Energy Recovery Computing for Low-Energy and Secure IoT Devices

Dr. Himanshu Thapliyal

VLSI Emerging Design And Nano Things Security (VEDANTS) Lab

Department of Electrical and Computer Engineering,

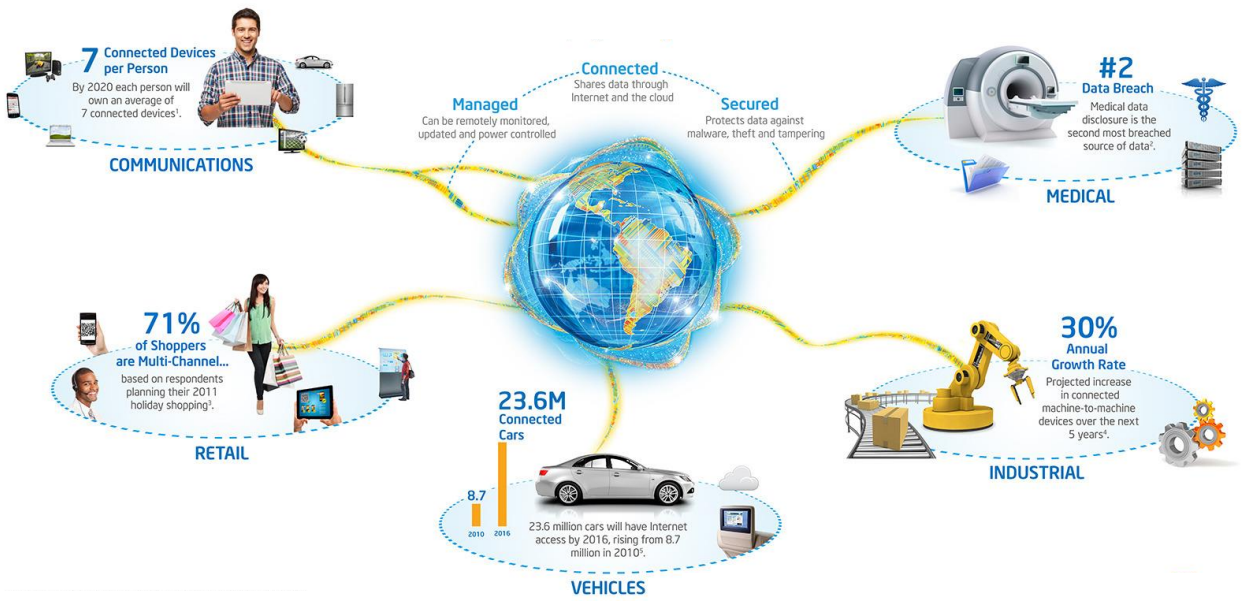
University of Kentucky, Lexington, KY

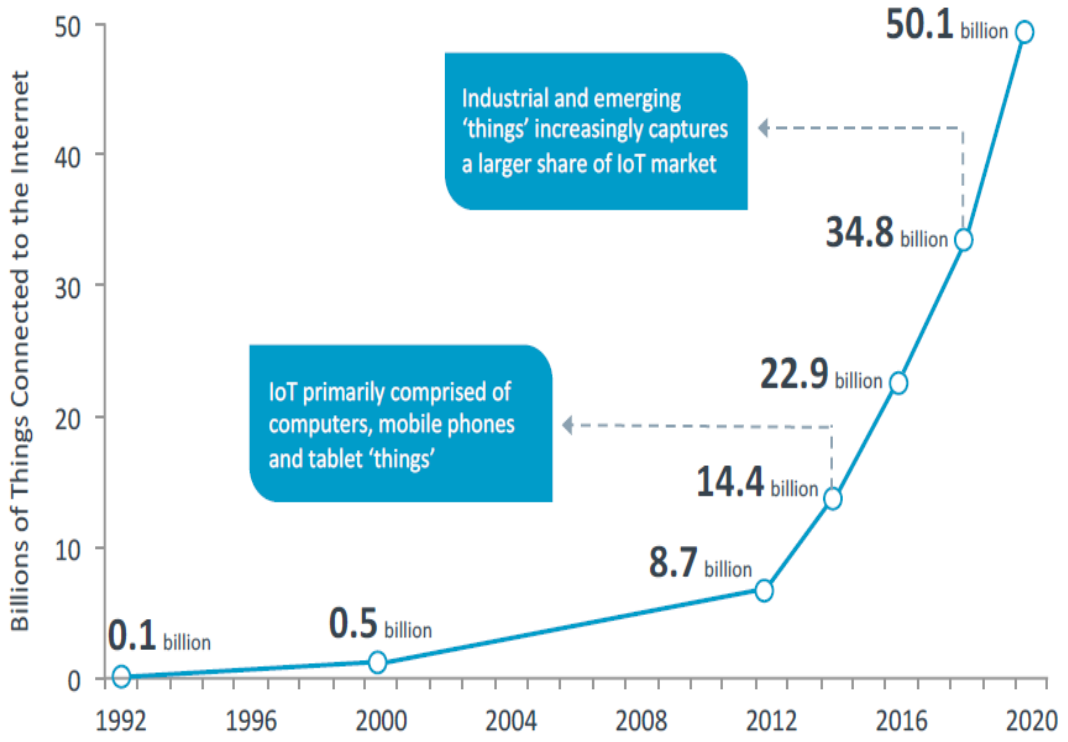
hthapliyal@uky.edu

Web: http://hthapliyal.engr.uky.edu/

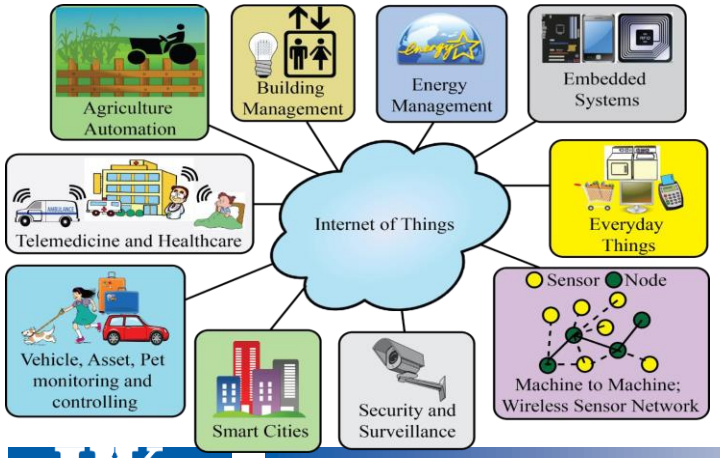
UNIVERSITY OF KENTUCKY

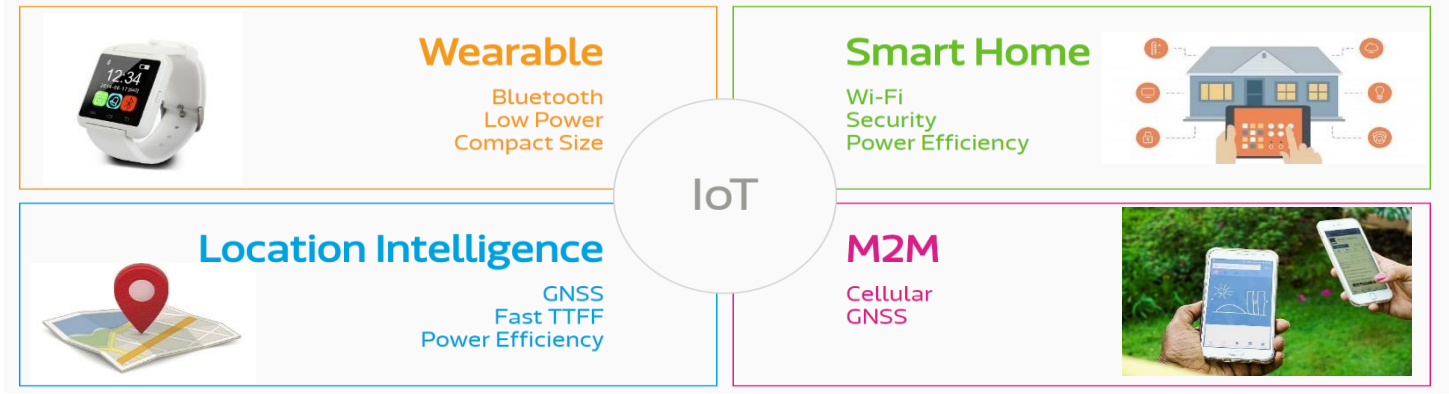
Internet of Things (IoT)





Source: R. K. Krishnamurthy (Intel), Panel, ICCE 2019

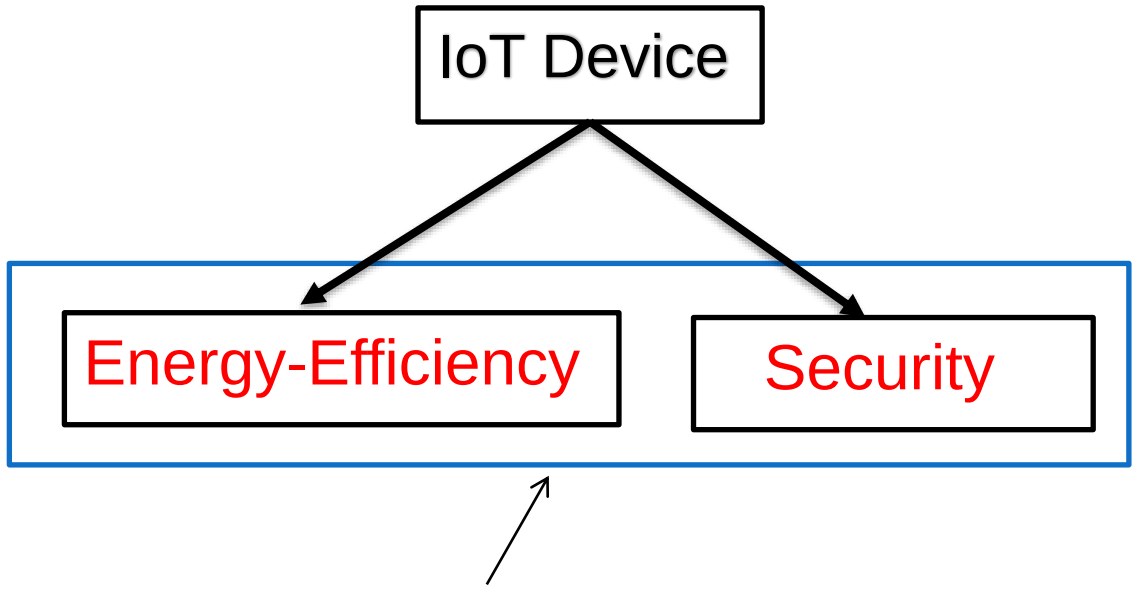




"Mediatek iot chipsets," https://labs.mediatek.com/en/chipset/overview, 2019

Ref: Evans, D.: The internet of things: how the next evolution of the internet is changing everything. CISCO white paper, vol. 1, pp. 1–11 (2011)

