



---

Welcome to the Webinar Offered by:

# National Microelectronics Security Training (MEST) Center



# Unlocking the Potential of Impedance Side-channel: Expanding Horizons in Hardware Security and Privacy

Tauhidur Rahman

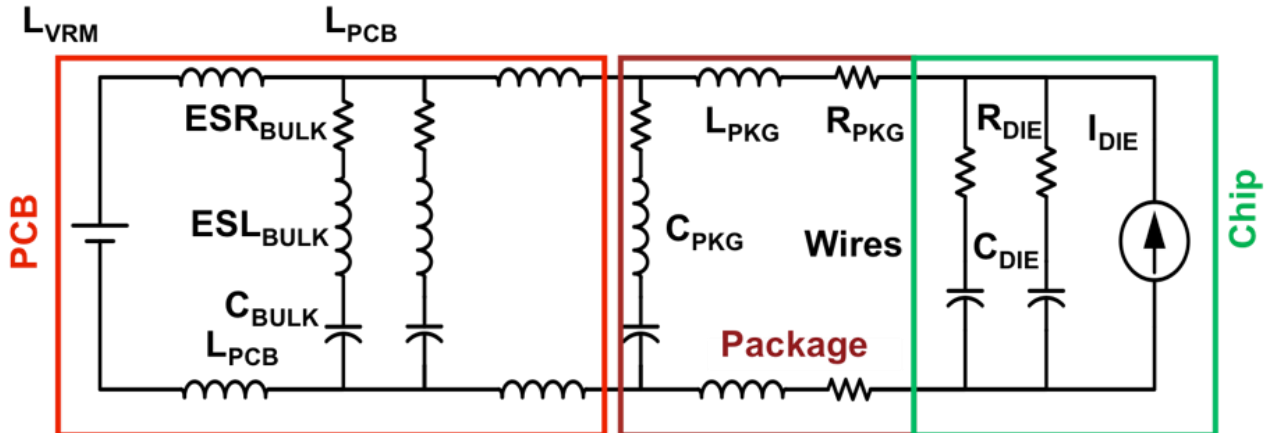
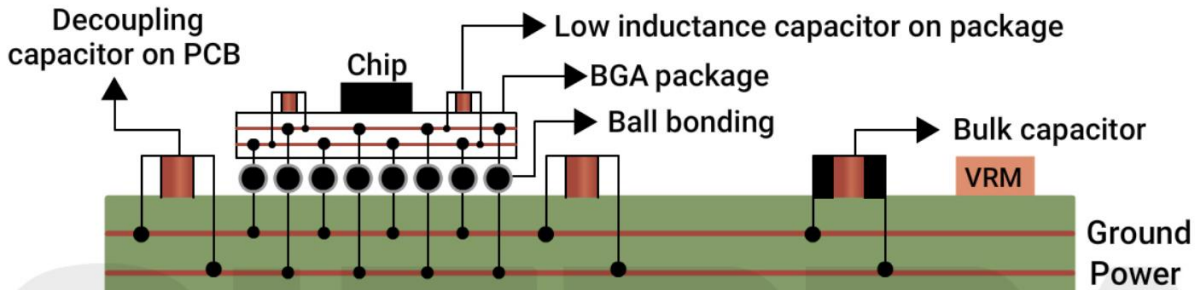
Assistant Professor, Dept. of Electrical and Computer Engineering  
Florida International University

MEST Center – National Microelectronic Security Training Center

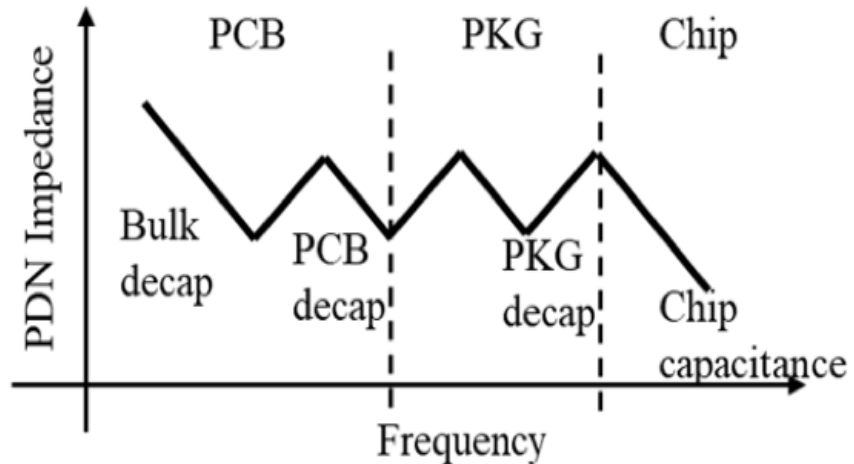
SeRLoP Research

- Introduction to power delivery network (PDN) impedance
- PDN impedance in hardware security
- Introduction to impedance side channel
- Impedance side-channel in disassemble software instructions
- Impedance side-channel in AES-128 Key extraction
- Impedance side-channel vs. power side-channel attacks
- Conclusion

# Power Distribution or Delivery Network (PDN)

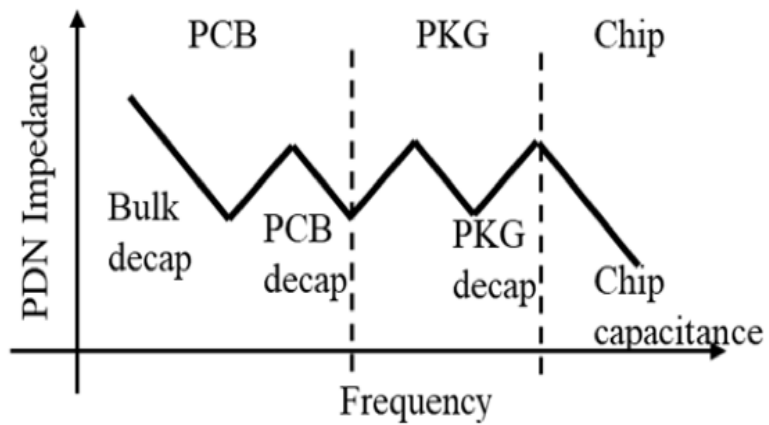
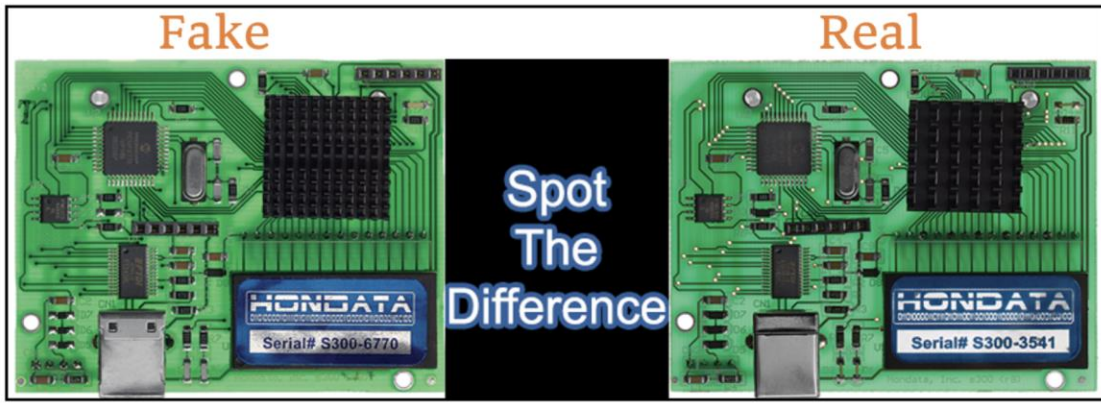
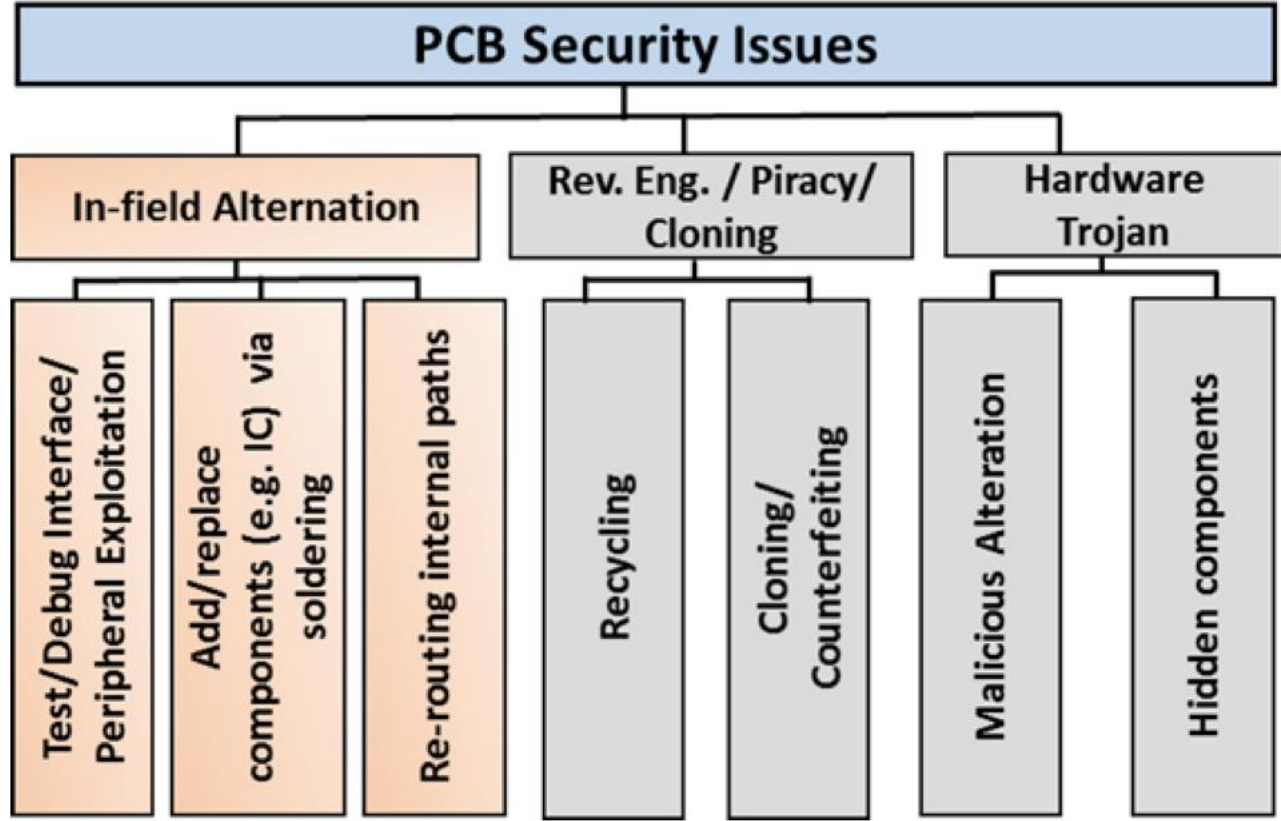


- PDN provides enough current and voltage to every load to meet their requirements
- Frequency dependent
- Target PDN impedance: to minimize supply and ground bounce
- Decoupling capacitors



$$\text{Impedance, } Z = R + j(2\pi fL - \frac{1}{2\pi fC})$$

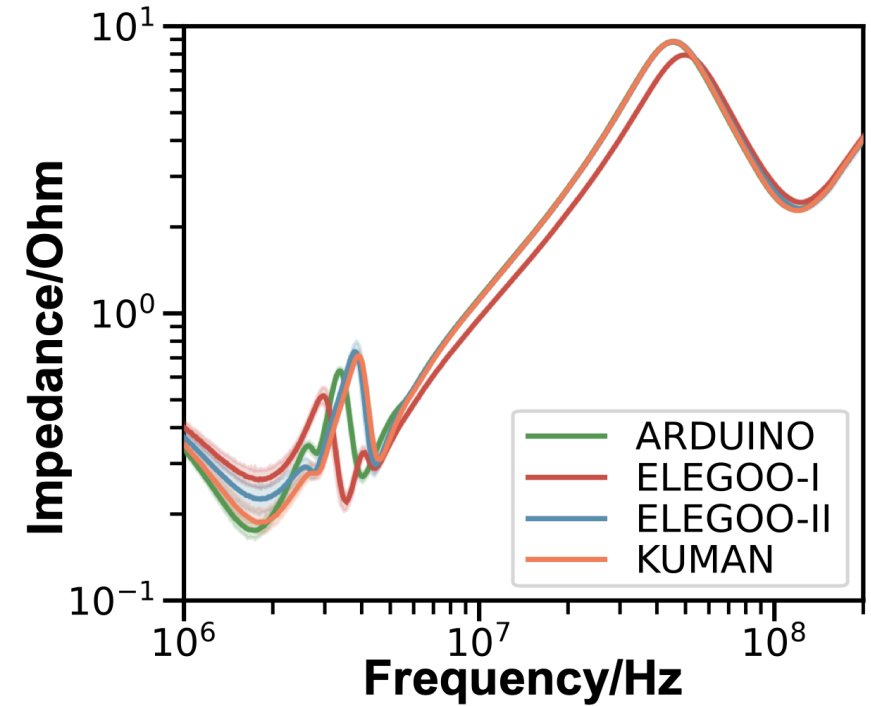
# PDN in Hardware Security: PCB Security



