Physical Unclonable Function (PUF) as the Hardware-Assisted Security (HAS) Primitive

Expert Lecture – VIT-AP Workshop on VLSI

Vijayawada, India, 23 June 2022

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu Website: http://www.smohanty.org

The Big Picture

Issues Challenging City Sustainability

Pollution

Water Crisis

Energy Crisis

Traffic

Smart City Technology - As a Solution

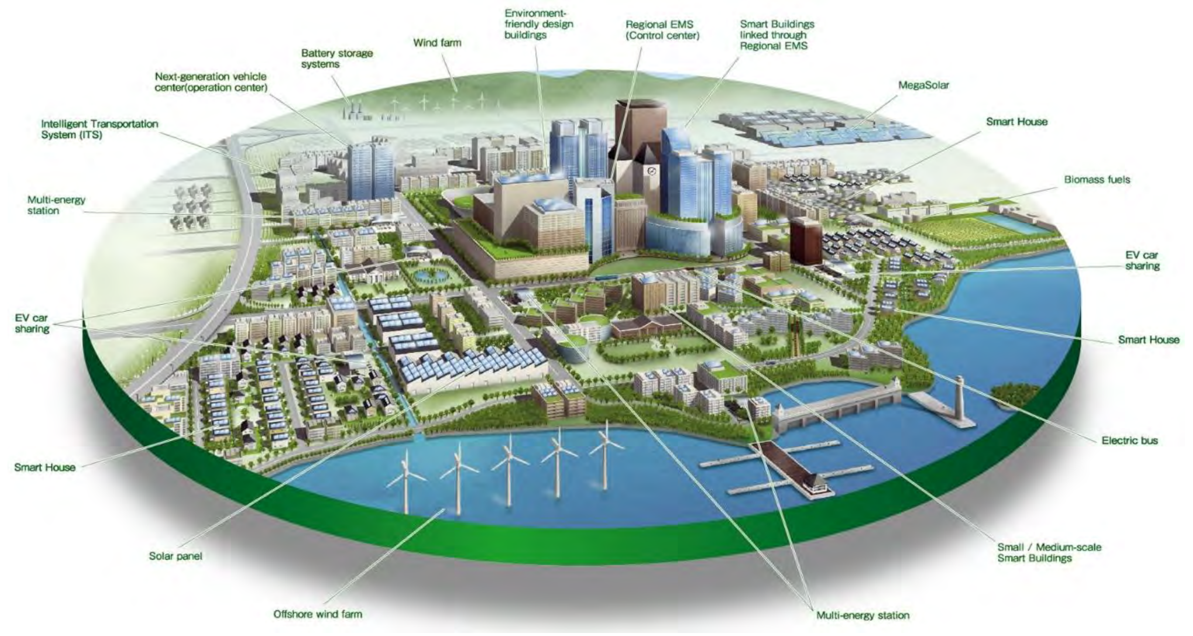
- Smart Cities: For effective management of limited resource to serve largest possible population to improve:
  - Livability
  - Workability
  - Sustainability

At Different Levels:
- Smart Village
- Smart State
- Smart Country

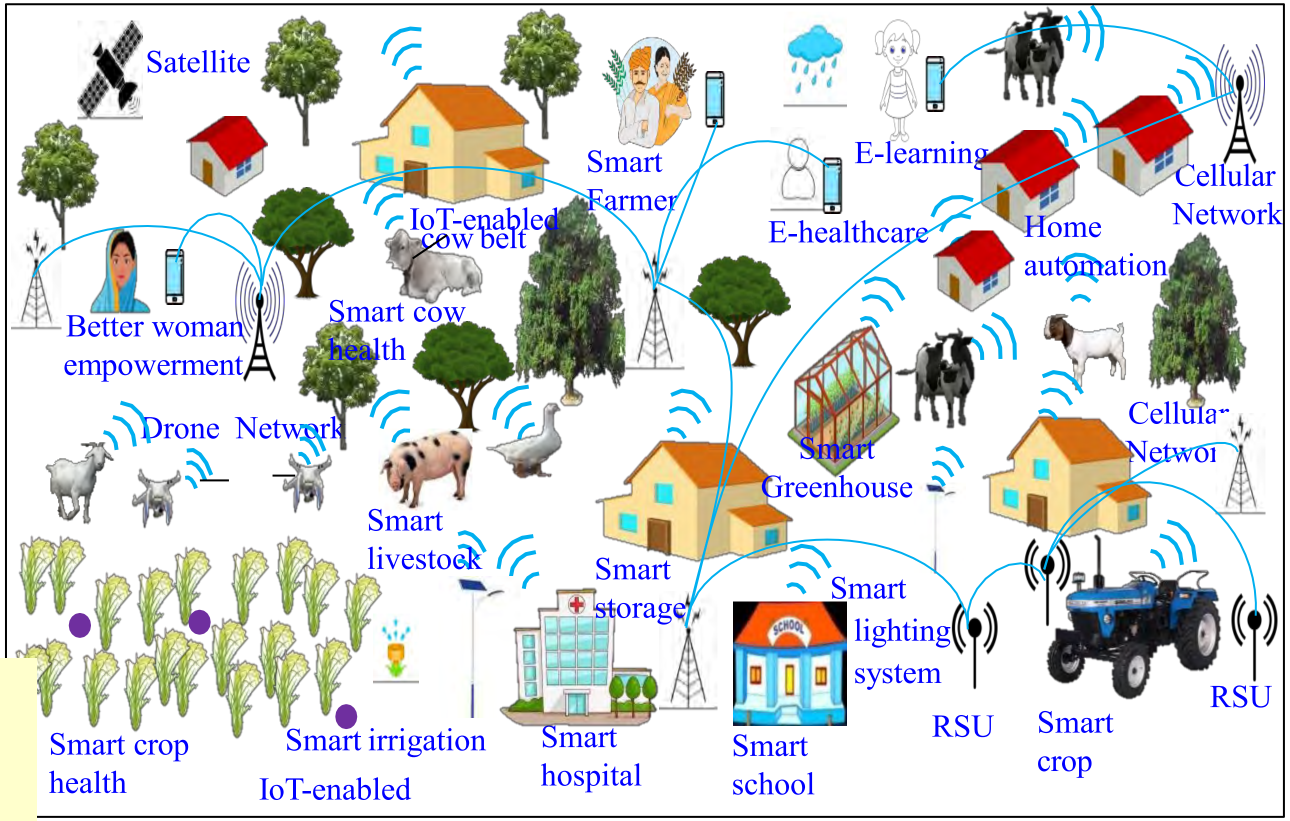
- Year 2050: 70% of world population will be urban

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything You wanted to Know about Smart Cities”, *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

Smart Cities Vs Smart Villages



Source: http://edwingarcia.info/2014/04/26/principal/



Smart Cities
CPS Types - More
Design Cost - High
Operation Cost – High
Energy Requirement - High

Smart Villages
CPS Types - Less
Design Cost - Low
Operation Cost – Low
Energy Requirement - Low

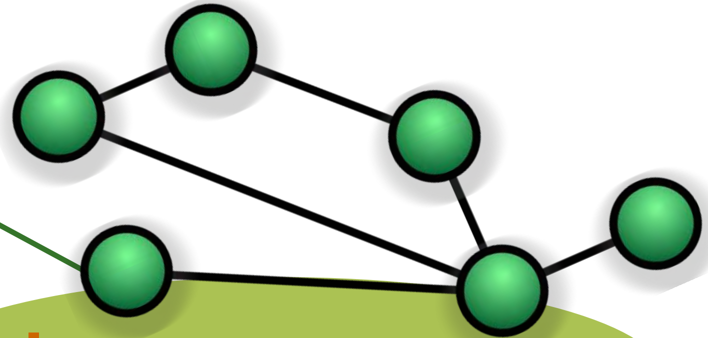
Source; P. Chanak and I. Banerjee, "Internet of Things-enabled Smart Villages: Recent Advances and Challenges," *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.3013244.

Smart Cities or Smart Villages - 3 Is

Instrumentation

The 3Is are provided by the Internet of Things (IoT).

Smart Cities

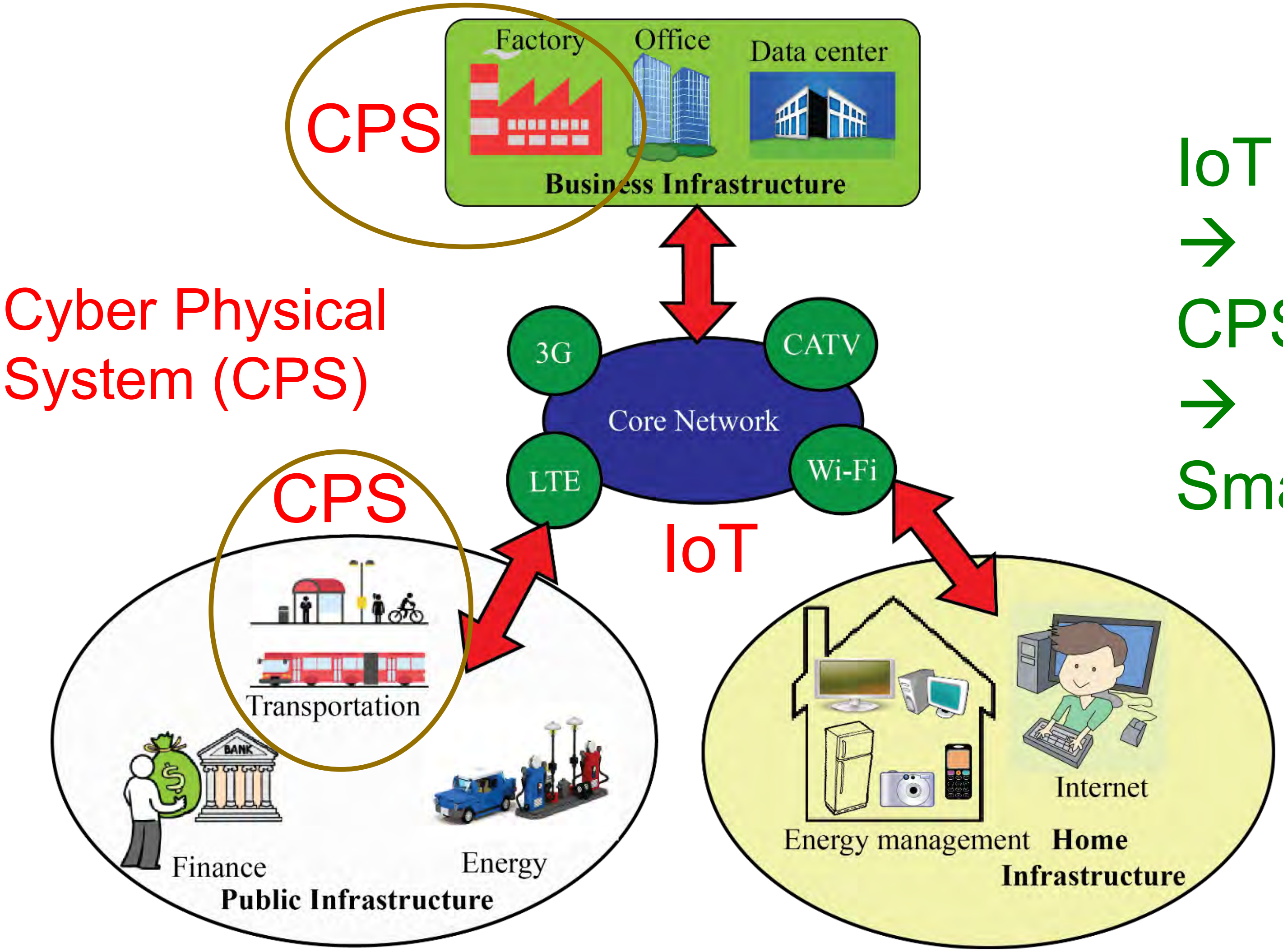


Intelligence

Interconnection

Source: Mohanty ISC2 2019 Keynote

IoT → CPS → Smart Cities or Smart Villages

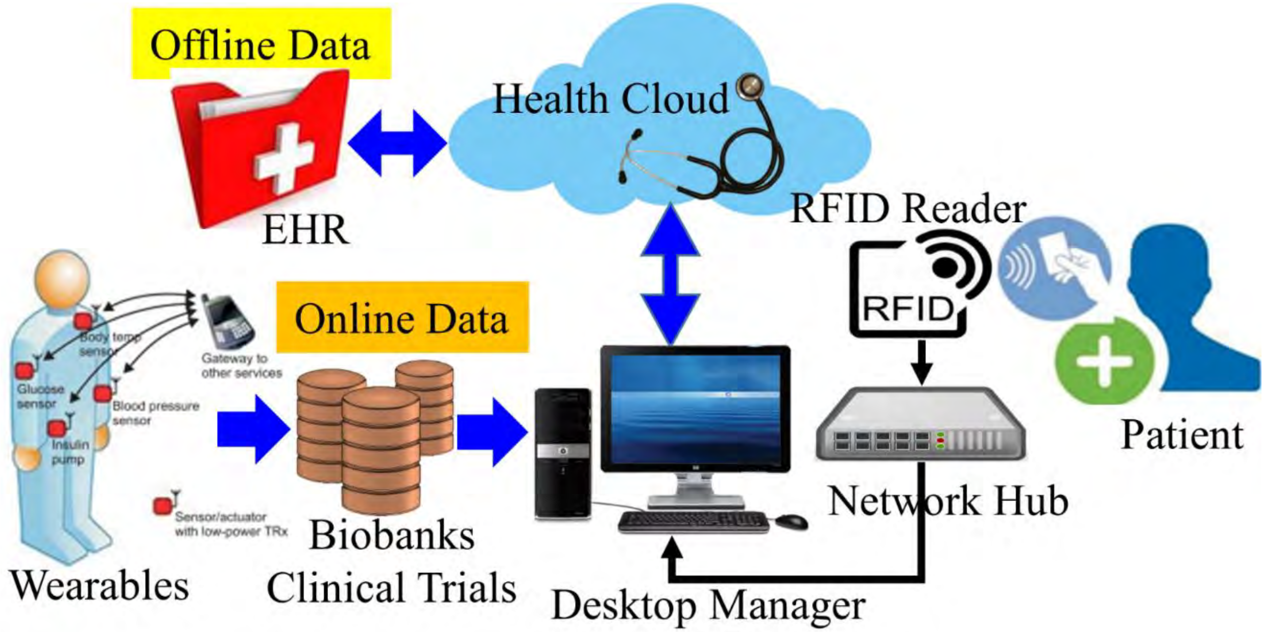


IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

IoT is the backbone

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

Healthcare Cyber-Physical System (H-CPS)