Challenges in IoT Devices



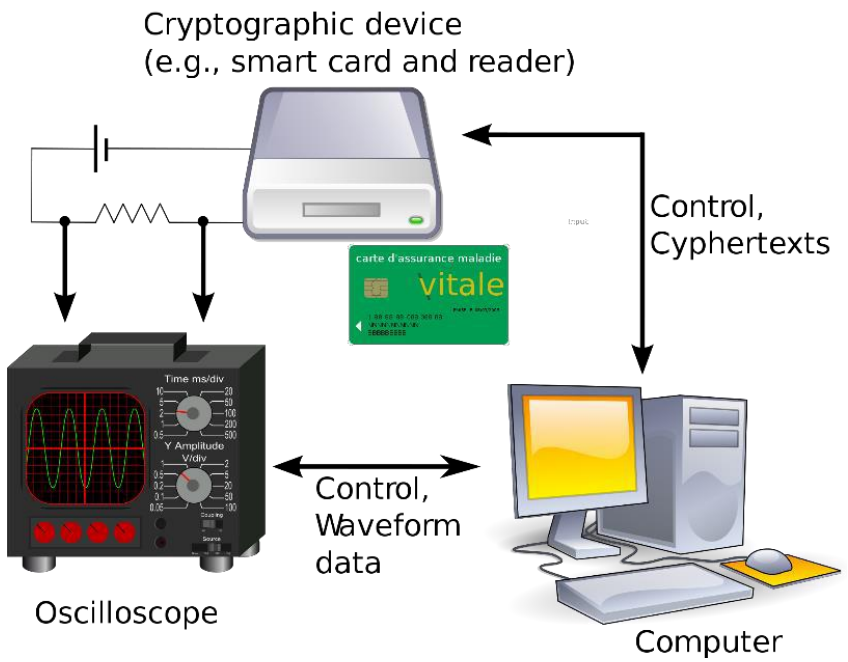
Security/Energy-Efficiency

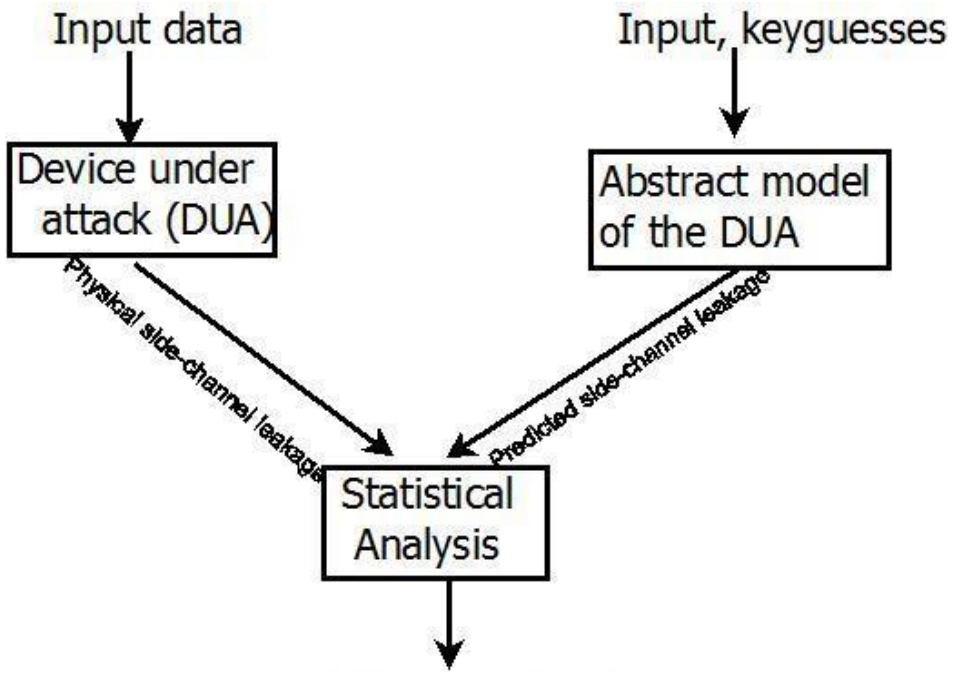
- Typically battery operated
- Energy-efficient design
- Vulnerable to hardware/malware attacks
- Power analysis attacks
- IC piracy, IC counterfeiting, Hardware trojan

Cyberattacks are threat to reliability, safety, consumer's personal information and piracy or cloning of intellectual property.

Ref: D Blaauw, D Sylvester, P Dutta, Y Lee, I Lee, S Bang, Y Kim, G Kim, P Pannuto, Y-S Kuo, et al. Iot design space challenges: Circuits and systems. In 2014 Symposium on VLSI Technology (VLSI-Technology): Digest of Technical Papers, pages 1–2. IEEE, 2014.

Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CPA)

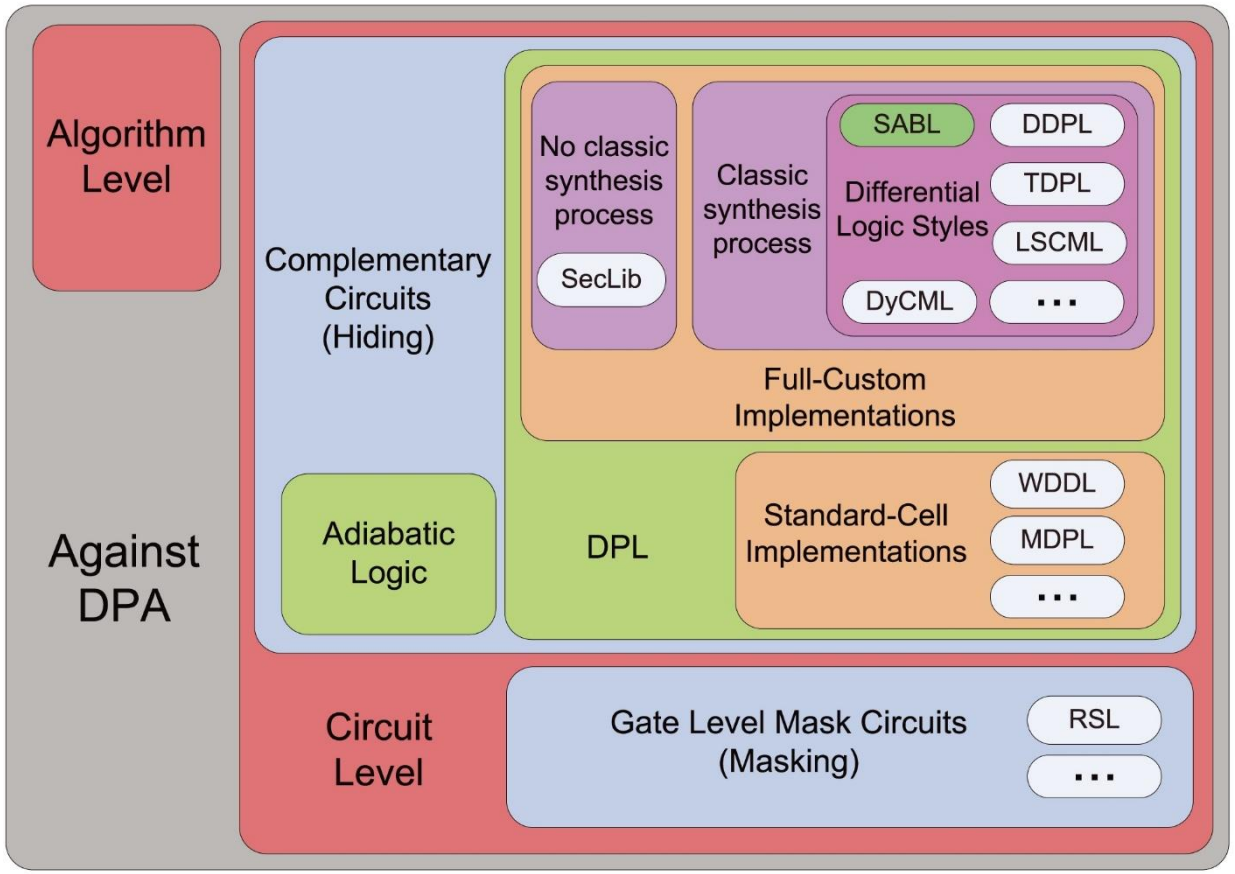




Decision on key guess

1. H. Thapliyal, T.S.S. Varun, S.D. Kumar, "Adiabatic Computing Based Low-Power and DPA-Resistant Lightweight Cryptography for IoT Devices", Proceedings of the *2017 IEEE Computer Society Annual Symposium on VLSI*, Bochum, July 2017, pp. 621-626.