Taxonomy of various security issues in a PCB during its life-cycle

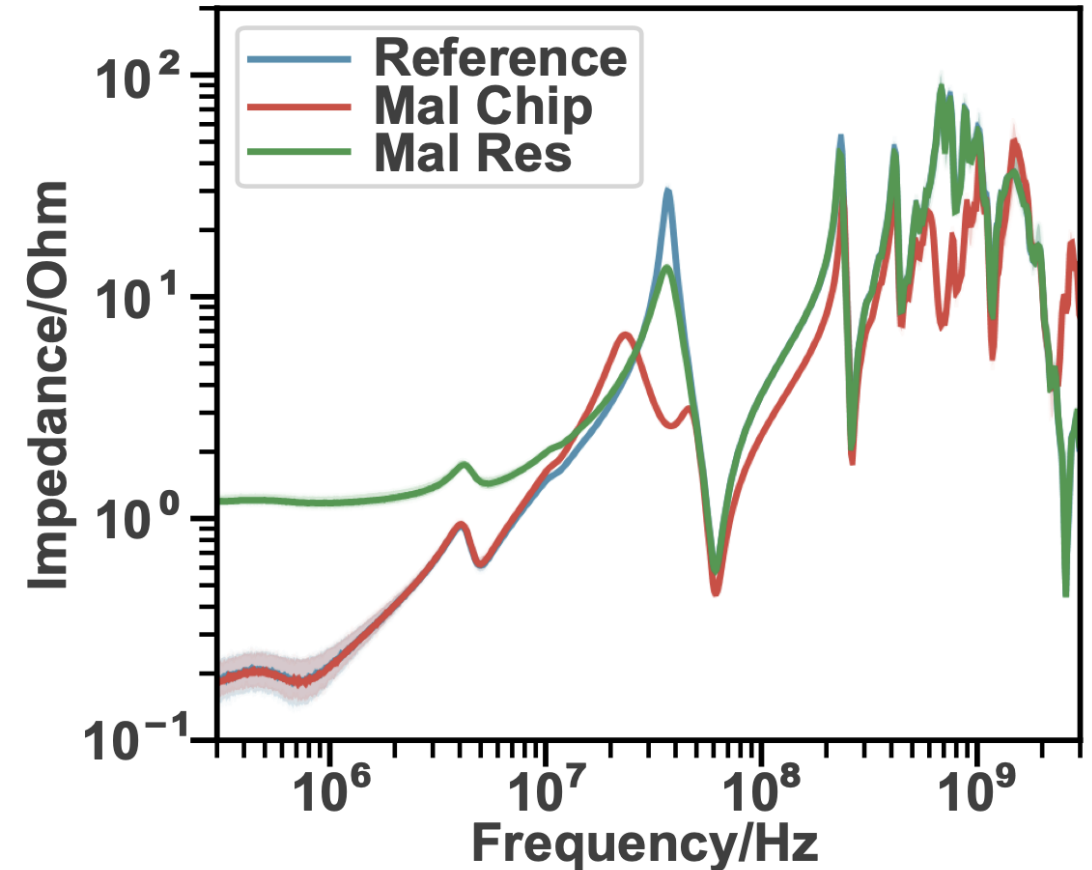
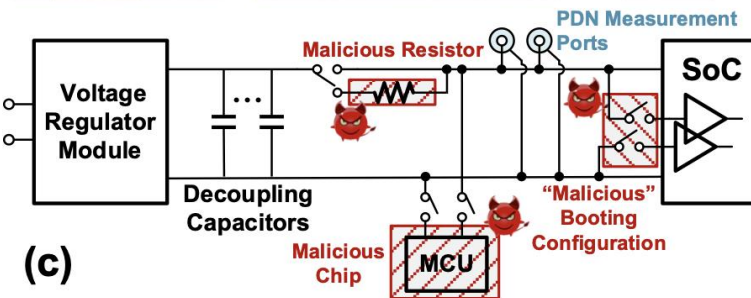
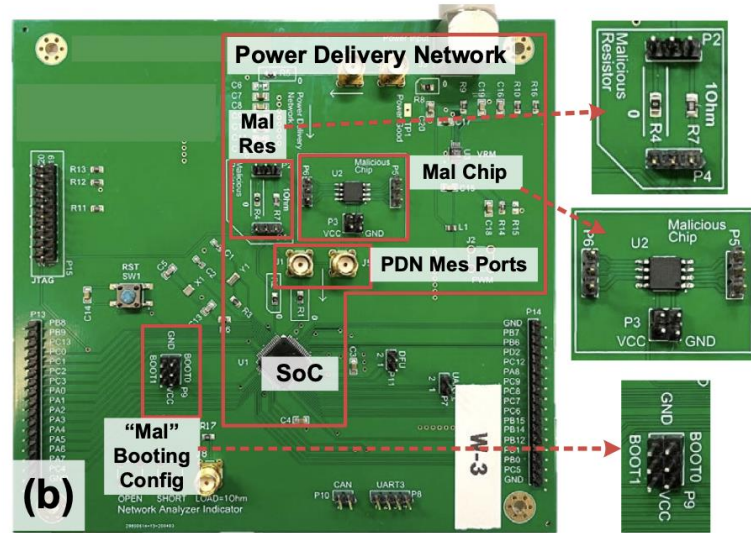
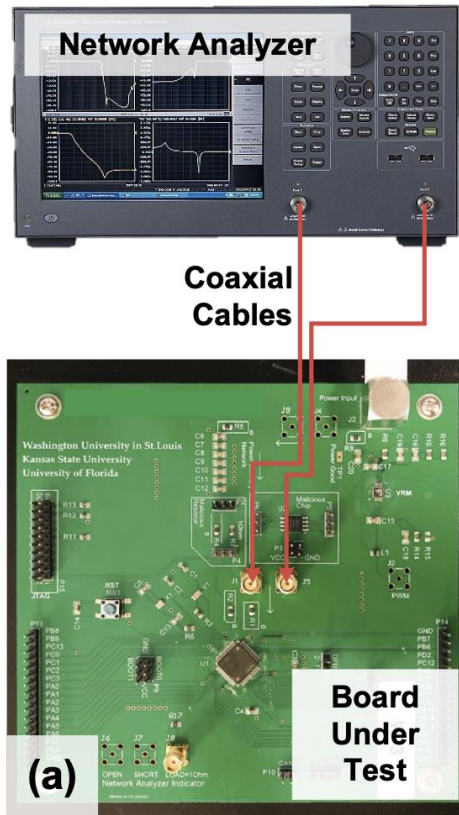
Paley, Steven, Tamzidul Hoque, and Swarup Bhunia. "Active protection against PCB physical tampering." 2016 17th International Symposium on Quality Electronic Design (ISQED). IEEE, 2016.

# PDN Impedance in Hardware Security: Counterfeit Detection



Zhu, Huifeng, et al. "PDNPulse: Sensing PCB anomaly with the intrinsic power delivery network." IEEE Transactions on Information Forensics and Security (2023).

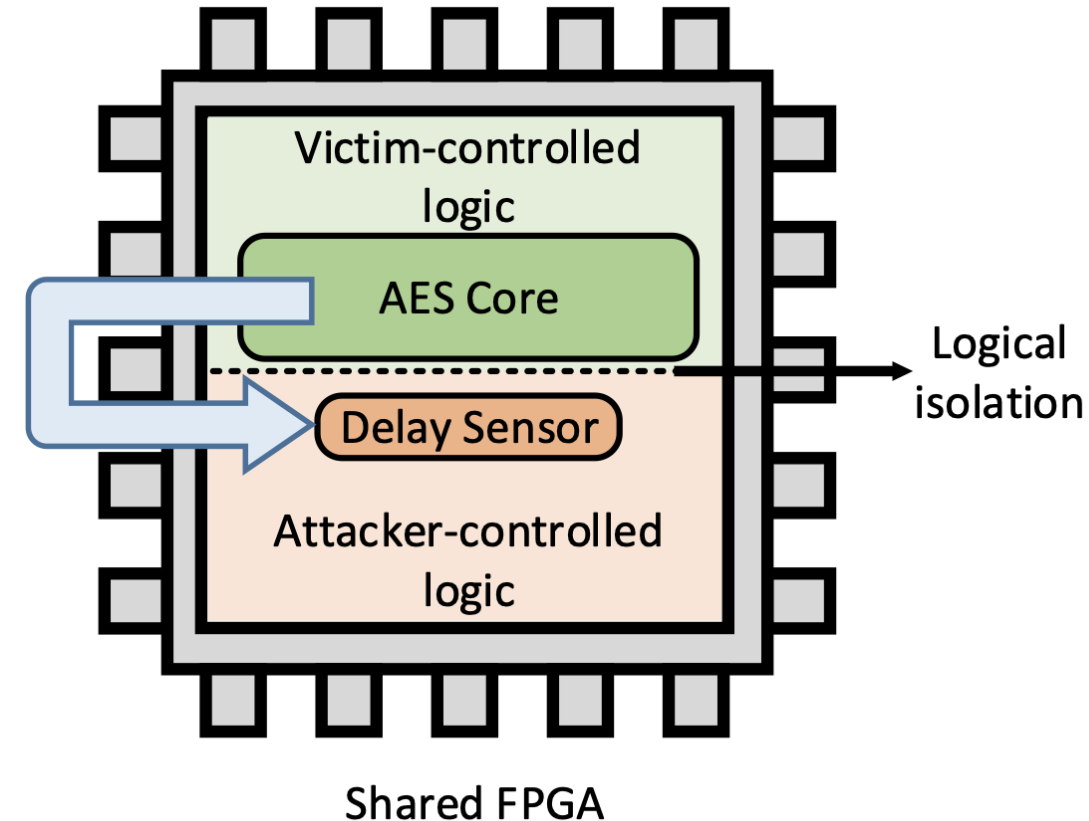
# PDN Impedance in Hardware Security: Detection of Hardware Trojan



Zhu, Huifeng, et al. "PDNPulse: Sensing PCB anomaly with the intrinsic power delivery network." IEEE Transactions on Information Forensics and Security (2023).

# PDN Voltage Fluctuation in Hardware Security: Remote FPGA Attack

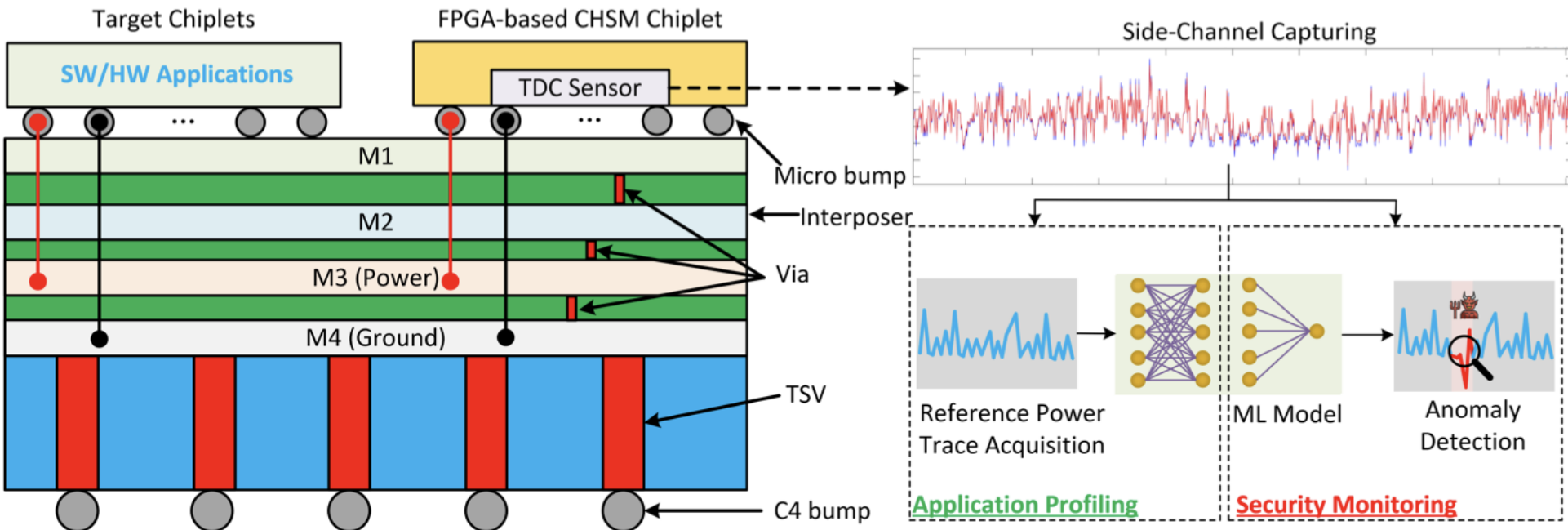
- Every modern IC is supplied by power through a complex PDN that starts at the printed circuit board (PCB) and spans to individual logic gates in the IC.
- The supply voltage at different locations of a PDN is not constant and depends on the activity of the logic
- $L \frac{di}{dt}$  and IR drop
- PDN is shared
- Sensors to locally monitor the dynamic change in the supply voltage
- Computation on victim can change the sensor data



Chenglu Jin et al., Security of Cloud FPGAs: A Survey

# PDN Voltage Fluctuation in Hardware Security: Monitoring Run-time Activities

- Having a power sensor to monitor the run-time activities through the power noise variations on the shared PDN



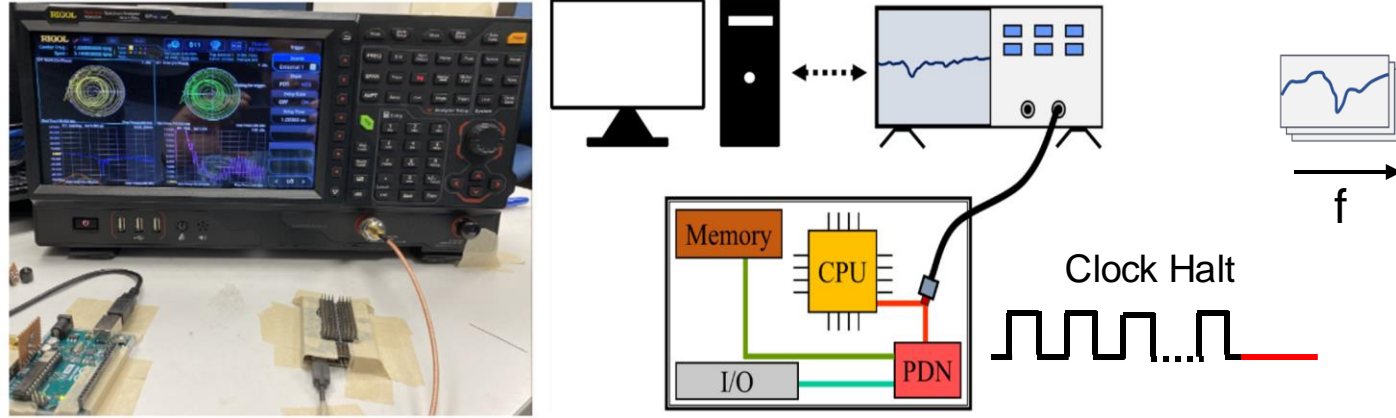
Tao zhang et al., SiPGuard: Run-time System-in-Package Security Monitoring via Power Noise Variation