Internet-of-Medical-Things (IoMT)

OR

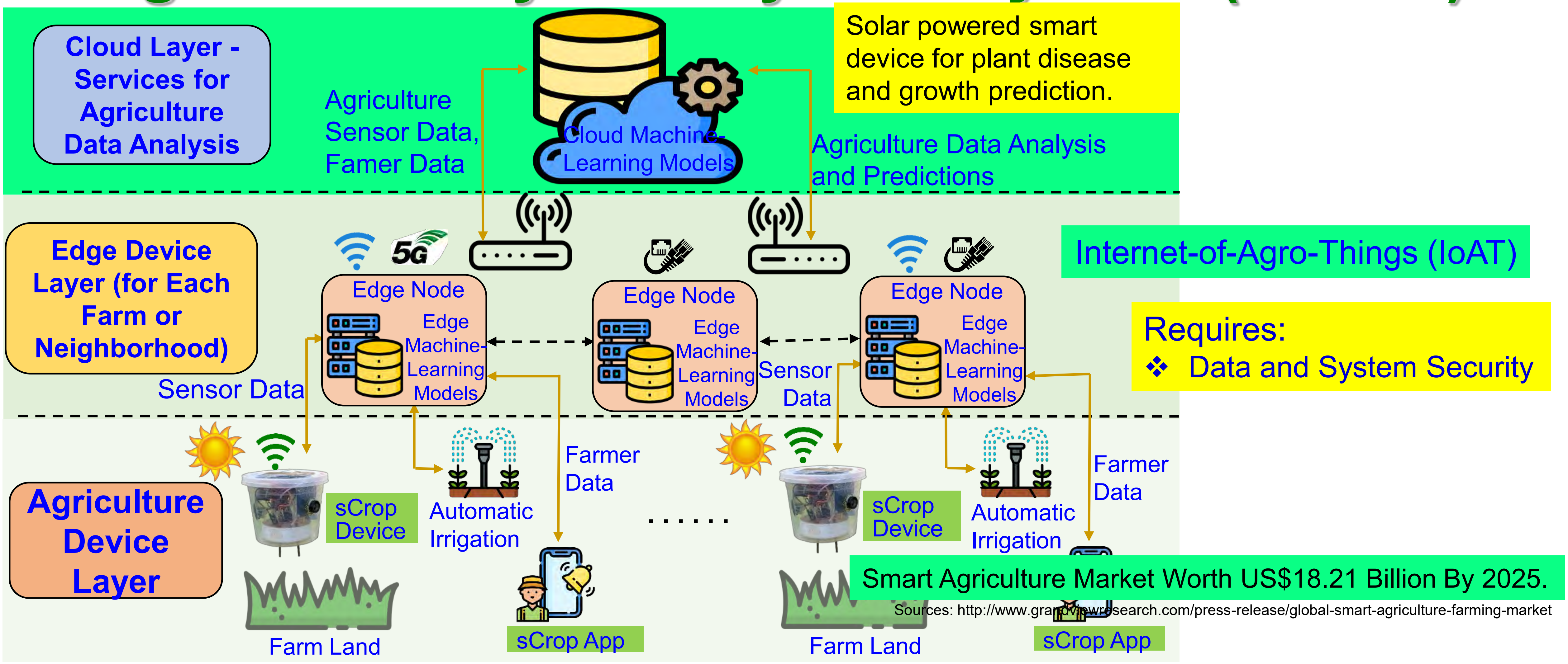
Internet-of-Health-Things (IoHT)

H-CPS ← Biosensors + Medical Devices + Wearable Medical Devices (WMDs) + Implantable Medical Devices (IMDs) + Internet + Healthcare database + AI/ML + Applications that connected through Internet.

Requires:
- ❖ Data and Device Security
- ❖ Data Privacy

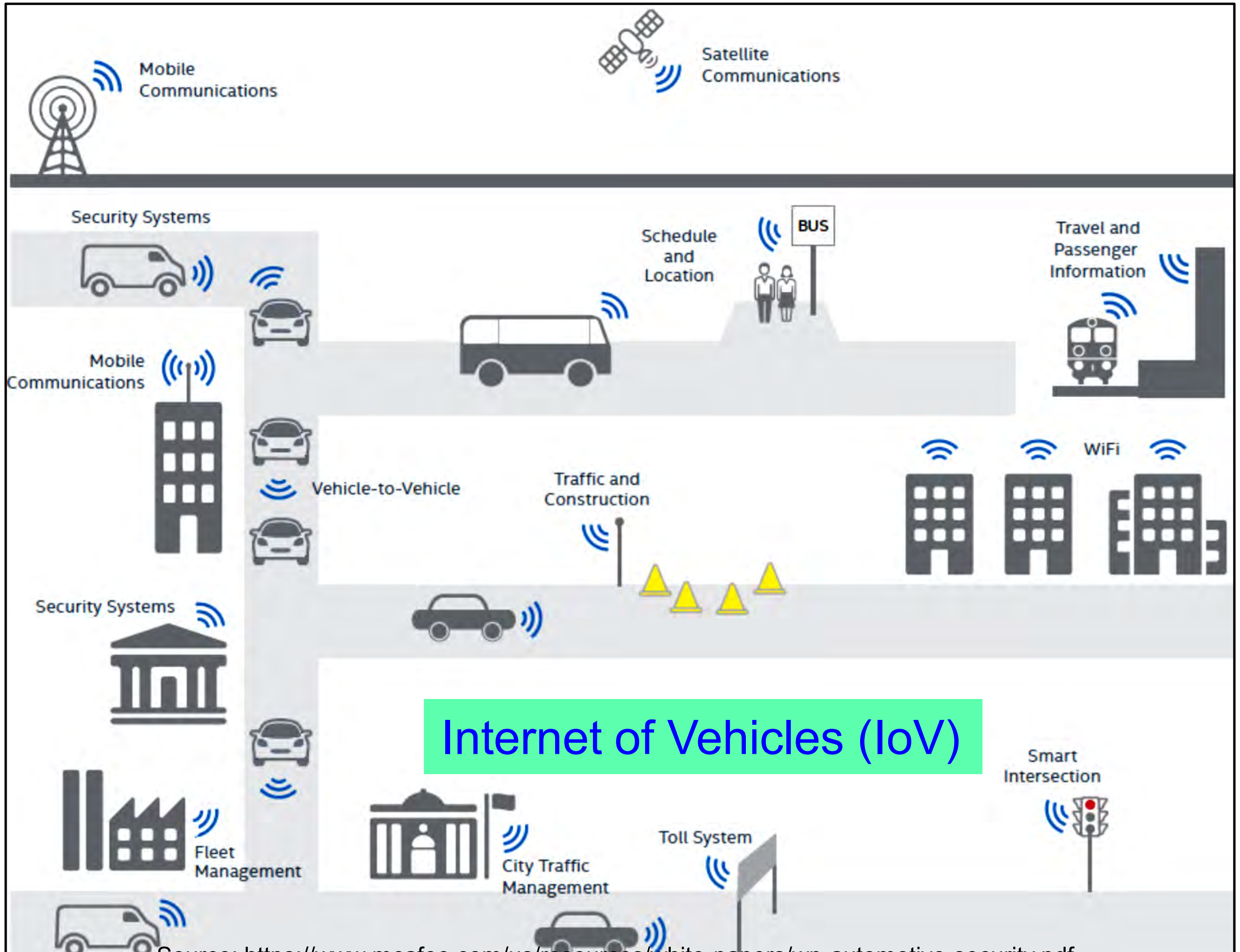
Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

Agriculture Cyber-Physical System (A-CPS)



Source: V. Udutalapally, S. P. Mohanty, V. Pallagani, and V. Khandelwal, "sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture", *IEEE Sensors Journal*, Vol. 21, No. 16, August 2021, pp. 17525--17538, DOI: 10.1109/JSEN.2020.3032438.

Transportation Cyber-Physical System (T-CPS)



Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

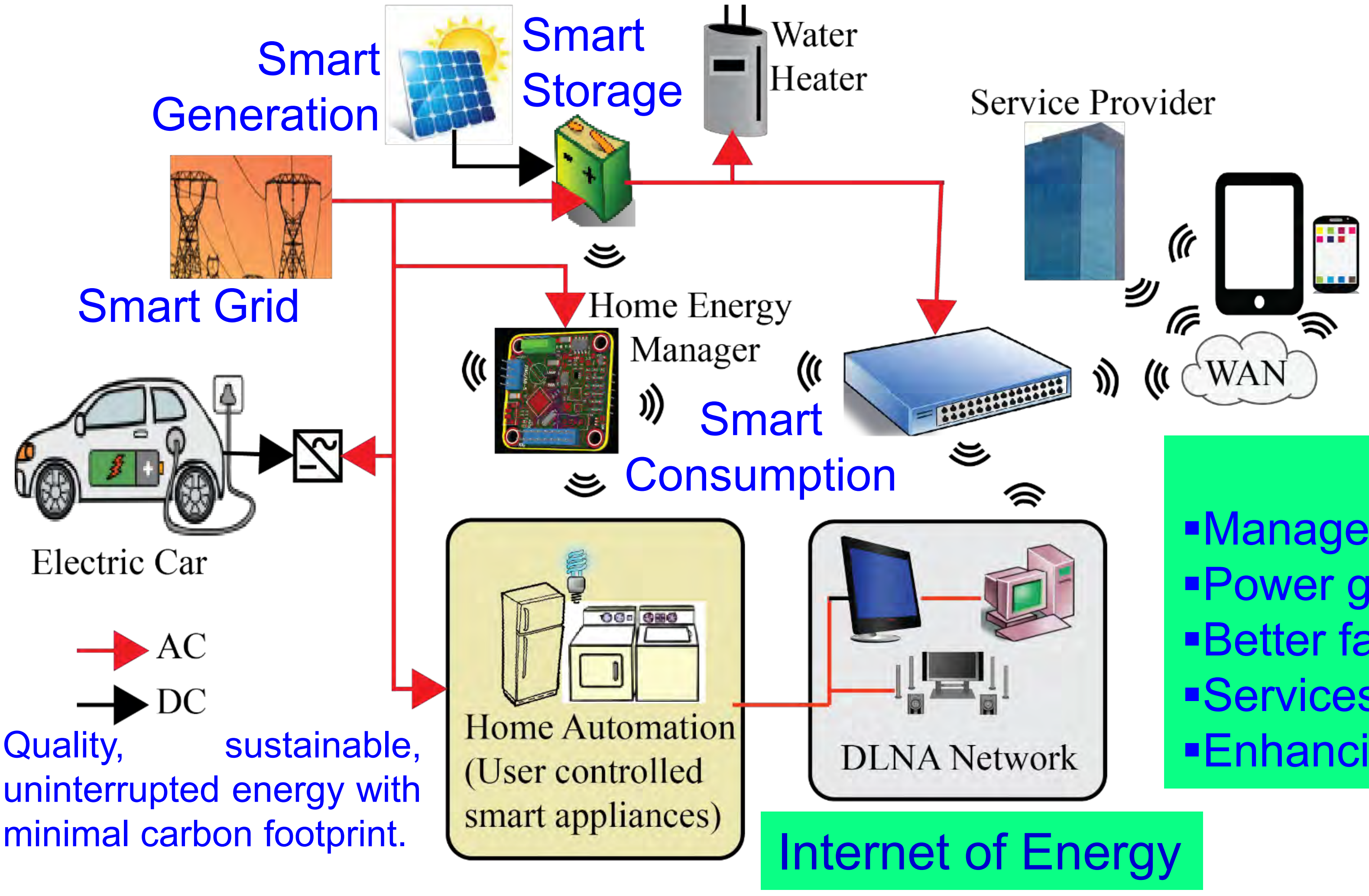
IoT Role Includes:
- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