DPA Countermeasures



Acosta, A. J., Addabbo, T., & Tena-Sánchez, E. (2017). Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. International Journal of Circuit Theory and Applications, 45(2), 145-169.

Parameter	ER based [2]*	JSSC'18 [3]	JSCC'10 [4]	ISSCC'11 [5]
Technology	65nm	130nm	130nm	130nm
Standalone AES power/Freq	138.1mW/ 1.2GHz	10.5mW/ 40 MHz	33.32mW/ 100MHz	-/50MHz
Operating Voltage (V)	1 (External)	0.4-1 (from IVR)	1.2 (External)	1.2 (External)
Power Overhead	-30%	5%	33%	-
Area overhead	6000um^2 (25%)	2135um^2 (103 gates)	7900um^2 (20%)	11K gates (67%)
Performance Overhead	0%	3.33%	50%	0%
Analysis Method	DPA	CPA, TVLA	DPA	CPA/ Fault-Attack

Table 2. Comparison of ASIC-based DPA countermeasures with energy Recovery (ER) based design. Comparison is based on results in [1].

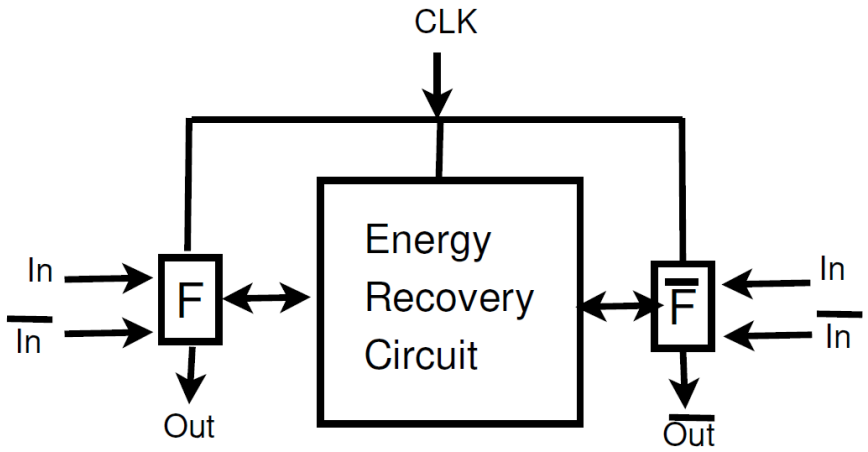
1. M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," *IEEE Journal of Solid-State Circuits*, pp. 1–16, 2018.
2. S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32 GHz high-throughput charge-recovery AES core with resistance to DPA attacks," in *2015 Symposium on VLSI Circuits (VLSI Circuits)*, 2015, pp. C246–C247.
3. M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," *IEEE Journal of Solid-State Circuits*, pp. 1–16, 2018.
4. C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," IEEE J. Solid-State Circuits, vol. 45, no. 1, pp. 23–31, Jan. 2010
5. M. Doulcier-Verdier, J. M. Dutertre, J. Fournier, J. B. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant AES circuit working on duplicated complemented values," in 2011 IEEE International Solid-State Circuits Conference, 2011, pp. 274–276.

UNIVERSITY OF KENTUCKY

Talk Overview

- Energy Recovery Logic for low-power and DPA resistant circuits
- FinFET and Tunnel FET based energy recovery family
- Lightweight PRESENT-80 algorithm as benchmark circuit
- Adiabatic Logic-Based Energy-Efficient and Reliable PUF
- Hardware Trojan Detection Method Based on Energy Recovery Logic
- Adoption in Industry

Energy Recovery Logic



- Energy dissipated in the adiabatic circuit is given by:

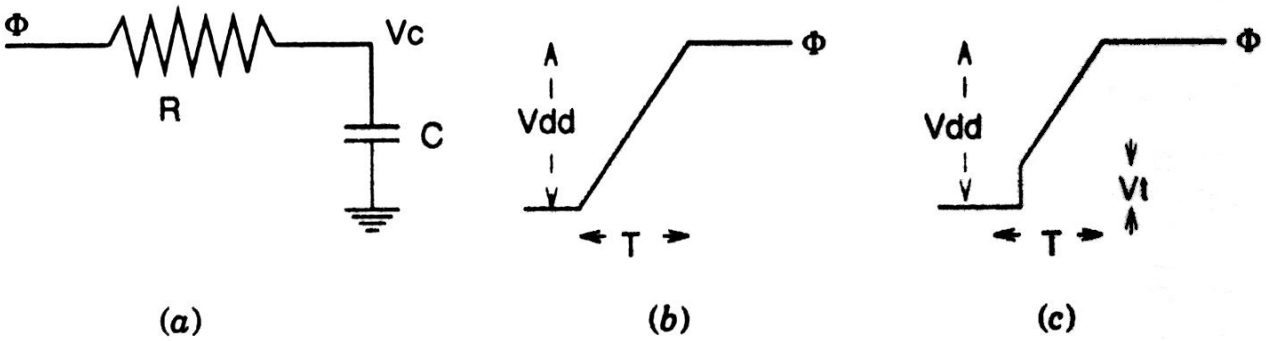
$$E_{diss} = \frac{RC}{T} C V_{dd}^{2}$$

