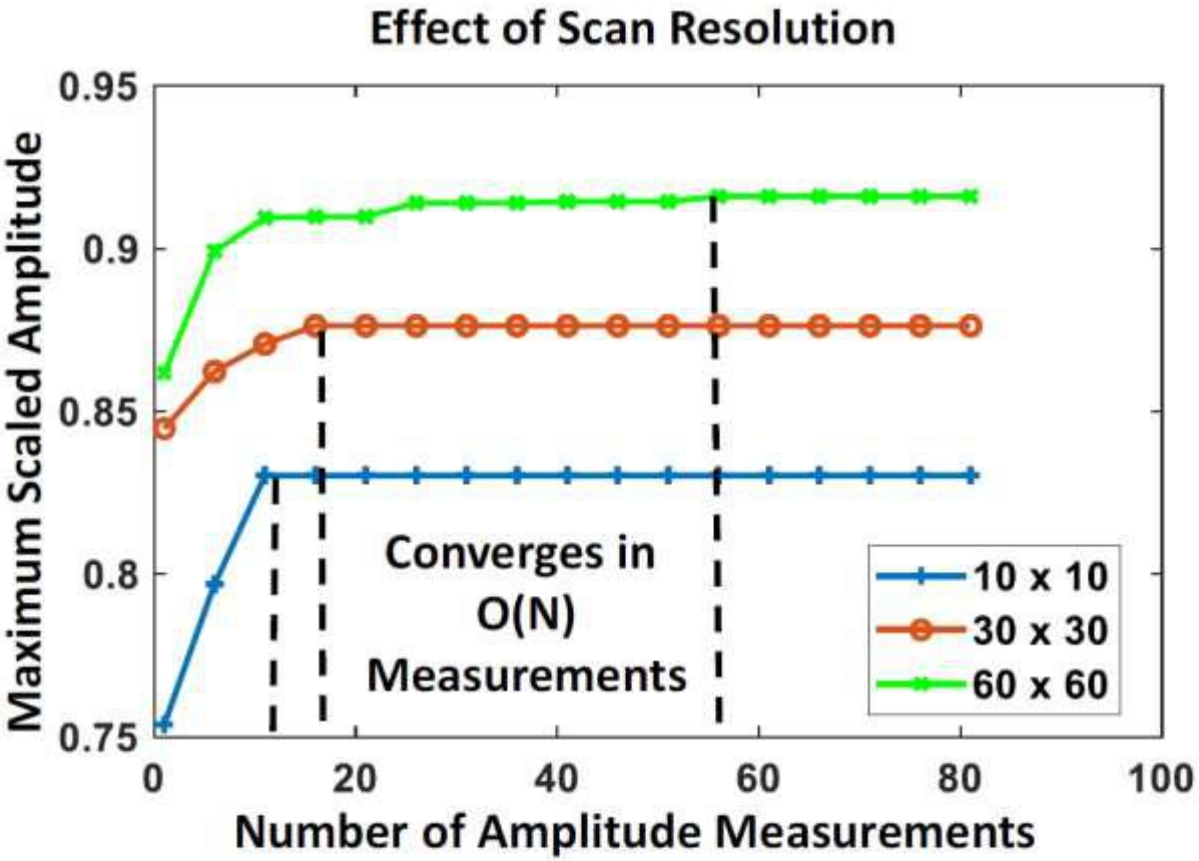


- TVLA: 2 sets of traces collected: fixed PT (f) and random PT (r).
- TVLA = $\frac{\mu_r - \mu_f}{\sqrt{\frac{\sigma_r^2}{n_r} + \frac{\sigma_f^2}{n_f}}}$
- TVLA < 4.5: traces do not have data-dependent leakage.
- TVLA $\propto \frac{1}{SNR}$
- MTD $\propto \frac{1}{SNR^2}$

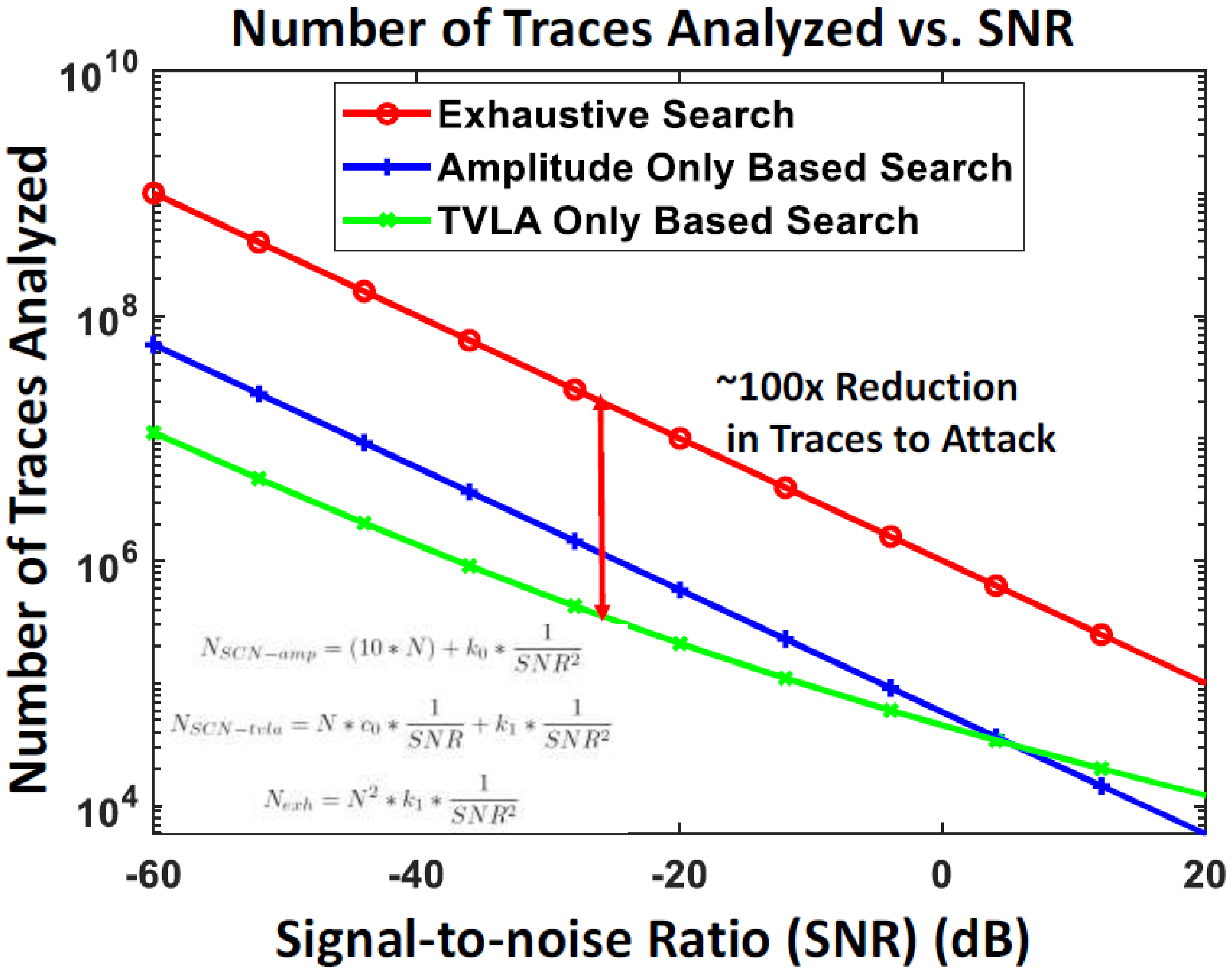
- TVLA requires much lower number of traces than CEMA at each point.

SCNIFFER: Finding Point of Max Leakage

- Gradient descent heuristic to converge to the best point of leakage on an N x N chip within N iterations.



SCNIFFER Attack Comparison



~100x Reduction in Traces to Attack

$$N_{SCN-amp} = (10 * N) + k_0 * \frac{1}{SNR^2}$$

$$N_{SCN-tvla} = N * c_0 * \frac{1}{SNR} + k_1 * \frac{1}{SNR^2}$$

$$N_{exh} = N^2 * k_1 * \frac{1}{SNR^2}$$

SCNIFFER Demo

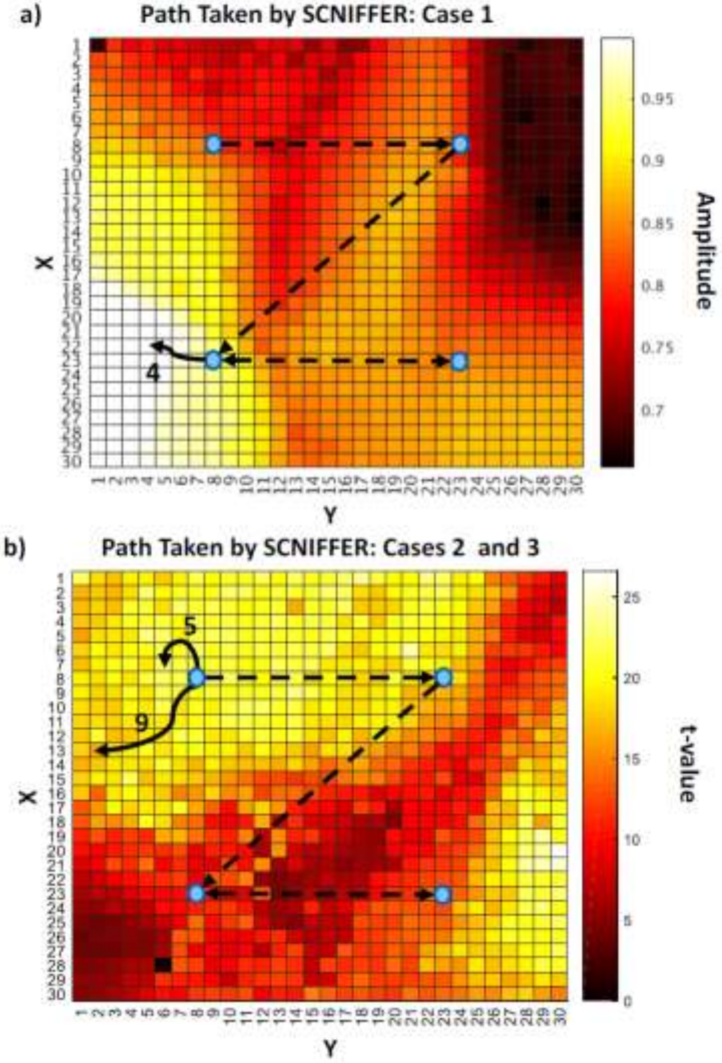
SCNIFFER: Context-Aware Intelligent EM Side-Channel Sniffing

SCNIFFER Attack Comparison

Case	Initial Search	Gradient Search	Convergence Location	MTD	Total Traces
1	Amplitude	Amplitude	(7, 1)	1713*	1793
2	TVLA	TVLA	(2, 2)	223	5847
3	TVLA	Amplitude	(4, 2)	358	2488
4	Amplitude	TVLA	(8, 2)	>5000	>14,640

TABLE II: Comparison of different combinations of TVLA and amplitude used with SCNIFFER. The total traces includes the traces needed for the initial search, gradient search, and CEMA.

*Amplitude based search provides faster convergence, but gives no guarantees that the location found is not a location without information leakage as TVLA does.