Requires:
- ❖ Data, Device, and System Security
- ❖ Location Privacy

"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

Source: Datta 2017, CE Magazine Oct 2017

Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Requires:
- ❖ Data, Device, and System Security

IoT Role:
- ▪Management of energy usage
- ▪Power generation dispatch for solar, wind, etc.
- ▪Better fault-tolerance of the grid
- ▪Services for plug-in electric vehicles (PEV)
- ▪Enhancing consumer relationships

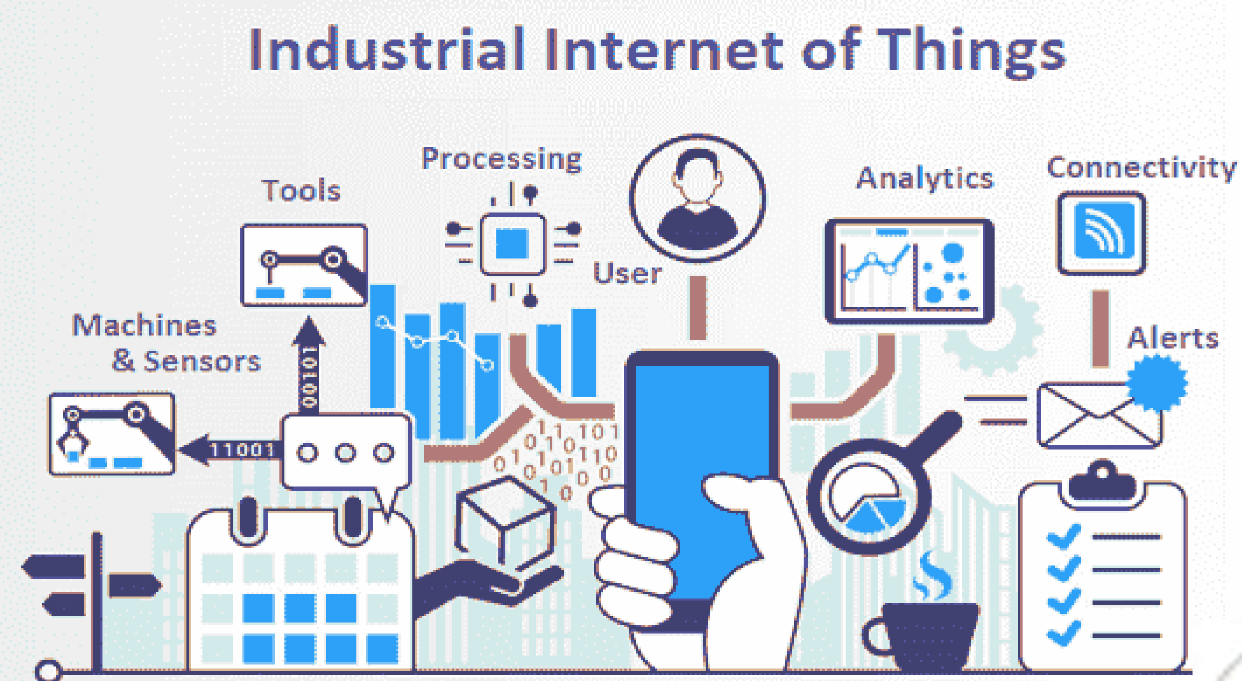
Source: S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything You wanted to Know about Smart Cities”, *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

Services in Smart Cities and Smart Village

In Smart Cities	In Smart Village	Communication Type	Energy Source	Feasibility
Waste Management	Waste Management	WiFi, Sigfox, Neul, LoRaWAN	Battery Powered and Energy Harvesting	Feasible but smart containers adds in cost
Air Quality Monitoring	Smart Weather and Irrigation	BLE, ZigBee, 6LoWPAN, WiFi, Cellular, Sigfox, LoRaWAN	Solar Panels, Battery Power and Energy Harvesting	Feasible
Smart Surveillance	NA	BLE, WiFi, ZigBee, Cellular, Sigfox, LoRaWAN	Battery Power and Energy Harvesting	Feasible but additional sensors needed
Smart Energy	Smart Energy	ZigBee, Z-Wave, 6LoWPAN, Sigfox, LoRaWAN	PowerGrid, Solar Power, Wind Power, Energy Harvesting	Feasible
Smart Lighting	Smart Lighting	WiFi, ZigBee, Z-Wave, Sigfox, LoRaWAN	Power Grid, Solar Power, Energy Harvesting	Feasible
Smart Healthcare	Smart Healthcare	BLE, Bluetooth, WiFi, Cellular, Sigfox	Power Grid, Battery Power, and Energy Harvesting	Feasible
Smart Education	Smart Education	LR-WPAN, WiFi and Ethernet	Power Grid, Battery Power, and Energy Harvesting	Feasible
Smart Parking	NA	Z-Wave, WiFi, Cellular, Sigfox, LoRaWAN	Power Grid, Solar Power, Energy Harvesting	Feasible
Structural Health Monitoring	NA	BLE, WiFi, ZigBee, 6LoW-PAN, Sigfox	Power Grid, Solar Power, Battery Power, Energy Harvesting	Energy harvesting can be useful for power specs
Noise Monitoring	NA	6LoWPAN, WiFi, Cellular	Battery Power, Energy Harvesting, and Energy Scavenging	Sound pattern identification is a bottleneck
NA	Smart Farming	BLE, Bluetooth, WiFi, 6LoW-PAN, Sigfox, LoRaWAN	Power Grid, Battery Power and Energy Harvesting	Feasible
NA	Smart Diary	Bluetooth, WiFi, ZigBee, 6LoWPAN, LoRaWAN	Power Grid, Battery Power and Energy Harvesting	Feasible

Source: S. K. Ram, B. B. Das, K. K. Mahapatra, S. P. Mohanty, and U. Choppali, “Energy Perspectives in IoT Driven Smart Villages and Smart Cities”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 19-28, DOI: 10.1109/MCE.2020.3023293.

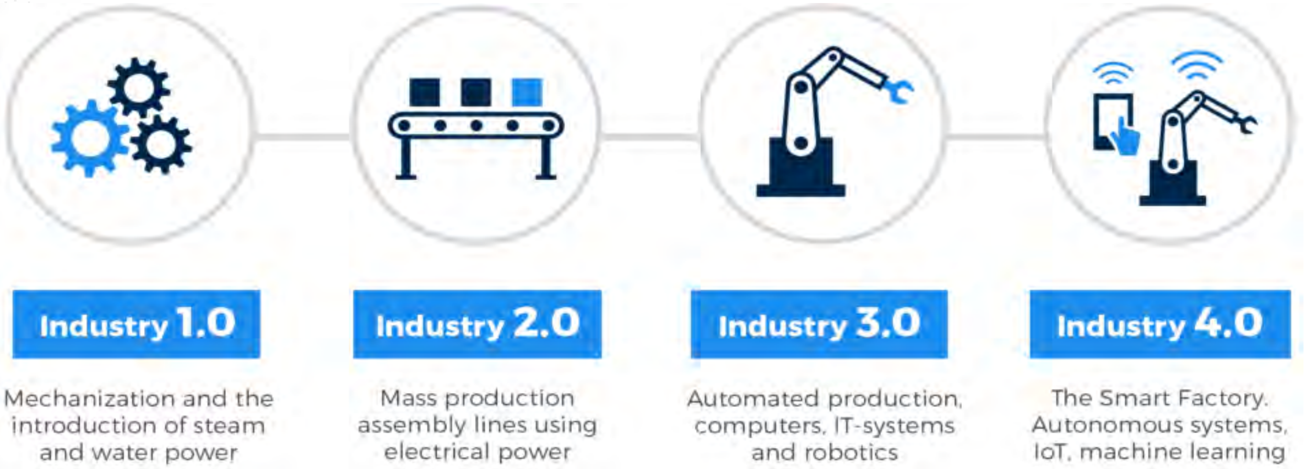
Industrial Internet of Things (IIoT)



Source: https://www.rfpage.com/applications-of-industrial-internet-of-things/

Applications

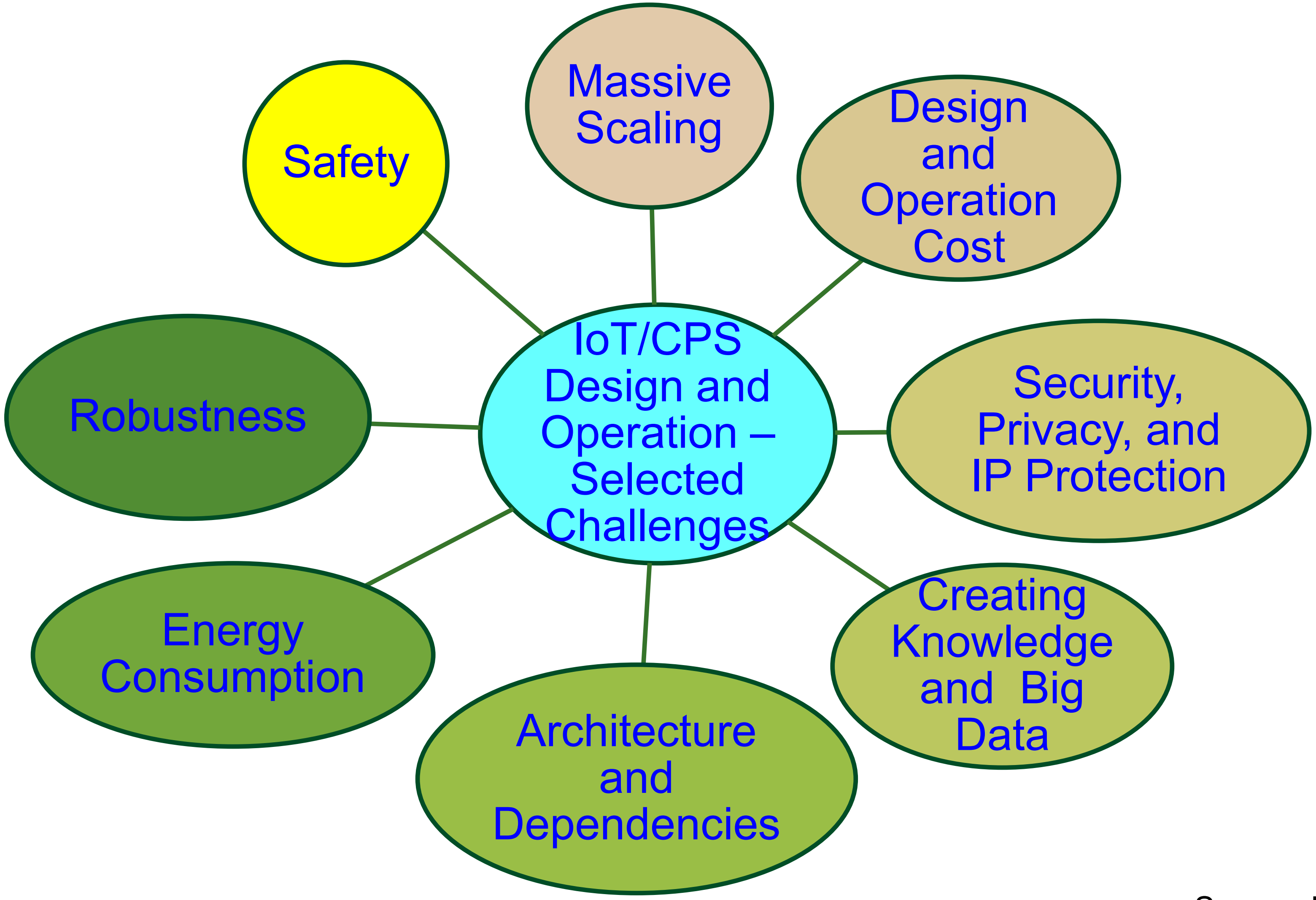
- Industrial Automation
- Smart Robotics
- Predictive Maintenance
- Integration of Tools / Wearables
- Smart Logistics



Source: https://www.spectralengines.com/articles/industry-4-0-and-how-smart-sensors-make-the-difference