T -> Transition period of power clock

R -> parasitic resistance

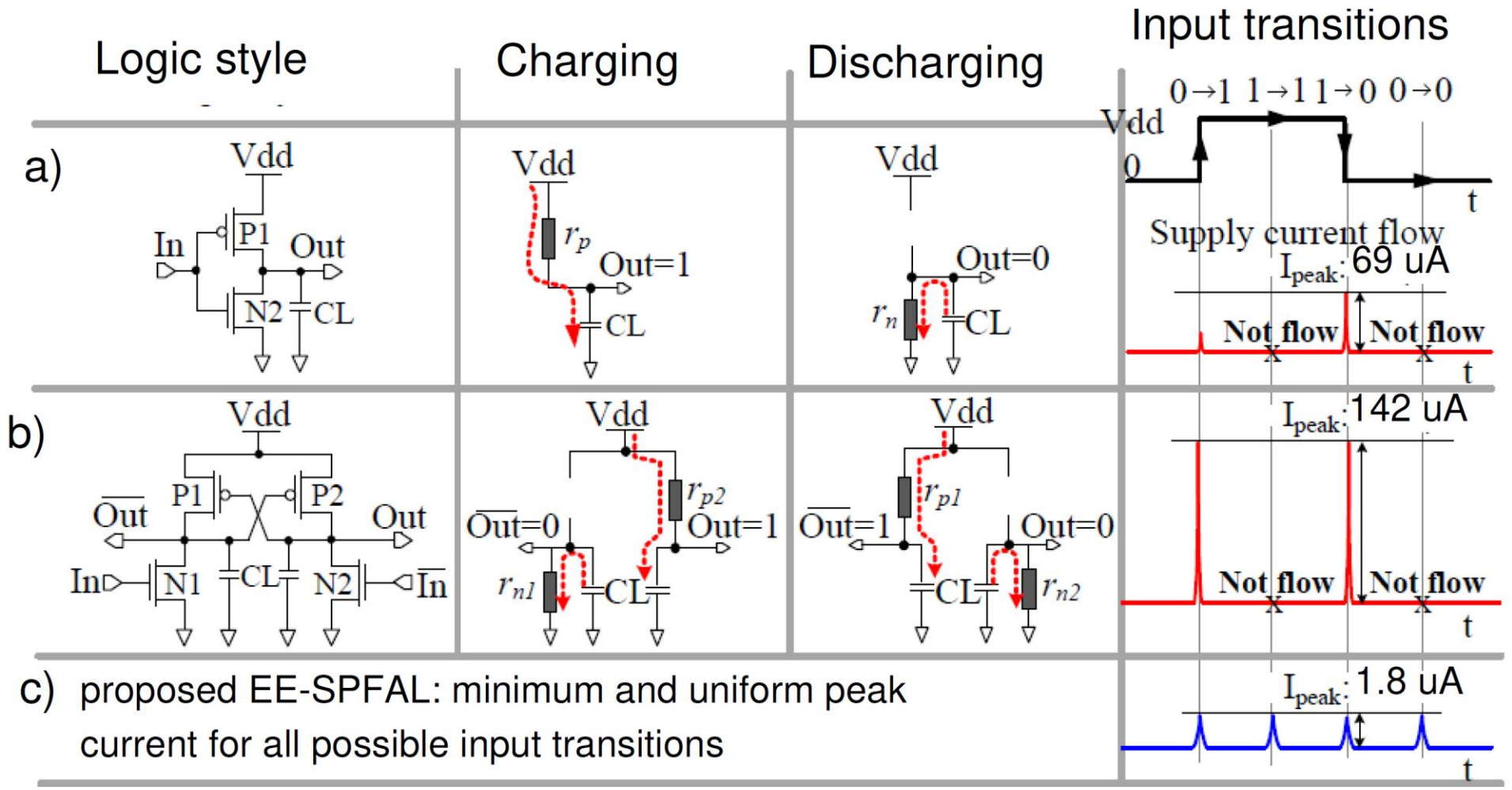
C ->load capacitance

V_{dd} -> voltage swing of the clock



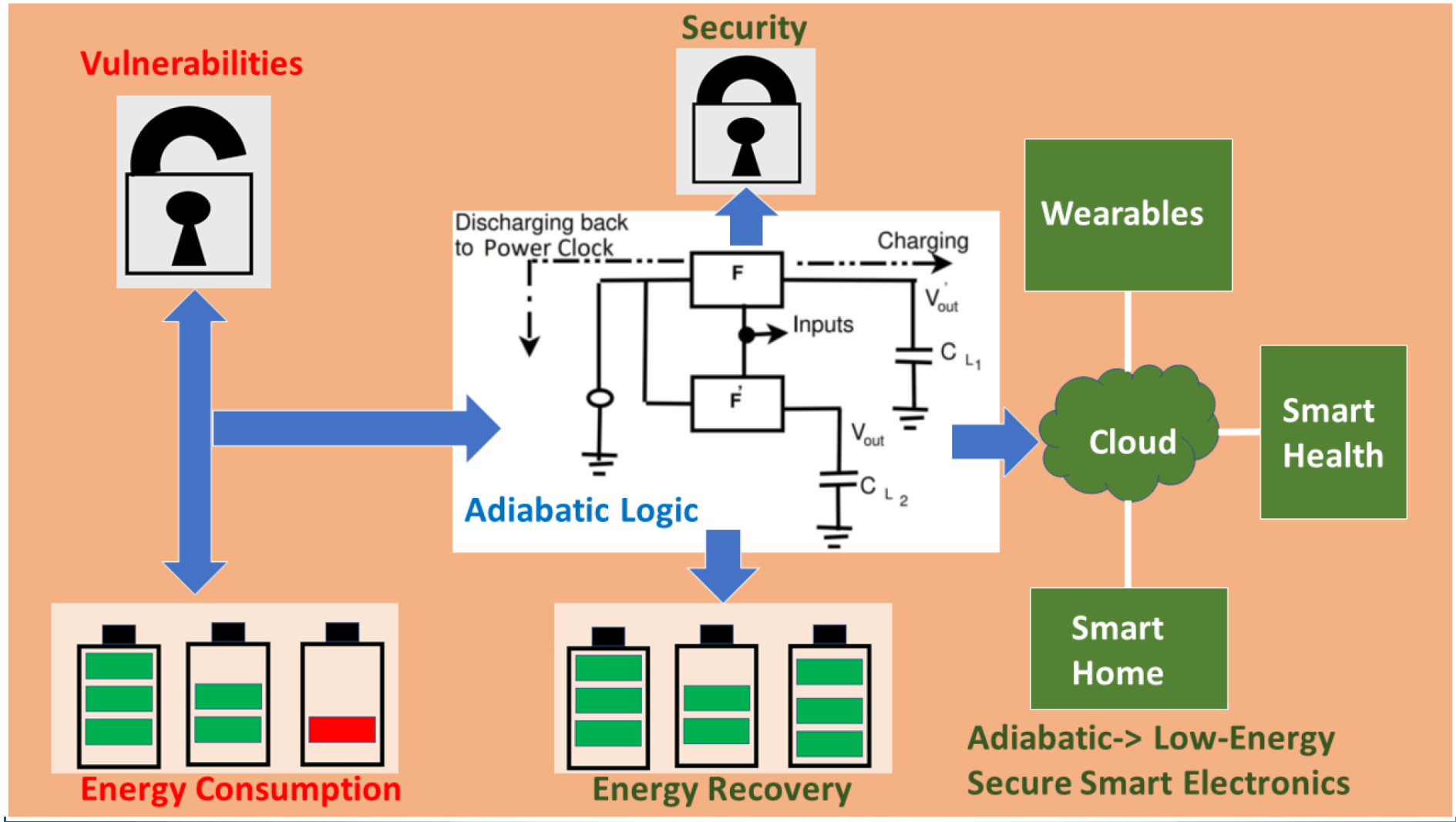
1. H. Thapliyal, T.S.S. Varun, S.D. Kumar, "Adiabatic Computing Based Low-Power and DPA-Resistant Lightweight Cryptography for IoT Devices", Proceedings of the *2017 IEEE Computer Society Annual Symposium on VLSI*, Bochum, July 2017, pp. 621-626.

Current Traces of an Inverter

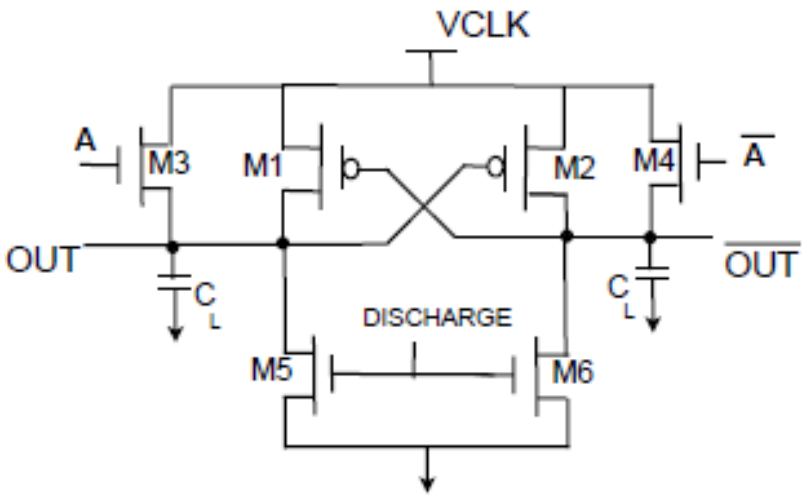


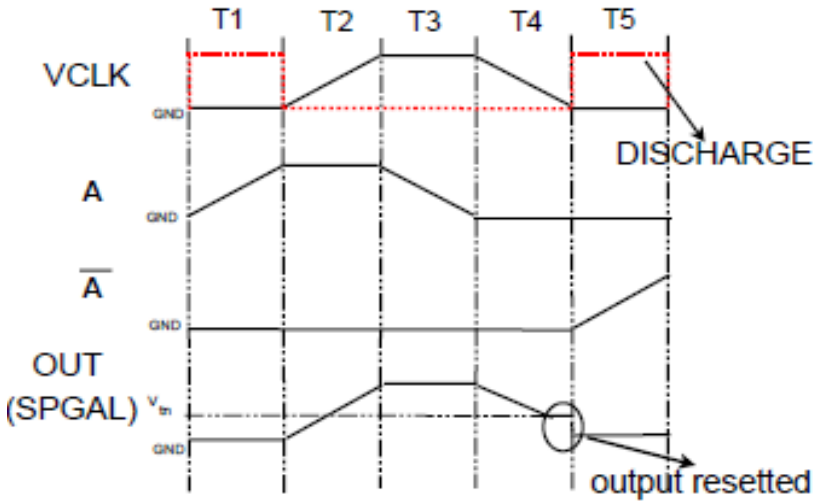
S.D. Kumar, H. Thapliyal, and A. Mohammad, "EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card", *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 281-293, 1 April-June 2019.

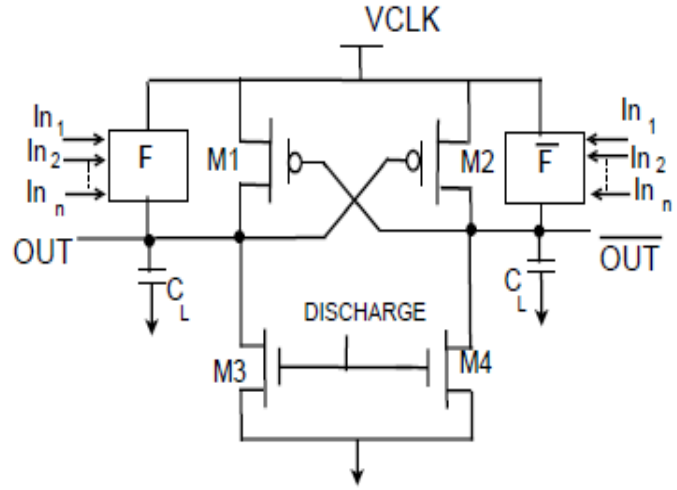
Adiabatic Logic base Low-Energy and Secure Solutions



Symmetric Pass Gate Adiabatic Logic (SPGAL)

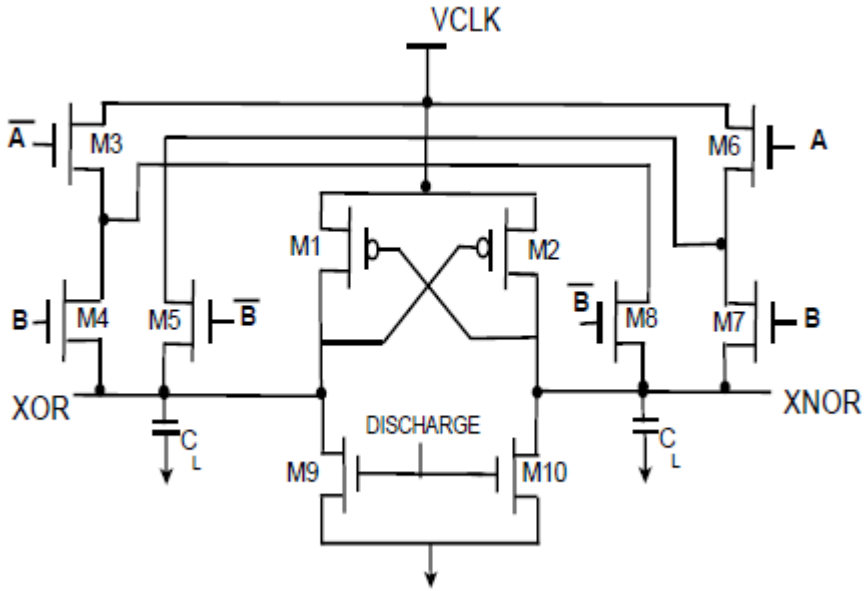




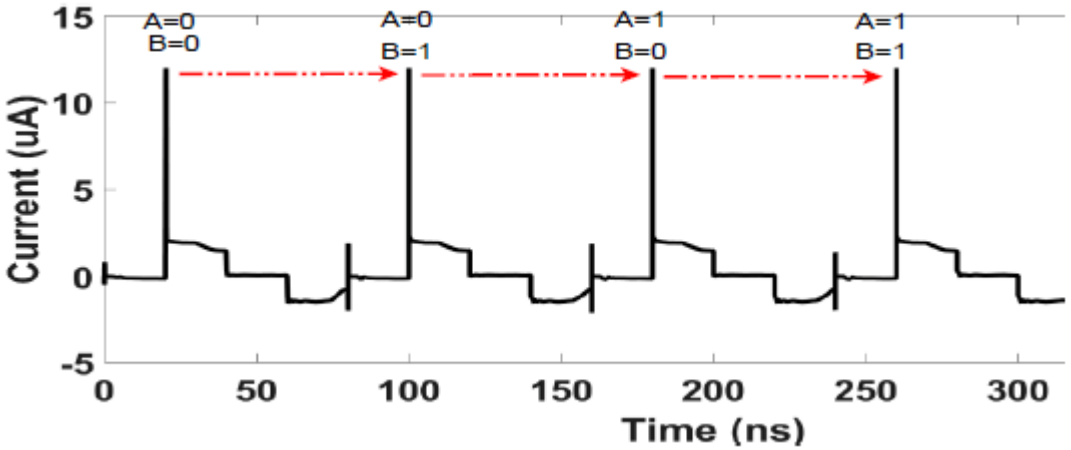


Transistors	Functionality
M1, M2	Recover the energy from load capacitors
M3, M4	Perform logic operations
M5, M6	Reset the outputs (discharge the redundant charge)