Q&A

Outline

Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

Overview: New Attacks and Defenses

Attack

SCNIFFER: Automated EM leakage point detection

X-DeepSCA: Cross-Device Deep-Learning SCA

Power & Electro-Magnetic Side-Channel

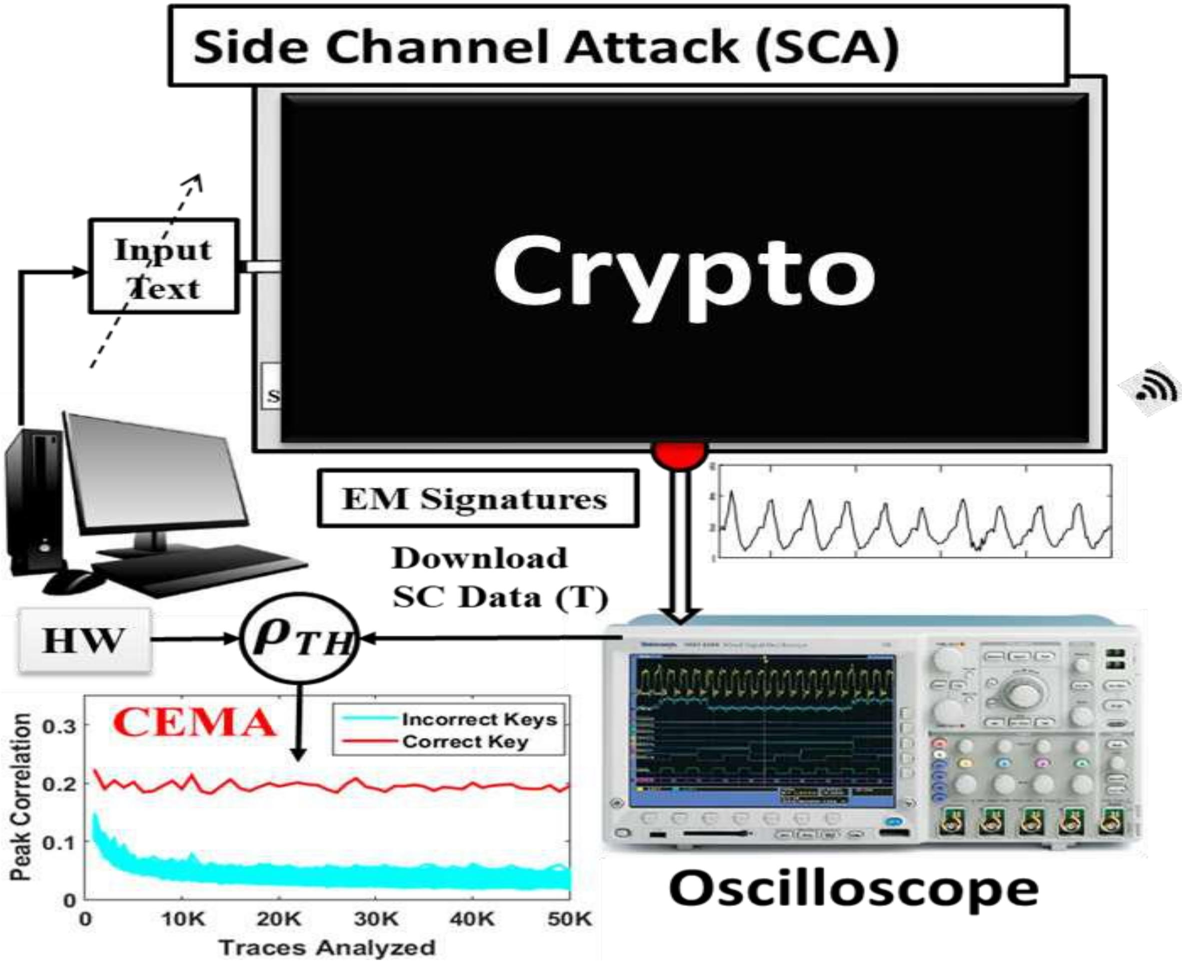
Defense

ASNI: Attenuated Signature Noise Injection

White-Box Root-Cause Analysis

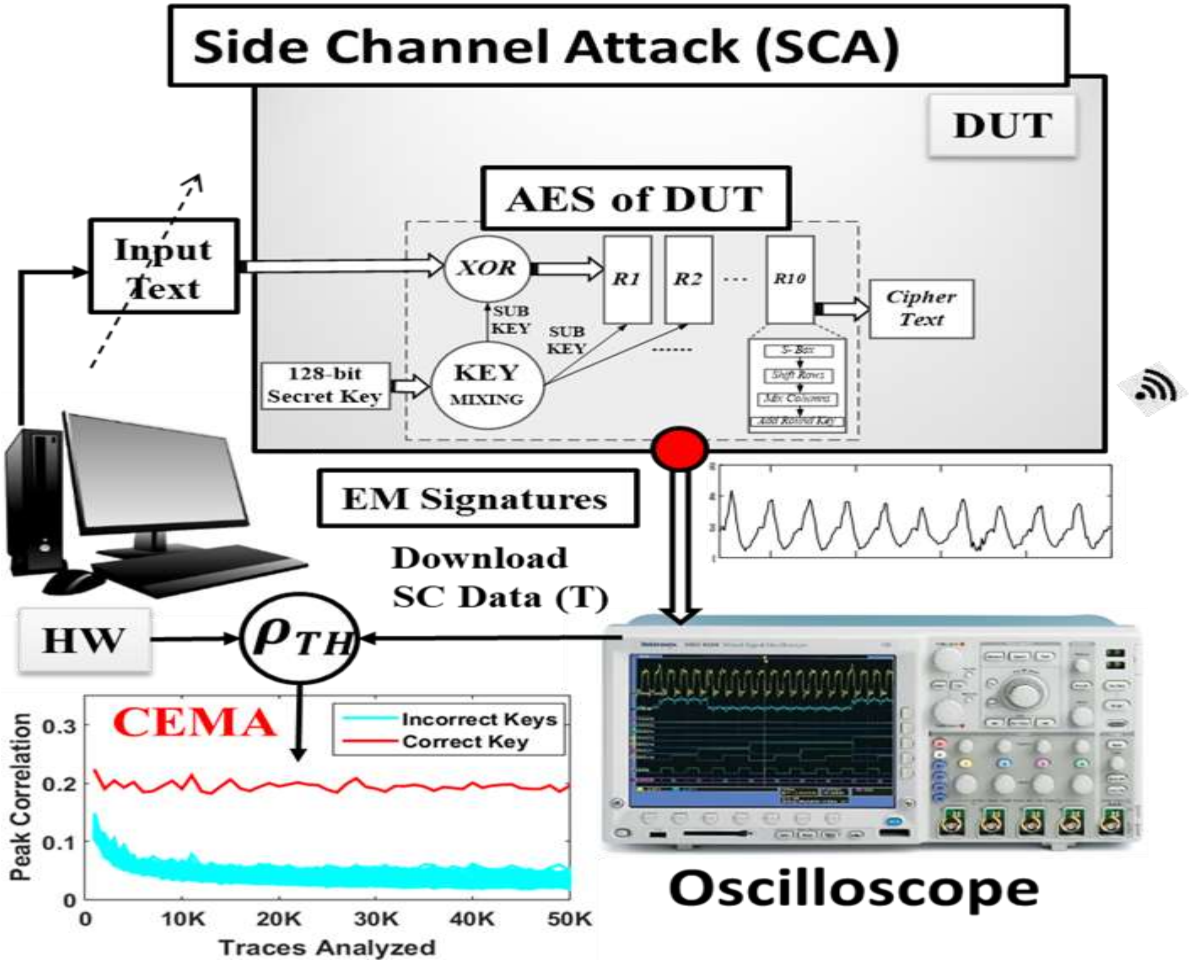
STELLAR: Generic EM SCA Tolerance

EM-SC: Black Box Analysis



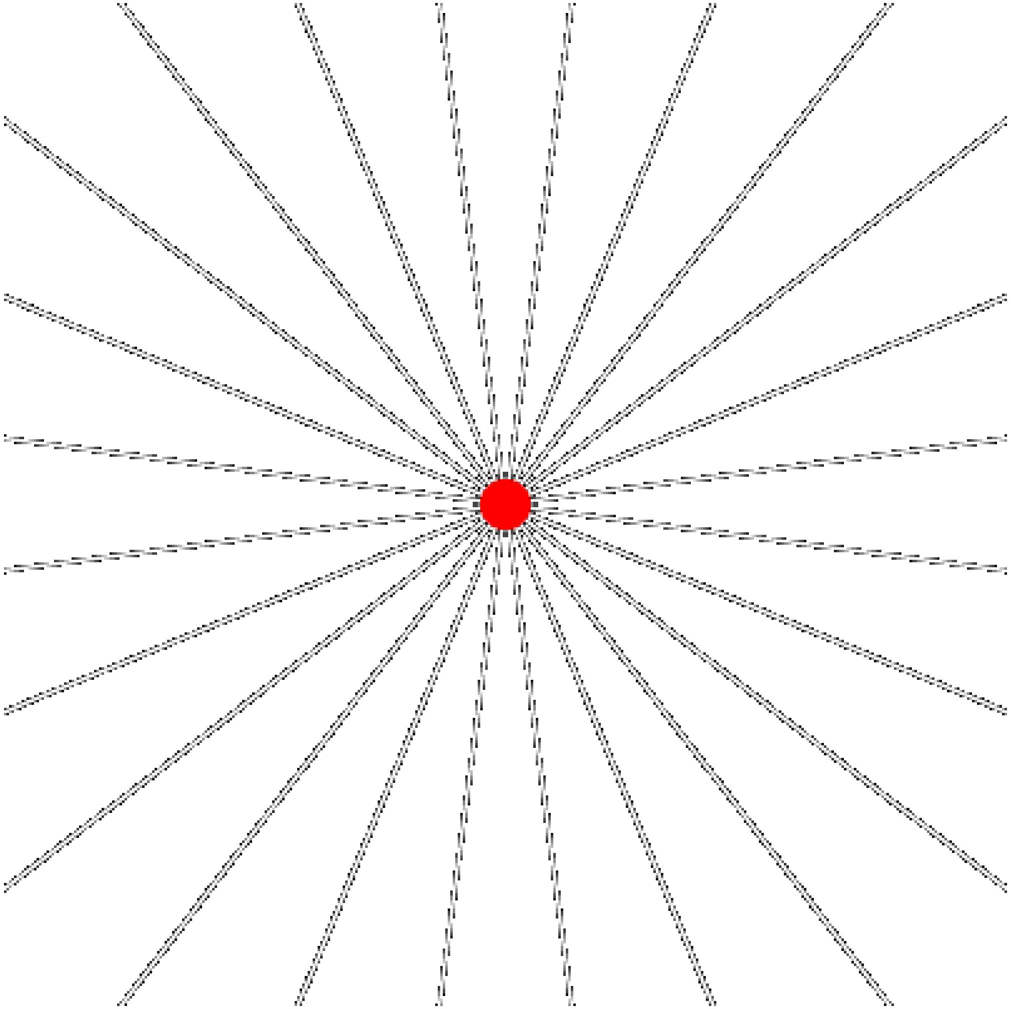
- Most EM SC work treat the EM emanation as a Black Box!

EM-SC: White Box Analysis (STELLAR)



White-Box Analysis: What is the source of the EM leakage from an IC?

Maxwell and Accelerating Electrons



1. $\nabla \cdot \mathbf{D} = \rho_V$

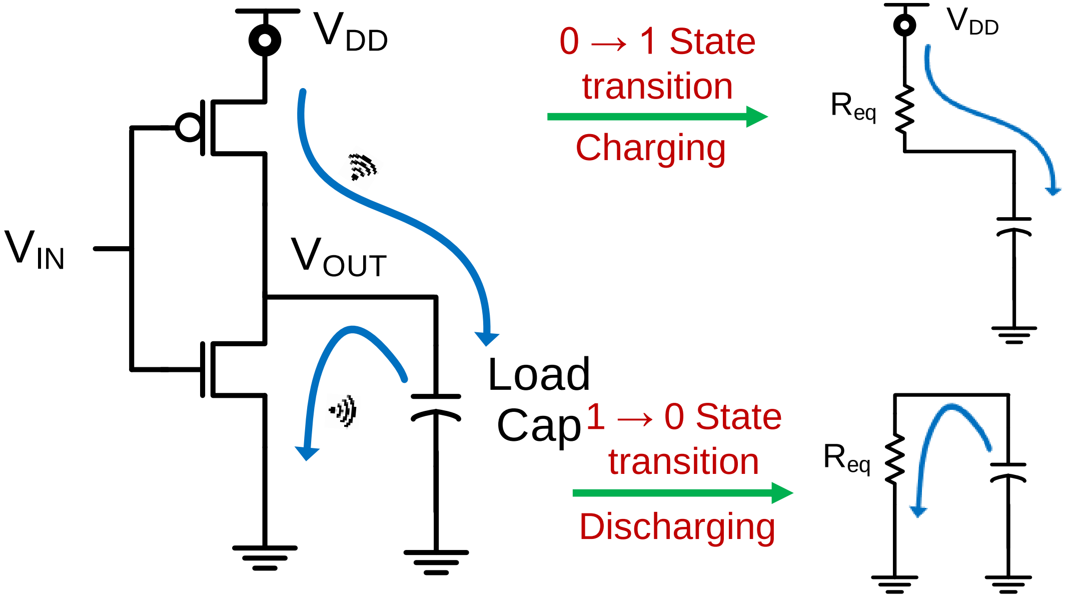
2. $\nabla \cdot \mathbf{B} = 0$

3. $\nabla \times \mathbf{E} = -\dfrac{\partial \mathbf{B}}{\partial t}$

4. $\nabla \times \mathbf{H} = \dfrac{\partial \mathbf{D}}{\partial t} + \mathbf{J}$

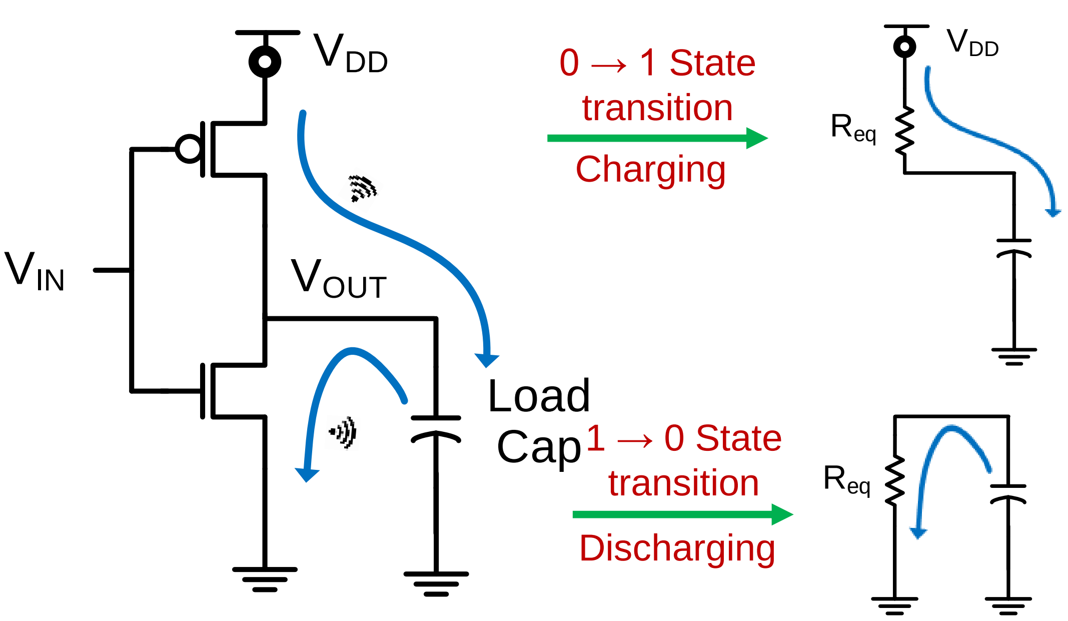
Genesis of the EM Leakage

- Crypto engines like AES/SHA/ECC consist of multiple digital gates



Genesis of the EM Leakage

- Crypto engines like AES/SHA/ECC consist of multiple digital gates



0 → 1 State transition

Charging

1 → 0 State transition

Discharging

$$\frac{di_c(t)}{dt} = \frac{d^2 q}{dt^2} \neq 0,$$

State Switching
→ Changing Currents
→ Acceleration of charges

$$\nabla^2 E = \mu\epsilon \frac{\partial^2 E}{\partial t^2} \neq 0$$

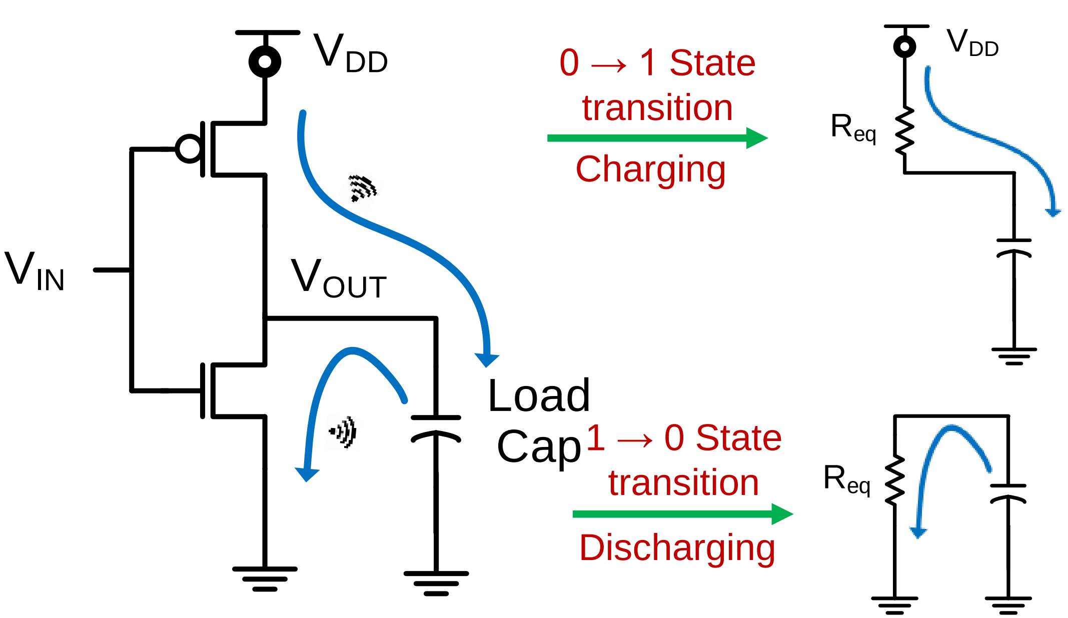
$$\nabla^2 H = \mu\epsilon \frac{\partial^2 H}{\partial t^2} \neq 0$$

E, H fields propagate together and EM fields exist.

Transistor switching creates changing currents leading to EM radiation.

Genesis of the EM Leakage

- Crypto engines like AES/SHA/ECC consist of multiple digital gates



$$\frac{di_c(t)}{dt} = \frac{d^2q}{dt^2} \neq 0,$$

State Switching
→ Changing Currents
→ Acceleration of charges

$$\nabla^2 E = \mu\epsilon \frac{\partial^2 E}{\partial t^2} \neq 0$$

$$\nabla^2 H = \mu\epsilon \frac{\partial^2 H}{\partial t^2} \neq 0$$

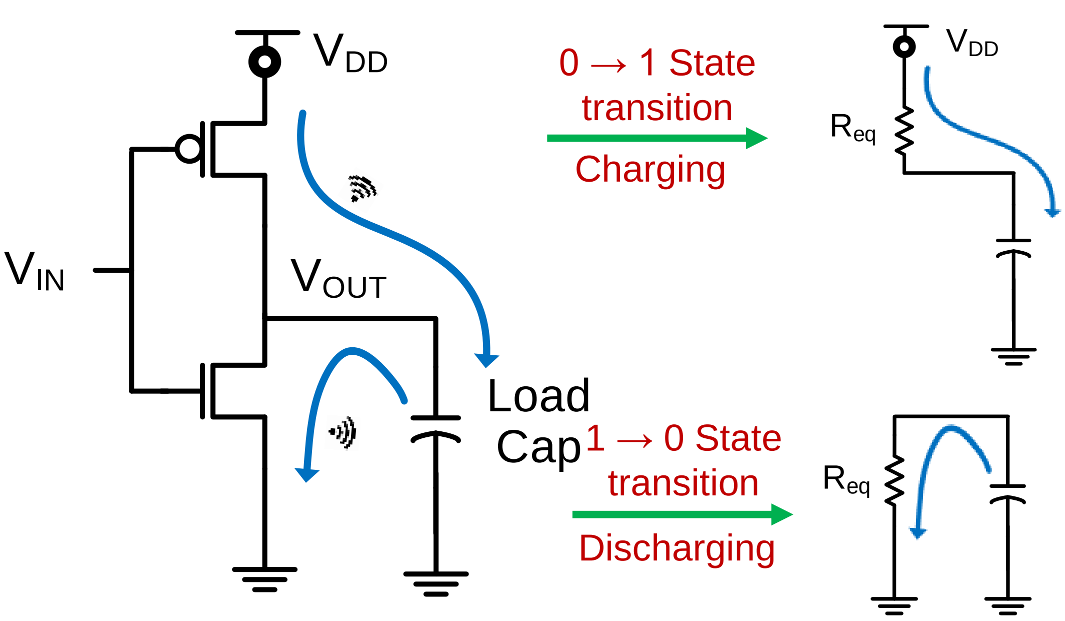
E, H fields propagate together and EM fields exist.

Transistor switching creates changing currents leading to EM radiation.

But what does the generated EM fields depend on?

Genesis of the EM Leakage

- Crypto engines like AES/SHA/ECC consist of multiple digital gates



0 → 1 State transition

Charging

1 → 0 State transition

Discharging

$$\frac{di_c(t)}{dt} = \frac{d^2q}{dt^2} \neq 0,$$

State Switching
→ Changing Currents
→ Acceleration of charges

$$\nabla^2 E = \mu\epsilon \frac{\partial^2 E}{\partial t^2} \neq 0$$

$$\nabla^2 H = \mu\epsilon \frac{\partial^2 H}{\partial t^2} \neq 0$$

E, H fields propagate together and EM fields exist.

Transistor switching creates changing currents leading to EM radiation.

But what does the generated EM fields depend on? Metals carrying the current!