# Prior Research Assumptions

---

- Runtime PDN impedance is constant
- Logic activities don't change runtime PDN impedance
- PDN impedance changes when device component is changed or altered
- Logic activities don't change run-time PDN impedance, but it fluctuates voltage

# Measurement Setup

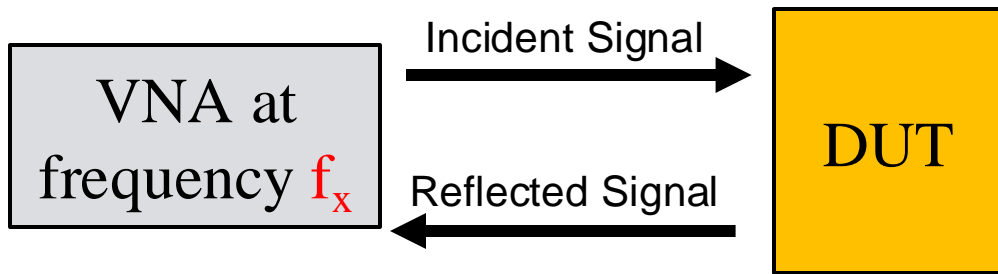


Experimental Setup

$$S_{11} = \frac{\text{Reflected}}{\text{Incident}}$$

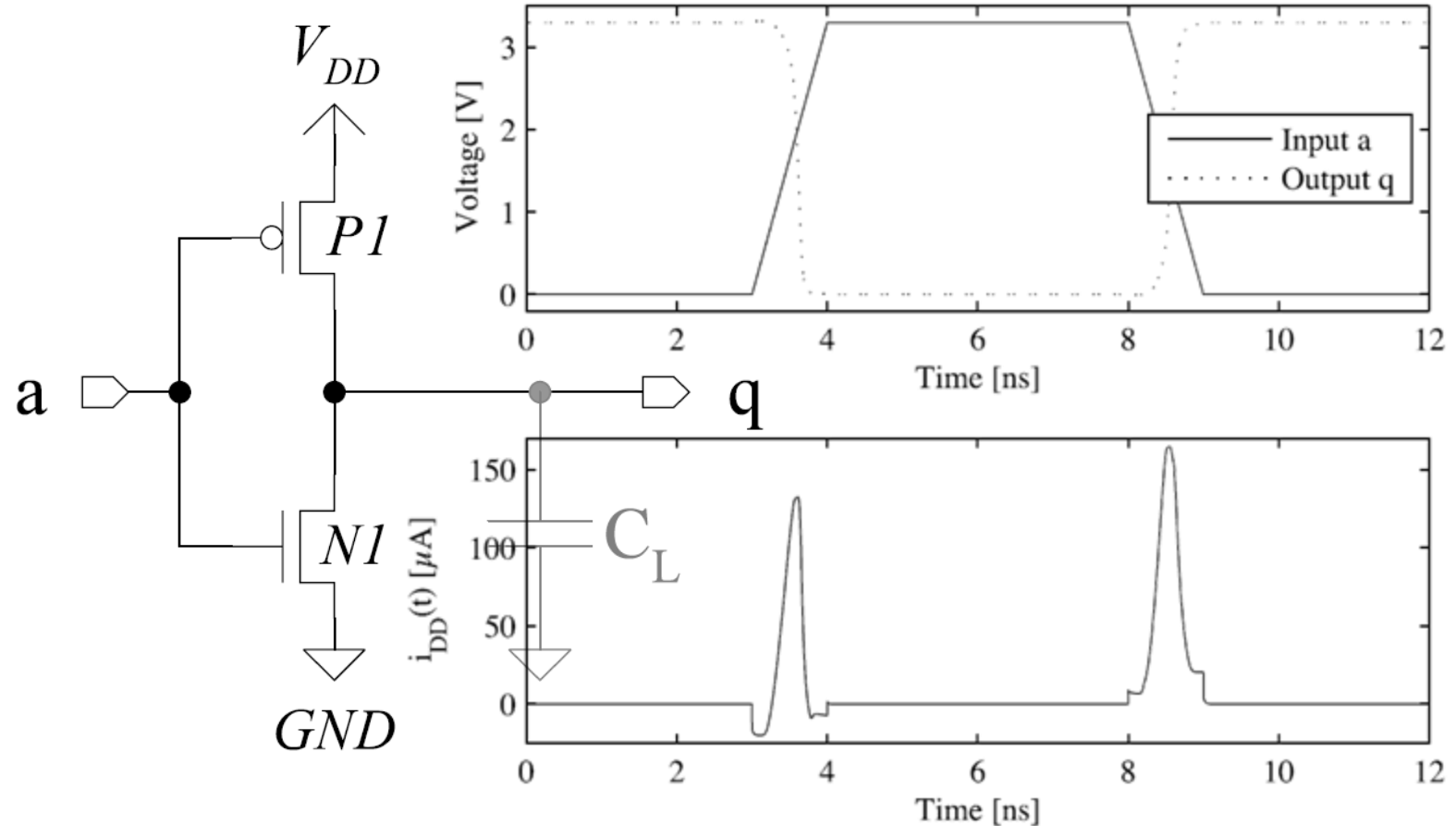
$$Z = Z_{\text{ref}} * \frac{1+S_{11}}{1-S_{11}}$$

$$\text{Impedance, } Z = R + j(2\pi fL - \frac{1}{2\pi fC})$$



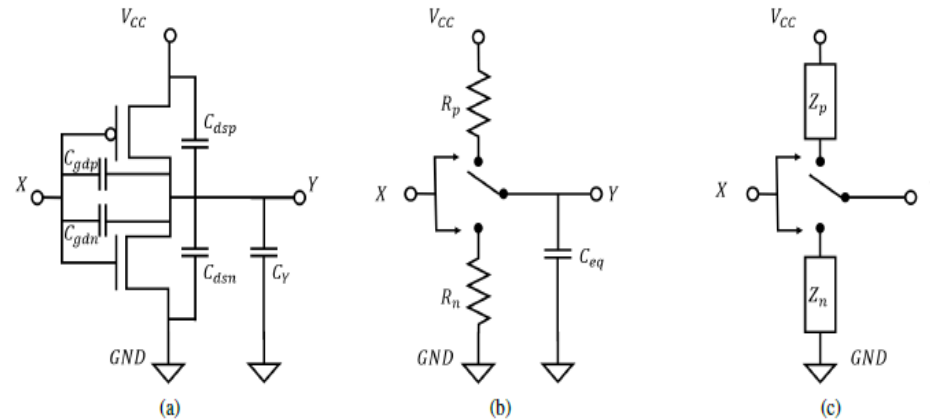
VNA working principle

# Power Consumption is Variable!



Source: DPA Book and Dr. Yossi Oren

# Runtime Device Impedance is Variable

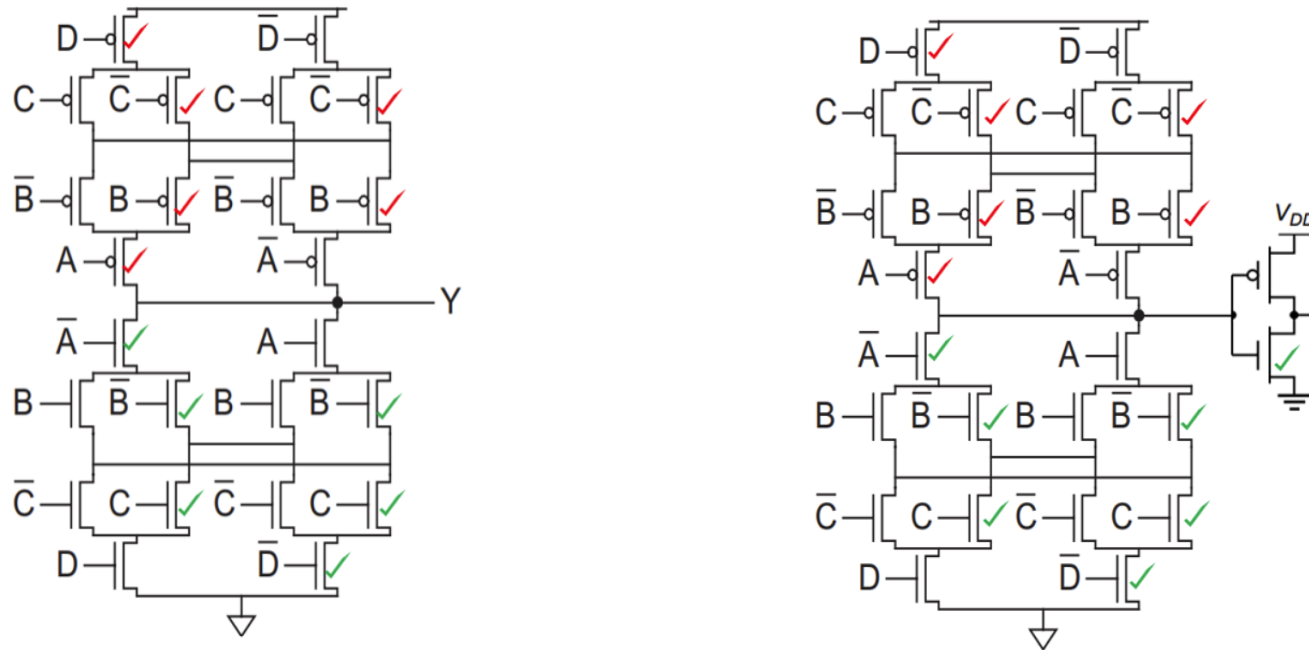


$$Z_{p/n} = R_{p/n} + jX_{p/n}$$

CMOS inverter – equivalent impedance model

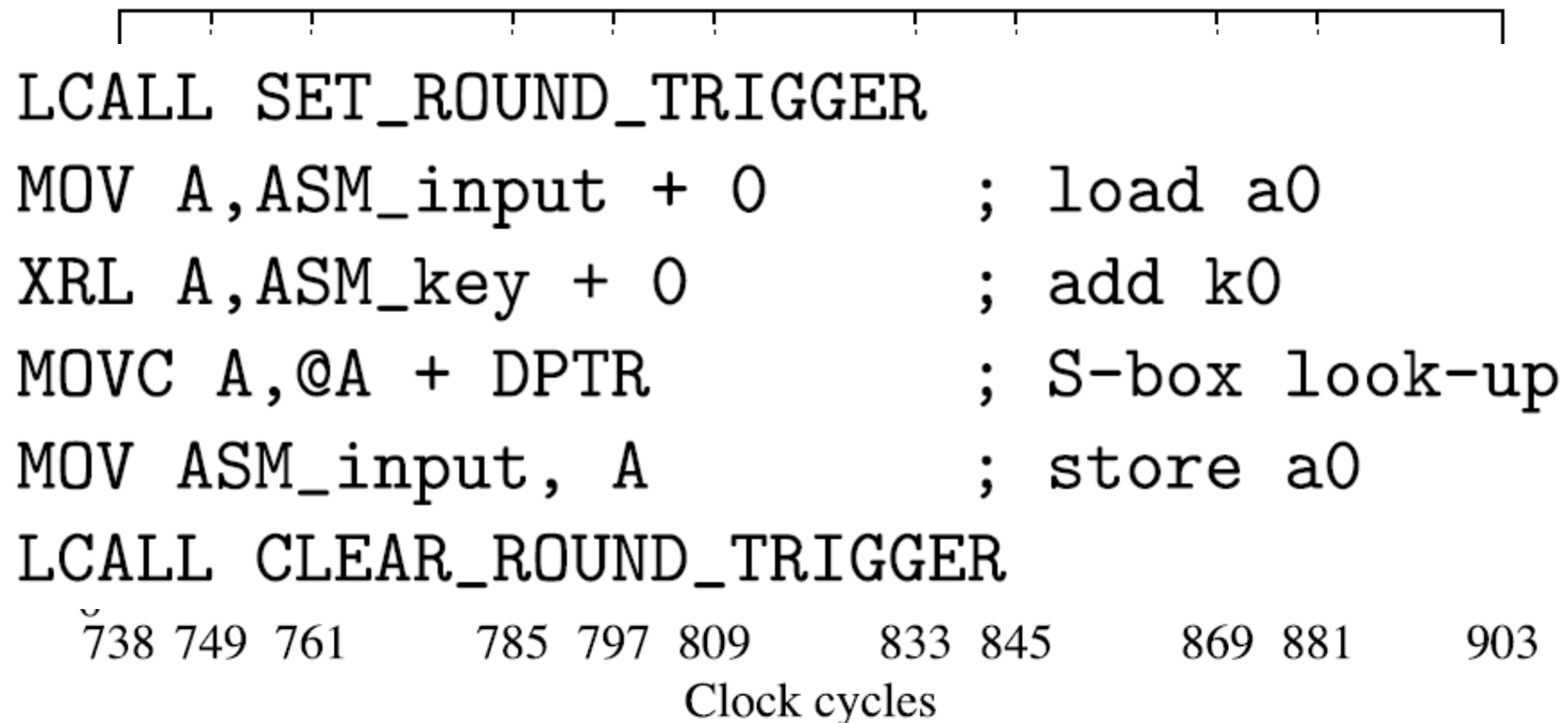
- M. S. Awal and M. T. Rahman, "Disassembling Software Instruction Types through Impedance Side-channel Analysis," IEEE HOST, 2023