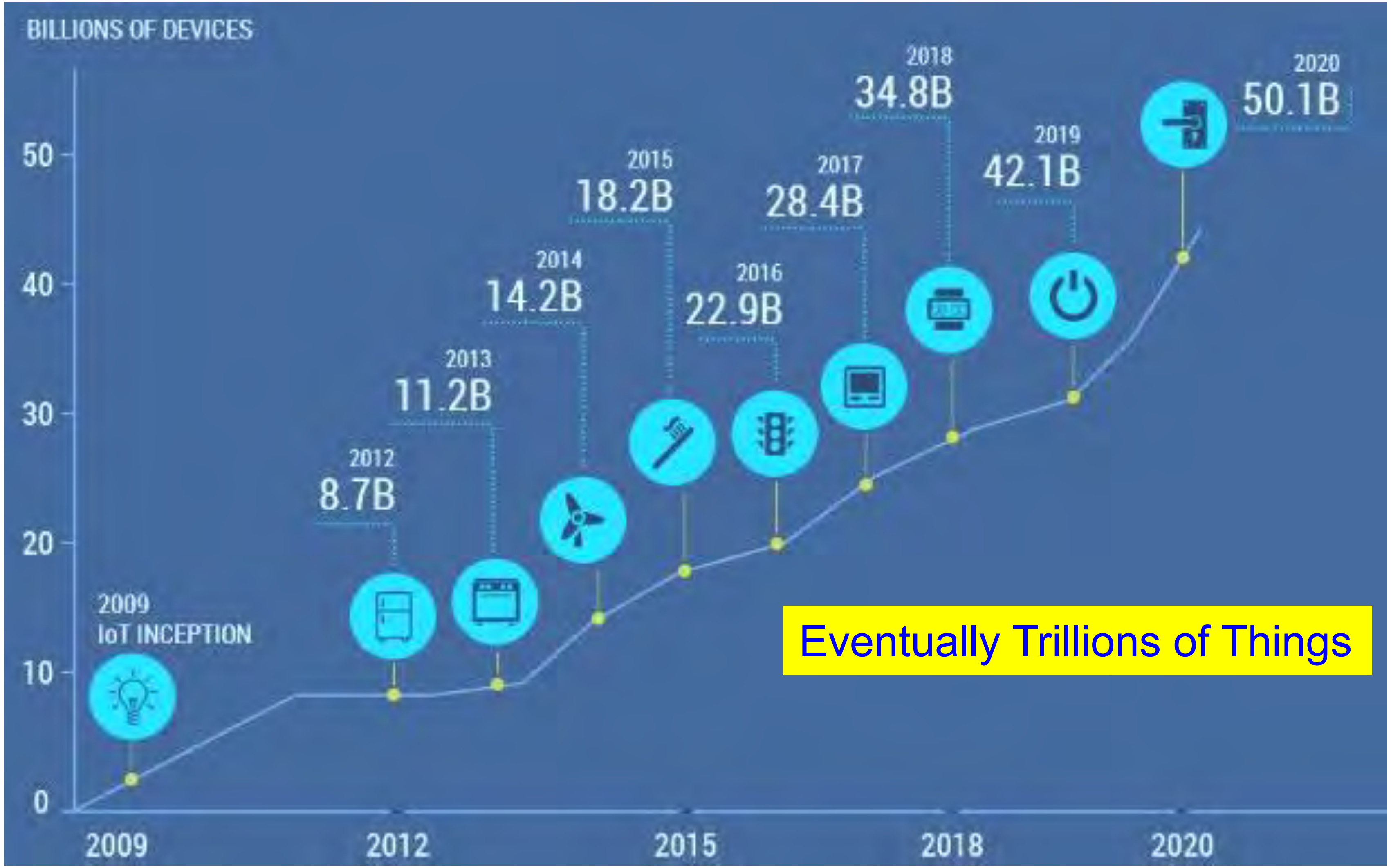
Challenges in IoT/CPS Design

IoT/CPS – Selected Challenges



Source: Mohanty ICIT 2017 Keynote

Massive Growth of Sensors/Things



Source: https://www.linkedin.com/pulse/history-iot-industrial-internet-sensors-data-lakes-0-downtime

Security – Information versus System

Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html

Security Challenges – Information

Online Banking

Credit Card Theft

Hacked: Linkedin, Tumbler, & Myspace

LinkedIn
tumblr.
myspace

Who did it: A hacker going by the name Peace.

What was done: 500 million passwords were stolen.

Details: Peace had the following for sale on a Dark Web Store:

- 167 million Linkedin passwords
- 360 million Myspace passwords
- 68 million Tumbler passwords
- 100 million VK.com passwords
- 71 million Twitter passwords

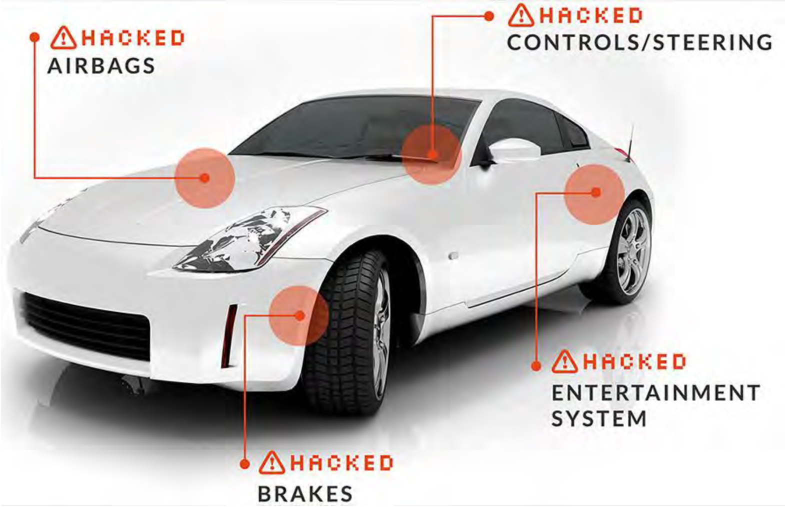
Personal Information

Credit Card/Unauthorized Shopping

Cybersecurity Challenges - System

Power Grid Attack

Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html

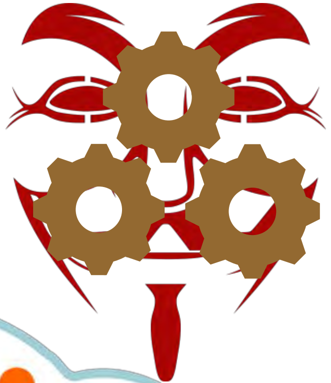


Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Attacks on IoT Devices

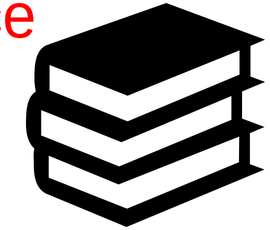
Impersonation Attack



Reverse Engineering Attack

Denial of Service Attack

Dictionary and Brute Force Attack



Eavesdropping Attack

Smart Healthcare - Cybersecurity and Privacy Issue

Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity
- Device Security

Impersonation Attacks

Eavesdropping Attacks

Smart Healthcare

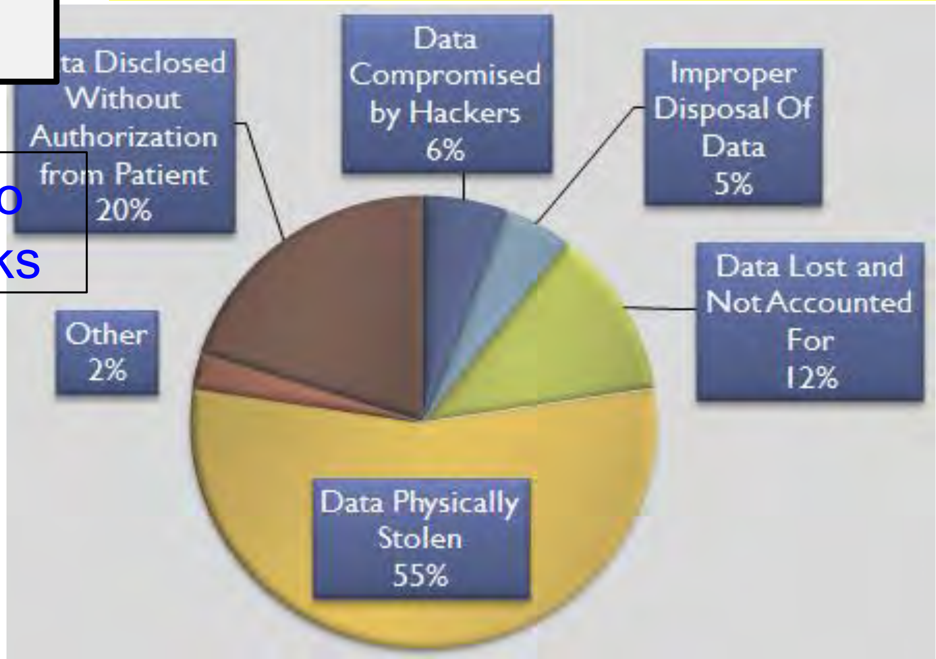
Reverse Engineering Attacks

Radio Attacks

HIPAA

Health Insurance Portability and Accountability Act

HIPPA Privacy Violation by Types



IoMT/H-CPS Security Issue is Real and Scary

- Insulin pumps are vulnerable to hacking, FDA warns amid recall:

https://www.washingtonpost.com/health/2019/06/28/insulin-pumps-are-vulnerable-hacking-fda-warns-amid-recall/

- Software vulnerabilities in some medical devices could leave them susceptible to hackers, FDA warns:

https://www.cnn.com/2019/10/02/health/fda-medical-devices-hackers-trnd/index.html

- FDA Issues Recall For Medtronic mHealth Devices Over Hacking Concerns:

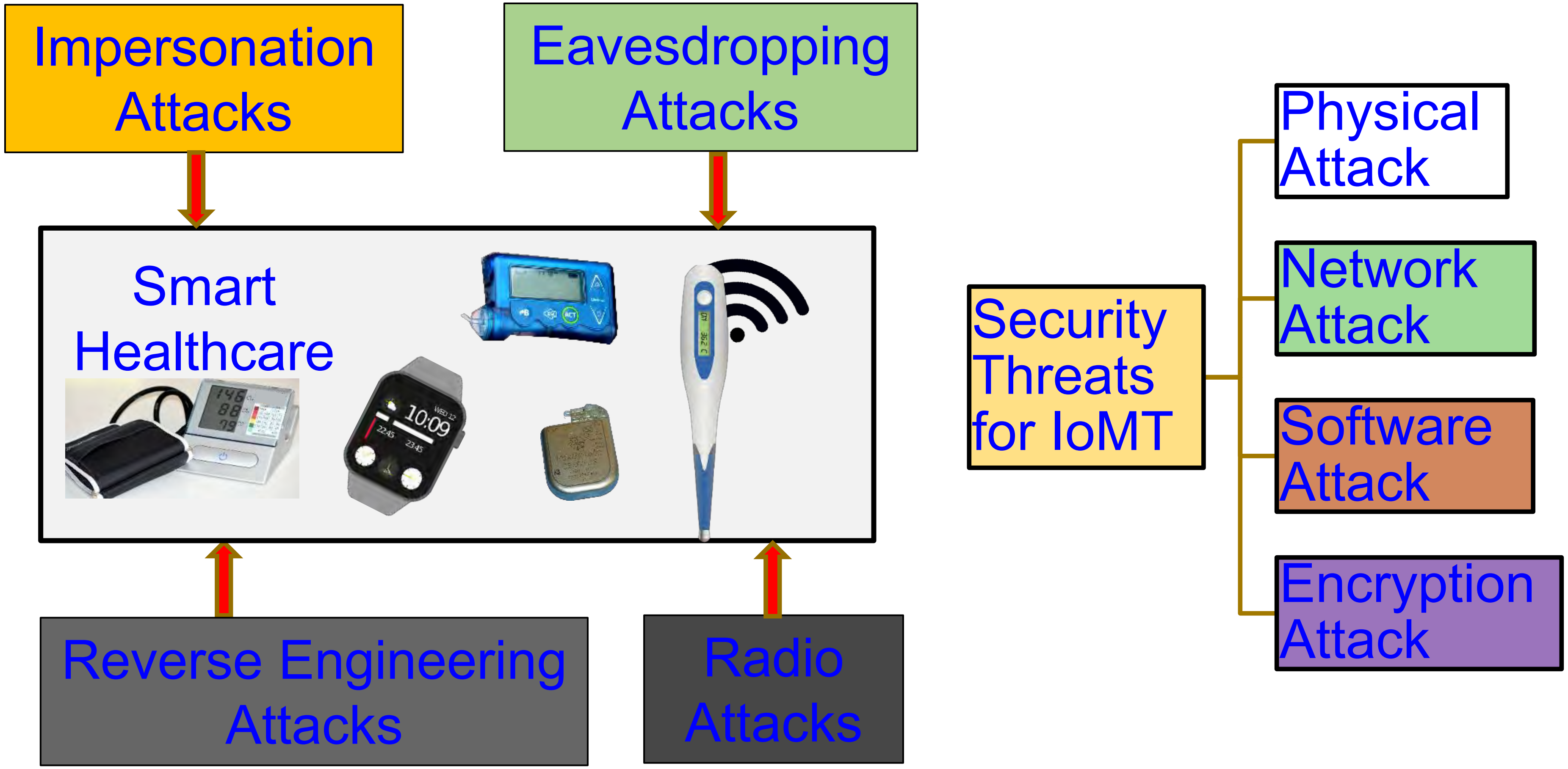
https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns

Implantable Medical Devices - Attacks

- The vulnerabilities affect implantable cardiac devices and the external equipment used to communicate with them.
- The devices emit RF signals that can be detected up to several meters from the body.
- A malicious individual nearby could conceivably hack into the signal to jam it, alter it, or snoop on it.