Metal Layers in Intel 32nm

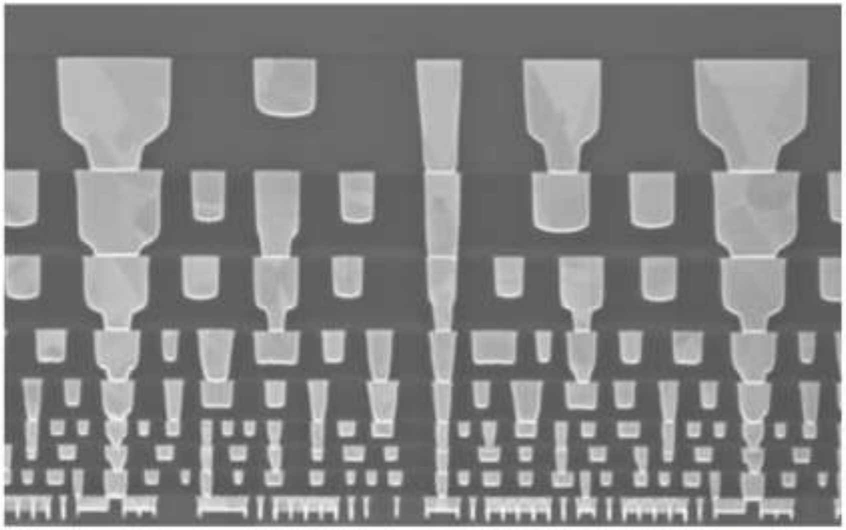
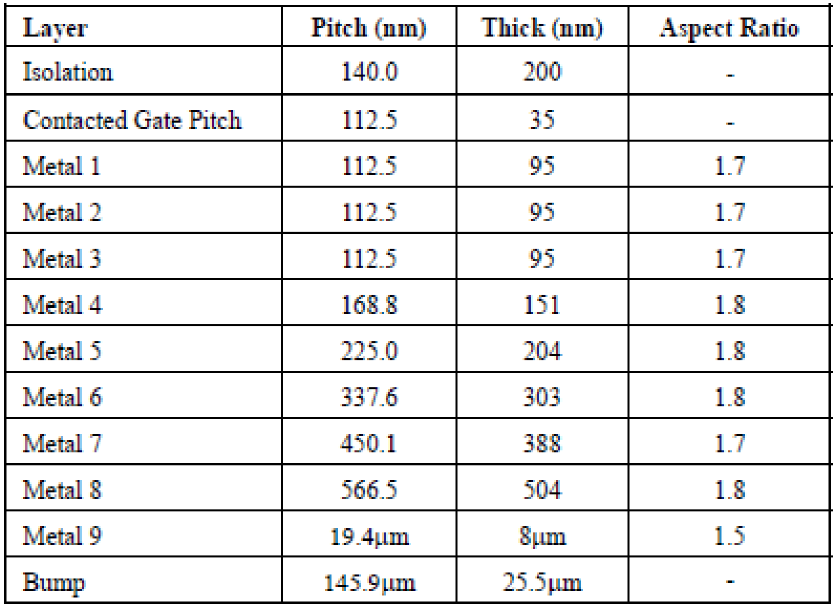


Figure 11: Cross-section of interconnect stack (8 layers)



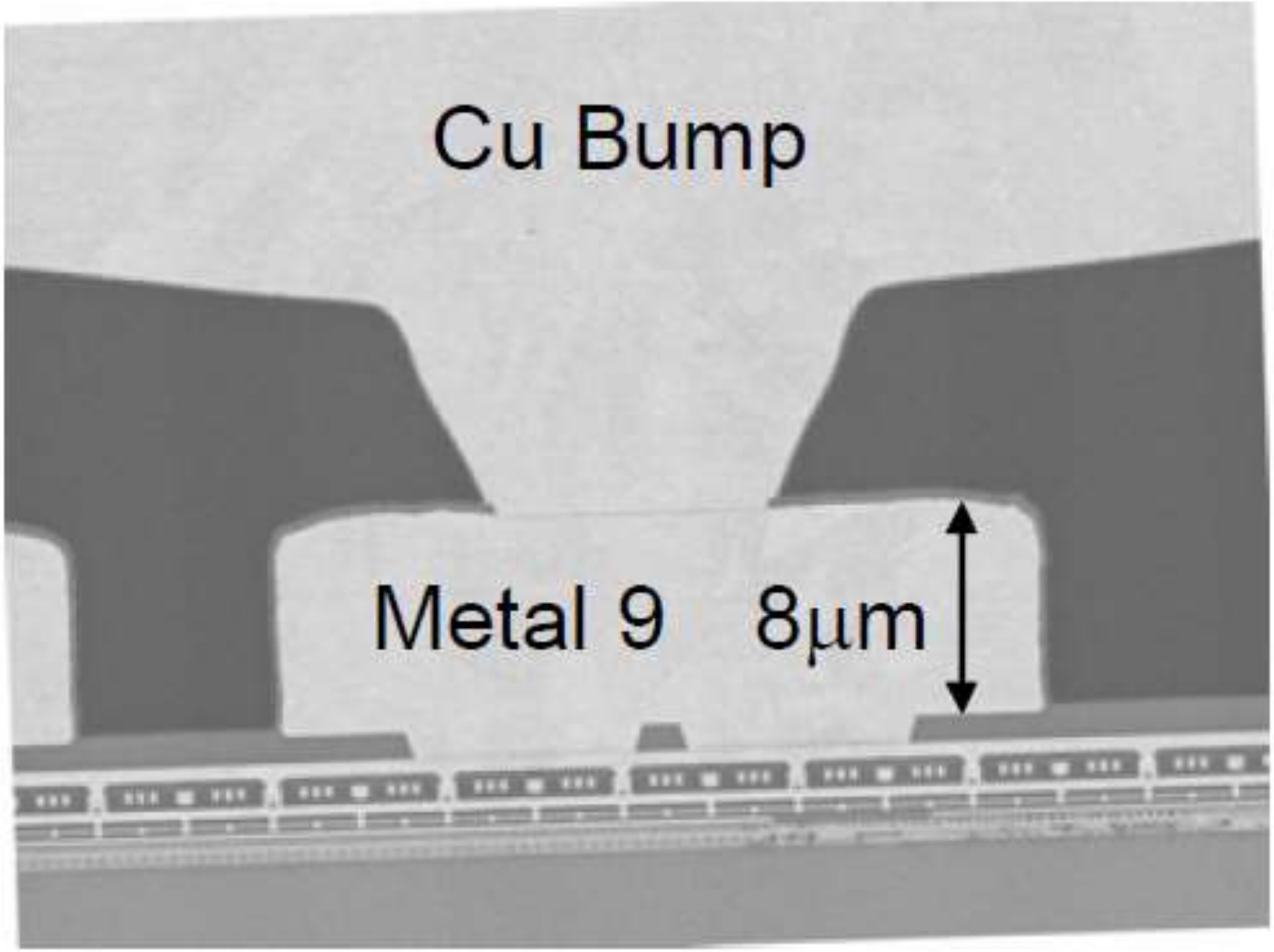
Layer	Pitch (nm)	Thick (nm)	Aspect Ratio
Isolation	140.0	200	-
Contacted Gate Pitch	112.5	35	-
Metal 1	112.5	95	1.7
Metal 2	112.5	95	1.7
Metal 3	112.5	95	1.7
Metal 4	168.8	151	1.8
Metal 5	225.0	204	1.8
Metal 6	337.6	303	1.8
Metal 7	450.1	388	1.7
Metal 8	566.5	504	1.8
Metal 9	19.4µm	8µm	1.5
Bump	145.9µm	25.5µm	-

Table 1: Layer pitch, thickness and aspect ratio

Reference: *A 32nm Logic Technology Featuring 2nd-Generation High-k + Metal-Gate Transistors, Enhanced Channel Strain and 0.171µm2 SRAM Cell Size in a 291Mb Array, Intel Corporation*

- Interconnect stack dimension, from Intel 32 nm technology
- Simulation performed in ANSYS HFSS
- Goal: Find out how the different metal layers contribute to the radiated electric field, due to a modulated signal flow through the stacks

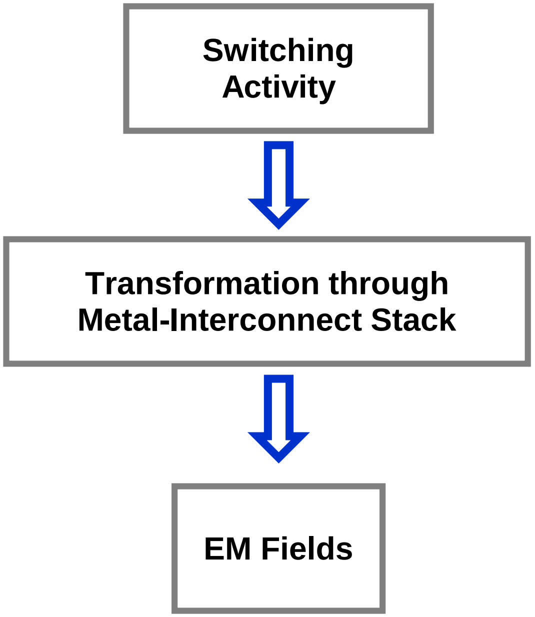
Simulation Setup



SEM image detailing Metal 9 and Cu Bump layers

Reference: *A 32nm Logic Technology Featuring 2nd-Generation High-k + Metal-Gate Transistors, Enhanced Channel Strain and 0.171µm2 SRAM Cell Size in a 291Mb Array, Intel Corporation*

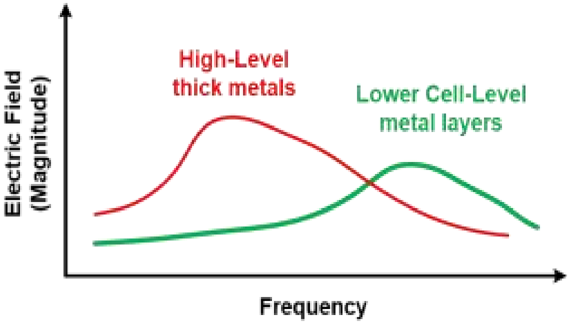
Ground-Up Root-Cause Analysis



Switching Activity

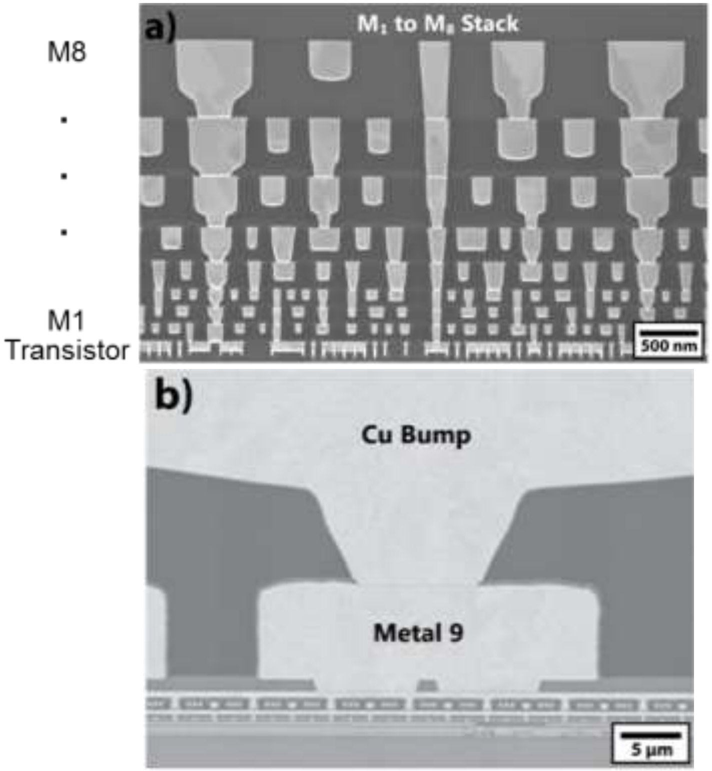
Transformation through Metal-Interconnect Stack

EM Fields



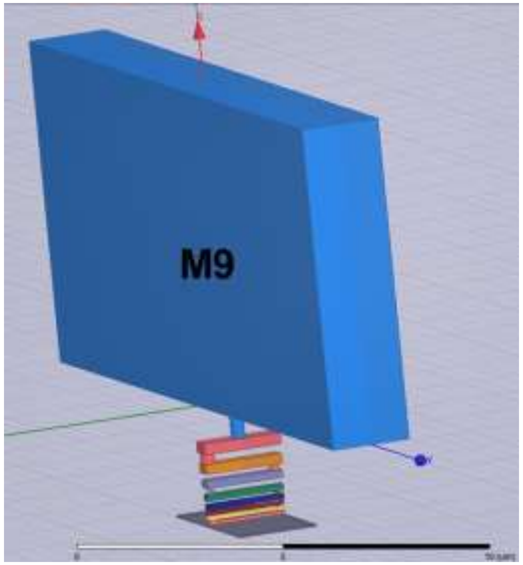
- EM leakage from higher metal layer has higher probability of detection.

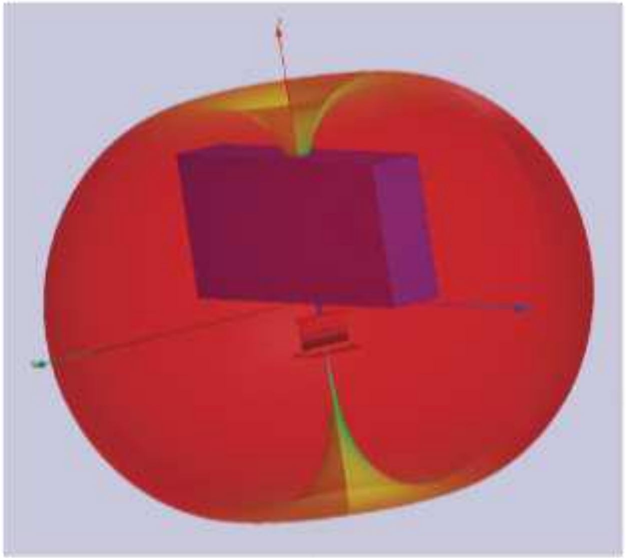
Intel 32nm Metal-Interconnect Stack



[NAB+08]

Metal-Interconnect Stack Modeling

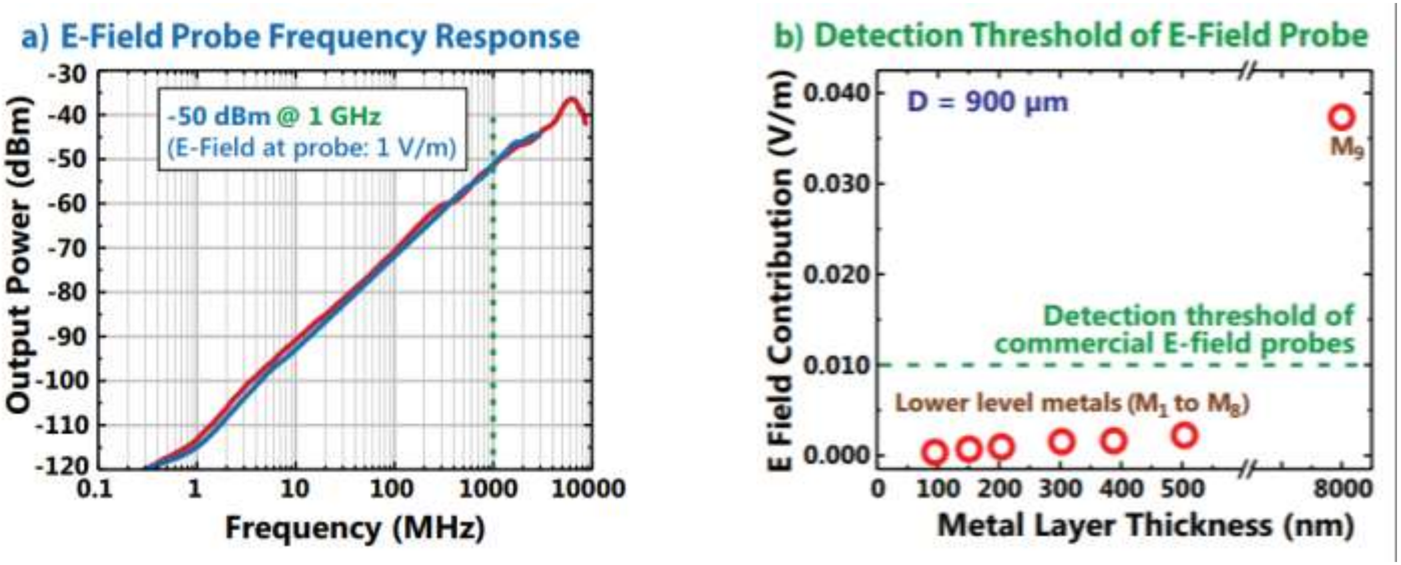




[DNC+19]

- Isometric Projection of the Intel 32nm interconnect stack model for EM analysis in HFSS.
- Lumped port excitation between the lowest metal layer and the PEC plate (ground).
- Far-field radiation pattern is analogous to infinitesimal dipole ($l << \lambda$).

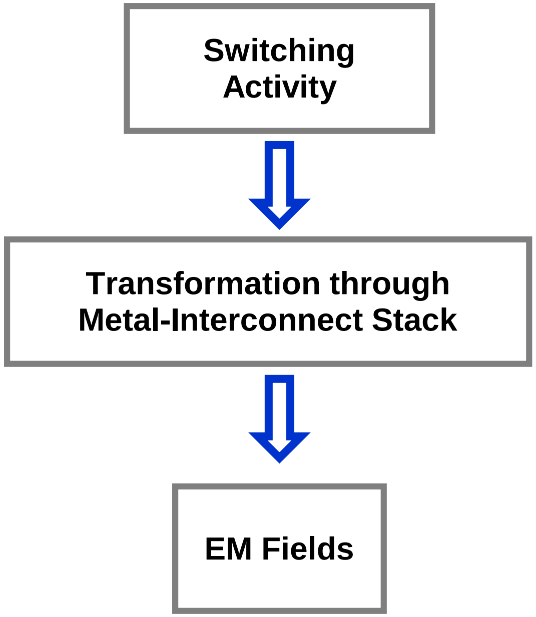
E-field Contribution of the Metal Stack


a) E-Field Probe Frequency Response
-50 dBm @ 1 GHz
(E-Field at probe: 1 V/m)
Output Power (dBm)
-30
-40
-50
-60
-70
-80
-90
-100
-110
-120
0.1
1
10
100
1000
10000
Frequency (MHz)
b) Detection Threshold of E-Field Probe
D = 900 µm
M9
Detection threshold of
commercial E-field probes
Lower level metals (M1 to M8)
E Field Contribution (V/m)
0.040
0.030
0.020
0.010
0.000
0
100
200
300
400
500
8000
Metal Layer Thickness (nm)

[DNC+19]

- At 1GHz operating frequency, detectable E-field for the state-of-the-art EM probes is 10 mV/m.
- For Intel 32nm, M9 is vulnerable to EM side-channel leakages.