# Impedance: Operation Dependencies



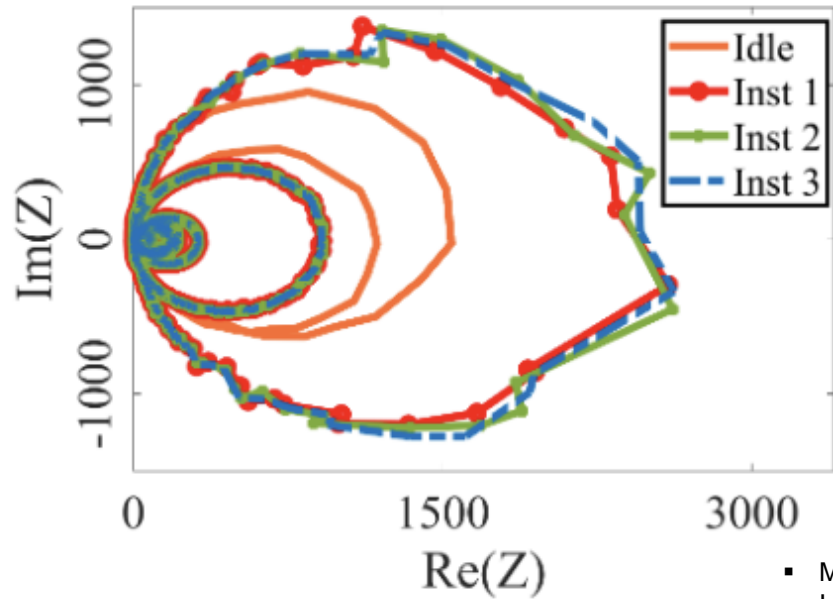
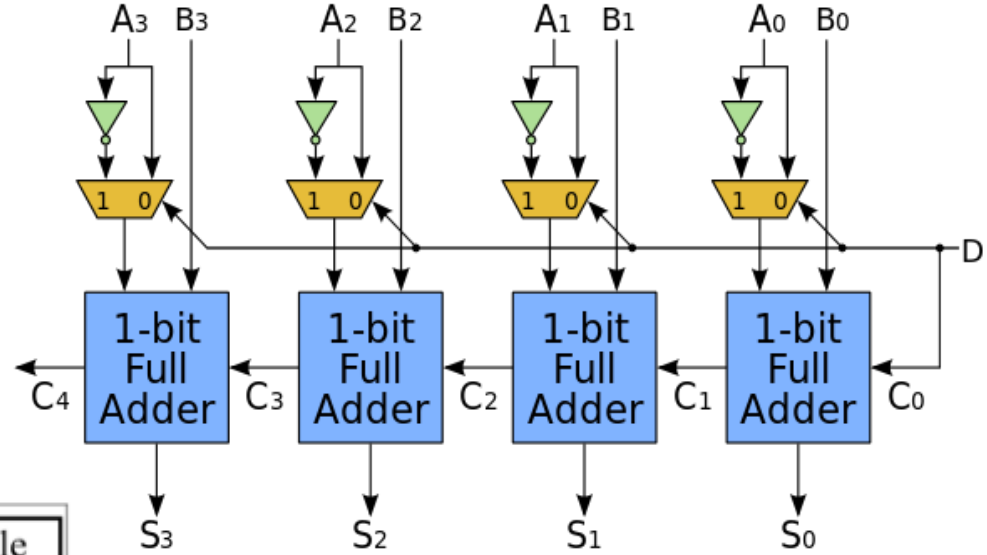
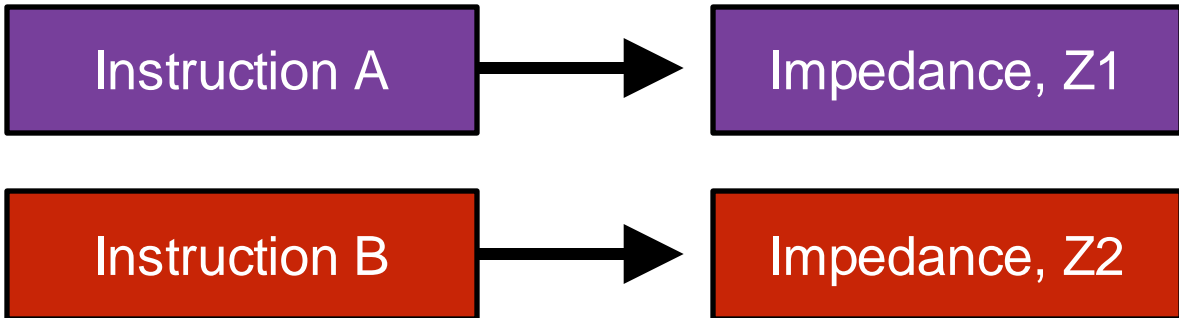
Impedance operation dependency (a) XOR, (b) XNOR (A=0,B=0,C=1,D=0)

# Power Depends on Instruction



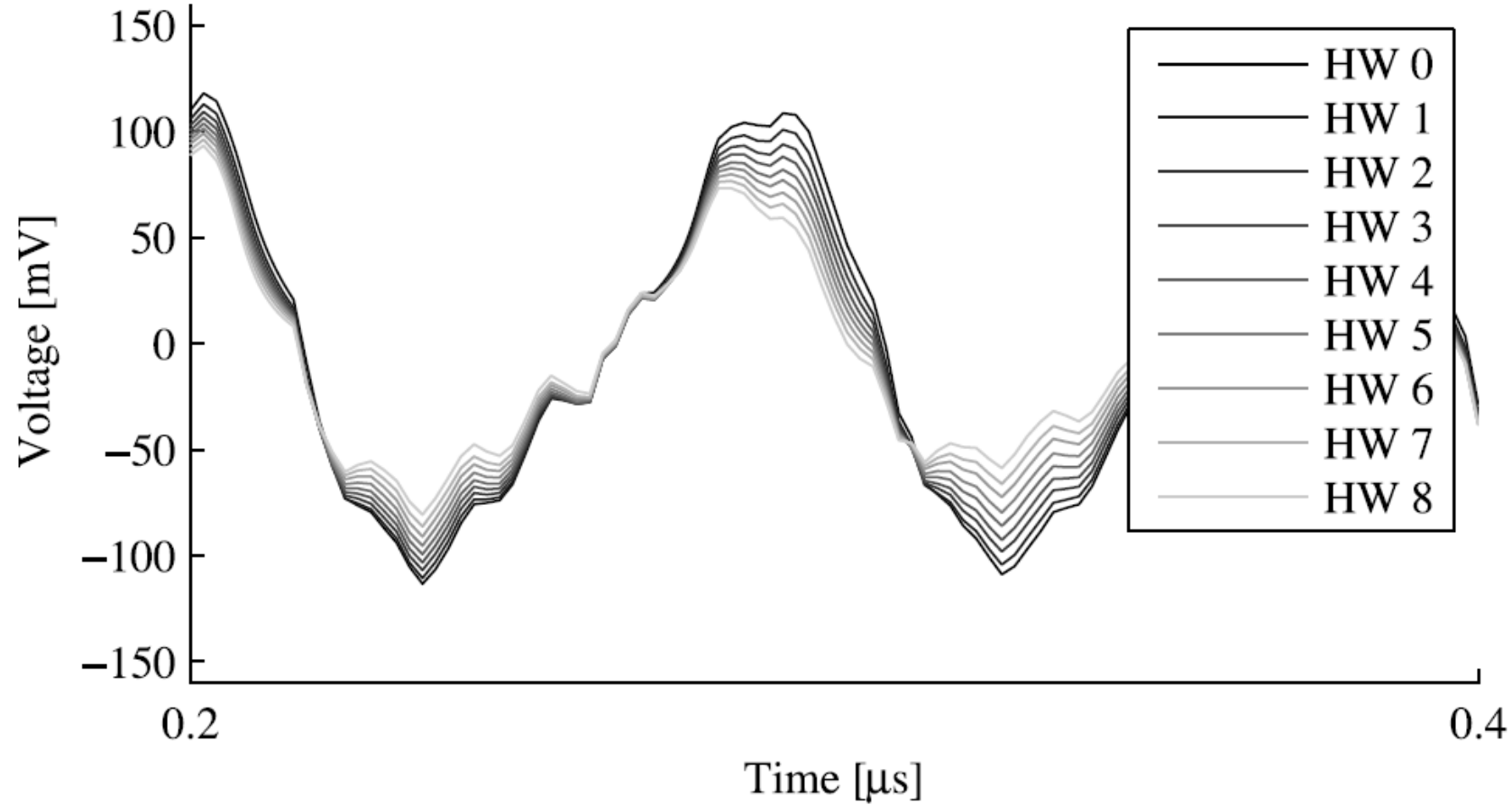
Source: DPA Book and Dr. Yossi Oren

# Device Impedance Depends on Instructions



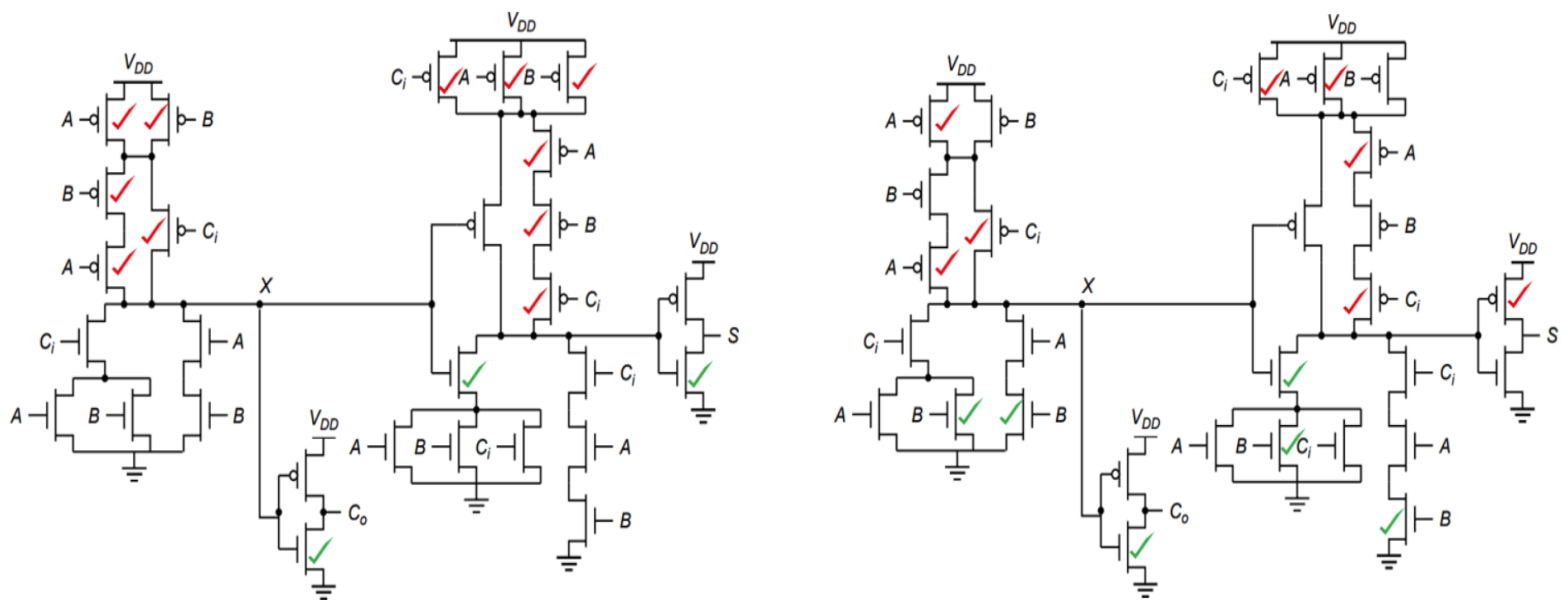
▪ M. S. Awal and M. T. Rahman, "Disassembling Software Instruction Types through Impedance Side-channel Analysis," IEEE HOST, 2023

# Power Depends on Data



Source: DPA Book and Dr. Yossi Oren

# Device Impedance Depends on Data

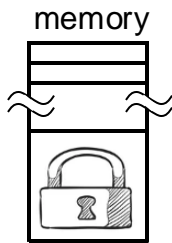


Adder - impedance data dependency (a)  $A=0, B=0$ , (b)  $A=0, B=1$

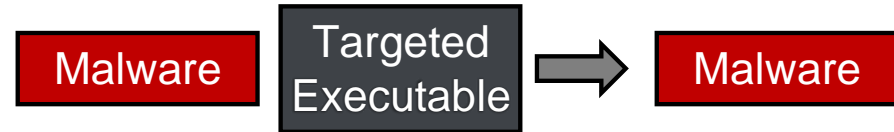
# Disassembling Software Instructions using Impedance Side-channel Leakage

# Impedance Side-channel: Disassembling Instructions

- **Software/Firmware** may be
  - Protected in memory
  - Unavailable
  - Decrypted before execution
    - IP stealing