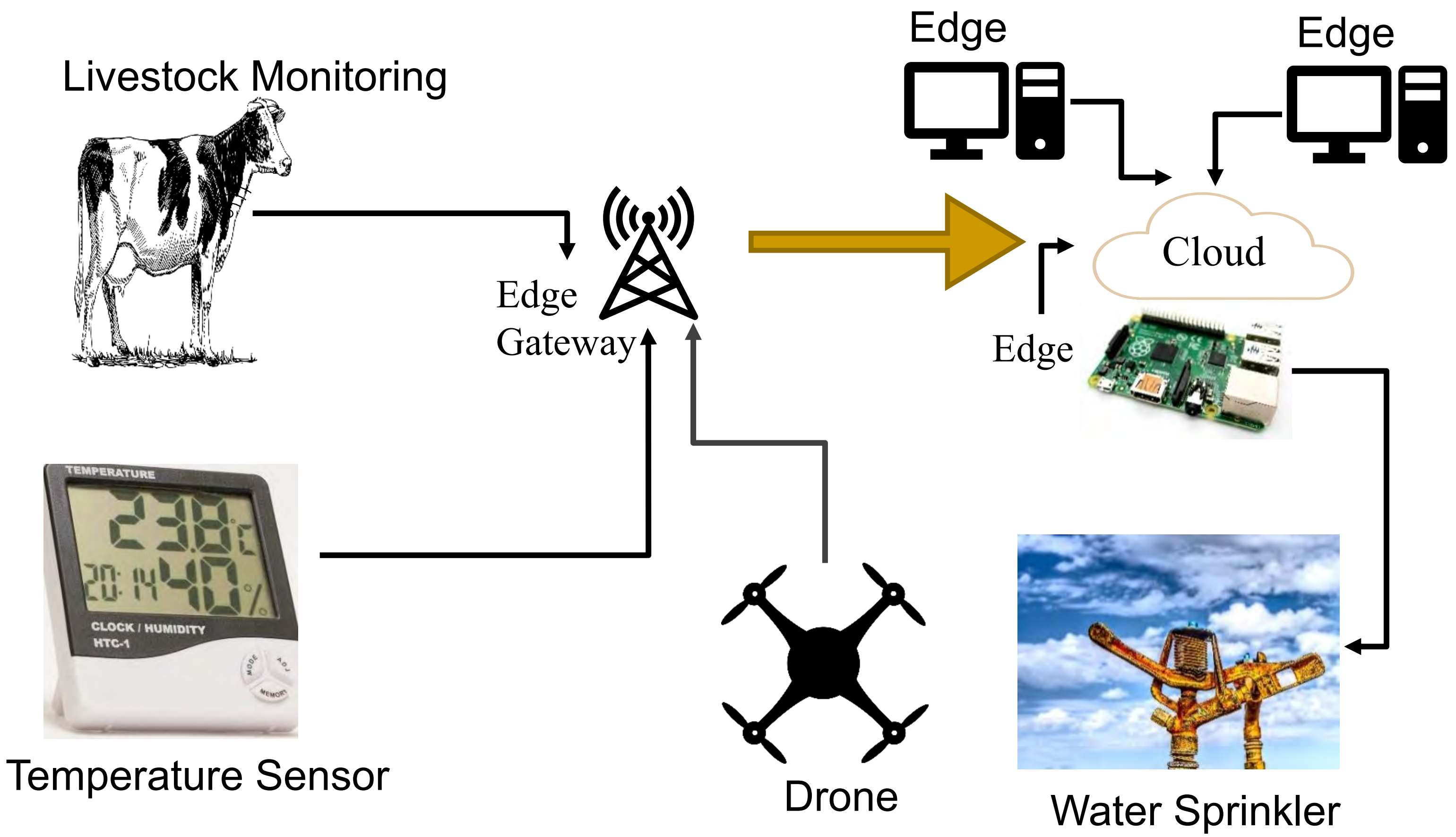
Source: Emily Waltz, Can "Internet-of-Body" Thwart Cyber Attacks on Implanted Medical Devices?, *IEEE Spectrum*, 28 Mar 2019, https://spectrum.ieee.org/the-human-os/biomedical/devices/thwart-cyber-attacks-on-implanted-medical-devices.amp.html.

IoMT Security – Selected Attacks



Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Broadview of Internet of Agro-Things (IoAT)



Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture,“ in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Security Issues in IoAT

- Smart Farms are Hackable Farms: IoT in Agriculture can improve the efficiency in productivity and feed 8.5 billion people by 2030. But it can also become vulnerable to various cyber security threats.

  https://spectrum.ieee.org/cybersecurity-report-how-smart-farming-can-be-hacked

  https://cacm.acm.org/news/251235-cybersecurity-report-smart-farms-are-hackable-farms/fulltext

- DHS report highlights that implementation of advanced precision farming technology in livestock monitoring and crop management sectors is also bringing new security issues along with efficiency

https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Smart Agriculture - Security Challenges

- Access Control
  - Develop farm specific access control mechanisms.
  - Develop data sharing and ownership policies.
- Trust
  - Prevent insider data leakage.
  - Zero day attack detection.
- Information Sharing
- Machine Learning and Artificial Intelligence Attacks
- Next Generation Network Security implementation
- Trustworthy Supply chain and Compliance

Source: M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564-34584.

Smart Agriculture - Security Challenges

- Harsh Environment
- Threats from equipment
  - High voltage pulses
  - Interference
- Unauthorized access
- Interception of node communication
- Malicious data attacks
- Control system intrusion

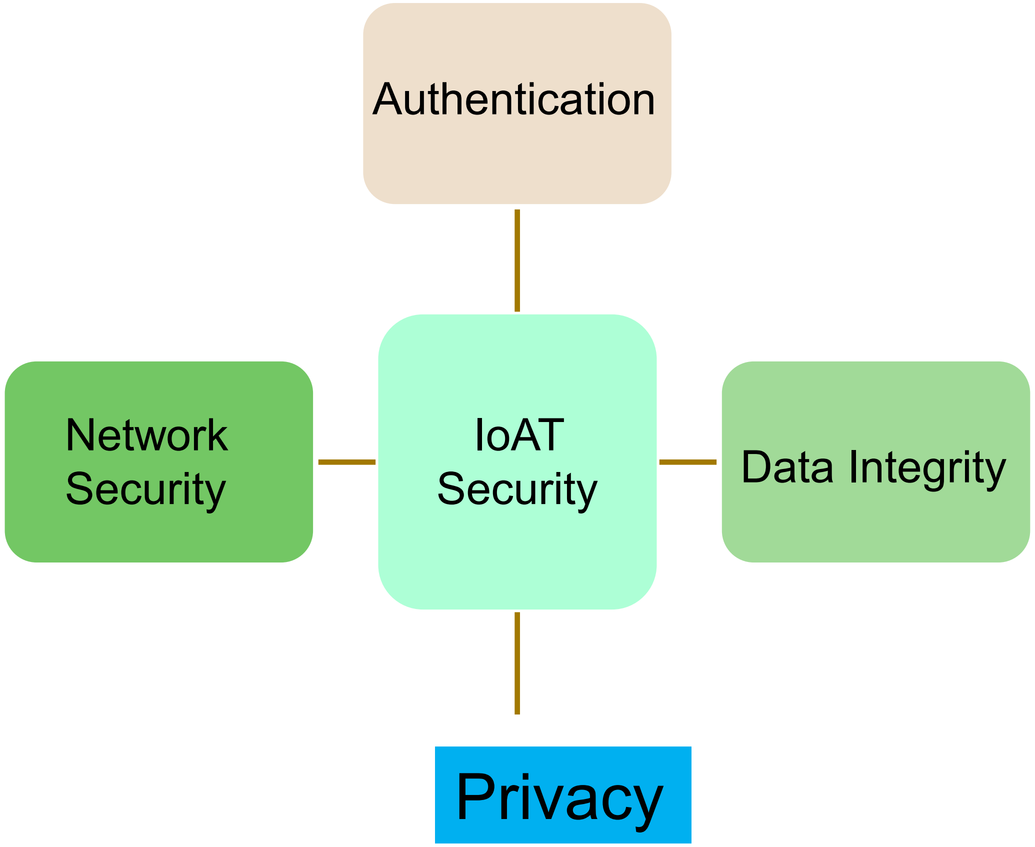
Source: X. Yang *et al*., "A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273-302,

Smart Agriculture - Security Challenges

- Cyber Attacks
  - Data Attacks
    - Insider Data Leakage
    - Cloud Data Leakage
    - False Injection
  - Network and Equipment Attacks
    - Radio Jamming
    - Malware Injection
    - Denial of Service
  - Supply Chain Attacks
    - Third Party Attack
    - Software Update Attacks
    - Data Fabrication
  - Other Attacks
    - Cloud Computing
    - Cyber Terrorism
    - Compliance and Regulation Invalidation

Source: M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564-34584

Cybersecurity Requirements for IoAT



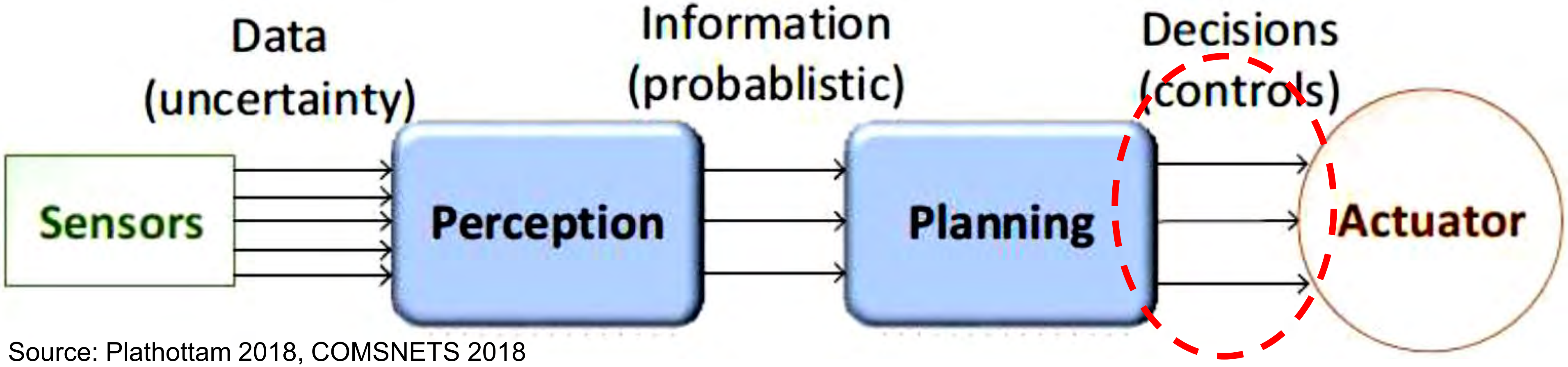
Internet of Agro-Things Characteristics:

- ✓ Smaller Size
- ✓ Smaller weight
- ✓ Safer Device
- ✓ Less Computational resources

Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Smart Car – Modification of Input Signal of Control Can be Dangerous

- Typically vehicles are controlled by human drivers
- Designing an Autonomous Vehicle (AV) requires decision chains.
- AV actuators controlled by algorithms.
- Decision chain involves sensor data, perception, planning and actuation.
- Perception transforms sensory data to useful information.
- Planning involves decision making.