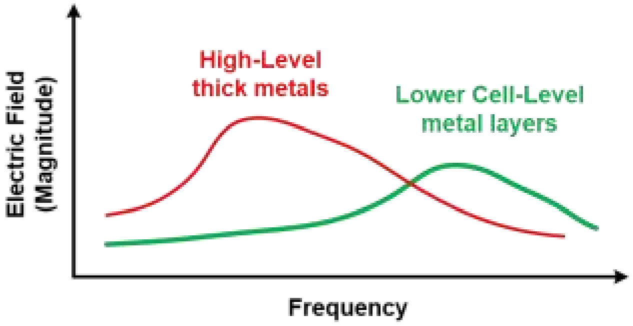
Ground-Up Root-Cause Analysis

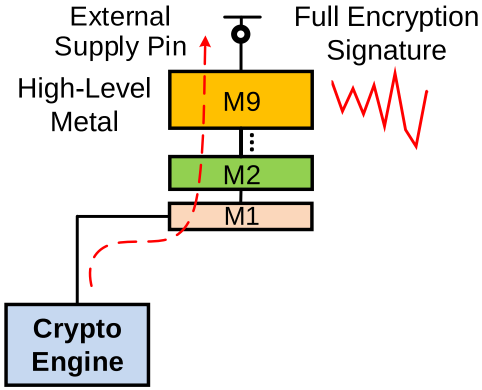


Switching Activity

Transformation through Metal-Interconnect Stack

EM Fields

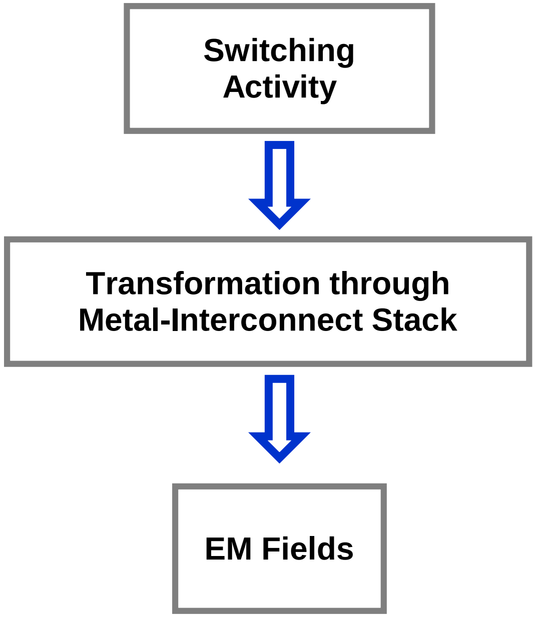




Goals:

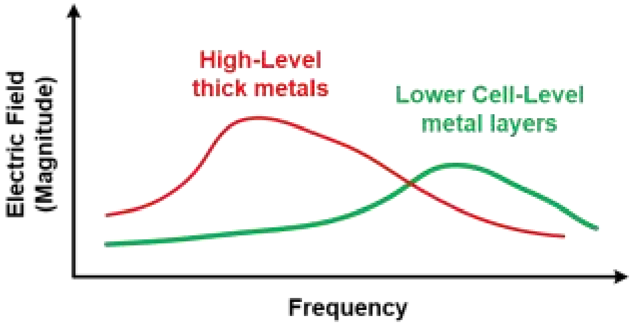
- Not pass the Correlated Current through the high-level metal layers.

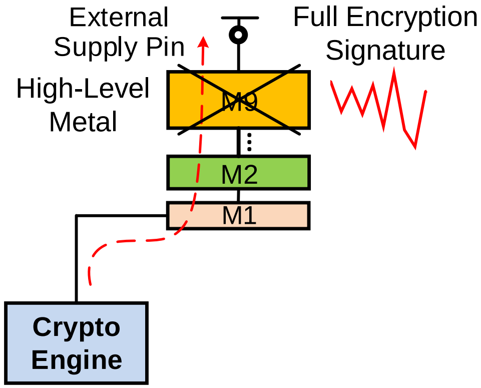
Ground-Up Root-Cause Analysis


Switching Activity

Transformation through Metal-Interconnect Stack

EM Fields

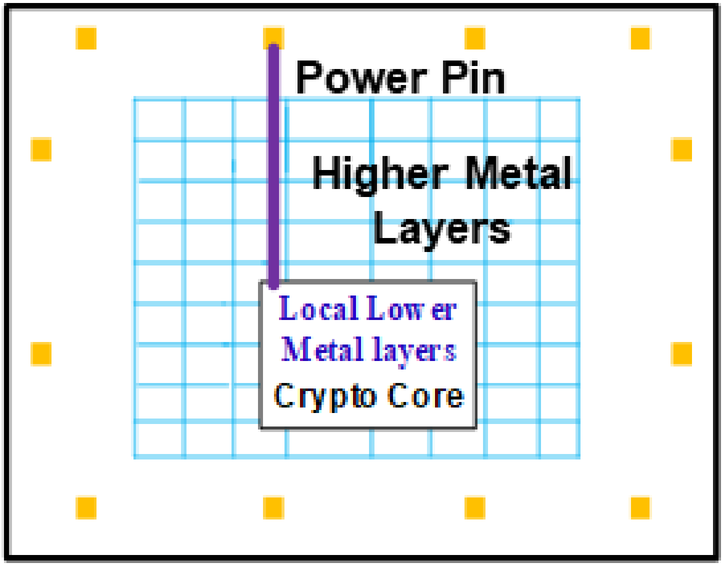




Goals:

- Not pass the Correlated Current through the high-level metal layers.
- But how can we achieve that?

Ground-Up Root-Cause Analysis



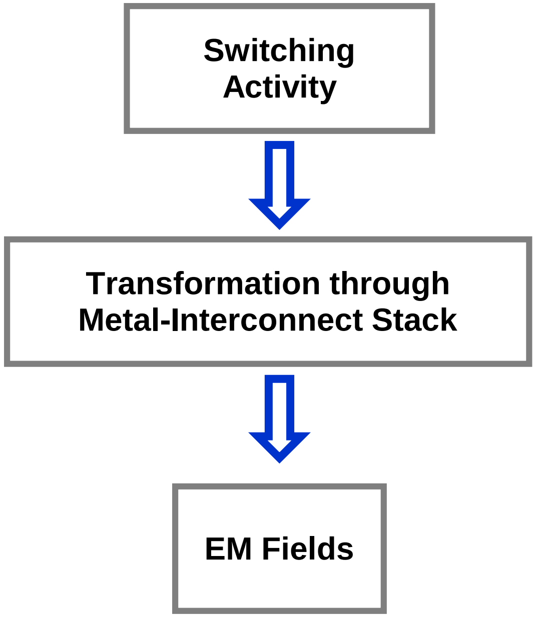
Power SCA Protection ✗

EM SCA Protection ✗

[DNC+19]

- Sensitive **signals** can be routed in the lower metal layers.
- But **power** has to come from off-chip components and hence needs to connect to the external pins through the higher metal layers.
- How can we restrict correlated power signatures to the lower metal layers?

Ground-Up Root-Cause Analysis



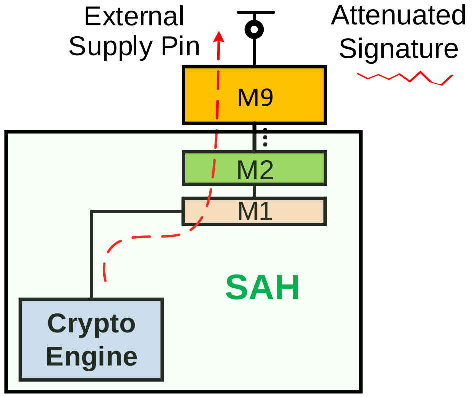
Switching Activity

Transformation through Metal-Interconnect Stack

EM Fields

Challenge:
EM SCA Resistant Design

Solution: STELLAR
Signature Attenuation Hardware (SAH) with Lower Metal Routing



Goals:

- Not pass the Correlated Current through the high-level metal layers.

Technique:

- Suppress the critical correlated signature in the lower metals before it reaches the top metal layers.

Overview: New Attacks and Defenses

Attack

SCNIFFER: Automated EM leakage point detection

X-DeepSCA: Cross-Device Deep-Learning SCA

Power & Electro-Magnetic Side-Channel

Defense

ASNI: Attenuated Signature Noise Injection

White-Box Root-Cause Analysis

STELLAR: Generic EM SCA Tolerance

STELLAR: Basics

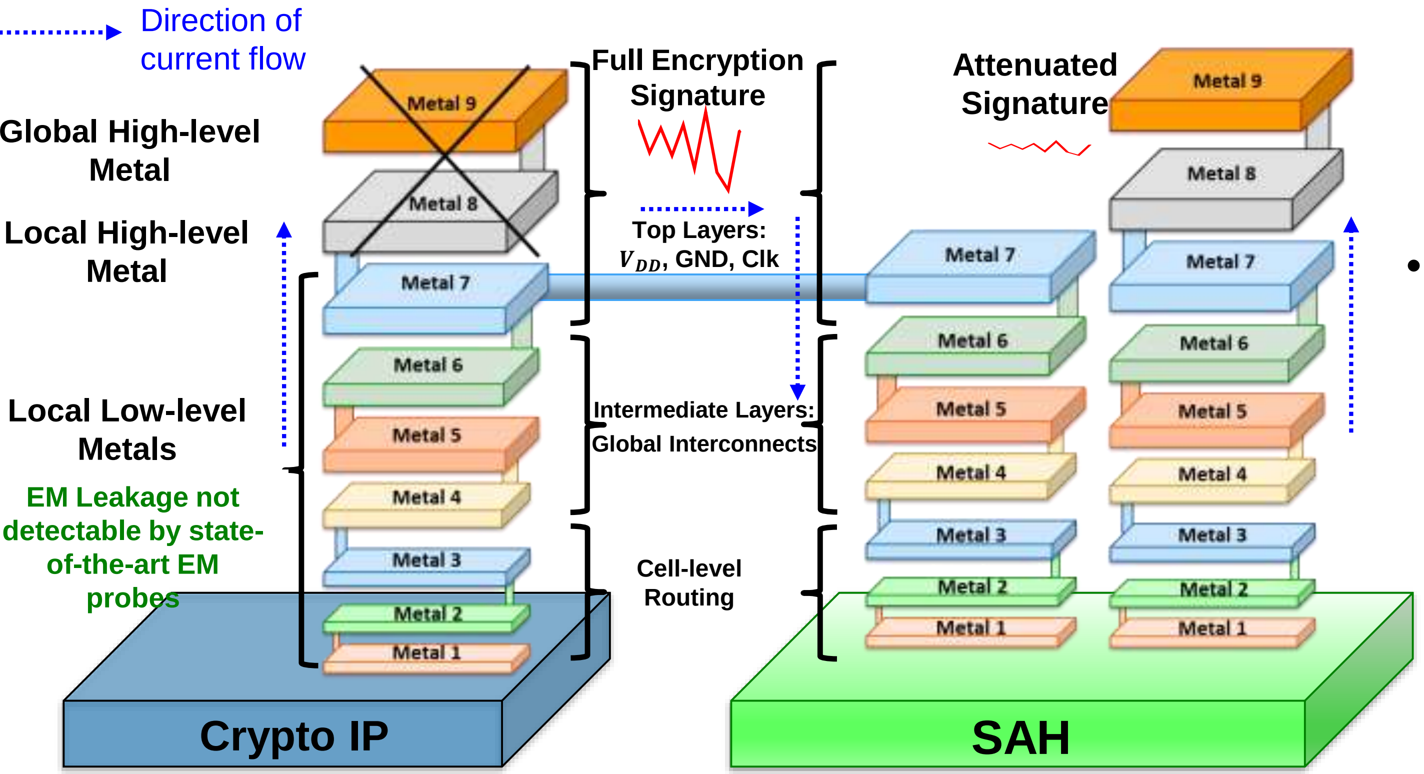
$$\text{MTD} \propto \frac{1}{SNR^2}$$

$$\text{MTD} \propto \frac{1}{SNR^2} * AT^2$$

Signature Attenuation

EM White Box Analysis: Countermeasure

STELLAR: Signature aTtenuation Embedded CRYPTO with Low-Level metAL Routing



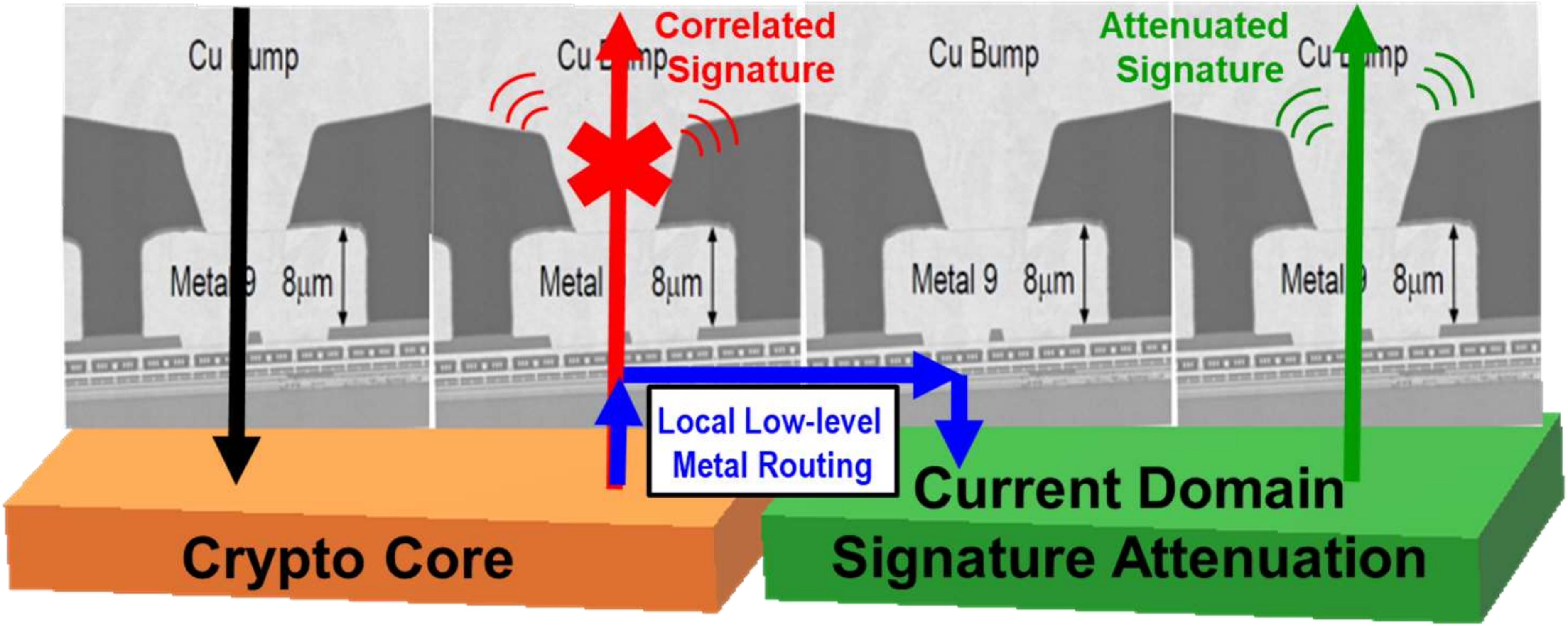
Crypto IP may include all the encryption algorithms: AES-128, SHA-3, ECC.

Generic Countermeasure

[DNC+19]

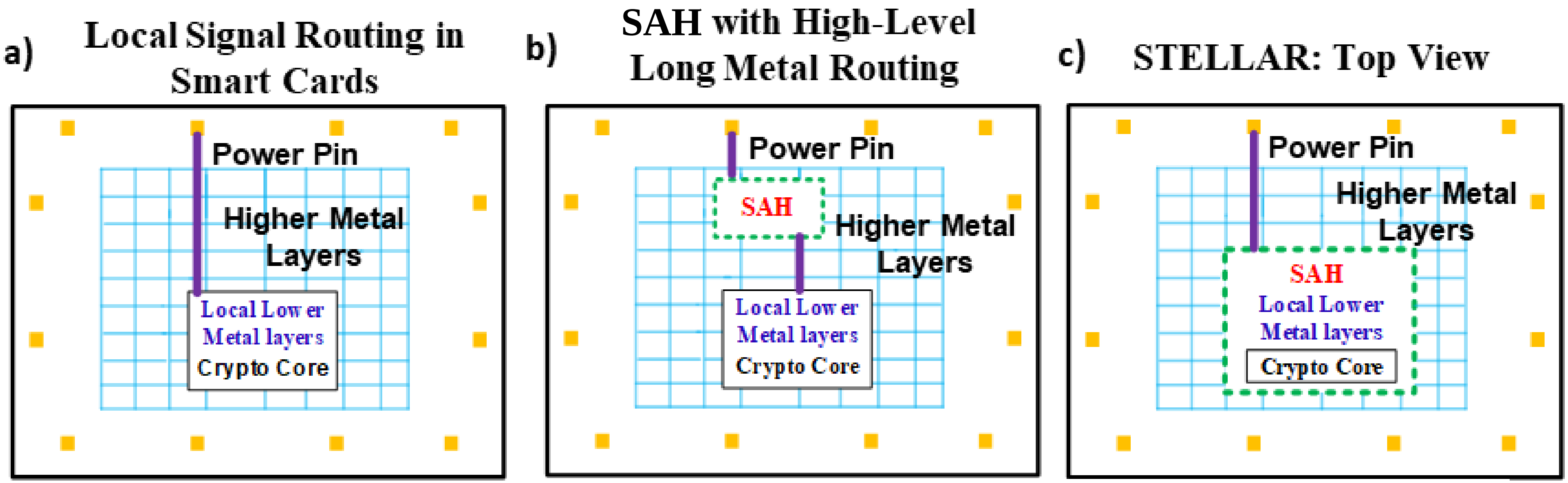
- Goal is to significantly suppress the crypto current in the lower level metal layers.
- Suppress Crypto Signature in higher metal layers (M9 and above) by placing a Signature Attenuation circuit embedding the crypto IP within the lower metal layers.