SPGAL XOR gate



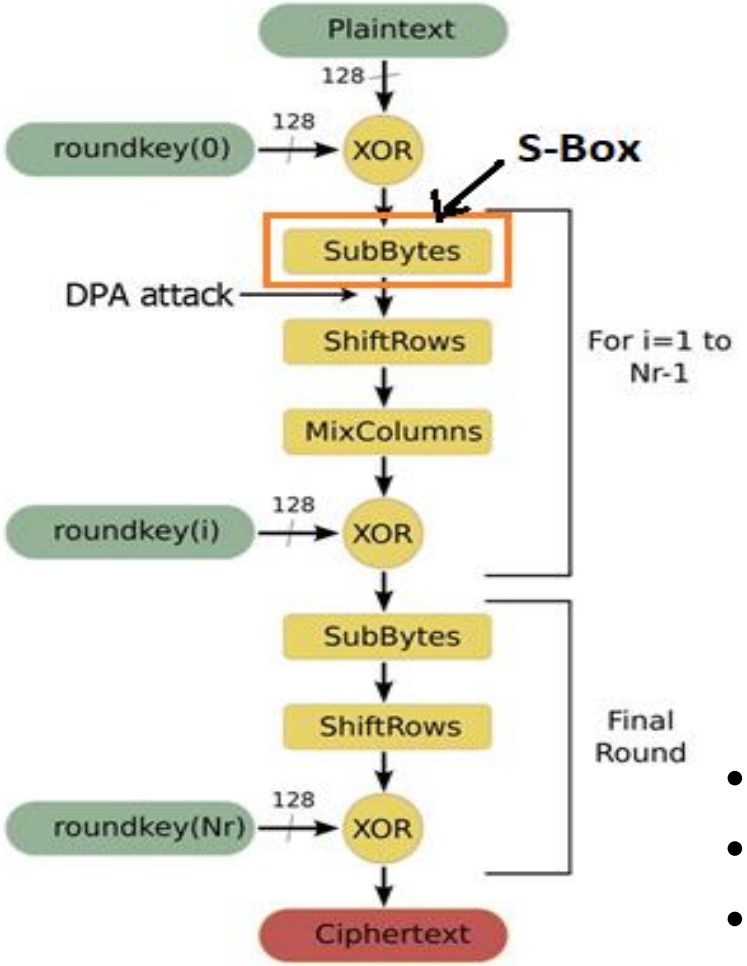
(a)



(b)

(a) Shows the schematic of SPGAL based XOR gate
(b) Shows the uniform current consumption of the SPGAL based XOR gate for various input transition.

AES Cryptographic Algorithm



AES component	Max. Power (uW @10MHz)	Power ratio (%)
SubBytes (S-Box)	1940	75
MixColumns	262	10
AddRoundKey	>10	>1
Data Selectors	>10	>1
FFs and Clock Drivers	400	15

Power consumption of each AES component [1], 1.5V CMOS standard cell

- AES is symmetric encryption algorithm
- Applications: Network appliances, voice communications etc.
- S-Box consumes much of the total power of AES designs

Ref: Morioka, Sumio, and Akashi Satoh. "An optimized S-Box circuit architecture for low power AES design." *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, Berlin, Heidelberg, 2002.

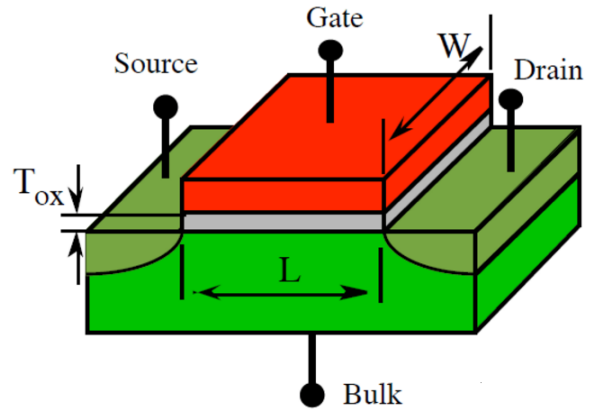
S-Box circuit comparison results

Logic	No. of transistors (S-Box)	Overhead (transistor)	Area (um^2)	Energy dissipation	ESF
CMOS	2202	-	0.04	11.45 pJ	-
SQAL	3401	54%	0.0723	2.52 pJ	4.54
SPGAL (Proposed)	3624	64%	0.08	0.825 pJ	13.878

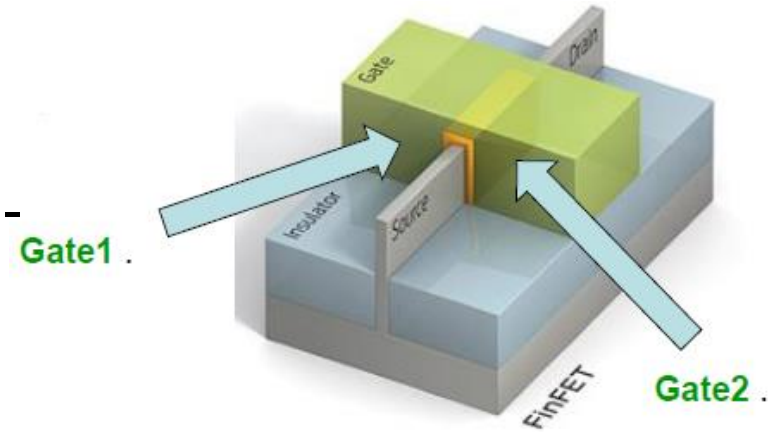
- **Energy Saving Factor (ESF)** is a measure of how much energy is used in a conventional CMOS gate or system with respect to its adiabatic logic counterpart

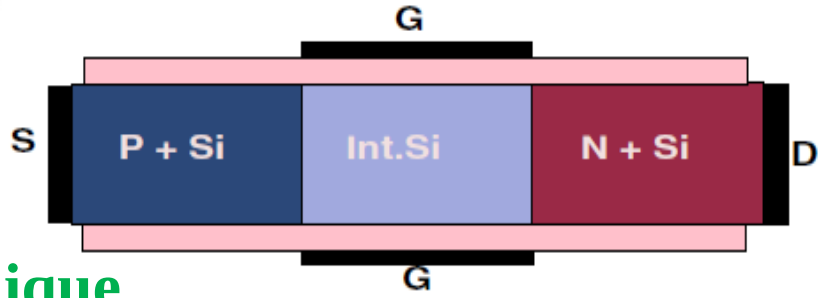
- M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, “Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes,” Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 62, no. 1, pp. 149–156, 2015.
- S.D. Kumar, H. Thapliyal, A. Mohammad, and K.S. Perumalla, "Design Exploration of Symmetric Pass Gate Adiabatic Logic for Energy-Efficient and Secure Hardware", Integration, VLSI Journal, Available online Sep 17, 2016: http://dx.doi.org/10.1016/j.vlsi.2016.08.007
- S. D. Kumar, H. Thapliyal, A. Mohammad, V. Singh, and K. S. Perumalla, "Energy-Efficient and Secure SBox Circuit Using Symmetric Pass Gate Adiabatic Logic," in VLSI (ISVLSI), 2016 IEEE Computer Society Annual Symposium on, 2016, pp. 308–313.