Source: Plathottam 2018, COMSNETS 2018

Smart Grid Attacks can be Catastrophic

Threats	Vulnerabilities
Security group knowledge	Management deficiencies of network access rules; Inaccurate critical assests documentation
Information leakage	Unencrypted services in IT; Weak protection credentials
Access point	Improper access point; Remote access deficiency; Firewall filtering deficiency
Unpatched System	Unpatched operating system; Unpatched third party application
Weak cyber security	Buffer overflow in control system services; SQL injection vulnerability

Source of Threats

- Phishers
- Nation
- Hacker
- Insider
- Terrorist
- Spammers
- Spyware / Malware authors

Attacks

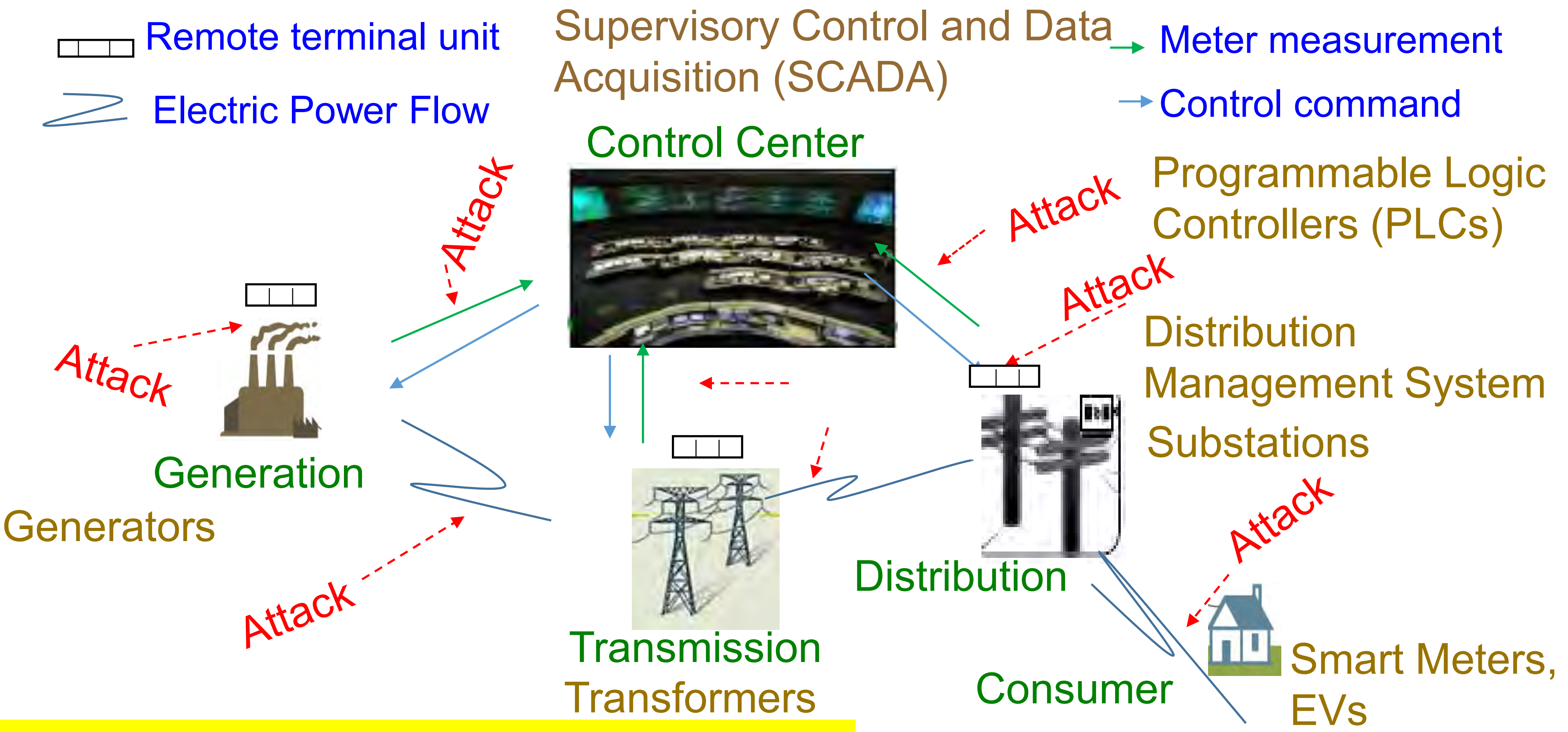
- Stuxnet
- Night Dragon
- Virus
- Denial of service
- Trojan horse
- Worm
- Zero day exploit
- Logical bomb
- Phishing
- Distributed DoS
- False data Injection

Impacts

- Ukraine power attack, 2015
- Stuxnet attack in Iran, 2010
- Browns Ferry plant, Alabama 2006
- Emergency shut down of Hatch Nuclear Power Plant, 2008
- Slammer attack at Davis-Besse power plant, 2001
- Attacks at South Korea NPP, 2015

Source: R. K. Kaur, L. K. Singh and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 10-15, Mar 2019.

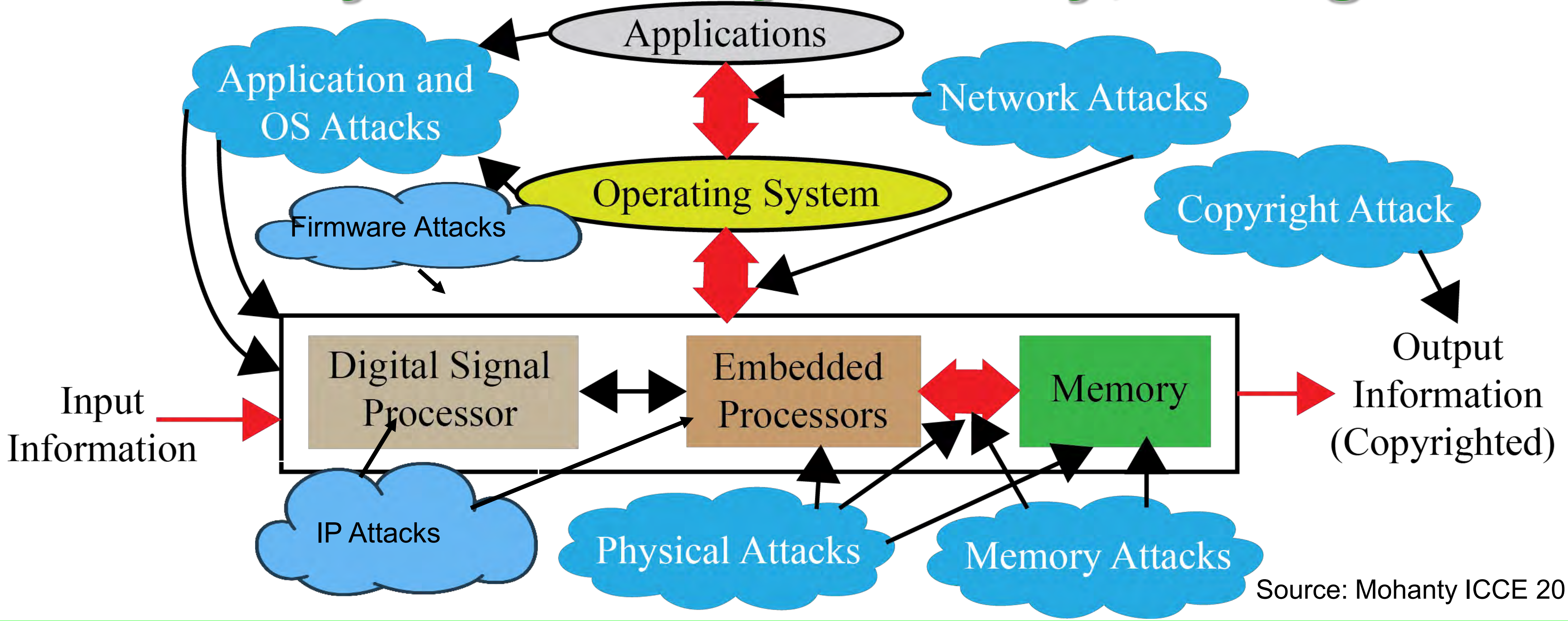
Smart Grid - Vulnerability



ICT components of smart grid is cyber vulnerable.

Source: (1) R. K. Kaur, L. K. Singh and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 10-15, March 2019.
(2)https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

Selected Attacks on an Electronic System – Cybersecurity, Privacy, IP Rights

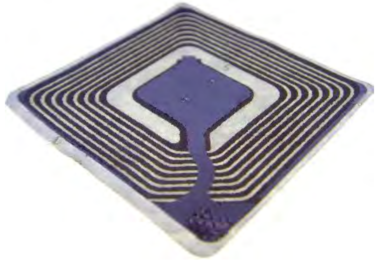


Source: Mohanty ICCE 2018 Keynote

Diverse forms of Attacks, following are not the same: System Security, Device Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

RFID Security - Attacks

- Selected RFID Attacks
  - Physical RFID Threats
    - Disabling Tags
    - Tag Modification
    - Cloning Tags
    - Reverse Engineering and Physical Exploration
  - RFID Channel Threats
    - Eavesdropping
    - Snooping
    - Skimming
    - Replay Attack
    - Relay Attacks
    - Electromagnetic Interference
  - System Threats
    - Counterfeiting and Spoofing Attacks
    - Tracing and Tracking
    - Password Decoding
    - Denial of Service (DoS) Attacks



Numerous Applications

Source: Khattab 2017: Springer 2017 RFID Security

NFC Security - Attacks

Selected NFC Attacks

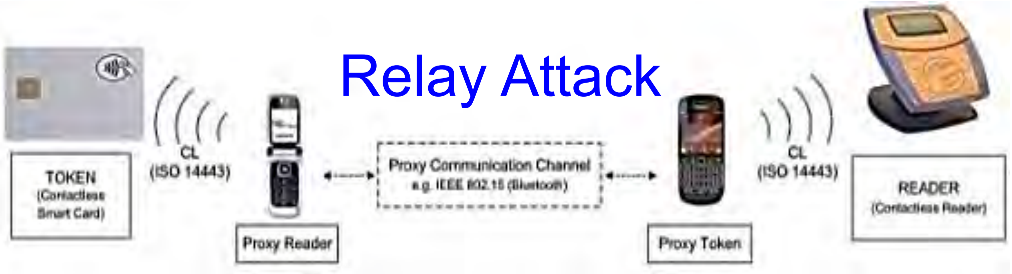
- Eavesdropping
- Data Modification
- Relay Attacks
- Data Corruption
- Spoofing
- Interception Attacks
- Theft

Source: http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497

Eavesdropping

Source: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

Relay Attack

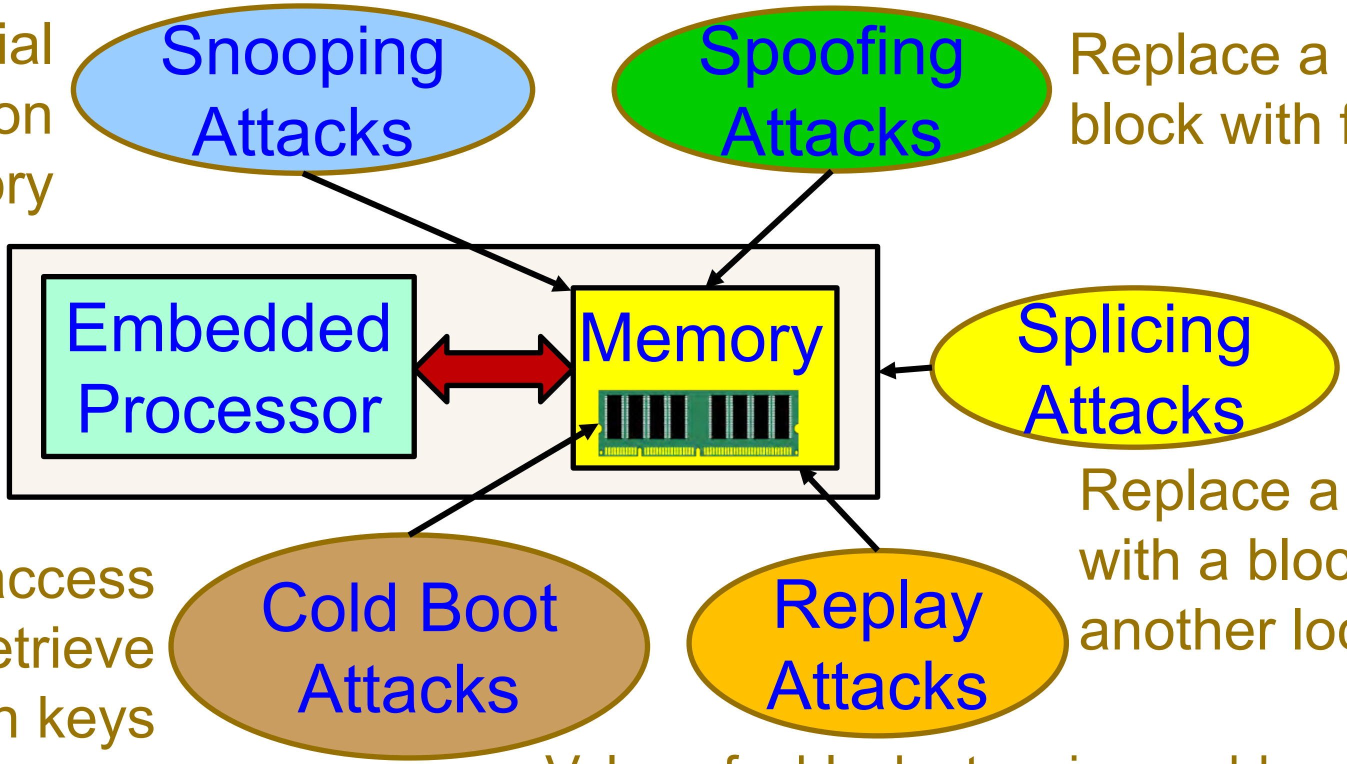


Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

Attacks on Embedded Systems' Memory

Read confidential information in memory

Replace a block with fake



Replace a block with a block from another location

Physical access memory to retrieve encryption keys

Value of a block at a given address at one time is written at exactly the same address at a different times; Hardest attack.