STELLAR: EM SCA Countermeasure: Simplified View



STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis
HOST 2019 (Best Student Paper Award)

STELLAR: Isolating Higher metals from the Crypto Core

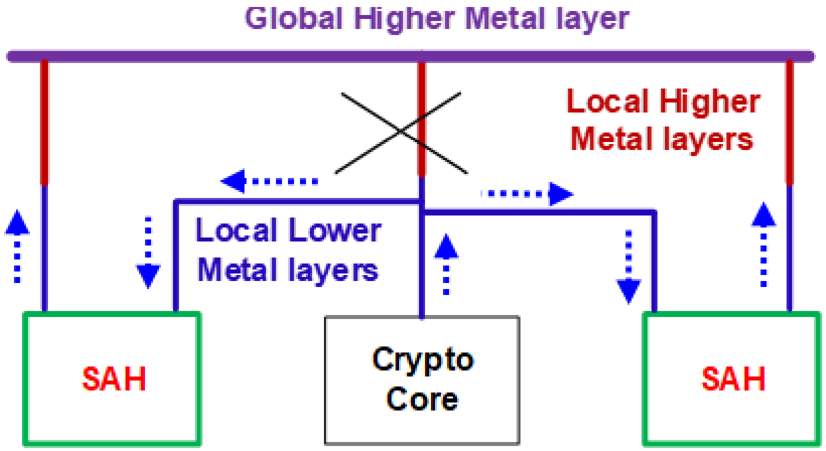


	a)	b)	c)
Power SCA Protection	✗	✓	✓
EM SCA Protection	✗	✗	✓

[DNC+19]

STELLAR – E-field Suppression

STELLAR: Cross Sectional Side View



[DNC+19]

- $E_{I_{unprot}} = 6\ mV/m$ for AES peak current of 3.2 m
- $AT_{Local} = \frac{M_9}{M_{X_{Crypto}}} \sim 20$
- $AT_{Global} = \frac{1}{AF_{SAH}} \sim 200$
- $E_{I_{STELLAR}} = \frac{E_{I_{Local}}}{AT_{Local}} + \frac{E_{I_{global}}}{AT_{global}}$

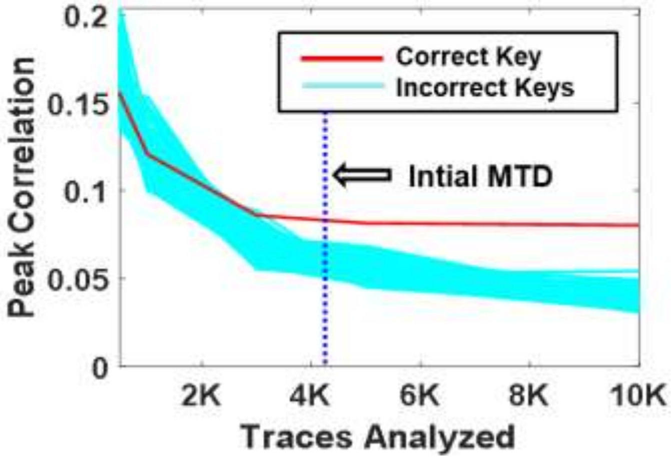
$$= \frac{0.25}{20} + \frac{5.75}{200} = 0.04\ \text{mV/m}$$

200x current signature attenuation

150x EM signature attenuation

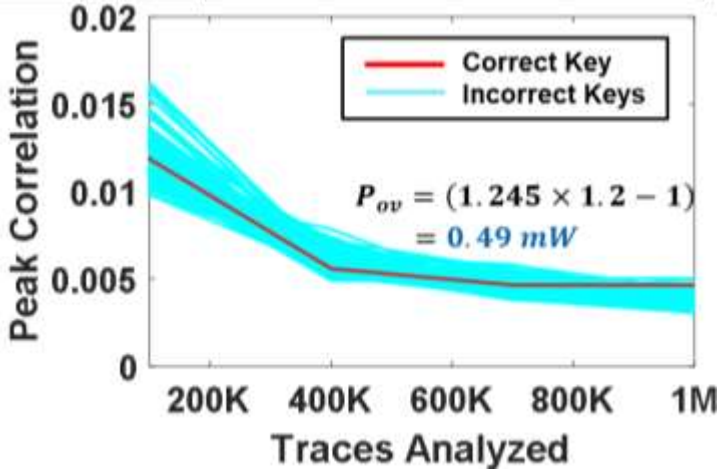
MTD Analysis

CEMA on Baseline AES



⟸ Intial MTD

CEMA on STELLAR-AES



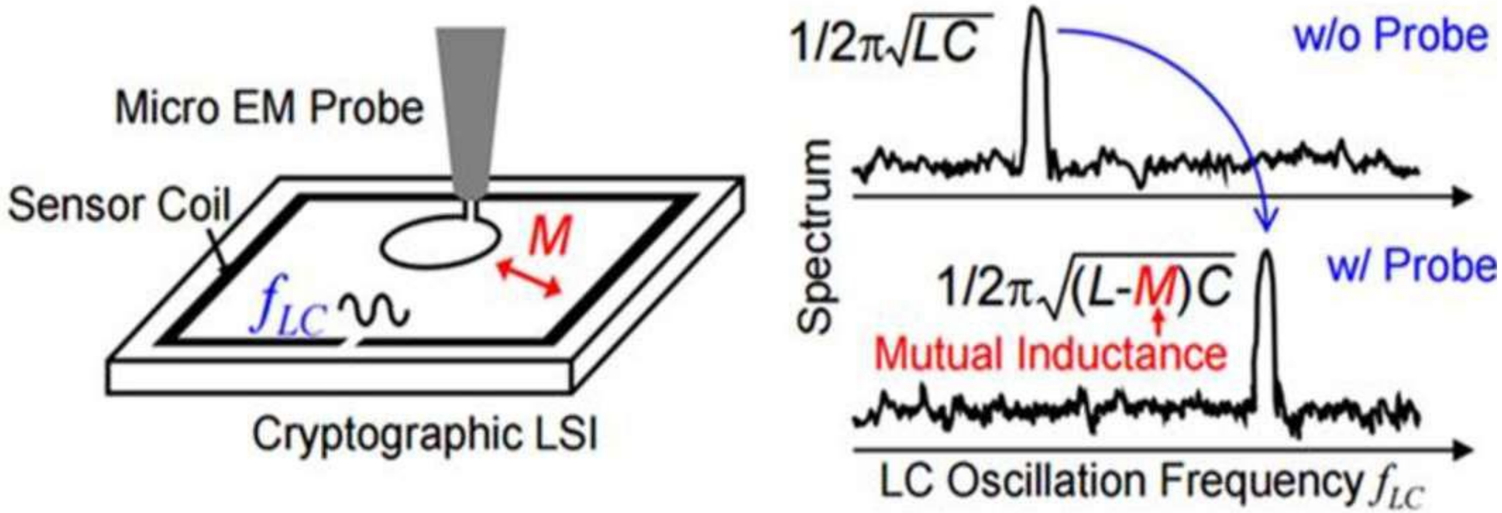
$P_{ov} = (1.245 \times 1.2 - 1)$
$= 0.49\ mW$

- Power Overhead = $\frac{1.49mW - 1mW}{1mW}$ * 100 = 49%.
- Area Overhead ~ 23%
- Both Power & EM SCA protection
- Generic Technique & can be extended to any crypto IP
- No degradation in Performance

DETECT APPROACHING EM PROBE

- BEFORE IT DETECTS YOUR CRITICAL SIGNAL

EM Attack Detection: Approaching Probe



Detection range 0.1mm

Detect the presence of a probe by LC oscillation frequency shift

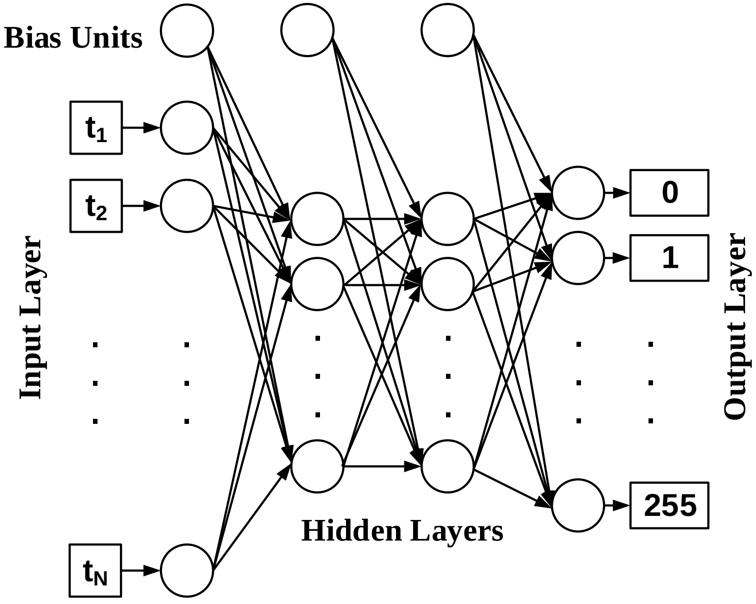
[HHM+14]

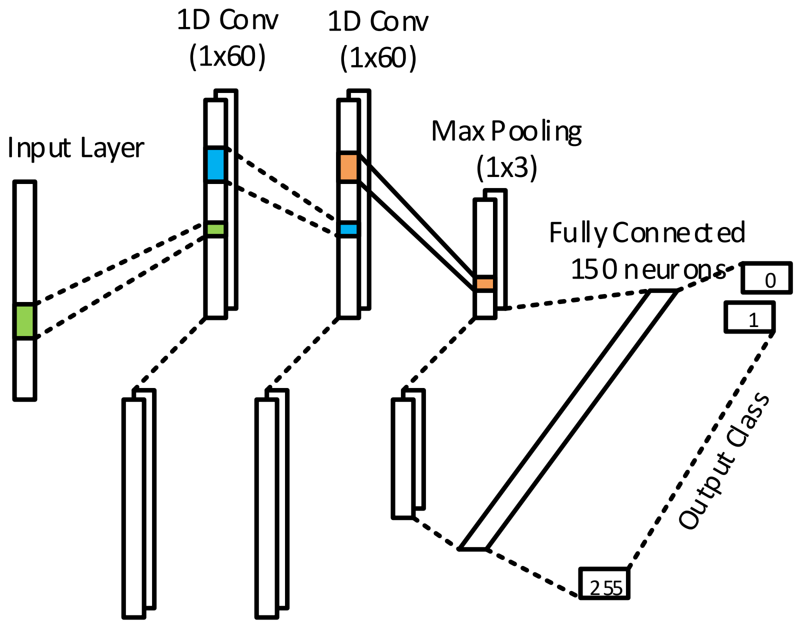
Q&A

Outline

Background	What & Why of Side Channel Attacks	
Power SCA	Attack	Defense using Power Management
EM SCA	Attack	Defense using Power Management
Profiled → ML SCA	Deep-Learning Attack and Defense	

Neural Network based Profiled Attack





Multi-Layer Perceptron (MLP)

1-D Convolutional Neural Network (CNN)

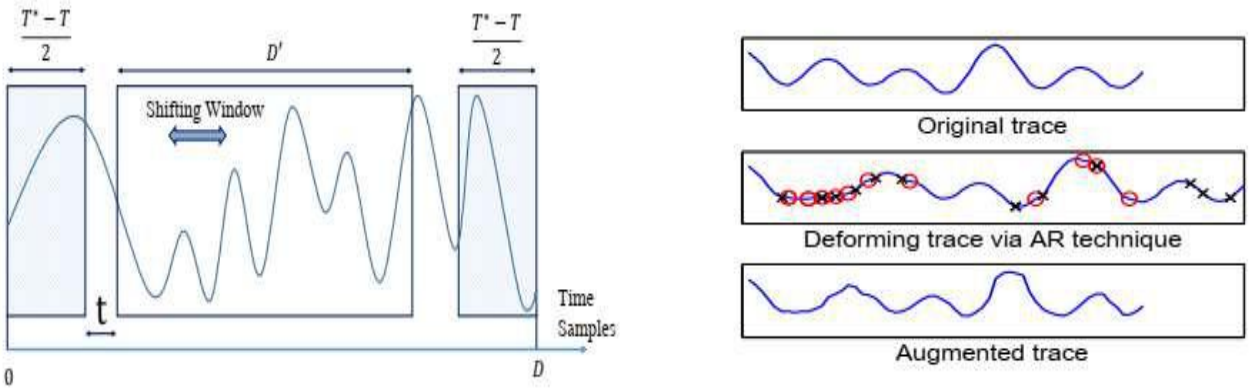
Typical Deep Neural Network Architectures Employed [GDD+19]

Number of layers and/or filters of MLP and 1-D CNN architectures depend on target platforms, and can be optimized using grid-search approach.

DNNs vs Gaussian Template Attacks

- Deep Neural Network based profiling attacks have several key advantages to the classical statistical template attacks:
  - Does not require a precise selection of Points of Interests (PoIs)
  - DNNs can handle large dimensions
  - Convolutional NNs can handle trace misalignment up to a certain degree.

CNN with Data Augmentation



Data Augmentation Techniques- Left: Shifting, Right: Add-Remove [CDP17]

- Data Augmentation reduces overfitting of CNN to training data
- Two data augmentation techniques were proposed in [CDP17]: (1) Shifting time samples, (2) Inserting and suppressing time samples, all chosen uniformly at random
- Data Augmentation helps achieve CNN better performance in the presence of jitter/misalignment based countermeasures