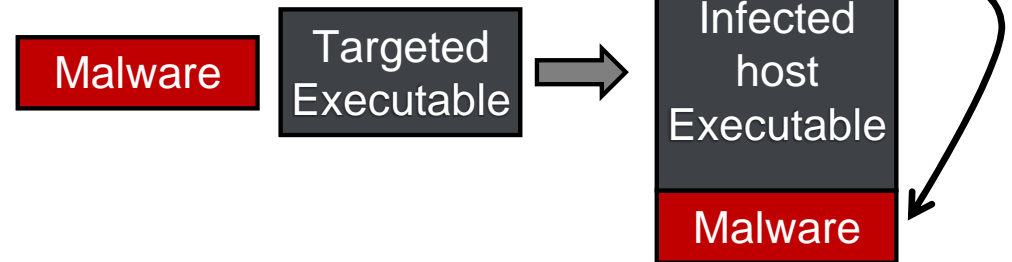
∅ **Overwriting malware**



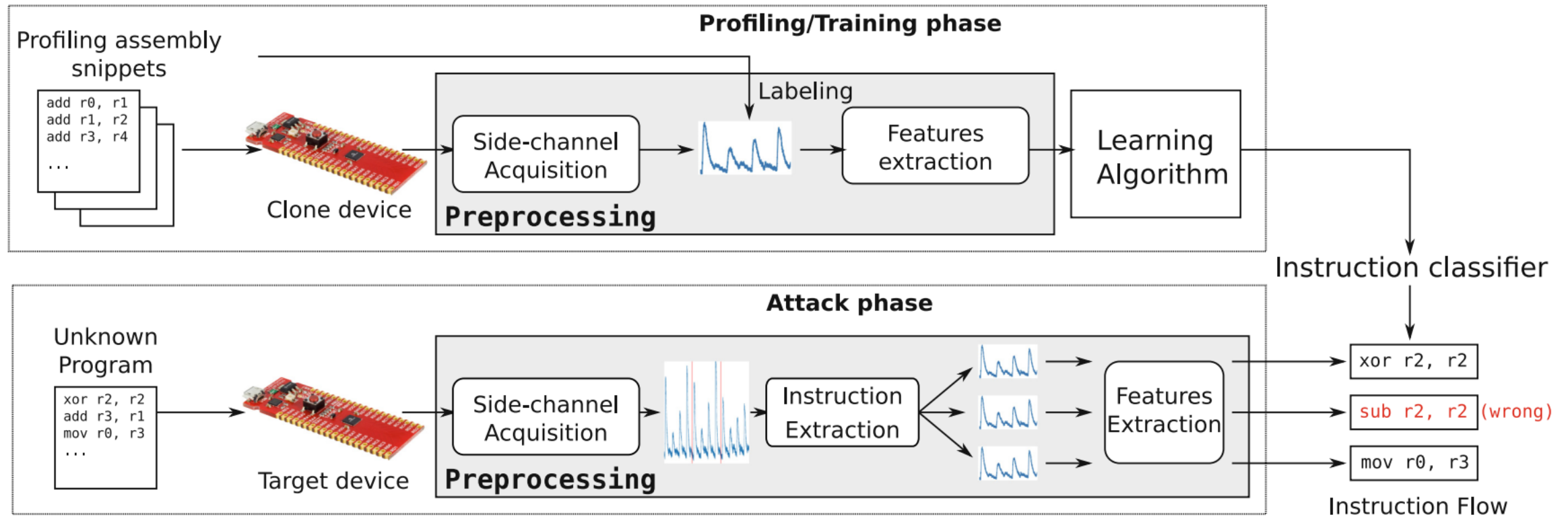
∅ **Prepending malware**



∅ **Appending malware**



# Side-channel to Disassemble SW Instructions



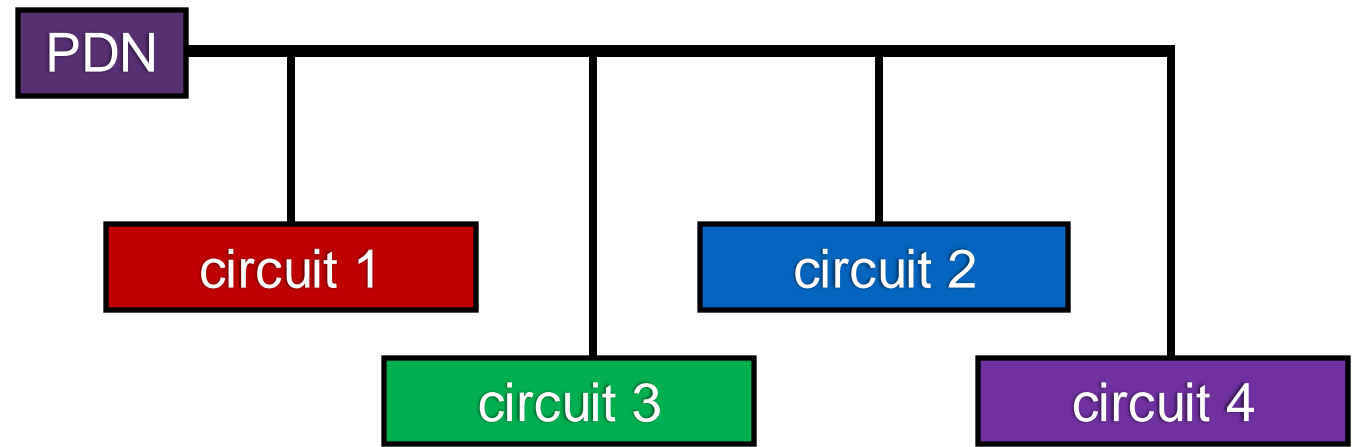
High level architecture of a side-channel disassembler

Cristiani, V., Lecomte, M., & Hiscock, T. (2020). A bit-level approach to side channel based disassembling. In *Smart Card Research and Advanced Applications: 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11–13, 2019*.

# Impedance Side-channel: Group of Instructions

➤ **Instruction group:**

- **Type 1: Data transfer**
- **Type 2: Arithmetic/logic**
- **Type 3: Rotate**
- **Type 4: Branch**

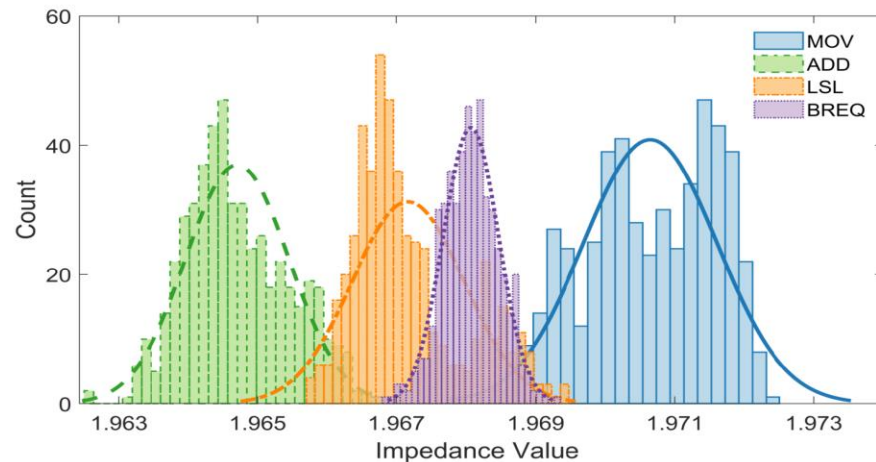


➤ **Different groups of circuits are used to execute different types of instructions**

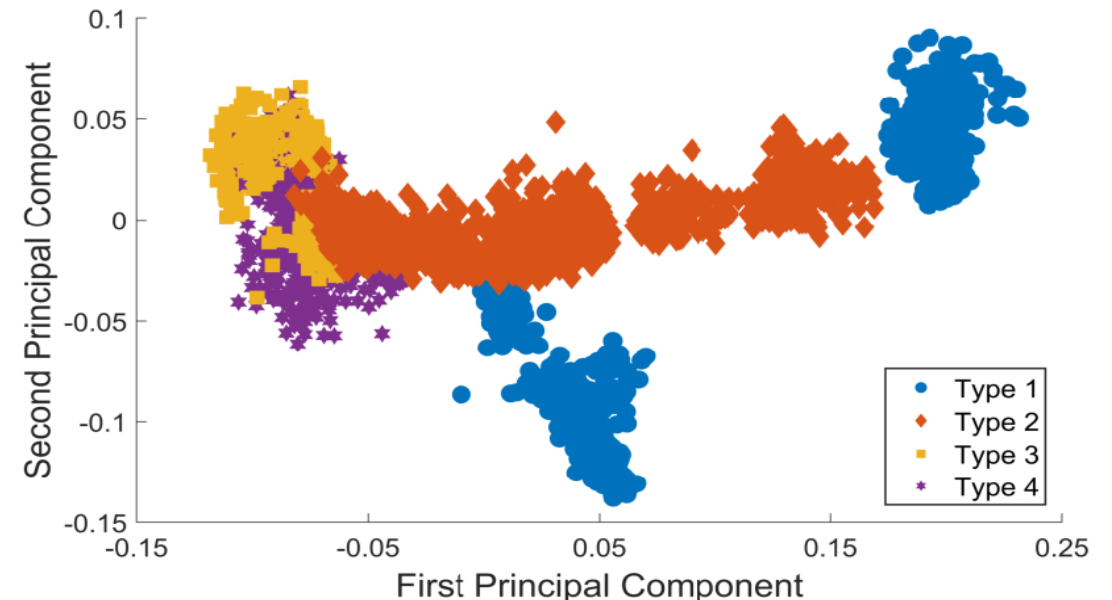
Instruction type	Opcode	Operands	Description	Operation
Type 1: Data transfer	MOV	R1, R2	Load from memory to register	$R1 \leftarrow R2$
	LDI	R1, K	Load an integer into register	$R1 \leftarrow K$
Type 2: Arithmetic/logic	ADD	R1, R2	Addition of two numbers	$R1 \leftarrow R1 + R2$
	SUB	R1, R2	Subtraction two numbers	$R1 \leftarrow R1 - R2$
	AND	R1, R2	Bit-wise AND operation	$R1 \leftarrow R1 \& R2$
	OR	R1, R2	Bit-wise OR operation	$R1 \leftarrow R1   R2$
	EOR	R1, R2	Bit-wise XOR operation	$R1 \leftarrow R1 \oplus R2$
Type 3: Rotate	LSL	R1	Binary shift to the left (1 bit)	$R1[n+1] \leftarrow R1[n], R[0] \leftarrow 0$
	LSR	R1	Binary shift to the right (1 bit)	$R1[n] \leftarrow R1[n+1], R[7] \leftarrow 0$
Type 4: Branch	BREQ	K	Branch if equal	if $Z = 1: PC \leftarrow PC+K+1$
	BRNE	K	Branch if not equal	if $Z = 0: PC \leftarrow PC+K+1$

## ➤ PCA:

- Linearly transforms the data into a new coordinate system to capture the most variation in the data
- Is used to reduce feature dimensionality
- Obtained 1273 features



Histogram of Impedance



Distribution of principal components

- M. S. Awal and M. T. Rahman, "Disassembling Software Instruction Types through Impedance Side-channel Analysis," IEEE HOST, 2023

## ➤ Machine learning

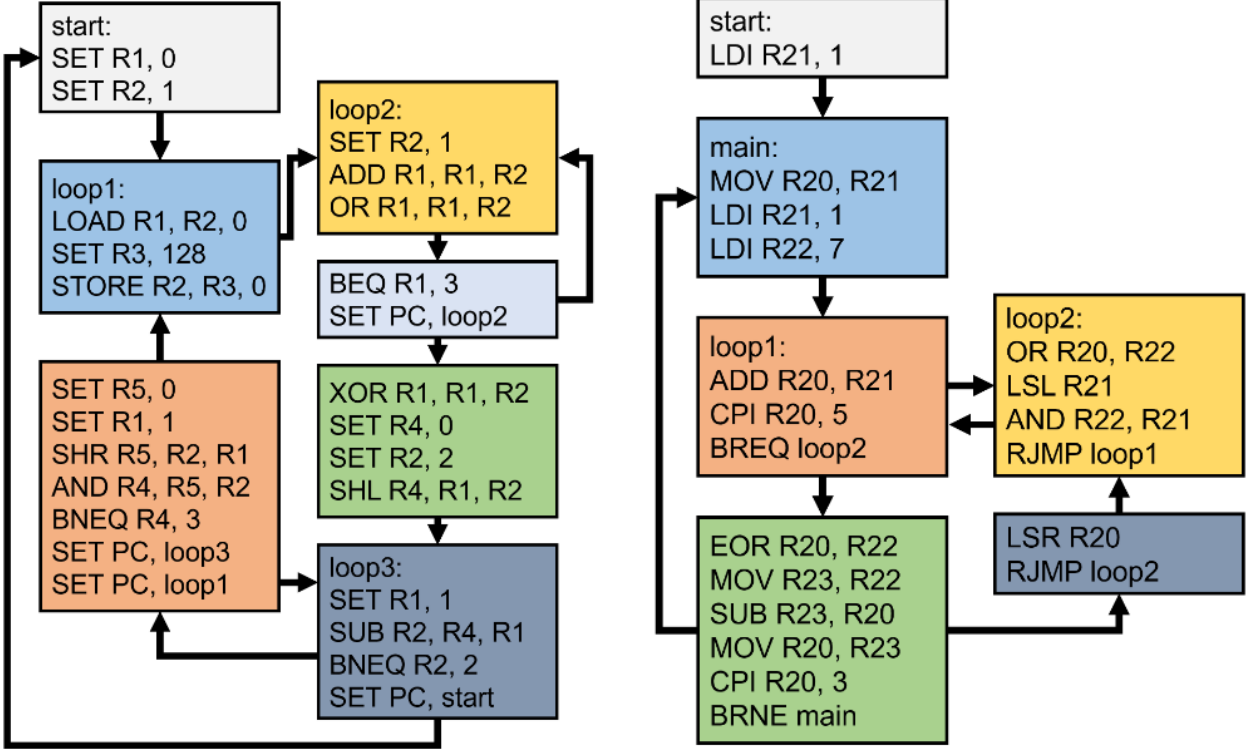
- SVM, AdaBoost, kNN, Linear discriminant analysis (LDA)
- F1, recall, specificity, precision, accuracy > 90%

Classifier	Validation	F1-Score	Recall	Specificity	Precision	Accuracy
SVM (Kernel: Cubic)	98.6%	98.6%	98.1%	99.6%	98.2%	98.6%
AdaBoost	97.2%	96.5%	96.4%	99.2%	96.6%	97.3%
kNN	96.5%	94.8%	94.6%	98.7%	95.0%	96.0%
Linear discriminant	94.9%	95.5%	95.5%	98.9%	95.5%	96.6%