FinFET and Tunnel FET



- FinFET: Strong gate control channels
- Higher on-state current, lower leakage, and faster switching speed
- Tunnel FET (TFET) subthreshold swing (SS) below 60 mV/dec (high on-current to off current ratio)
- Lower SS enables low-leakage with higher performance than CMOS at lower voltages

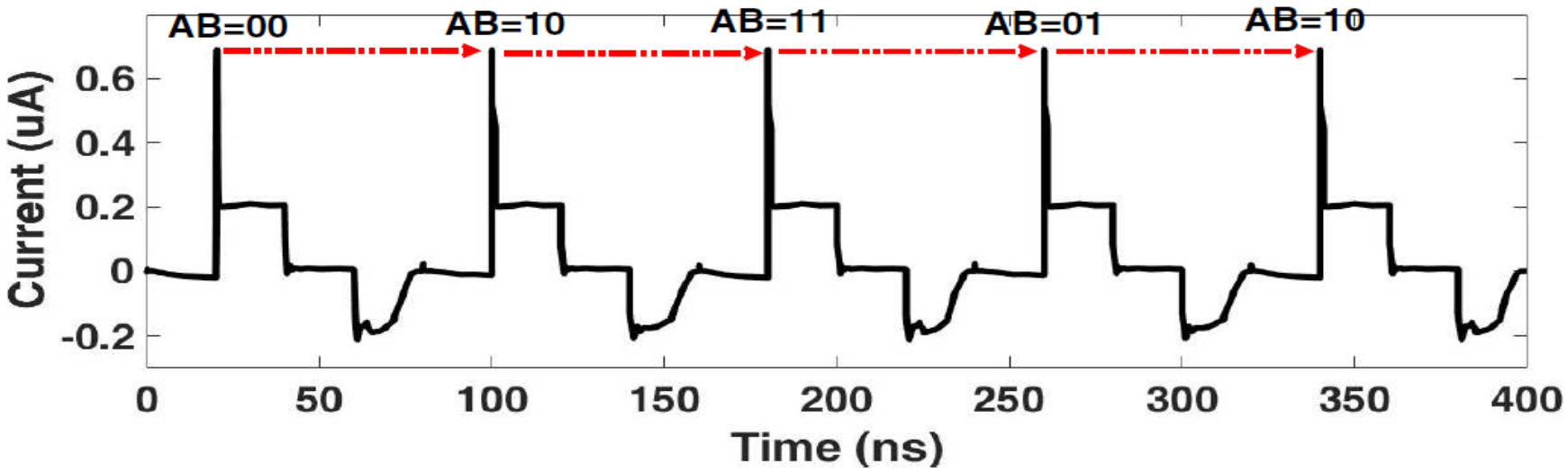




- **Energy-Efficient**
  - **Dynamic power reduction → Adiabatic logic technique**
  - **Leakage power reduction → FinFET/TFET devices**

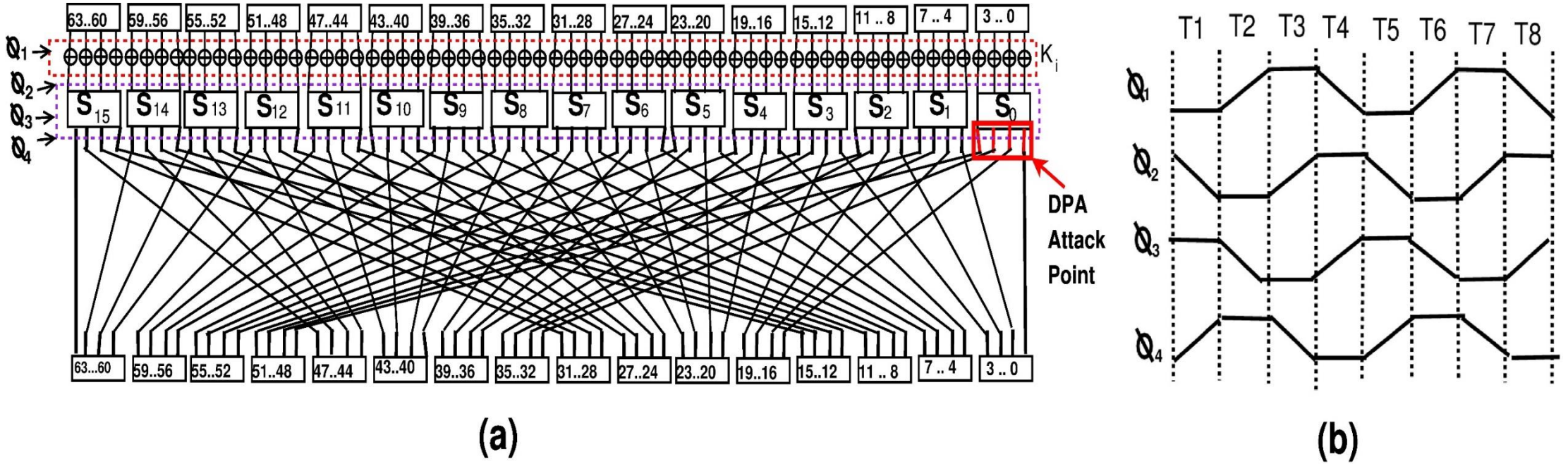
Ref: Chenming Hu, 3D FinFET and other sub-22nm Transistors, IPFA 2012

Current consumption of TunSAL XOR gate



- Uniform current consumption of TunSAL XOR for various input transitions
- Uniform current TunSAL gates makes it to countermeasure DPA attack at circuit level

Implementation of PRESENT-80



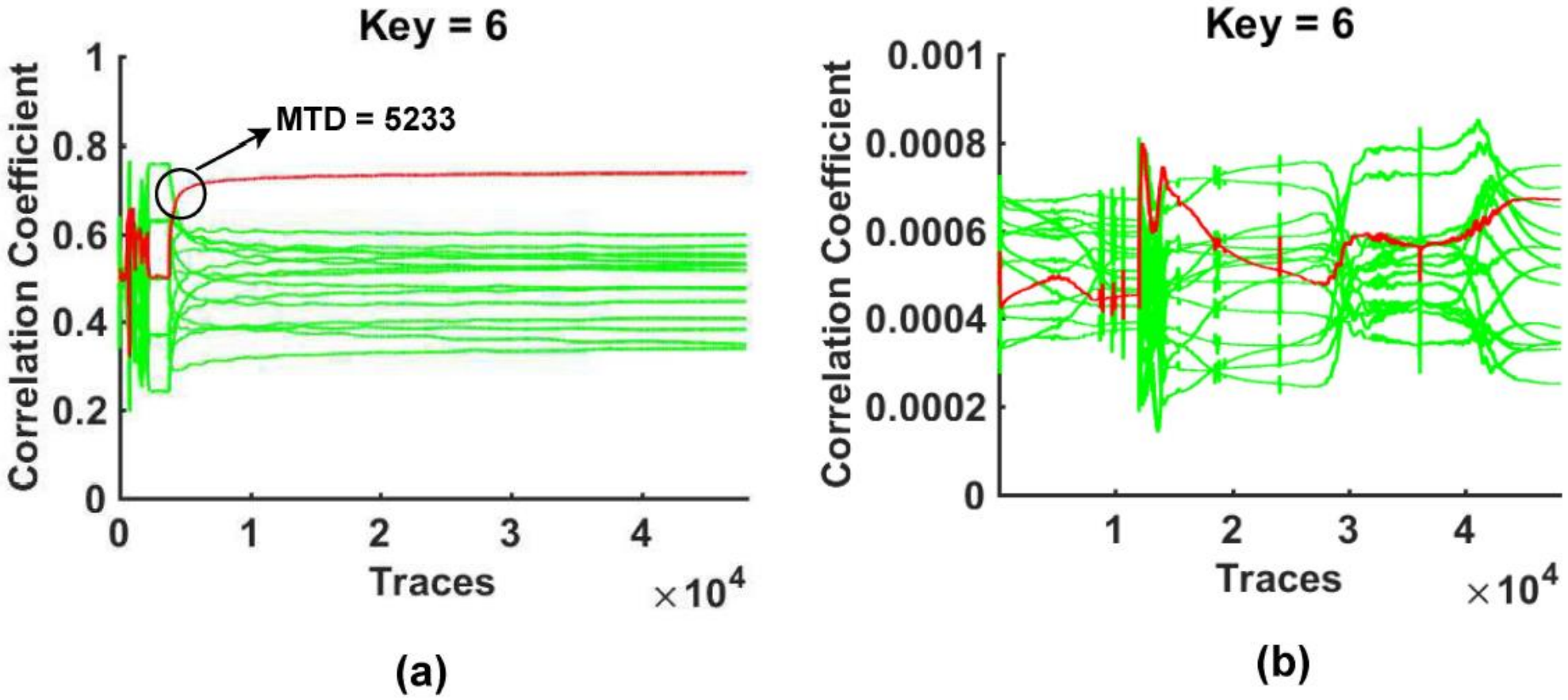
(a) One round implementation of PRESENT-80 using SPGAL, FinSAL and TunSAL gates

(b) 4-phase clocking scheme of SPGAL, FinSAL and TunSAL to implement PRESENT-80

Simulation Results on PRESENT-80 at 12.5 MHz:

Metric	CMOS [1]	SPGAL [2]	FinSAL [3]	TunSAL [4]	% imp of [4] wrt [1]	% imp of [4] wrt [2]	% imp of [4] wrt [3]
Device	MOSFET	MOSFET	FinFET	Tunnel FET	-	-	-
Tech (nm)	22	22	20	20	-	-	-
V_{DD} (V)	1	1	0.9	0.3	-	-	-
Avg. power (uW)	7.890	1.32	0.70	0.511	92	62	28
Avg energy (pJ)	20.83	3.564	1.795	1.257	93	65	30