Overview: New Attacks and Defenses

Attack

SCNIFFER: Automated EM leakage point detection

X-DeepSCA: Cross-Device Deep-Learning SCA

Power & Electro-Magnetic Side-Channel

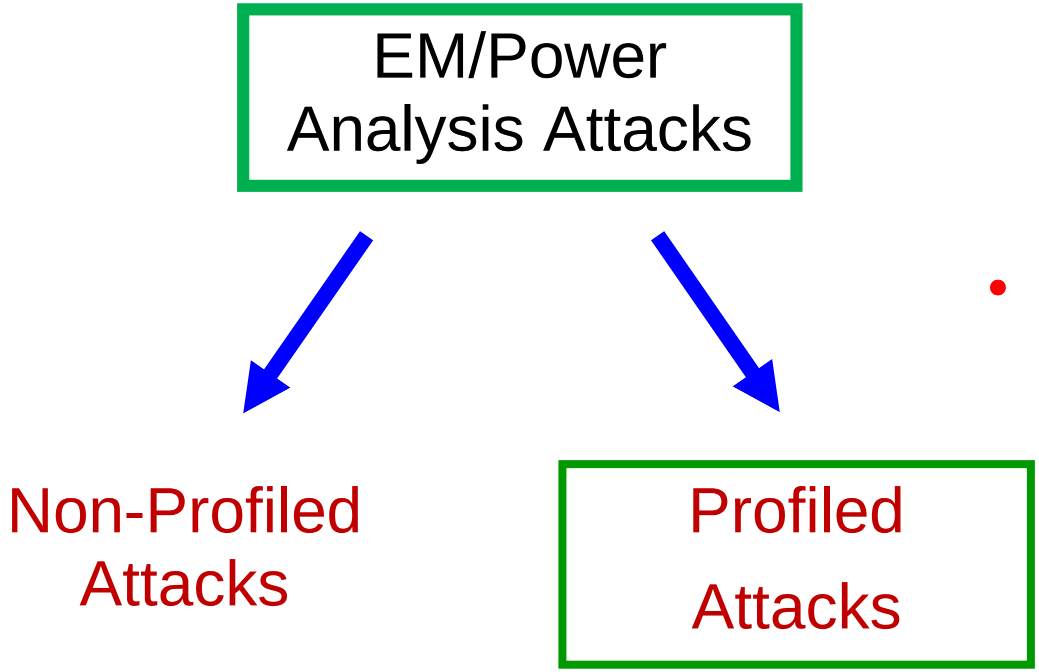
Defense

ASNI: Attenuated Signature Noise Injection

White-Box Root-Cause Analysis

STELLAR: Generic EM SCA Tolerance

Non-Profiled and Profiled attacks


EM/Power Analysis Attacks

Non-Profiled Attacks

Profiled Attacks

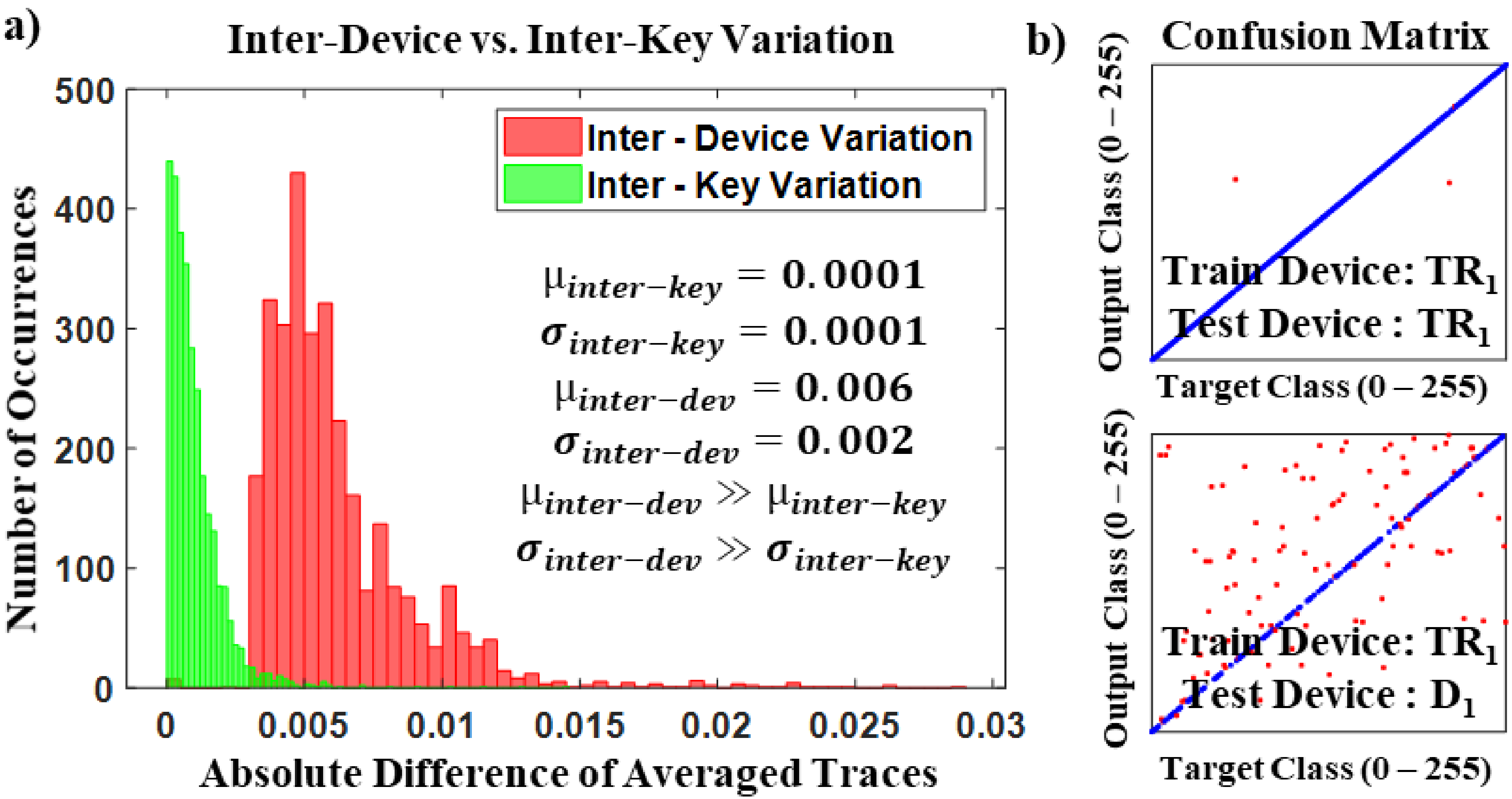
- Non-Profiled SCA:
  - Direct attack on a target device using HW/HD leakage model.
  - Eg. Differential/Correlational power analysis (DPA/CPA).
- Profiled SCA attack:
  - Build offline template using an identical device
  - Perform attack on a similar device with fewer traces (more powerful attack).
  - Eg. Statistical template attacks, machine learning based attacks.

Practical Issues with Profiled SCA

- Inherent Assumption in Profiled SCA is that the leakage profile of identical hardware running the same piece of software should be the same

- In reality, such assumption should be tested as works ([RSV+11], [MBT+13], [HOT+14], [OK18], [DGD+19], [GDD+19]) investigating Cross-Device attack using various profiling techniques showed that device to device variations can cause templates/classifiers to be biased towards the leakage profile of profiling device.

Challenges in Cross-device Attacks

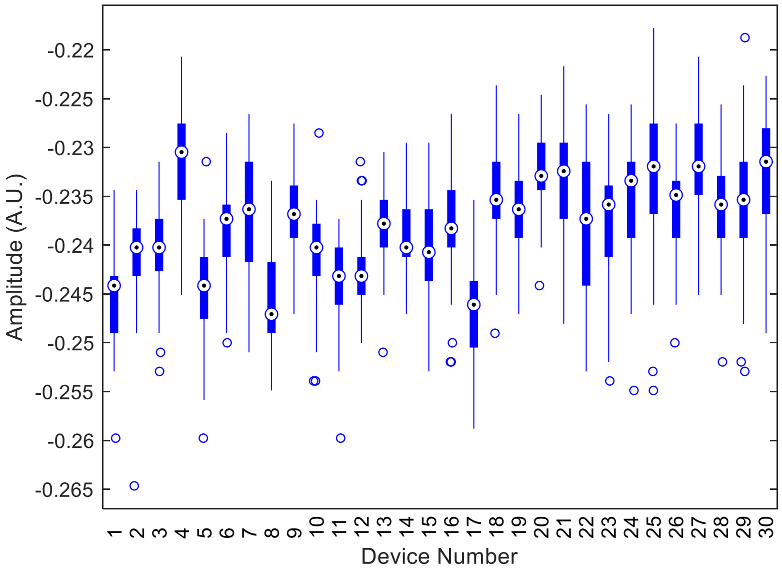


Practical Issues with Profiled SCA

- Sample Distribution of power consumption at a particular time instant is different for different devices of identical implementations, even with time-synchronized measurements.

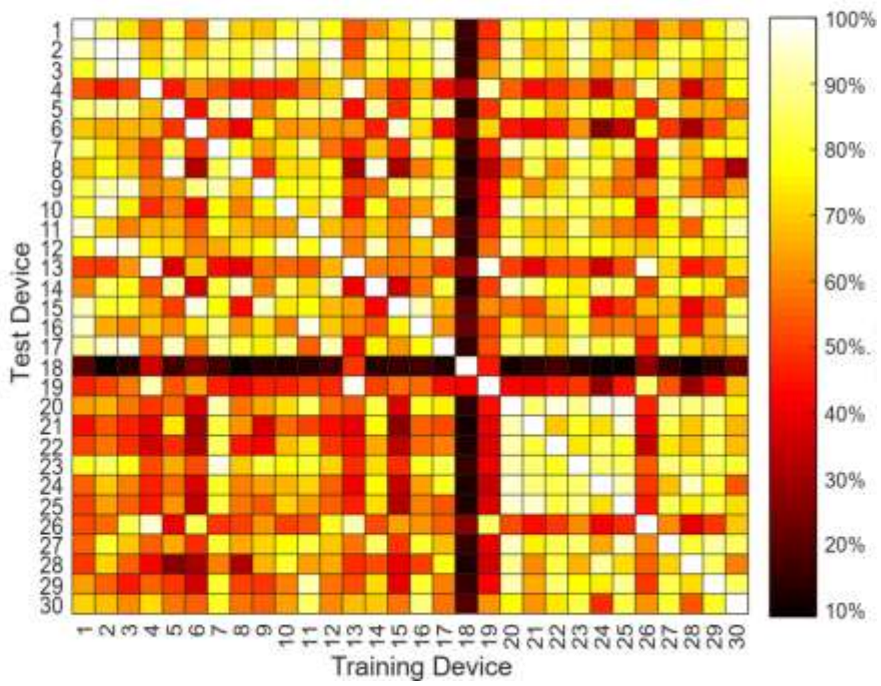
- Standard deviation of power consumption at any instant for the same key byte but from different devices can be much larger than that for different key bytes from the same device.

- These factors lead to high accuracy for test traces from the same device, but low accuracy for traces from a different one.

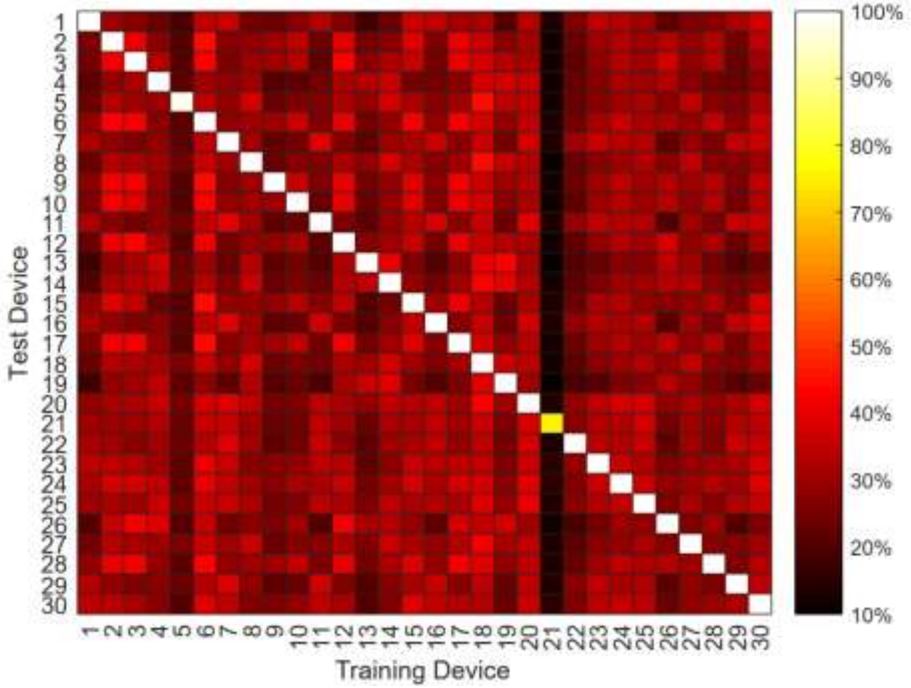


[GDD+19]

DNN Performance in Cross-Device Attack



Multi-Layer Perceptron (MLP)



1-D Convolutional Neural Network (CNN)

Performance of MLP and 1-D CNN after training with data from one device [GDD+19]

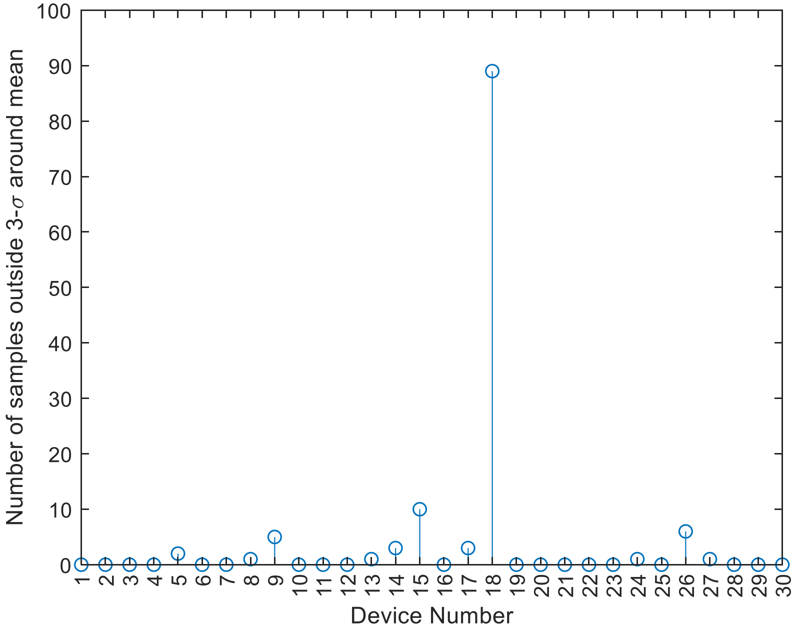
Performance of MLP and 1-D CNN is good for traces from same device, but poor for traces from a different device

DNN Performance in Cross-Device Attack

Rationale behind poor test accuracy:

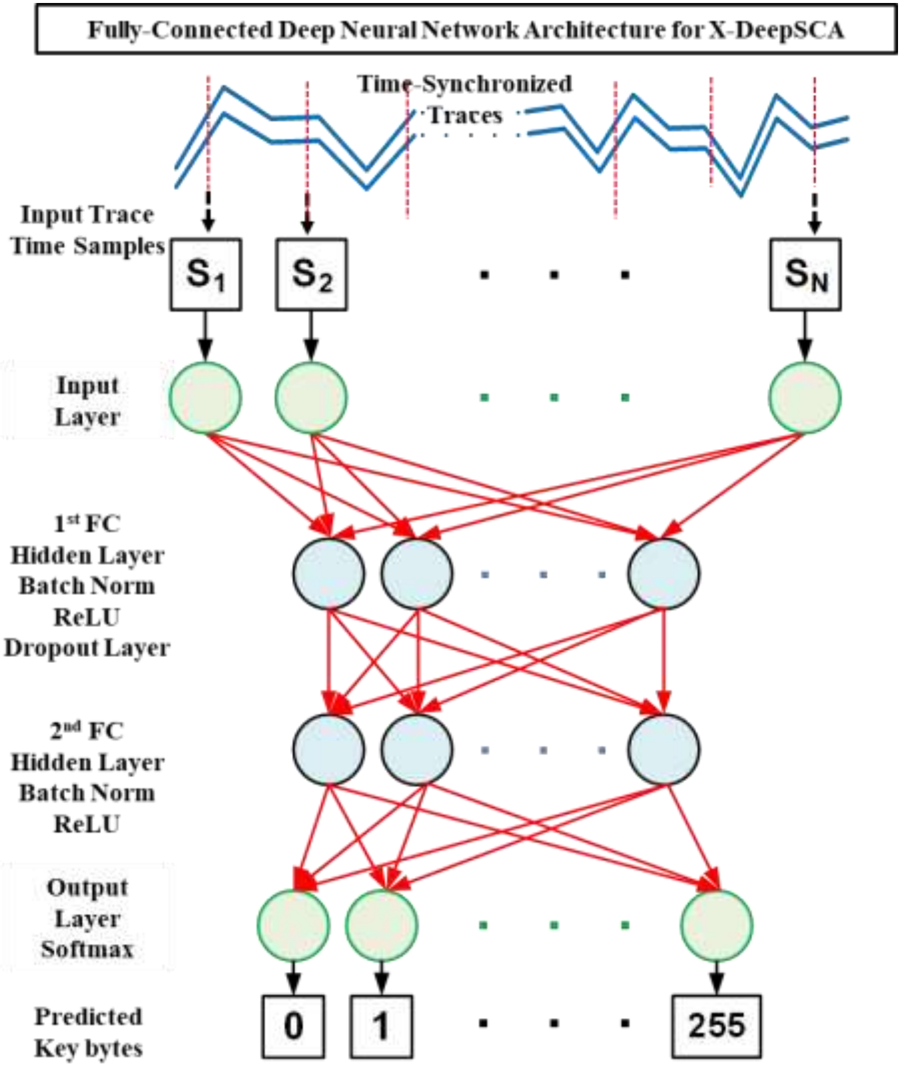
- Assuming an approximate Gaussian distribution, for all the devices, the trace samples of averaged trace for a particular device should have 99.7% of the samples within 3 standard deviation (σ) around the mean of averaged trace across all devices.

- Device 18 certainly is an outlier, which explains why Device 18 had poor test accuracy when the MLP was trained with traces from other devices and vice versa.



[GDD+19]

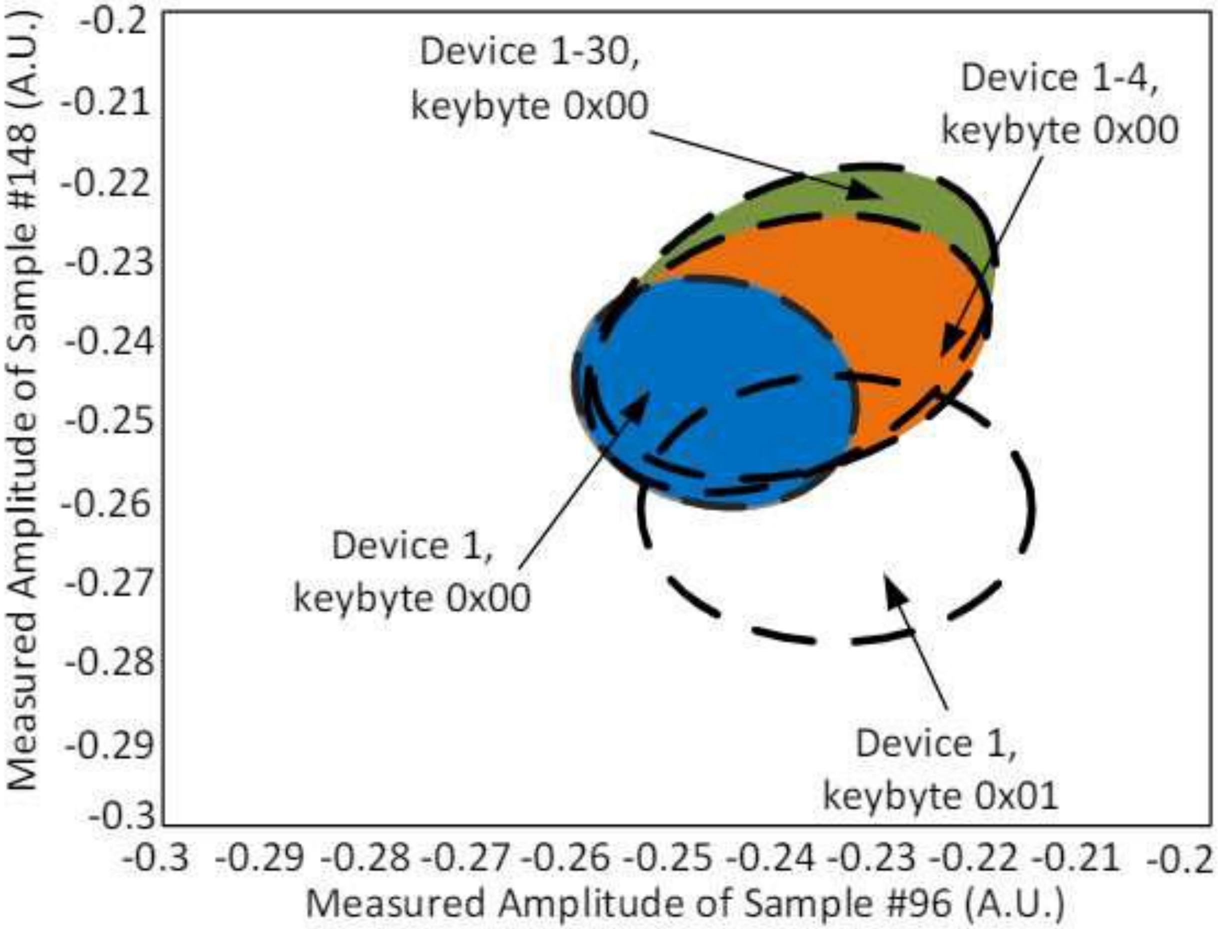
Neural Network Architecture


Fully-Connected Deep Neural Network Architecture for X-DeepSCA
Time-Synchronized Traces
Input Trace Time Samples
S_1
S_2
S_N
Input Layer
1st FC Hidden Layer Batch Norm ReLU Dropout Layer
2nd FC Hidden Layer Batch Norm ReLU
Output Layer Softmax
Predicted Key bytes
0
1
255

- Choice of the hyperparameters: Learning rate, number of hidden neurons, dropout optimized to prevent overfitting of the model to a certain device.