Table. Instruction Disassemble Accuracy

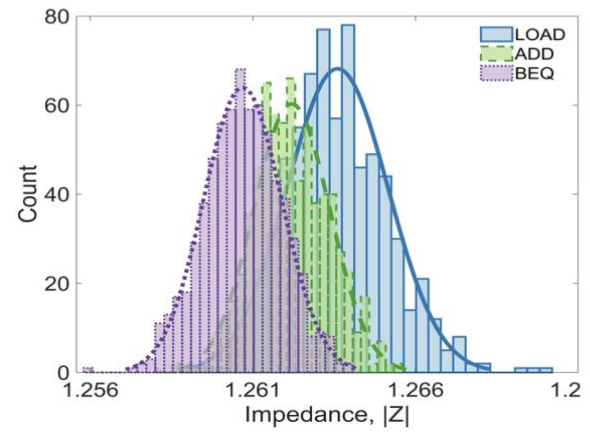
- M. S. Awal and M. T. Rahman, "Disassembling Software Instruction Types through Impedance Side-channel Analysis," IEEE HOST, 2023

# Impedance Side-channel: Individual Instruction

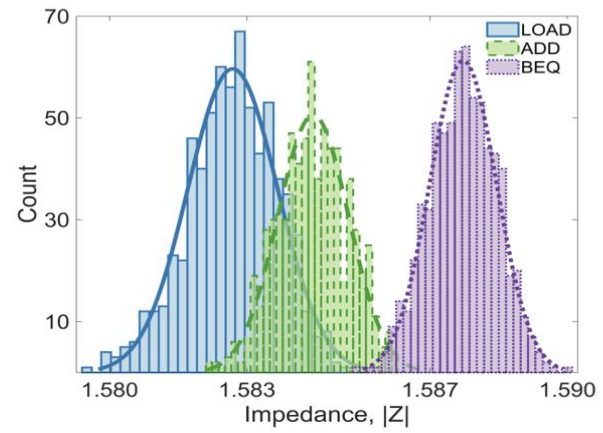


(a) (b)  
Code snippet used in experiment (a) Artix 7 FPGA, (b) ATmega328P

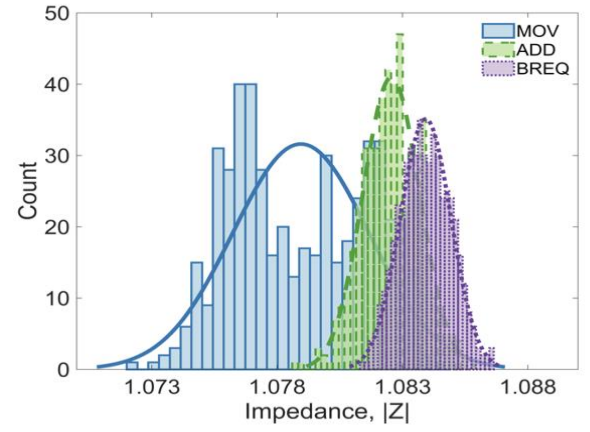
# ISCL at Different Frequency Points



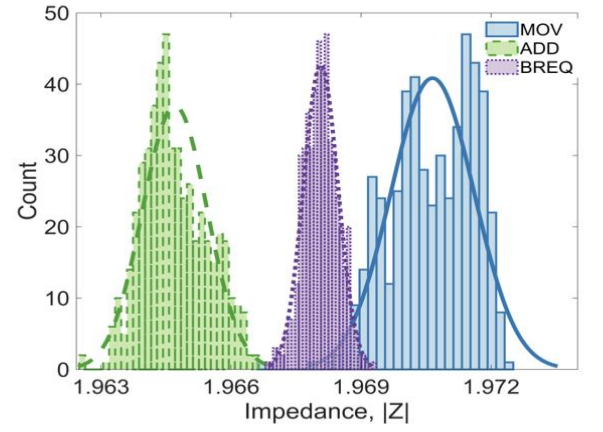
(a)



(b)



(c)

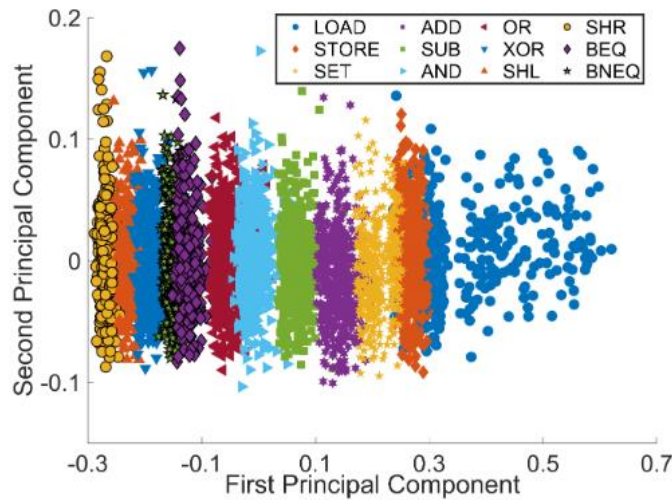


(d)

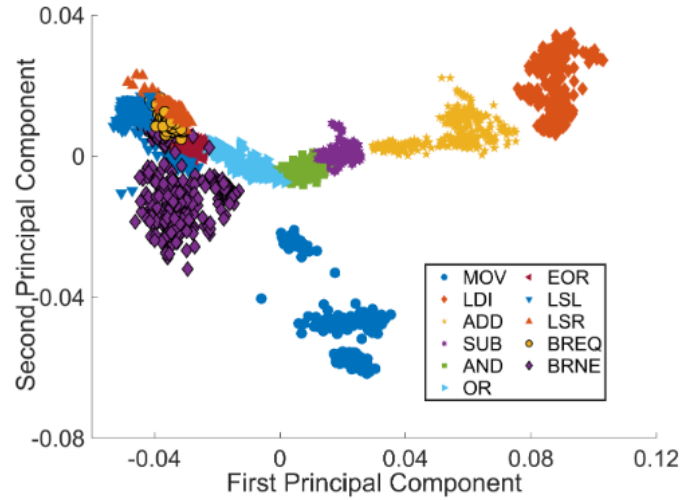
Impedance profile distribution: Artix 7 at (a) 1 GHz, (b) 2.3 GHz, and ATmega328P at (c) 1 GHz, (d) 2.3 GHz.

• M. S. Awal and M. T. Rahman, "Impedance Leakage Vulnerability and its Utilization in Reverse-engineering Embedded Software"

# Individual Instruction: Results and Analysis



(a) Artix 7: two major principal component distributions.



(b) ATmega328P: two major principal component distributions.

Distribution of principal components (a) Artix 7 FPGA, (b) ATmega328P

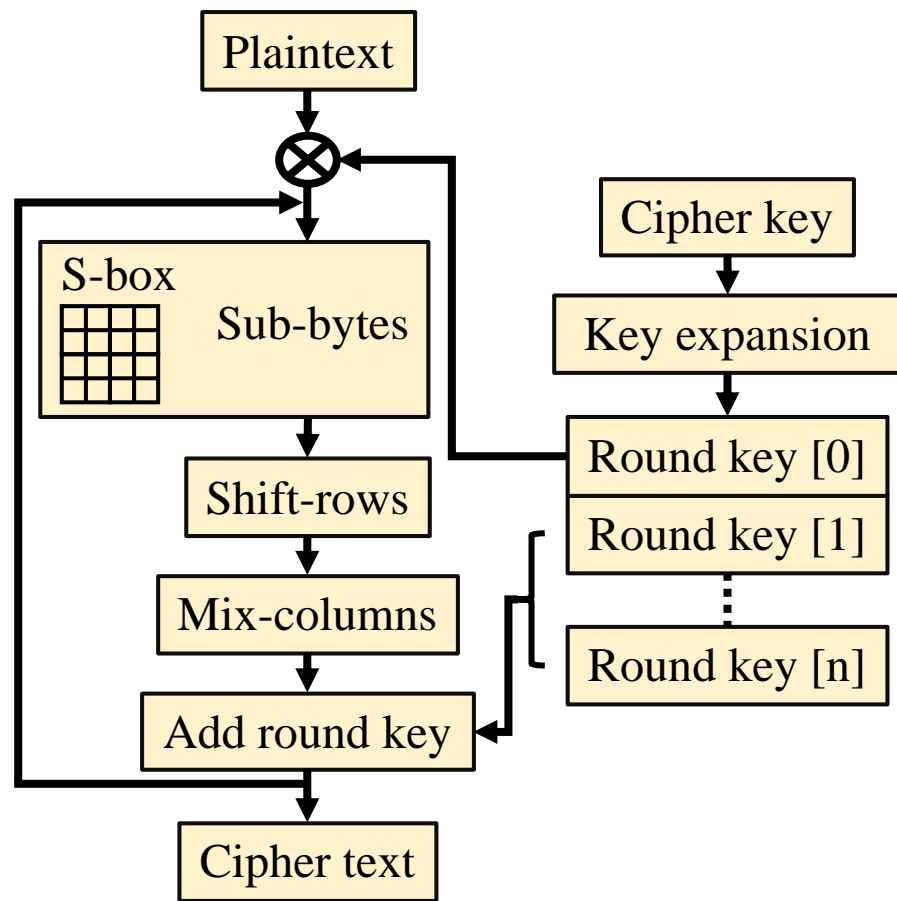
TABLE II: Classification scores for detecting program instruction.

Device	Classifier	Validation Score	F1-Score	Recall	Specificity	Precision	Accuracy
FPGA	SVM (Kernel: Linear)	92.8%	92.6%	92.7%	99.3%	92.7%	92.6%
	AdaBoost	91.8%	92.0%	92.0%	99.3%	92.1%	92.0%
	Linear Discriminant	86.6%	87.2%	87.3%	98.8%	87.3%	87.3%
ATmega328P	SVM (Kernel: Quadratic)	95.0%	96.1%	96.1%	99.6%	96.1%	96.1%
	Bagged trees	92.5%	91.6%	91.7%	99.2%	91.6%	91.6%
	Linear Discriminant	88.9%	92.2%	92.0%	99.2%	92.8%	92.2%

• M. S. Awal and M. T. Rahman, "Impedance Leakage Vulnerability and its Utilization in Reverse-engineering Embedded Software"