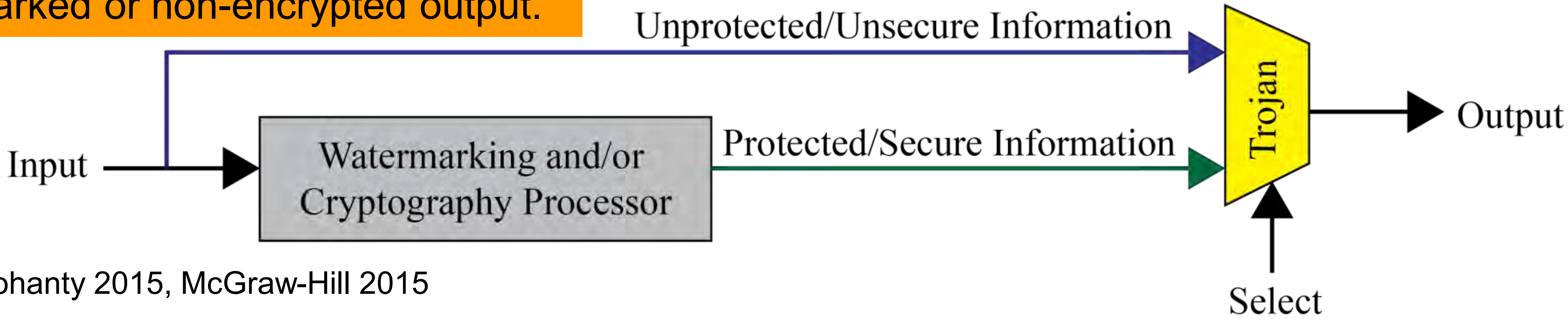
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "TSV: A Novel Energy Efficient Memory Integrity Verification Scheme for Embedded Systems", *Elsevier Journal of Systems Architecture*, Vol. 59, No. 7, Aug 2013, pp. 400-411.

Trojans can Provide Backdoor Entry to Adversary

Provide backdoor to adversary.
Chip fails during critical needs.

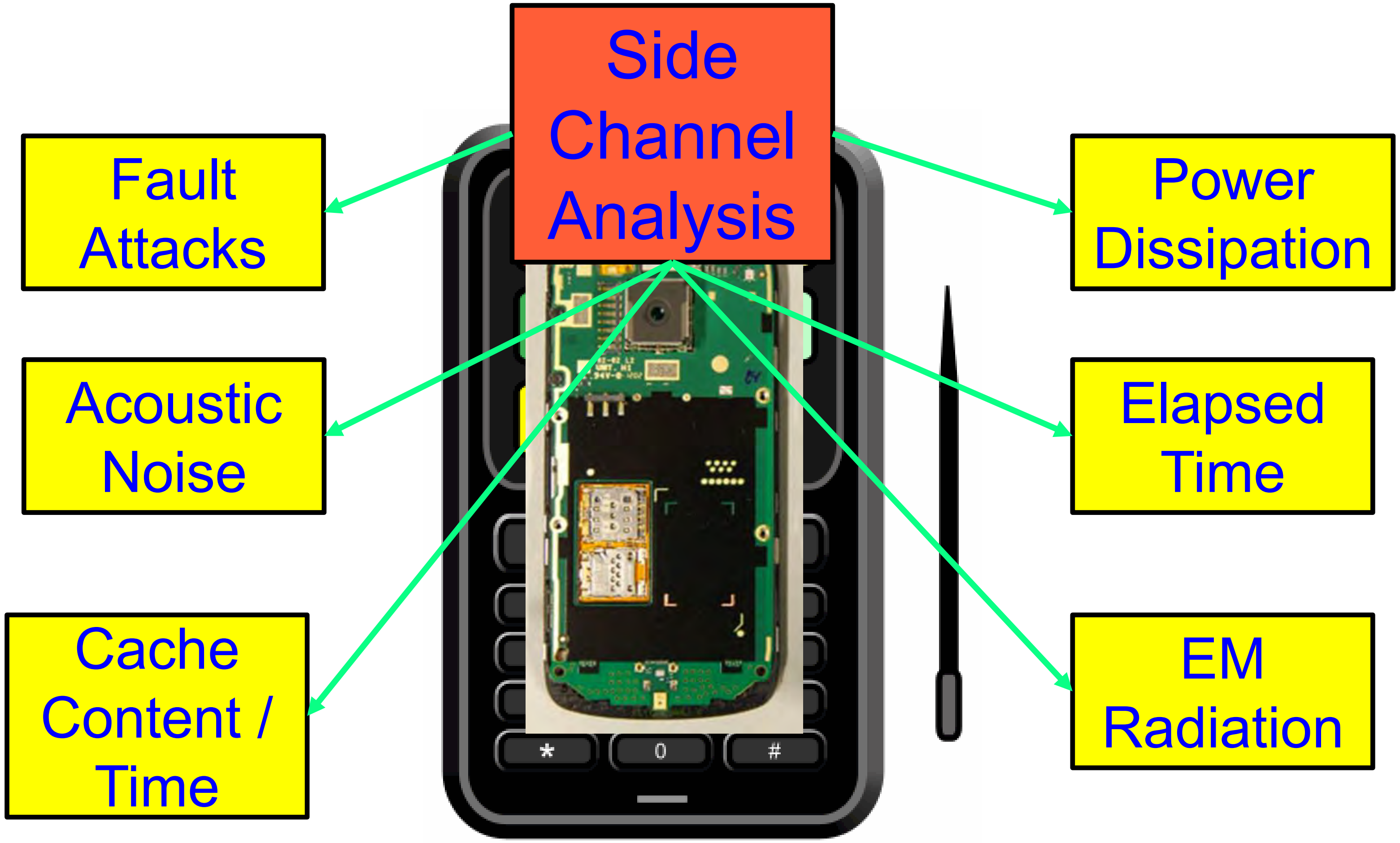
Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans



Source: Mohanty 2015, McGraw-Hill 2015

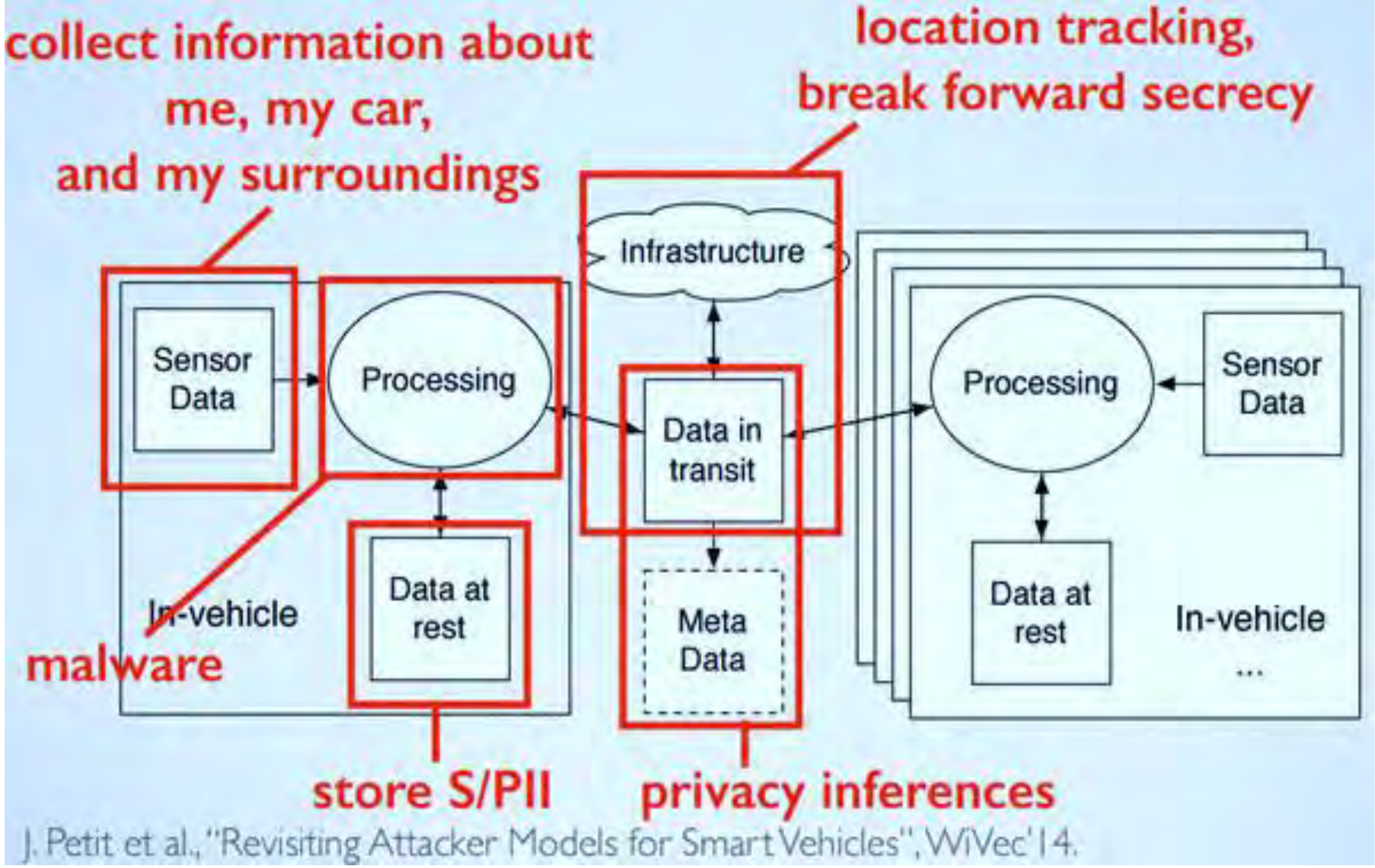
Side Channel Analysis Attacks

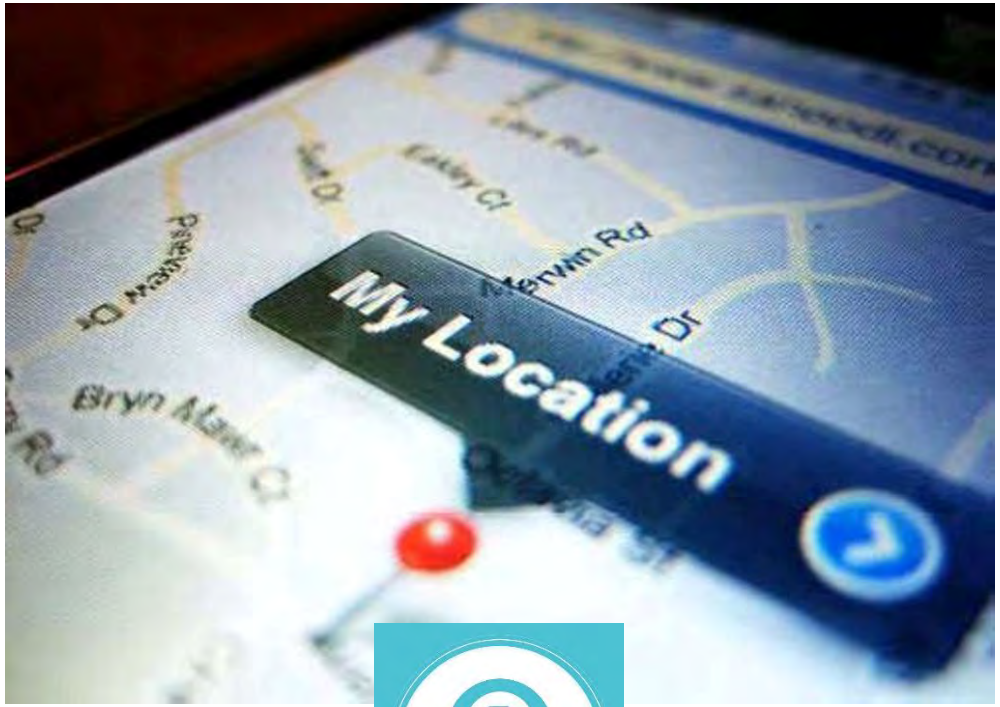


Breaking Encryption is not a matter of Years, but a matter of Hours.