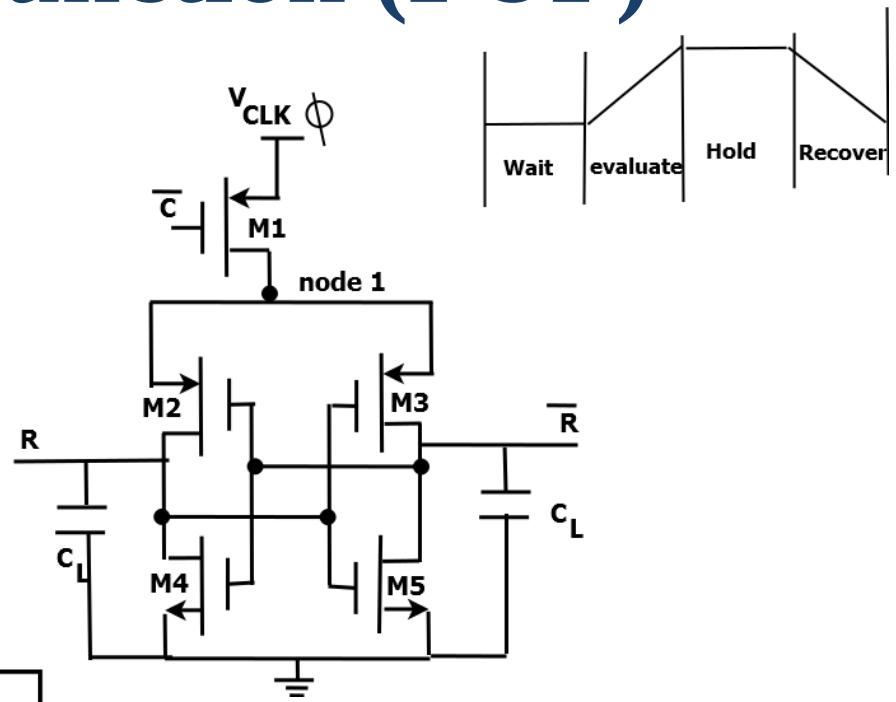
DPA attack on PRESENT-80

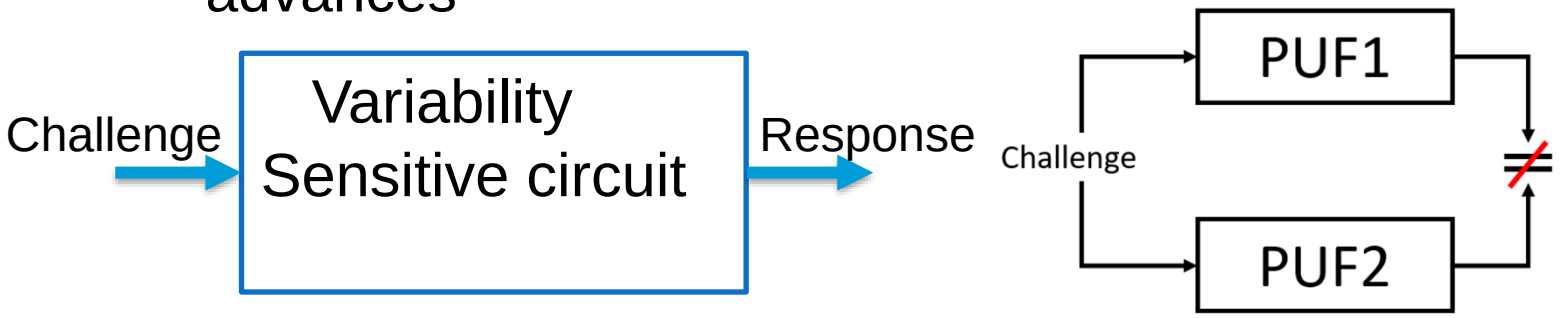


DPA attack on PRESENT-80 implemented using (a) Conventional CMOS gates (b) TunSAL gates

Adiabatic Physical Unclonable Function (PUF)

- Silicon fingerprint
- Process variations is boon
  - Variation is inherent in fabrication process
  - Unique for each physical instance
  - Hard to remove or predict
  - Relative variation increases as the fab process advances





Proposed	**45nm**	**1V**	**49.48%**	**49.41%**	**99.6%**	**0.08 fJ**

Kumar, S. Dinesh, and Himanshu Thapliyal. "Design of Adiabatic Logic-Based Energy-Efficient and Reliable PUF for IoT Devices." ACM Journal on Emerging Technologies in Computing Systems (JETC) 16, no. 3 (2020): 1-18.

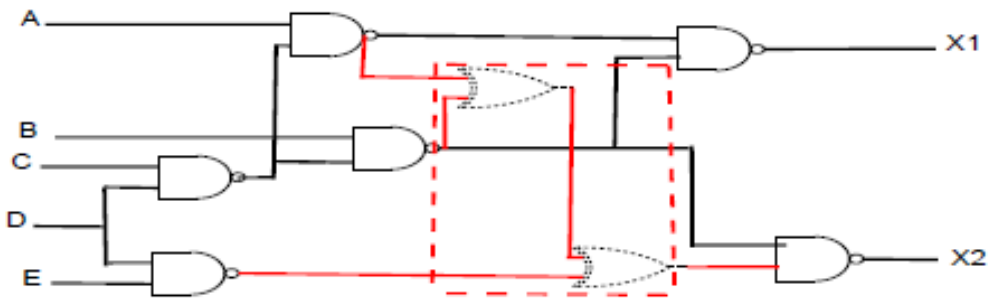
Proposed PUF Comparison

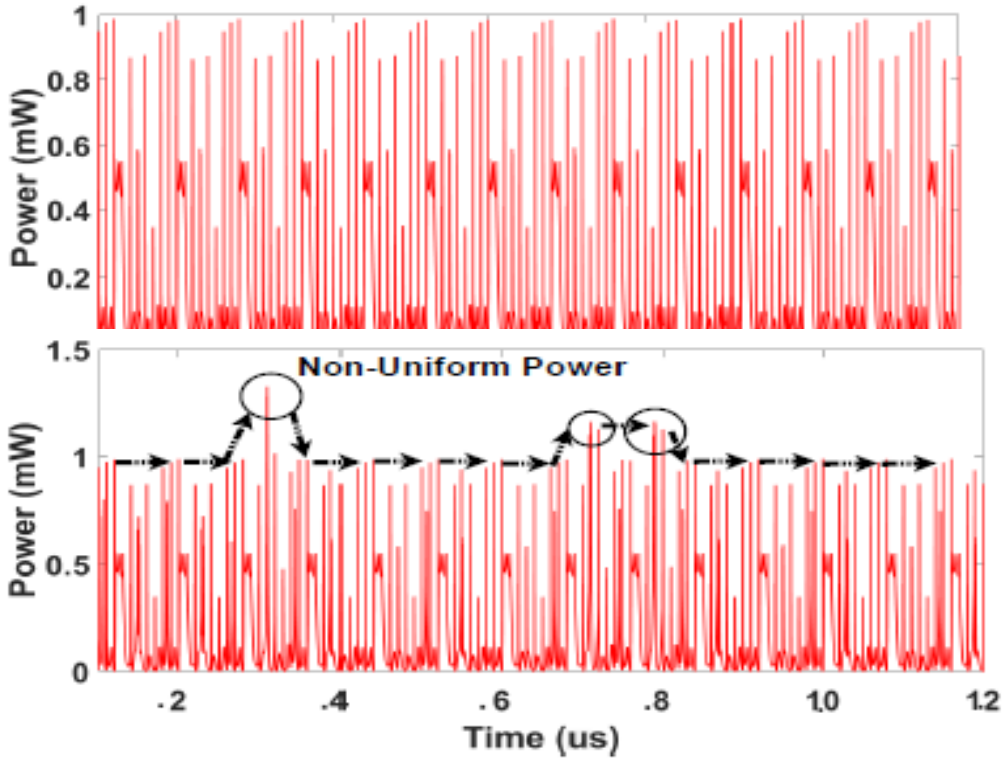
PUF	Tech.	Vdd	Uniqu-eness	Uniformity	Reliability	Energy/bit
[1]	180nm	1.8 V	NA	NA	95.18%	1.37 pJ
[2]	180nm	3.3 V	49.37 %	NA	99.1%	23.9 pJ
[3]	40nm	0.9 V	47.22 %	NA	>99.99 %	17.8 pJ
[4]	28nm	0.6 V	49.11%	49.96%	88.39	0.05 fJ
Proposed	45nm	1V	49.48%	49.41%	99.6%	0.08 fJ

[1] Daihyun Lim,et.al., Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 13(10):1200–1205, 2005.
[2] Yuan Cao, Le Zhang, et. al., A low-power hybrid ro puf with improved thermal stability for lightweight applications. IEEE Transactions on computer-aided design of integrated circuits and systems, 34(7):1143–1147, 2015.
[3] Kaiyuan Yang, et. al., a physically unclonable function with ber¡ 10- 8 for robust chip authentication using oscillator collapse in 40nm cmos. In Solid-State Circuits Conference-(ISSCC), 2015 IEEE International, pages 1–3. IEEE, 2015.
[4] Adam Neale and Manoj Sachdev. A low energy sram-based physically unclonable function primitive in 28 nm cmos. In Custom Integrated Circuits Conference (CICC), 2015 IEEE, pages 1–4. IEEE, 2015.

Adiabatic Logic Based Hardware Trojan Detection

- Malicious circuit in IC to perform faulty operations
- Designed to destroy systems or leak secret information
- Implemented as hardware modification to ASICs, microprocessor, DSP etc.

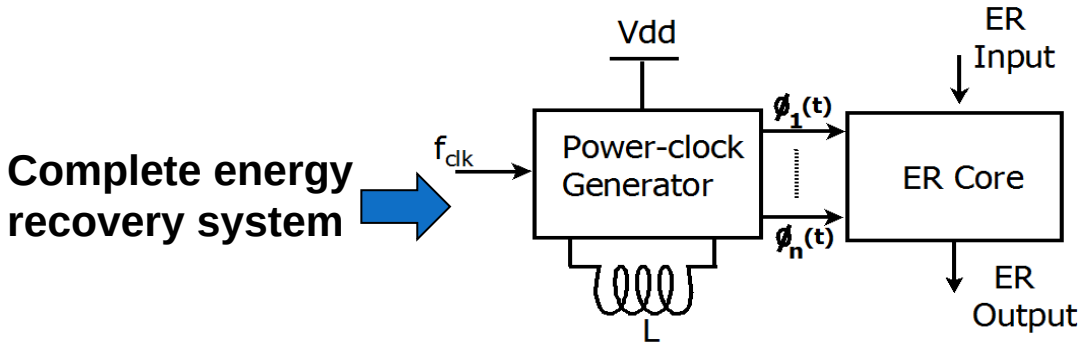




Thapliyal, Himanshu, and Zachary Kahleifeh. "Solving Energy and Cybersecurity Constraints in IoT Devices Using Energy Recovery Computing." In *Proceedings of the 2019 on Great Lakes Symposium on VLSI*, pp. 525-530. 2019.