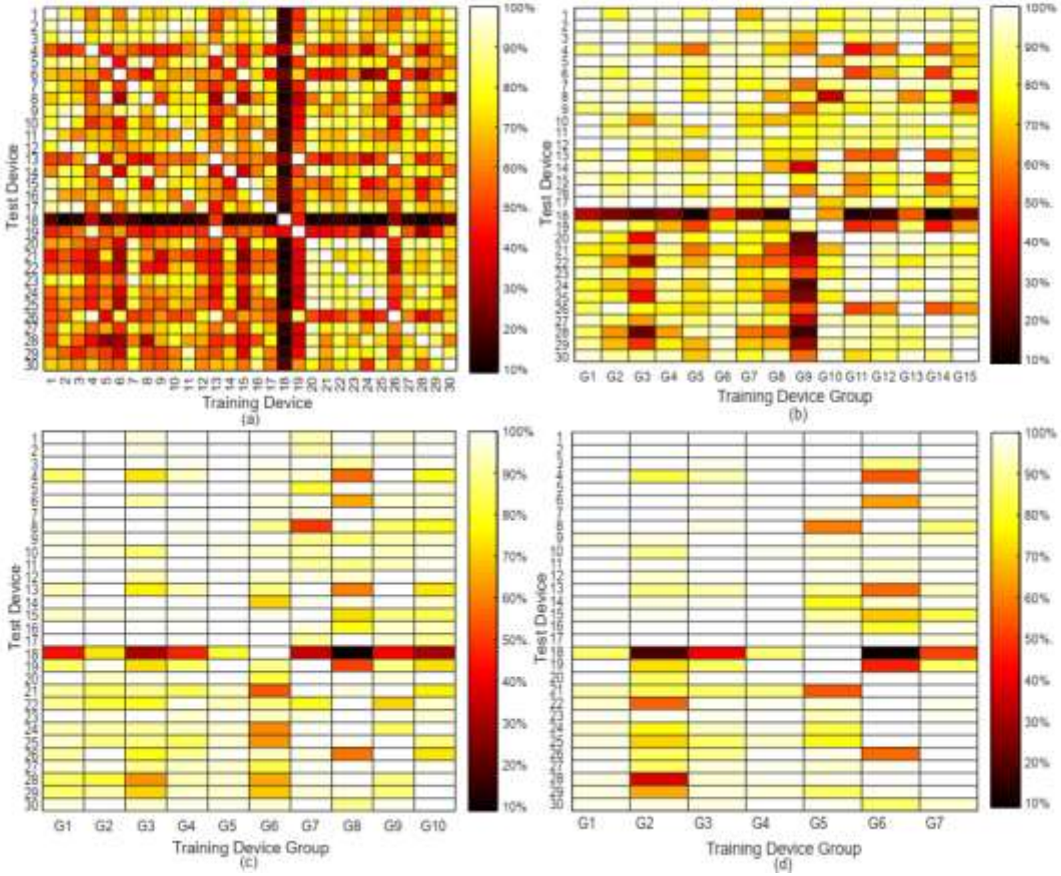
But how can we handle the inter-device variations?

X-DeepSCA Profiling: Multi-device Training



- As the no. of devices is inc. from 1 to 4, the sample PDF for a specific key byte value (0x00) approximates the total PDF for all the 30 devices
- 4 training devices are used to built the DNN model.

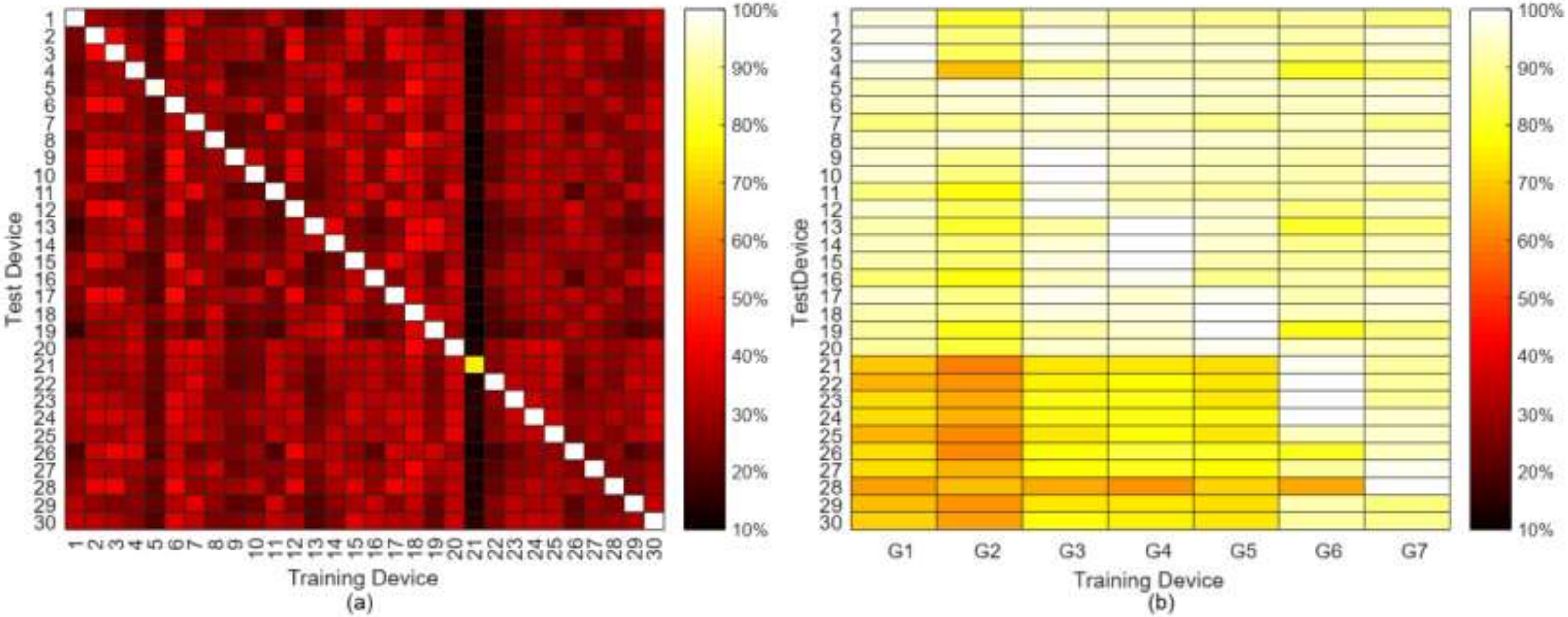
Effect of Multi-Device Training on Cross-Device Attack Performance of MLP



Performance of MLP after training with (a) 1 (b) 2 (c) 3 (d) 4 devices [GDD+19]

Test Accuracy of MLP improves with Multi-Device Training due to better leakage modeling.

Effect of Multi-Device Training on Cross-Device Attack Performance of CNN



Performance of CNN after training with (a) 1 (b) 4devices [GDD+19]

Test Accuracy of CNN improves with Multi-Device Training due to better leakage modeling.

PCA-MLP Performance in Cross-Device Attack

$$\boldsymbol{Traces} = \begin{bmatrix} trace_1 \\ trace_2 \\ \vdots \\ trace_M \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & \dots & t_{1N} \\ t_{21} & t_{22} & \dots & t_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ t_{M1} & t_{M2} & \dots & t_{MN} \end{bmatrix}$$

$$= \begin{bmatrix} t_1 & t_2 & \dots & t_N \end{bmatrix}$$

$$\boldsymbol{Traces_{adjust}} = \begin{bmatrix} t_1 - mean(t_1) & t_2 - mean(t_2) & \dots & t_N - mean(t_N) \end{bmatrix}$$

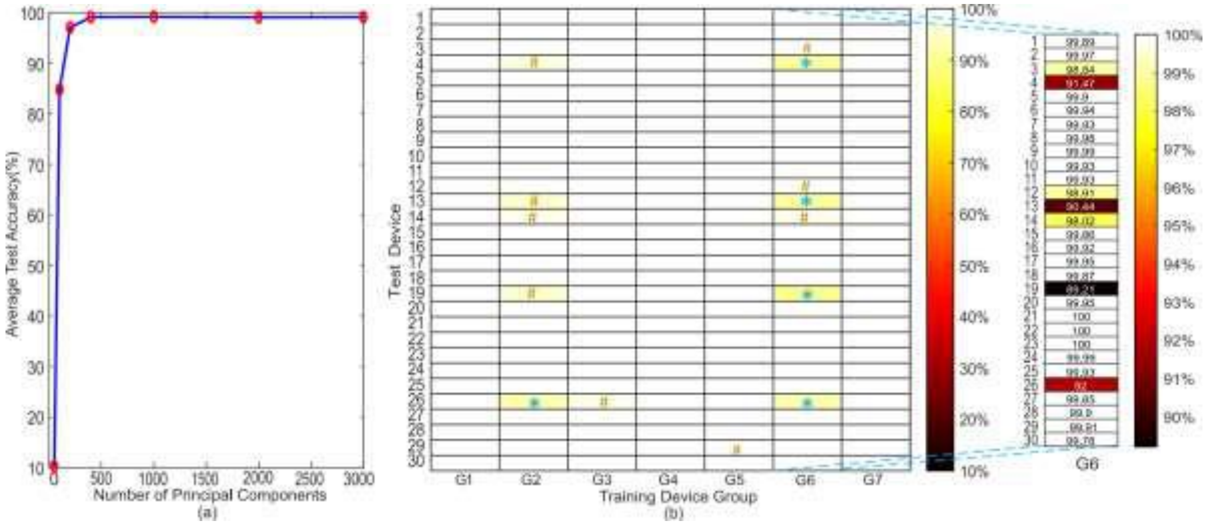
$$\text{Covariance matrix}, \boldsymbol{C} = cov(\boldsymbol{Traces}) = cov(\begin{bmatrix} t_1 & t_2 & \dots & t_N \end{bmatrix})$$

$$= \begin{bmatrix} cov(t_1, t_1) & cov(t_1, t_2) & \dots & cov(t_1, t_N) \\ cov(t_2, t_1) & cov(t_2, t_2) & \dots & cov(t_2, t_N) \\ \vdots & \vdots & \ddots & \vdots \\ cov(t_N, t_1) & cov(t_N, t_2) & \dots & cov(t_N, t_N) \end{bmatrix}$$

$$\boldsymbol{V} = \begin{bmatrix} v_1 & v_2 & \dots & v_N \end{bmatrix}$$

$$\boldsymbol{Traces_m} = (\boldsymbol{V_m}^T \times \boldsymbol{Traces_{adjust}}^T)^T$$

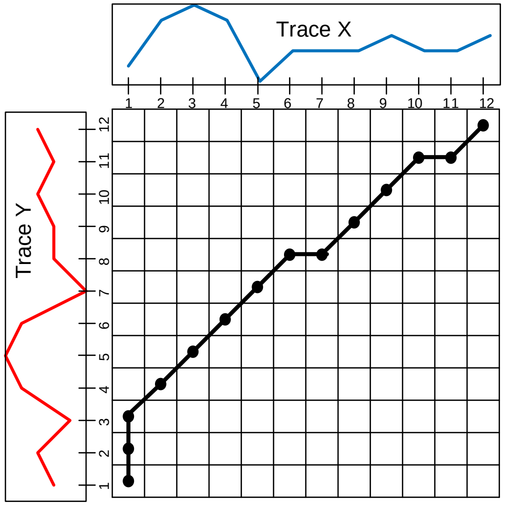
Principal Component Analysis (PCA)



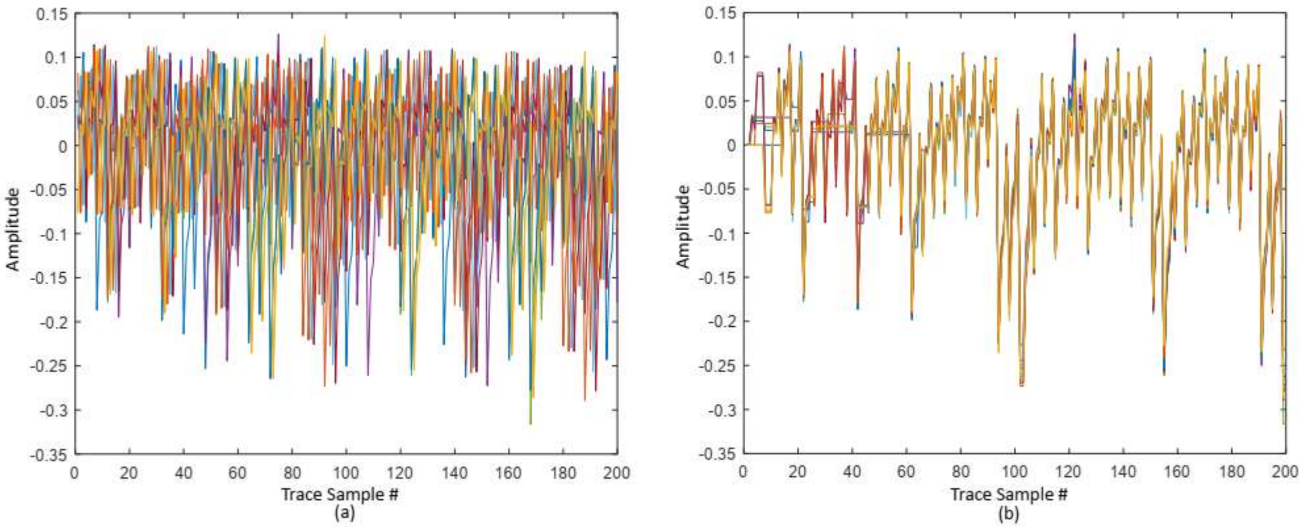
(a) Accuracy vs. Number of principal components used in training
(b) Performance of MLP with PCA and multi-device training
[GDD+19]

With 4 training devices and PCA based Pre-processing, average test accuracy across all devices reaches ~99.51% and test accuracy remains above ~90%.

Dynamic Time Warping (DTW) as pre-processing for PCA-MLP for misaligned traces



Warp Path in DTW

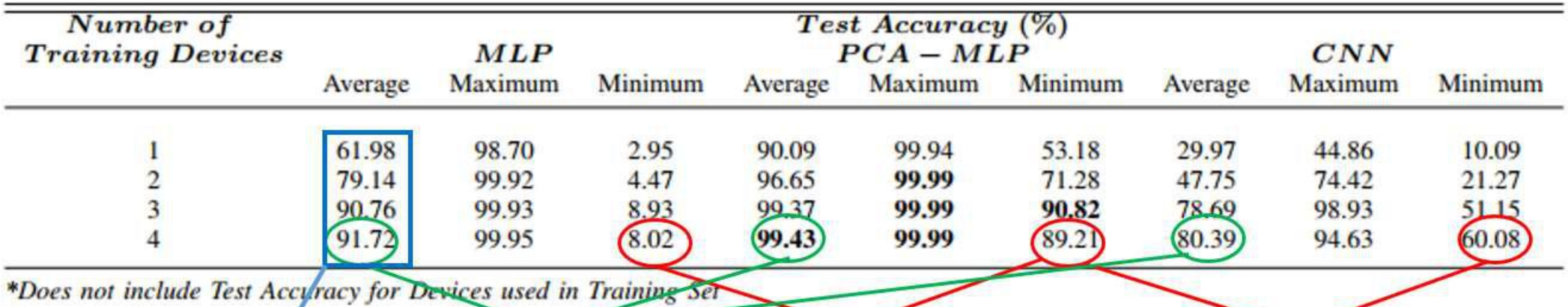


(a) Misaligned traces (b) Realigned traces using DTW [GDD+19]

Rationale behind use of DTW:

- Traces can be misaligned due to faulty triggering and/or countermeasures implemented
- PCA and MLP require realigned traces. DTW can realign them my stretching traces so as to minimize Euclidean distance between them.