# ISCL Exploitation: Extracting AES-128 Key

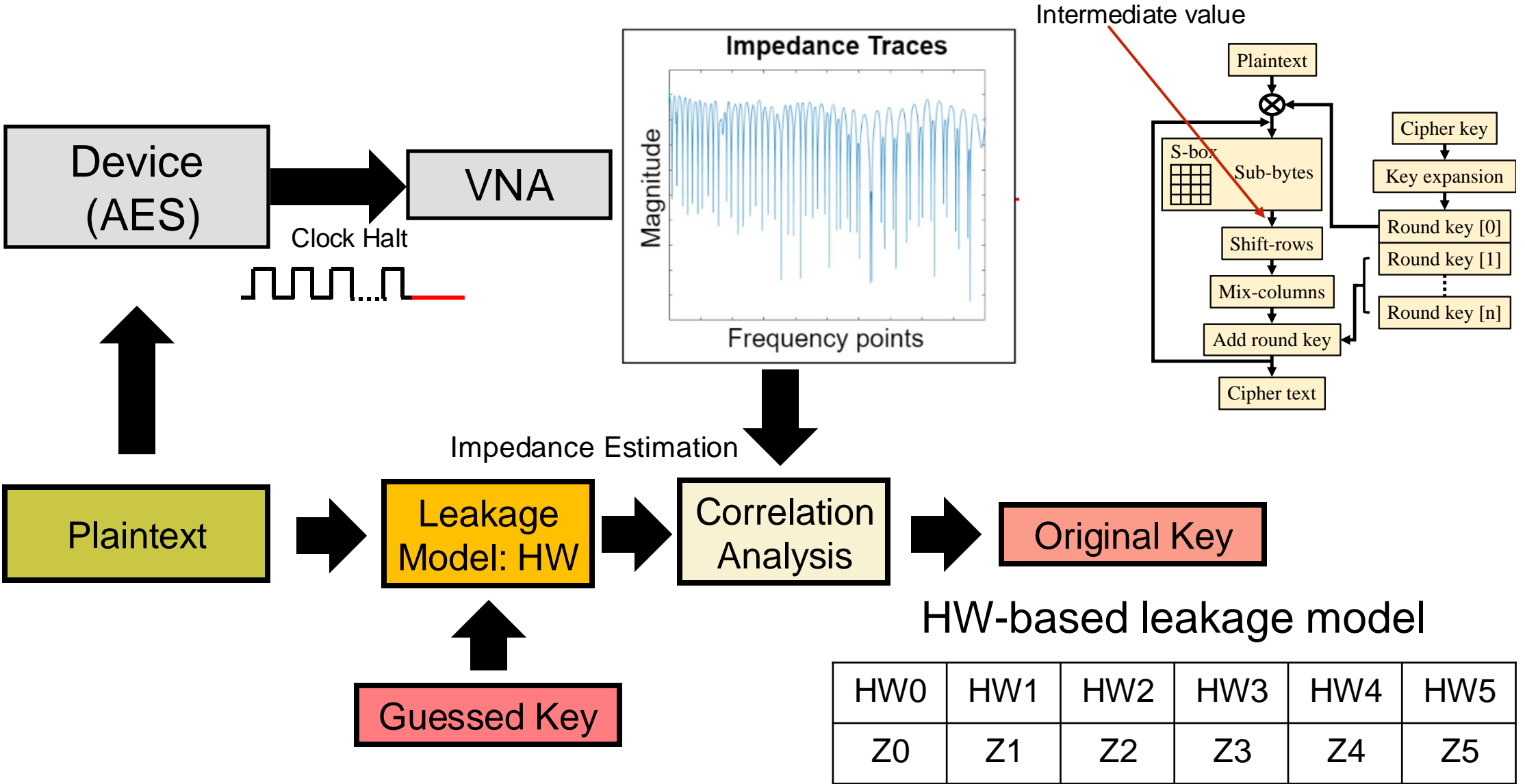
# AES Algorithm



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

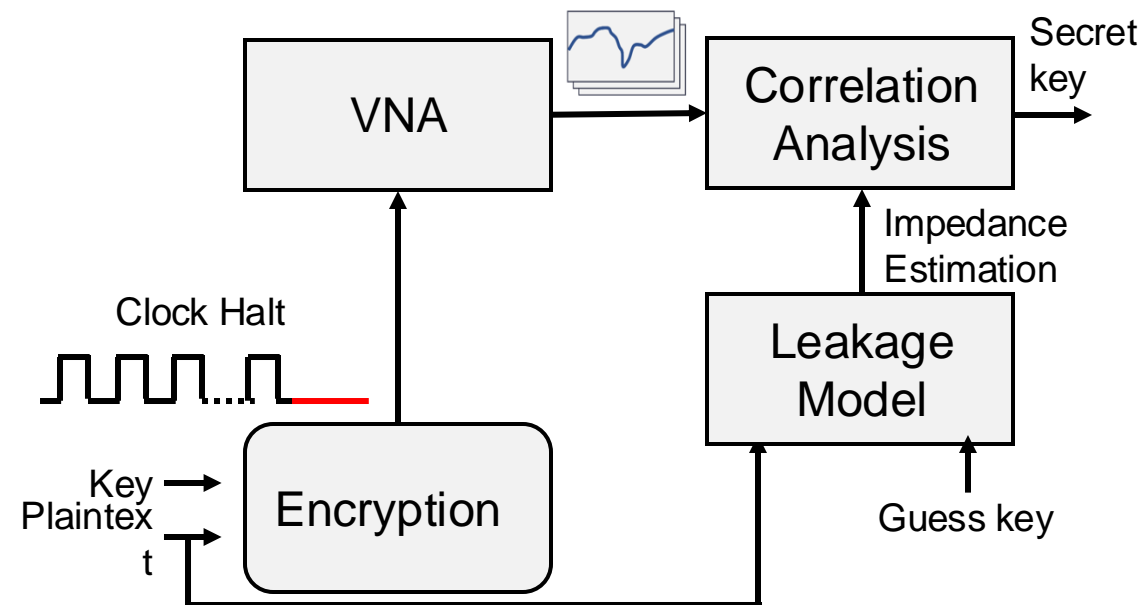
S-box

# Impedance Side-channel Analysis



# Side-channel Analysis: Impedance Estimation

- Estimate Impedance values for a key guess
- Guess what a byte of the key will be
- Compute the intermediate value-sbox (plaintext^key)
- Use the intermediate value in impedance model to estimate hypothetical leakage
- Do this for each plaintext and all key values



## Estimates

Key Guess	P1	P2	P3	P4	P5
K1	Z <sub>11</sub>	Z <sub>12</sub>	Z <sub>13</sub>	Z <sub>14</sub>	Z <sub>15</sub>
K2	Z <sub>21</sub>	Z <sub>22</sub>	Z <sub>23</sub>	Z <sub>24</sub>	Z <sub>25</sub>

# Side-channel Analysis: Correct Key Extraction



- Find correlation between estimated hypothetical leakage and measurement values
- Select the key guess with highest correlation
- Get the maximum absolute correlation value for each possible subkey
- Pick the subkey with the highest correlation

## Estimates

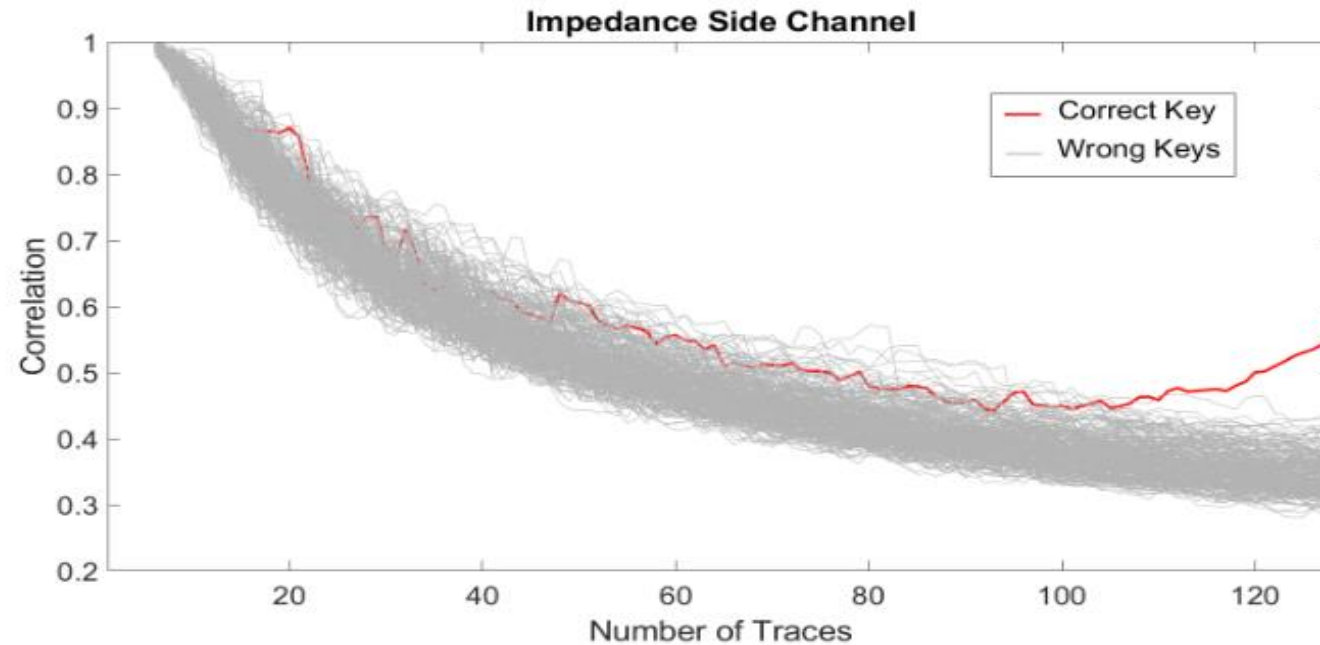
P1	P2	P3	P4	P5
Z <sub>1</sub>	Z <sub>2</sub>	Z <sub>3</sub>	Z <sub>4</sub>	Z <sub>5</sub>

## Measurements

T1	T2	T3	T4	T5	ρ
Z <sub>11</sub>	Z <sub>21</sub>	Z <sub>31</sub>	Z <sub>41</sub>	Z <sub>51</sub>	0.25
Z <sub>12</sub>	Z <sub>22</sub>	Z <sub>32</sub>	Z <sub>42</sub>	Z <sub>52</sub>	0.37
Z <sub>13</sub>	Z <sub>23</sub>	Z <sub>33</sub>	Z <sub>43</sub>	Z <sub>53</sub>	-0.82
Z <sub>14</sub>	Z <sub>24</sub>	Z <sub>3</sub>	Z <sub>44</sub>	Z <sub>54</sub>	0.76

- Breaks the full AES-128 key in 16 separate 1-byte chunks -subkeys (16\*8=128)
- Max attempts =  $16 \times 2^8 = 2^{12} = 4096$  instead of  $2^{128}$  attempts

# AES Key Extraction: Impedance Side-channel

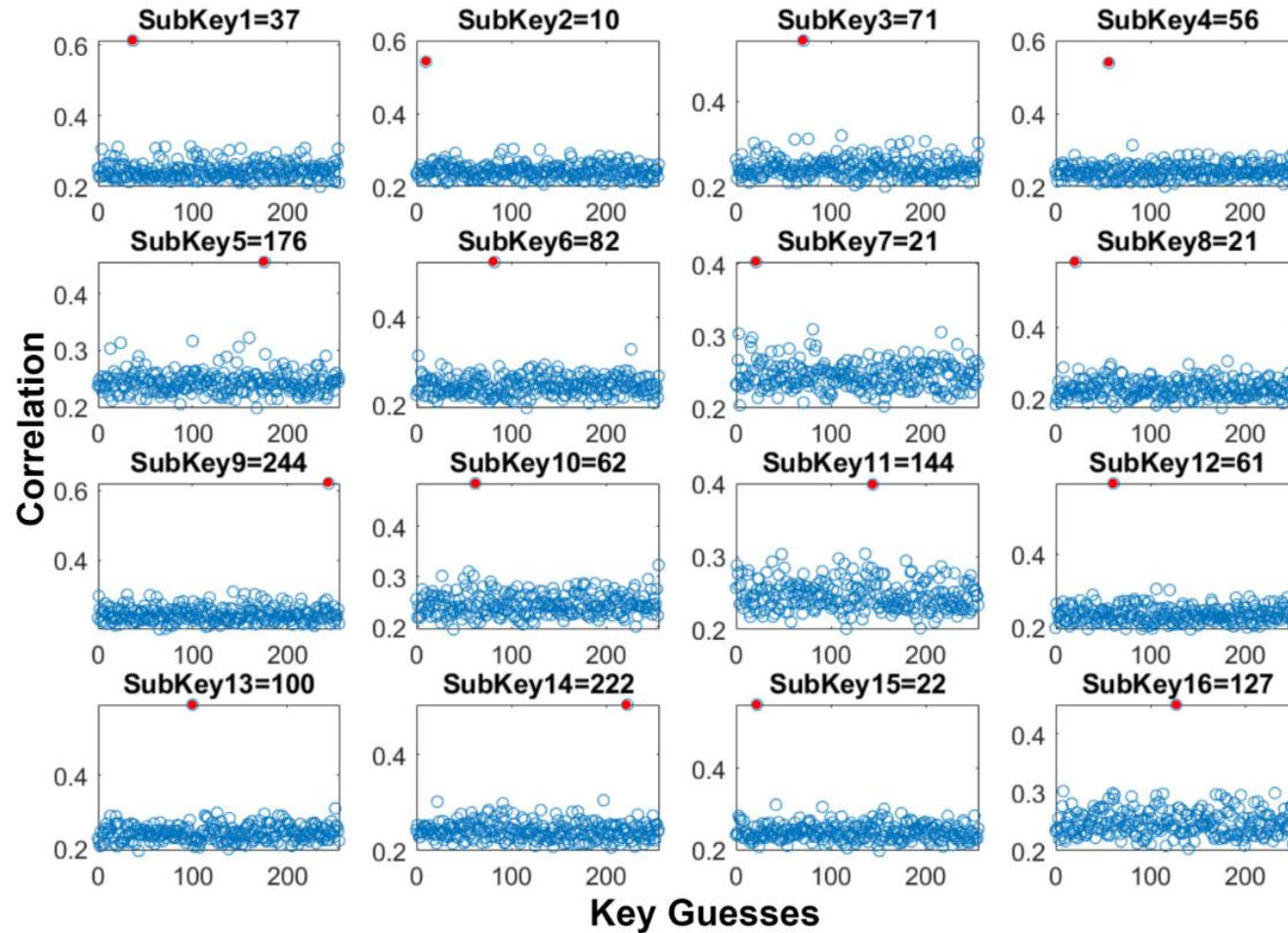


Number of plaintext vs correlation of guessed keys

Max attempts required to break 128-AES = 4096

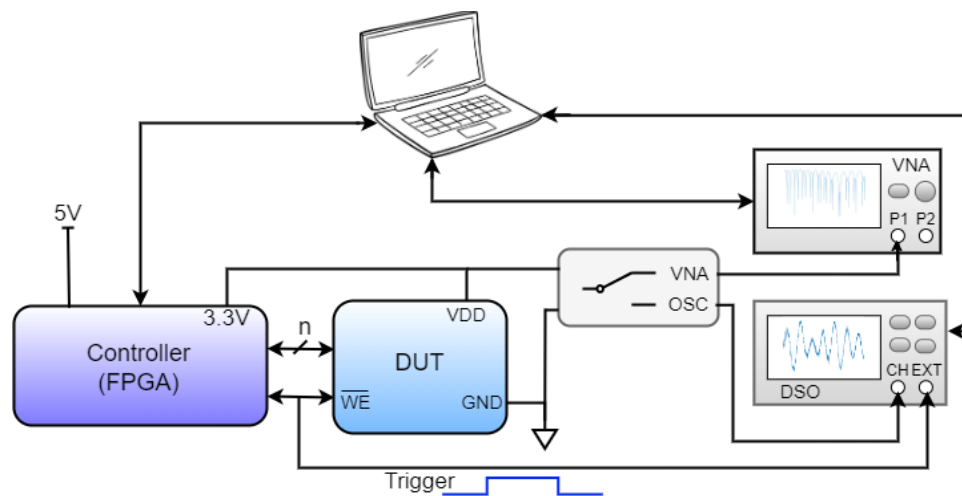
Awal, Md Sadik, Buddhipriya Gayanath, and Md Tauhidur Rahman. "Impedance vs. Power Side-channel Vulnerabilities: A Comparative Study."