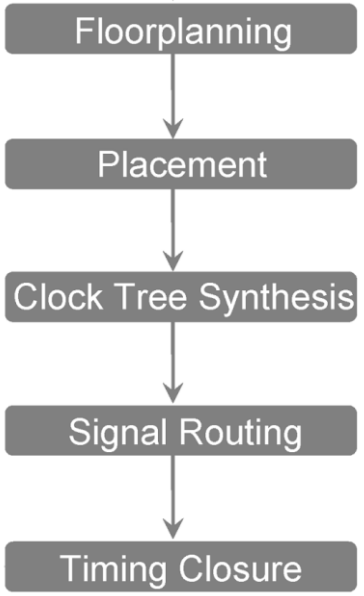
Ref: Tehranipoor, M., & Koushanfar, F. (2010). A survey of hardware trojan taxonomy and detection. *IEEE design & test of computers*, *27*(1).

Adoption in Industry



Main Challenges in ER Computing:

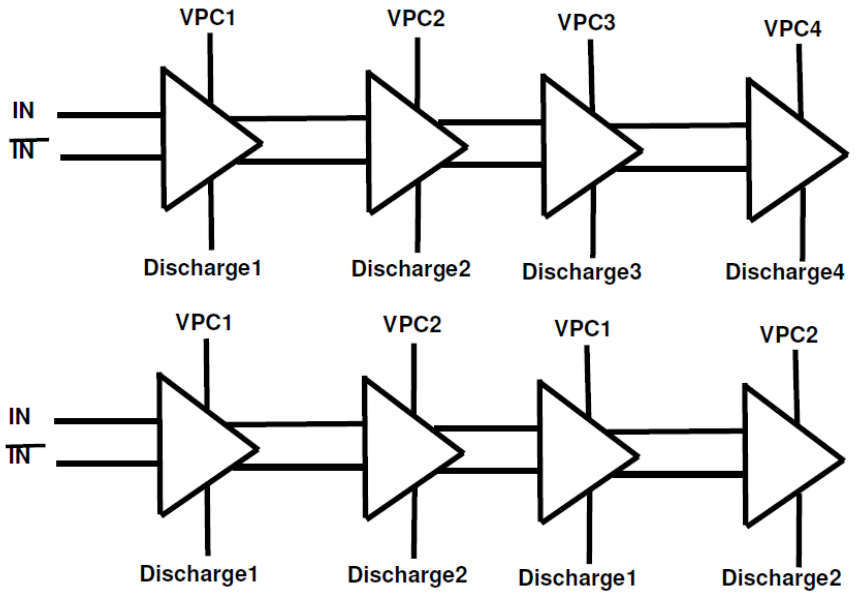
- Not been widely adopted in industry as a mainstream methodology.
- Amount of time and effort required to design customized ER circuits.
- Must acquire specialized skills and learn ER methodologies to design ER circuits.



Solutions:

- To mainstream ER computing, it needs to be made designer-friendly.
- Necessary to develop **a standard cell library and semi-automatic tools** to reduce the time and effort in the design and verification of ER circuits.
- Power clock generation and distribution play an important role in determining the overall energy efficiency of the ER system.

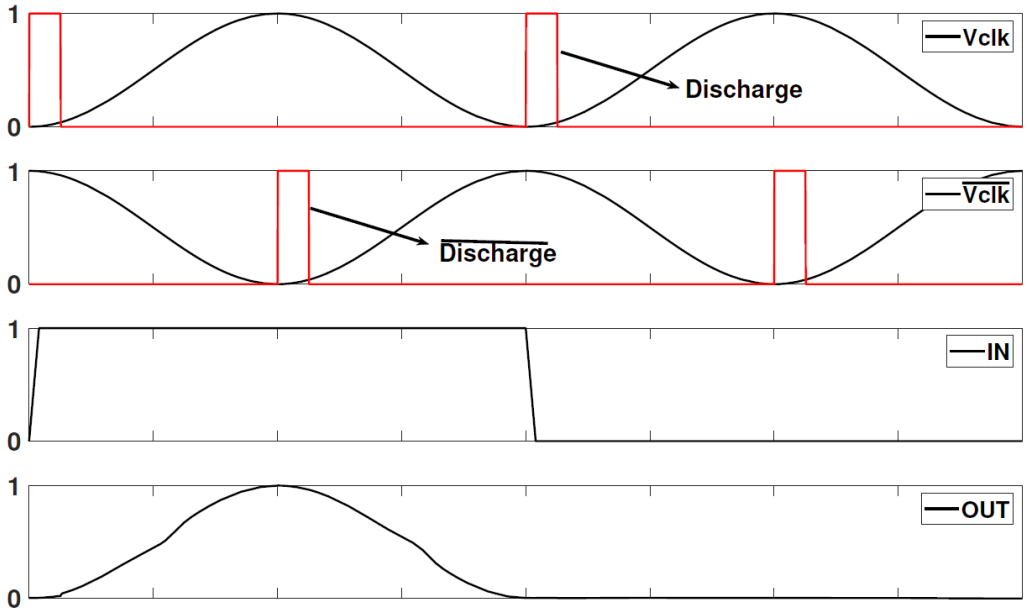
2-Phase Adiabatic Logic

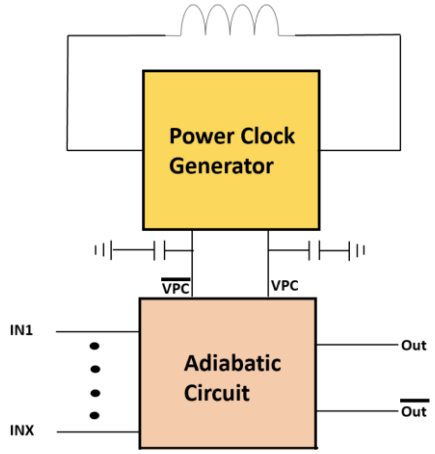


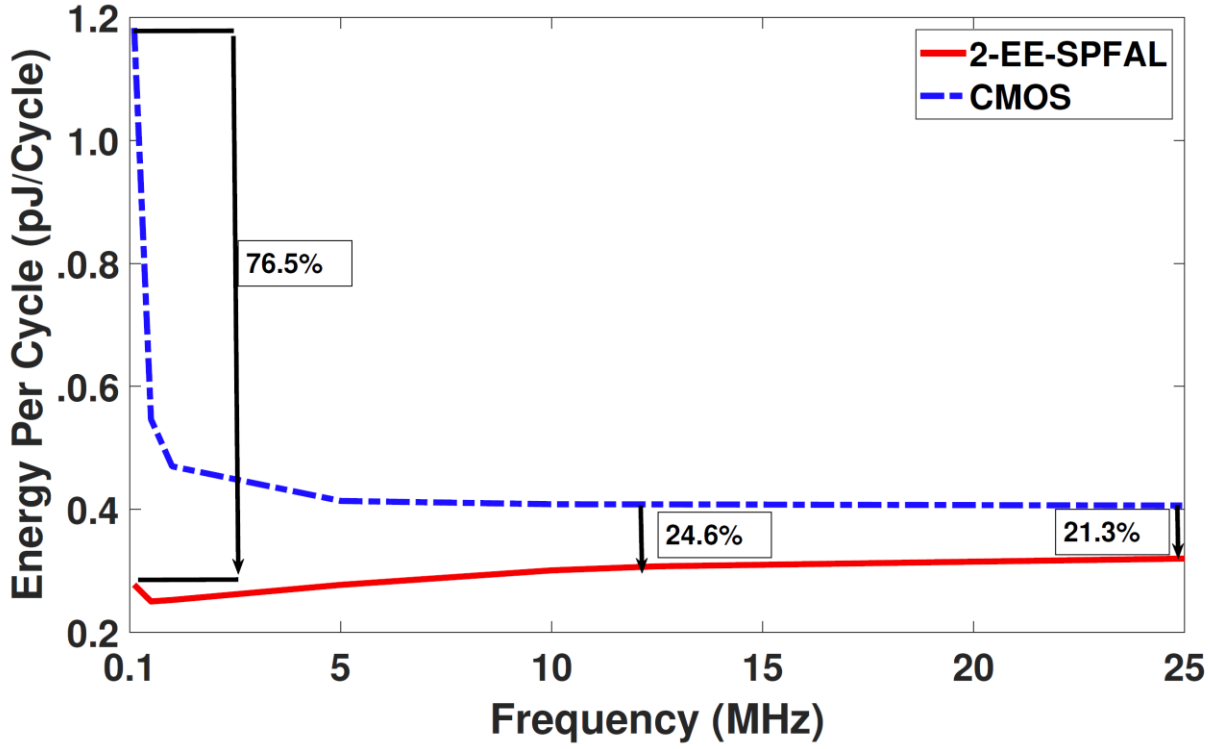
- 2-Phase CPA resistant, adiabatic logic only requires 4 signals to operate while 4-Phase requires 8.
- 2-Phase clock designs also consume less area and are less complex.
- The reduced interconnection area and complexity can lead to simpler yet energy efficient adiabatic designs

W. Athas, L. Svensson, and N. Tzartzanis, “A resonant signal driver for two-phase, almost-non-overlapping clocks,” 1996. ISCAS’96, ‘Connecting the World’, 1996 IEEE International Symposium on Circuits and Syst., vol.4, pp.129–132, May 1996.

2-Phase Adiabatic Logic







- 2-EE-SPFAL uses two sine waves 180° out of phase.
- 2-EE-SPFAL requires two discharge signals with equal period of their respective clocks.

Z. Kahleifeh and H. Thapliyal, "2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic for CPA-Resistant IoT Devices," *IEEE 6th World Forum on Internet of Things (WF-IoT)*, New Orleans, June 2020. (Best Paper Award)

Summary

ER computing is a promising candidate to implement hardware security primitives for IoT devices with stringent constraints on power consumption.