Summary of DTW-PCA-MLP [GDD+19]



Number of Training Devices	MLP Average	MLP Maximum	MLP Minimum	PCA – MLP Average	PCA – MLP Maximum	PCA – MLP Minimum	CNN Average	CNN Maximum	CNN Minimum
1	61.98	98.70	2.95	90.09	99.94	53.18	29.97	44.86	10.09
2	79.14	99.92	4.47	96.65	**99.99**	71.28	47.75	74.42	21.27
3	90.76	99.93	8.93	99.37	**99.99**	**90.82**	78.69	98.93	51.15
4	91.72	99.95	8.02	**99.43**	**99.99**	89.21	80.39	94.63	60.08

Test Accuracy (%)

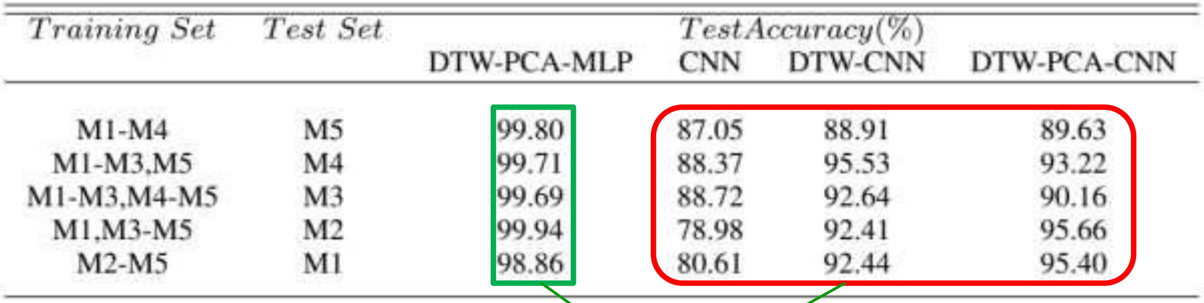
*Does not include Test Accuracy for Devices used in Training Set

Progressive Improvement with Multi-Device Training Compared to Single-Device Training

~8-20% improvement in average accuracy with PCA-MLP

An order of magnitude improvement in minimum accuracy with PCA-MLP compared to MLP

~30% better accuracy with PCA-MLP than CNN based approach



Training Set	Test Set	DTW-PCA-MLP	CNN	DTW-CNN	DTW-PCA-CNN
		TestAccuracy(%)			
M1-M4	M5	99.80	87.05	88.91	89.63
M1-M3,M5	M4	99.71	88.37	95.53	93.22
M1-M3,M4-M5	M3	99.69	88.72	92.64	90.16
M1,M3-M5	M2	99.94	78.98	92.41	95.66
M2-M5	M1	98.86	80.61	92.44	95.40

High accuracy of DTW-PCA-MLP on average compared to CNN based approaches for misaligned traces

Q&A

Remarks

- With the availability of low-cost EM probes, non-invasive EM side-channel attack can be used to attack commonplace IoT devices.
- The advancement in ML-based attacks can put a huge dent to the security of embedded devices.
- Low-Overhead Countermeasures against both power/EM SCA attacks are very critical.
- In order for industry to adopt the countermeasures, it needs to be low-overhead and generic to any algorithm.

SparcLab @ ECE, Purdue

PI: Shreyas Sen

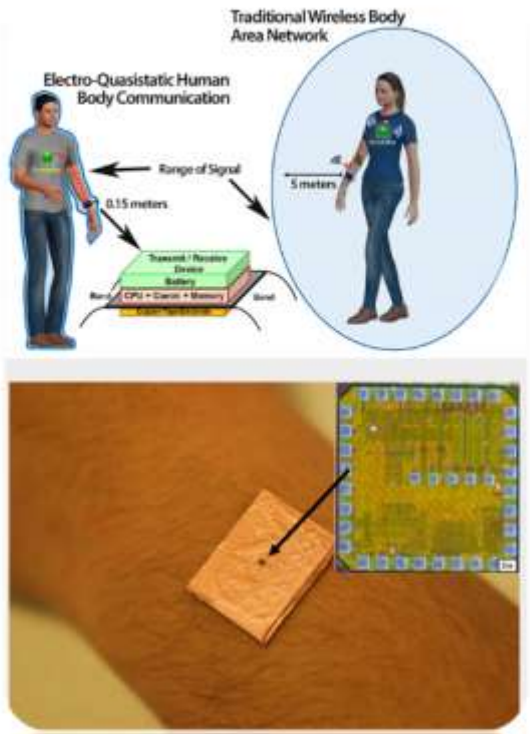
Assistant Professor, ECE, Purdue University

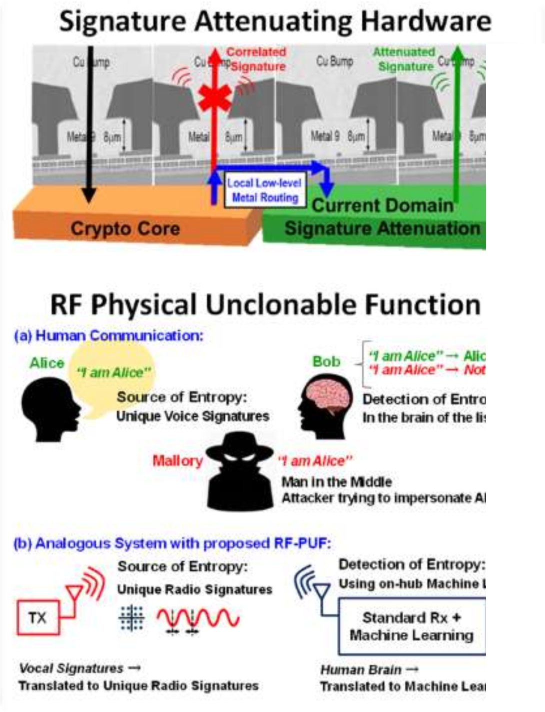
14+ years research experience @ **Purdue, Georgia Tech, Intel Labs, Qualcomm, Rambus**

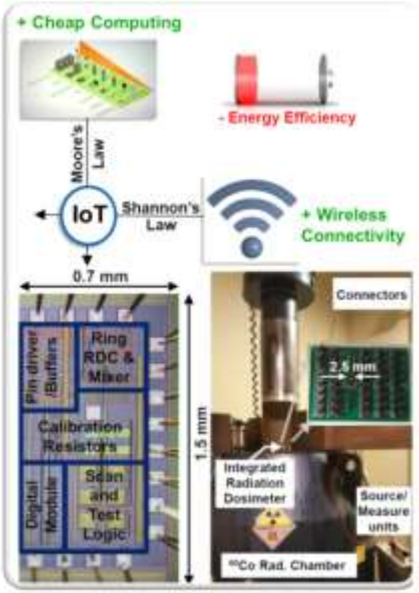
SPARC Lab: Sensing, Processing, Analytics & Radio Communication

SparcLab May 2019

Other On Going Project


Traditional Wireless Body Area Network
Electro-Quasistatic Human Body Communication
Range of Signal
0.15 meters
5 meters
Transmit / Receive Device
Battery
CPU + Clock + Memory


Signature Attenuating Hardware
Cu Bump
Correlated Signature
Attenuated Signature
Metal 9
8μm
Local Low-level Metal Routing
Crypto Core
Current Domain Signature Attenuation
RF Physical Unclonable Function
(a) Human Communication:
Alice
"I am Alice"
Source of Entropy: Unique Voice Signatures
Bob
"I am Alice" → Alic
"I am Alice" → Not
Detection of Entro
In the brain of the lis
Mallory
"I am Alice"
Man in the Middle
Attacker trying to impersonate Al
(b) Analogous System with proposed RF-PUF:
TX
Source of Entropy: Unique Radio Signatures
Detection of Entropy: Using on-hub Machine L
Standard Rx + Machine Learning
Vocal Signatures → Translated to Unique Radio Signatures
Human Brain → Translated to Machine Lea



Intelligent IoT Sensor Nodes

IoB/Bio-Medical

HBC (Physics to IC)

Hardware Security IC

Openings

We are Hiring!

Multiple Post-Doc and PhD openings

THANK YOU

References

[BGR+15] Balasch, J., Gierlichs, B., Reparaz, O. and Verbauwhede, I., 2015, September. DPA, bitslicing and masking at 1 GHz. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 599-619). Springer, Berlin, Heidelberg.

[BL12] Bartkewitz, T. and Lemke-Rust, K., 2012, November. Efficient template attacks based on probabilistic multi-class support vector machines. In International Conference on Smart Card Research and Advanced Applications (pp. 263-276). Springer, Berlin, Heidelberg.

[BPS+18] Benadjila, R., Prouff, E., Strullu, R., Cagli, E. and Dumas, C., 2018. Study of deep learning techniques for side-channel analysis and introduction to ASCAD database. ANSSI, France & CEA, LETI, MINATEC Campus, France. Online verfügbar unter https://eprint. iacr. org/2018/053. pdf, zuletzt geprüft am, 22, p.2018.

[BXC+12] Bo, Y., Xiangyu, L., Cong, C., Yihe, S., Liji, W. and Xiangmin, Z., 2012. An AES chip with DPA resistance using hardware-based random order execution. Journal of Semiconductors, 33(6), p.065009.

[CCC+19] Carbone, M., Conin, V., Cornélie, M.A., Dassance, F., Dufresne, G., Dumas, C., Prouff, E. and Venelli, A., 2019. Deep learning to evaluate secure RSA implementations. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.132-161.

[CDP17] Cagli, E., Dumas, C. and Prouff, E., 2017, September. Convolutional neural networks with data augmentation against jitter-based countermeasures. In International Conference on Cryptographic Hardware and Embedded Systems (pp. 45-68). Springer, Cham.

References

[CRR02] **Chari, S., Rao, J.R. and Rohatgi, P., 2002, August. Template attacks. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 13-28). Springer, Berlin, Heidelberg.**

[DGD+19] **Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A. and Sen, S., 2019, June. X-DeepSCA: Cross-device deep learning side channel attack. In Proceedings of the 56th Annual Design Automation Conference 2019 (p. 134). ACM.**

[DMN+18] **Das, D., Maity, S., Nasir, S.B., Ghosh, S., Raychowdhury, A. and Sen, S., 2018. ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity. IEEE Transactions on Circuits and Systems I: Regular Papers, 65(10), pp.3300-3311.**

[DNC+19] **Das, D., Nath, M., Chatterjee, B., Ghosh, S. and Sen, S., 2019, March. STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis. In Proc. 2019 IEEE Int. Symp. Hardw. Oriented Security Trust.**

[GDD+19] **Golder, A., Das, D., Danial, J., Ghosh, S., Sen, S. and Raychowdhury, A., 2019. Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. IEEE Transactions on Very Large Scale Integration (VLSI) Systems.**

[GHO15] **Gilmore, R., Hanley, N. and O'Neill, M., 2015, May. Neural network based attack on a masked implementation of AES. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 106-111). IEEE.**

References

[GM11] Güneysu, T. and Moradi, A., 2011, September. Generic side-channel countermeasures for reconfigurable devices. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 33-48). Springer, Berlin, Heidelberg.

[HHM+14] Homma, N., Hayashi, Y.I., Miura, N., Fujimoto, D., Tanaka, D., Nagata, M. and Aoki, T., 2014, September. Em attack is non-invasive?-design methodology and validity verification of em attack sensor. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 1-16). Springer, Berlin, Heidelberg.

[HOT+14] Hanley, N., O'Neill, M., Tunstall, M. and Marnane, W.P., 2014, October. Empirical evaluation of multi-device profiling side-channel attacks. In 2014 IEEE Workshop on Signal Processing Systems (SiPS) (pp. 1-6). IEEE.

[HZ12] Heuser, A. and Zohner, M., 2012, May. Intelligent machine homicide. In International Workshop on Constructive Side-Channel Analysis and Secure Design (pp. 249-264). Springer, Berlin, Heidelberg.

[KJJ98] Kocher, P, Jaffe, J. and Jun B., 1998. Differential Power Analysis. In CRYPTO 1999.

[KOP09] Kasper T., Oswald D. and Paar C., EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment, In WISA 2009.

[KSM+17] Kar, M., Singh, A., Mathew, S., Rajan, A., De, V. and Mukhopadhyay, S., 2017, February. 8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator. In 2017 IEEE International Solid-State Circuits Conference (ISSCC) (pp. 142-143). IEEE.

References

[LBM14] Lerman, L., Bontempi, G. and Markowitch, O., 2014. Power analysis attack: an approach based on machine learning. IJACT, 3(2), pp.97-115.

[LBM15] Lerman, L., Bontempi, G. and Markowitch, O., 2015. A machine learning approach against a masked AES. Journal of Cryptographic Engineering, 5(2), pp.123-139.

[LZP15] Lu, S., Zhang, Z. and Papaefthymiou, M., 2015, June. 1.32 GHz high-throughput charge-recovery AES core with resistance to DPA attacks. In 2015 Symposium on VLSI Circuits (VLSI Circuits) (pp. C246-C247). IEEE.

[MBT+13] Montminy, D.P., Baldwin, R.O., Temple, M.A. and Laspe, E.D., 2013. Improving cross-device attacks using zero-mean unit-variance normalization. Journal of Cryptographic Engineering, 3(2), pp.99-110.

[MDM16] Martinasek, Z., Dzurenda, P. and Malina, L., 2016, June. Profiling power analysis attack based on MLP in DPA contest V4. 2. In 2016 39th International Conference on Telecommunications and Signal Processing (TSP) (pp. 223-226). IEEE.

[MHM13] Martinasek, Z., Hajny, J. and Malina, L., 2013, November. Optimization of power analysis using neural network. In International Conference on Smart Card Research and Advanced Applications (pp. 94-107). Springer, Cham.

[MOP08] Mangard, S., Oswald, E. and Popp, T., 2008. Power analysis attacks: Revealing the secrets of smart cards (Vol. 31). Springer Science & Business Media.

References

[MPP16] Maghrebi, H., Portigliatti, T. and Prouff, E., 2016, December. Breaking cryptographic implementations using deep learning techniques. In International Conference on Security, Privacy, and Applied Cryptography Engineering (pp. 3-26). Springer, Cham.

[NAB+08] Natarajan, S., Armstrong, M., Bost, M., Brain, R., Brazier, M., Chang, C.H., Chikarmane, V., Childs, M., Deshpande, H., Dev, K. and Ding, G., 2008, December. A 32nm logic technology featuring 2 nd-generation high-k+ metal-gate transistors, enhanced channel strain and 0.171 μm 2 SRAM cell size in a 291Mb array. In 2008 IEEE International Electron Devices Meeting (pp. 1-3). IEEE.

[OK18] Choudary, M.O. and Kuhn, M.G., 2017. Efficient, portable template attacks. IEEE Transactions on Information Forensics and Security, 13(2), pp.490-501.

[OM07] Oswald, E. and Mangard, S., 2007, February. Template attacks on masking—resistance is futile. In Cryptographers’ Track at the RSA Conference (pp. 243-256). Springer, Berlin, Heidelberg.

[PKZ+07] Popp, T., Kirschbaum, M., Zefferer, T. and Mangard, S., 2007, September. Evaluation of the masked logic style MDPL on a prototype chip. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 81-94). Springer, Berlin, Heidelberg.

[PM05] Popp, T. and Mangard, S., 2005, August. Masked dual-rail pre-charge logic: DPA-resistance without routing constraints. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 172-186). Springer, Berlin, Heidelberg.

References

[RO04] Rechberger, C. and Oswald, E., 2004, August. Practical template attacks. In International Workshop on Information Security Applications (pp. 440-456). Springer, Berlin, Heidelberg.

[RSV+11] Renauld, M., Standaert, F.X., Veyrat-Charvillon, N., Kamel, D. and Flandre, D., 2011, May. A formal study of power variability issues and side-channel attacks for nanoscale devices. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 109-128). Springer, Berlin, Heidelberg.

[SKM+18] Singh, A., Kar, M., Mathew, S.K., Rajan, A., De, V. and Mukhopadhyay, S., 2018. Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering. IEEE Journal of Solid-State Circuits, 54(2), pp.569-583.

[SKR+16] Singh, A., Kar, M., Rajan, A., De, V. and Mukhopadhyay, S., 2016, May. Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines. In 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 145-148). IEEE.

[TAV02] Tiri, K., Akmal, M. and Verbauwhede, I., 2002, September. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In Proceedings of the 28th European solid-state circuits conference (pp. 403-406). IEEE.

[TB10] Tokunaga, C. and Blaauw, D., 2009. Securing encryption systems with a switched capacitor current equalizer. IEEE Journal of Solid-State Circuits, 45(1), pp.23-31.

References

[RO04] Rechberger, C. and Oswald, E., 2004, August. Practical template attacks. In International Workshop on Information Security Applications (pp. 440-456). Springer, Berlin, Heidelberg.

[RSV+11] Renauld, M., Standaert, F.X., Veyrat-Charvillon, N., Kamel, D. and Flandre, D., 2011, May. A formal study of power variability issues and side-channel attacks for nanoscale devices. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 109-128). Springer, Berlin, Heidelberg.

[TV04] Tiri, K. and Verbauwhede, I., 2004, February. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In Proceedings Design, Automation and Test in Europe Conference and Exhibition (Vol. 1, pp. 246-251). IEEE.

[WYR+13] Wang, X., Yueh, W., Roy, D.B., Narasimhan, S., Zheng, Y., Mukhopadhyay, S., Mukhopadhyay, D. and Bhunia, S., 2013, May. Role of power grid in side channel attack and power-grid-aware secure design. In Proceedings of the 50th Annual Design Automation Conference (p. 78). ACM.