# AES Key Extraction: Impedance Side-channel

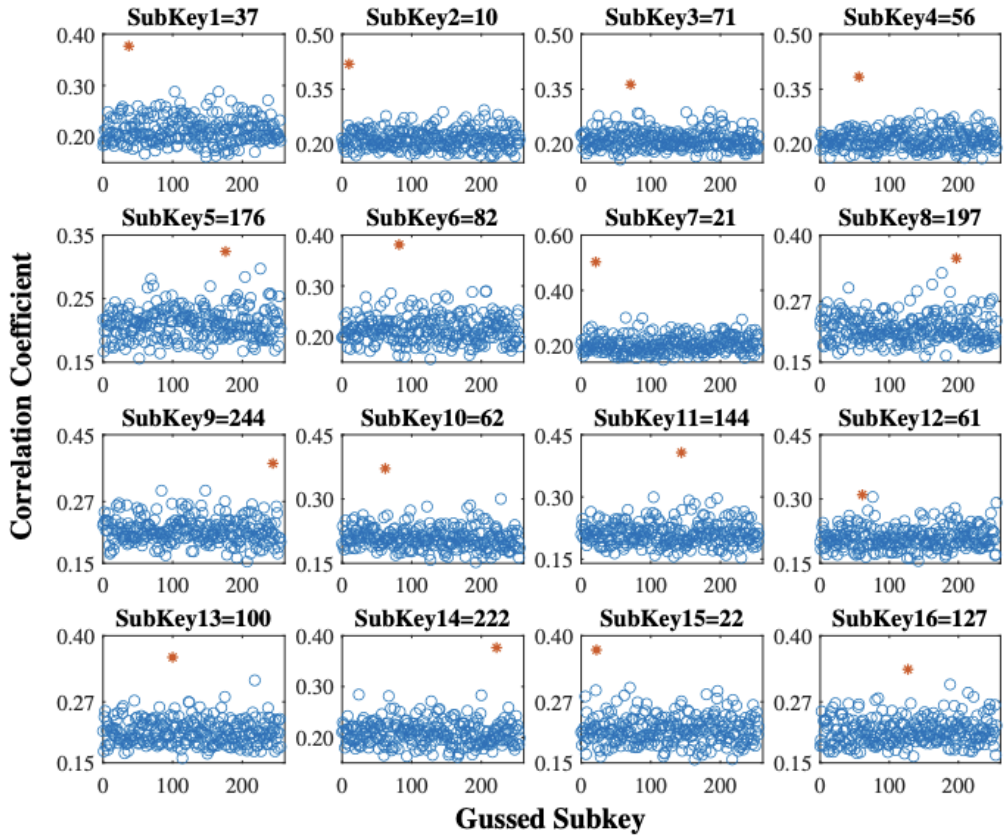


16 subkeys (8 bit) extraction of 128-AES

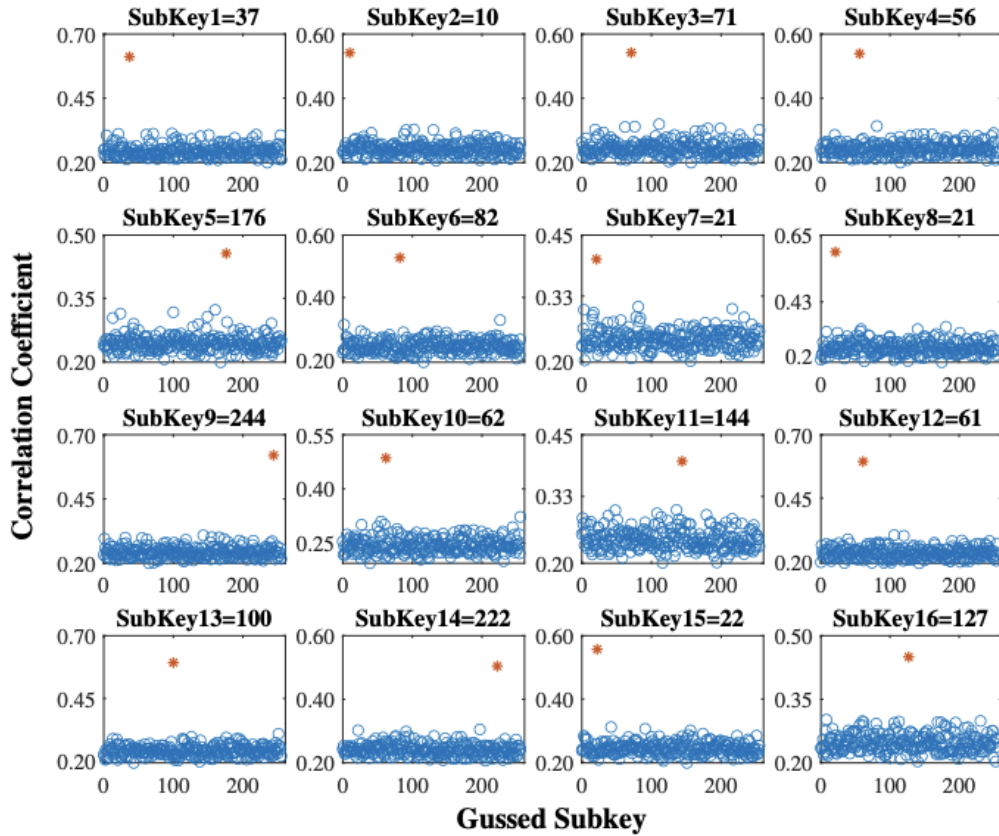
# Extracting AES-128 Key: Power vs. Impedance Side-channel



# Power vs. Impedance Side-channel Attack



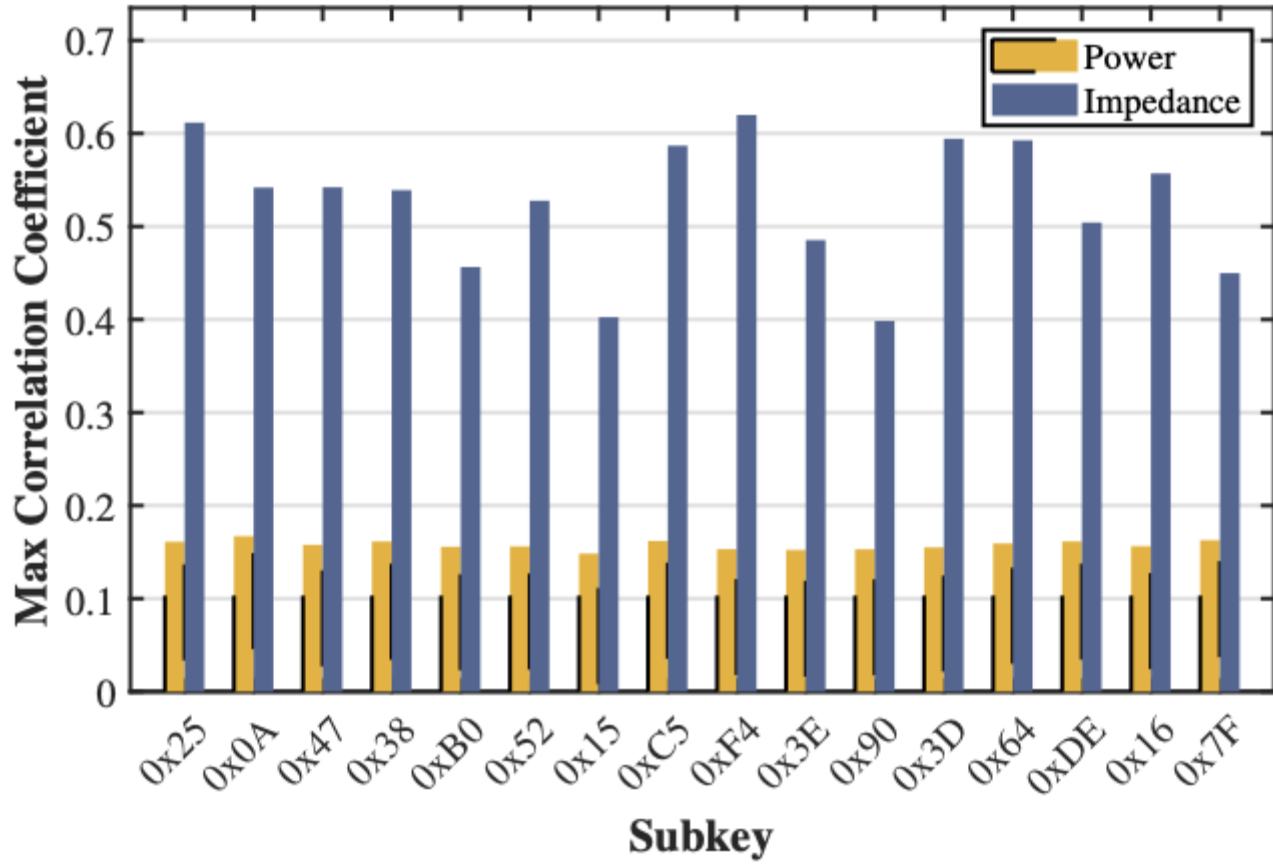
(a) Power side-channel



(b) Impedance side-channel

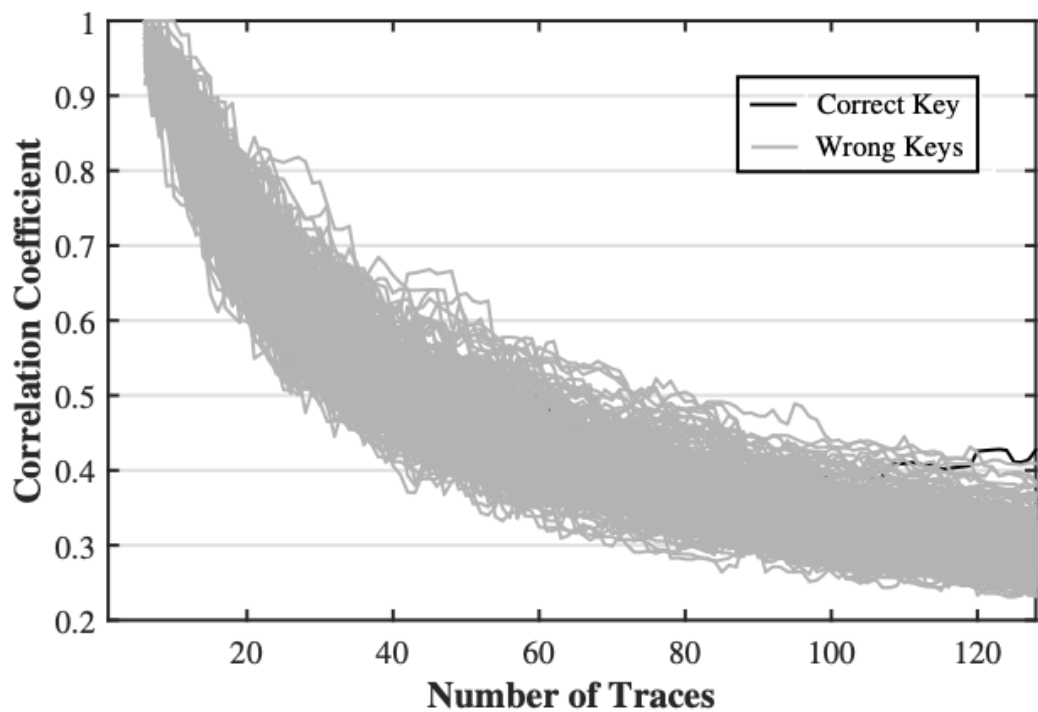
Awal, Md Sadik, Buddhipriya Gayanath, and Md Tauhidur Rahman. "Impedance vs. Power Side-channel Vulnerabilities: A Comparative Study."

# Power vs. Impedance Side-channel Attack

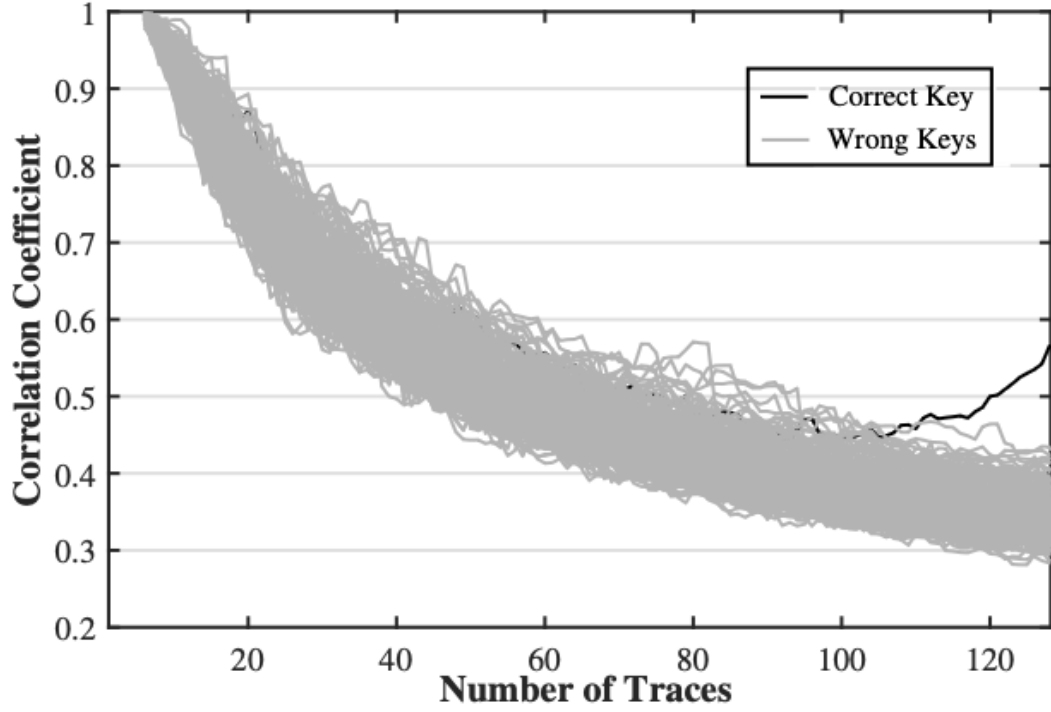


Awal, Md Sadik, Buddhipriya Gayanath, and Md Tauhidur Rahman. "Impedance vs. Power Side-channel Vulnerabilities: A Comparative Study."

# Power vs. Impedance Side-channel Attack (with Noise)



(a) Power side-channel



(b) Impedance side-channel

Awal, Md Sadik, Buddhipriya Gayanath, and Md Tauhidur Rahman. "Impedance vs. Power Side-channel Vulnerabilities: A Comparative Study."

- Impedance side-channel offers better information leakage compared to power side-channel
- Impedance side-channel is less noisy than power side-channel
- Noise that protects power side-channel may not protect systems from Impedance side-channel leakage. However, further study is required
- Countermeasures: Impedance randomization or impedance hiding

*Thank You!*

- Contact Information,
  - Tauhidur Rahman
  - Assistant professor, Dept. of ECE, Florida International University
  - E-mail: [mdtrahma@fiu.edu](mailto:mdtrahma@fiu.edu)