Source: Parameswaran Keynote iNIS-2017

Privacy Challenge – System, Location



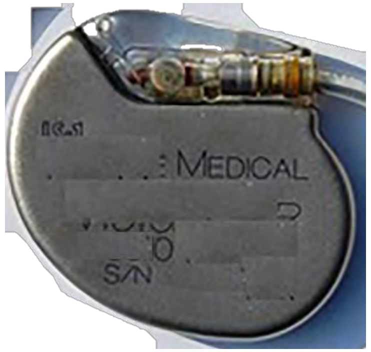


Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

Fake Data and Fake Hardware – Both are Equally Dangerous in CPS

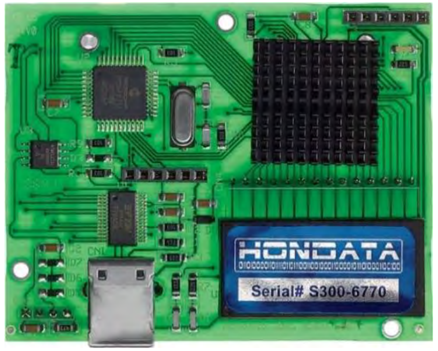
AI can be fooled by fake data

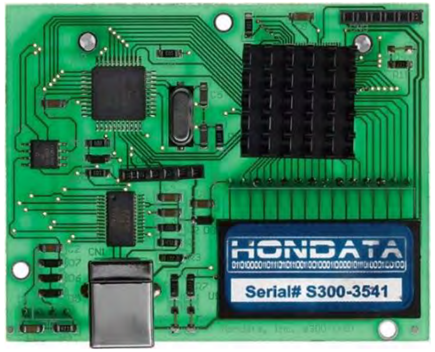
AI can create fake data (Deepfake)



Authentic Fake

An implantable medical device

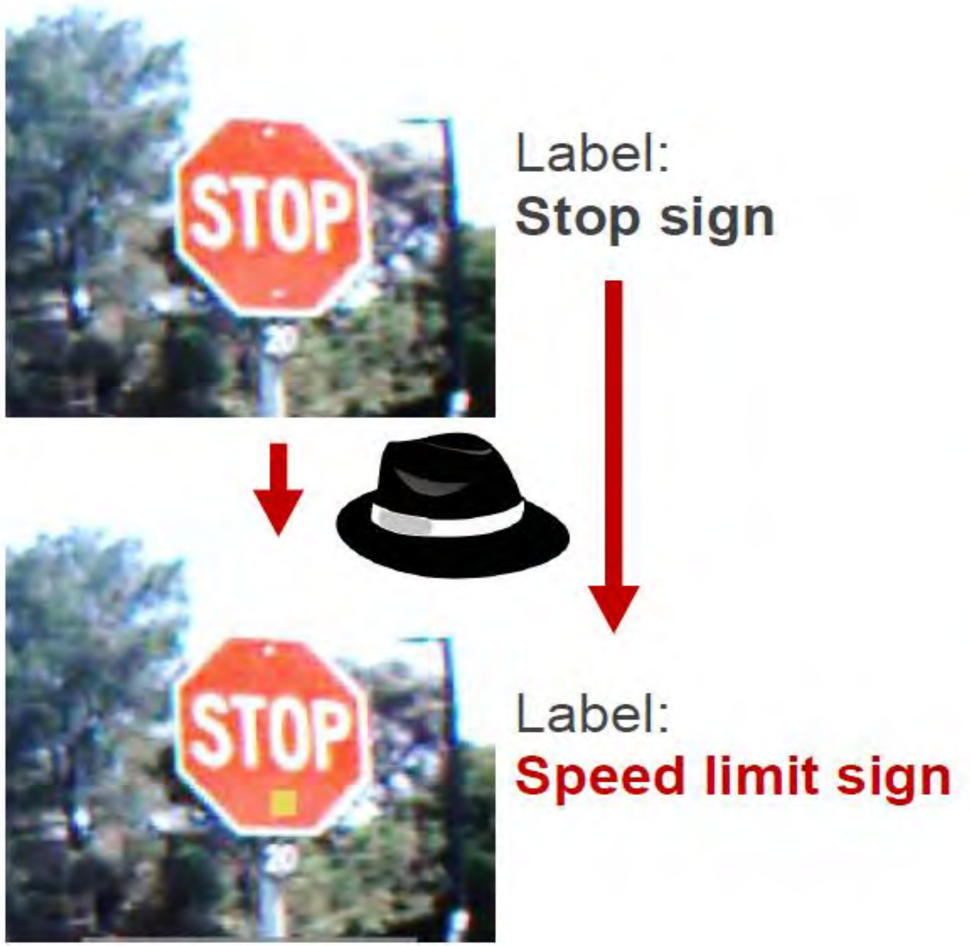




Authentic Fake

A plug-in for car-engine computers

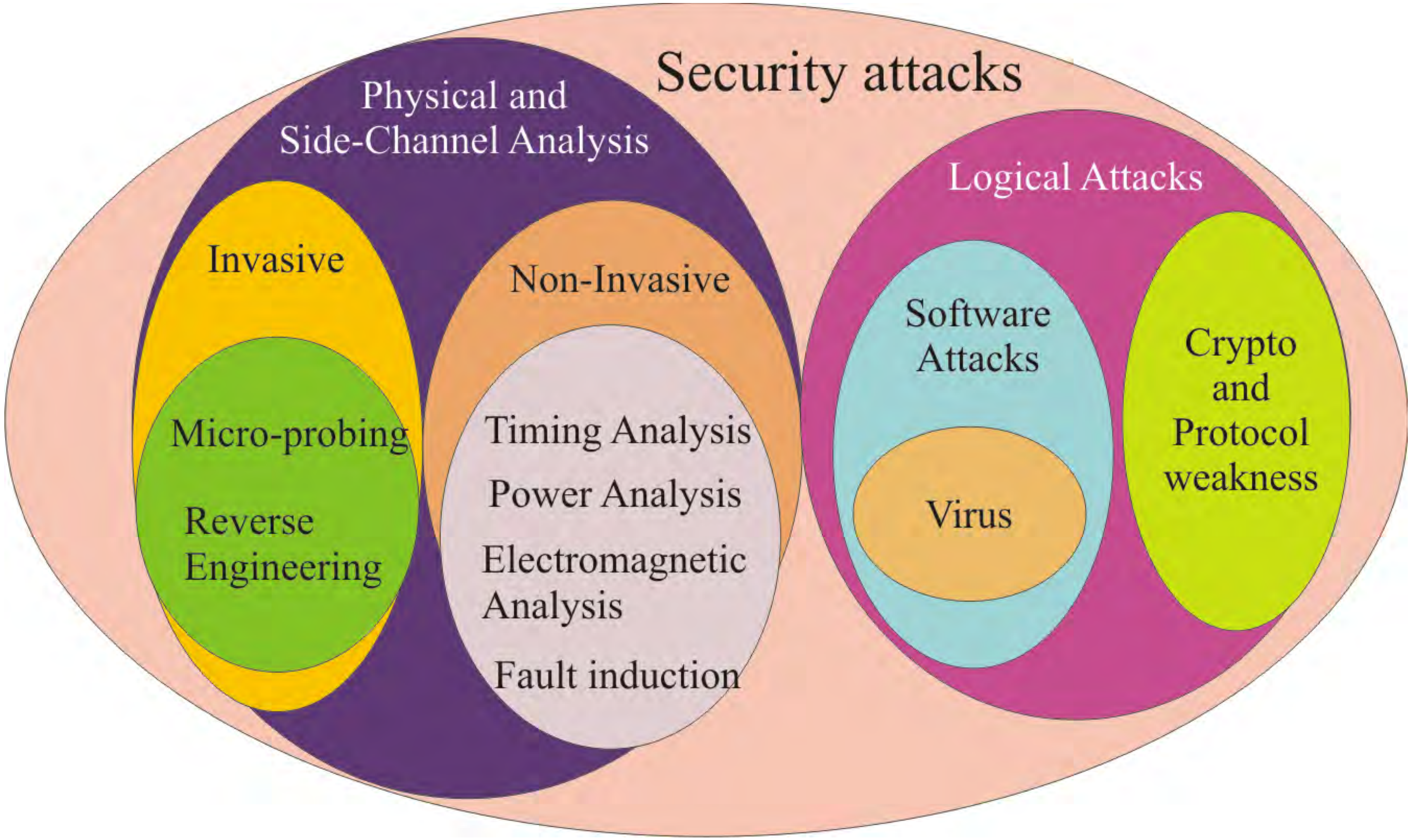
AI Security - Trojans in Artificial Intelligence (TrojAI)



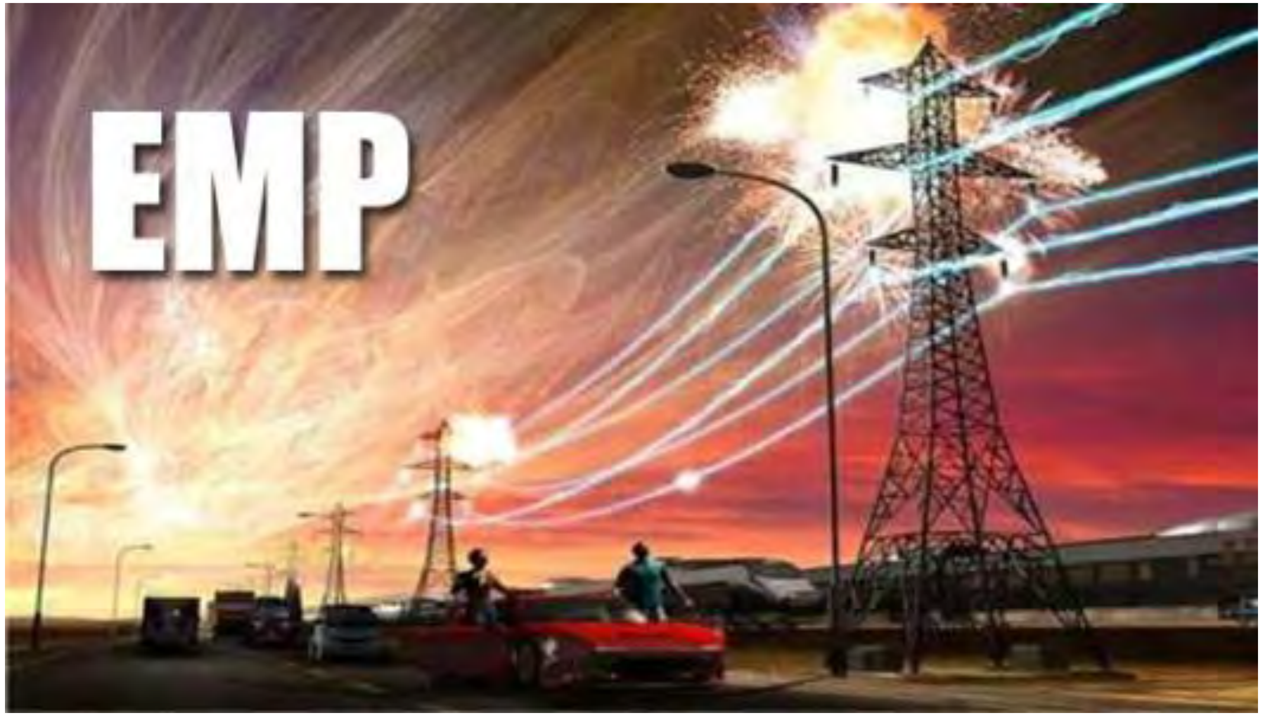
Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

Adversaries can insert **Trojans** into AIs, leaving a trigger for bad behavior that they can activate during the AI's operations

Different Attacks on a Typical Electronic System



Electromagnetic Pulse (EMP) Attack



- An electromagnetic pulse (EMP) is the electric wave produced by nuclear blasts which can knocking out electronics and the electrical grid as far as 1,000 miles away.
- The disruption could cause catastrophic damage and loss of life if power is not restored or backed up quickly.

Source: http://bwcentral.org/2016/06/an-electromagnetic-pulse-emp-nuclear-attack-may-end-modern-life-in-america-overnight/

Cybrsecurity Solution for IoT/CPS

IoT Cybersecurity - Attacks and Countermeasures

Edge nodes	Computing nodes	
	RFID tags	
Communication		
Edge computing		

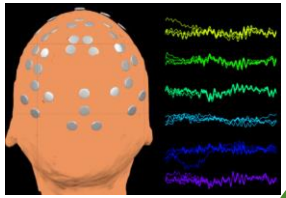
Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
Denial of Service (DoS)	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non-standard frameworks and inadequate testing	All
Insufficient/Inessential logging	C,AC,NR,P

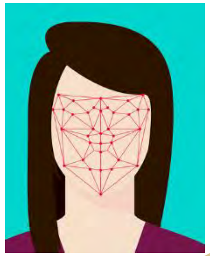
Countermeasures
Side-channel signal analysis
Trojan activation methods
Intrusion Detection Systems (IDSs)
Securing firmware update
Circuit/design modification
Kill/sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De-patterning and Decentralization
Role-based authorization
Information Flooding
Pre-testing
Outlier detection

C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

Security, Authentication, Access Control – Home, Facilities, ...



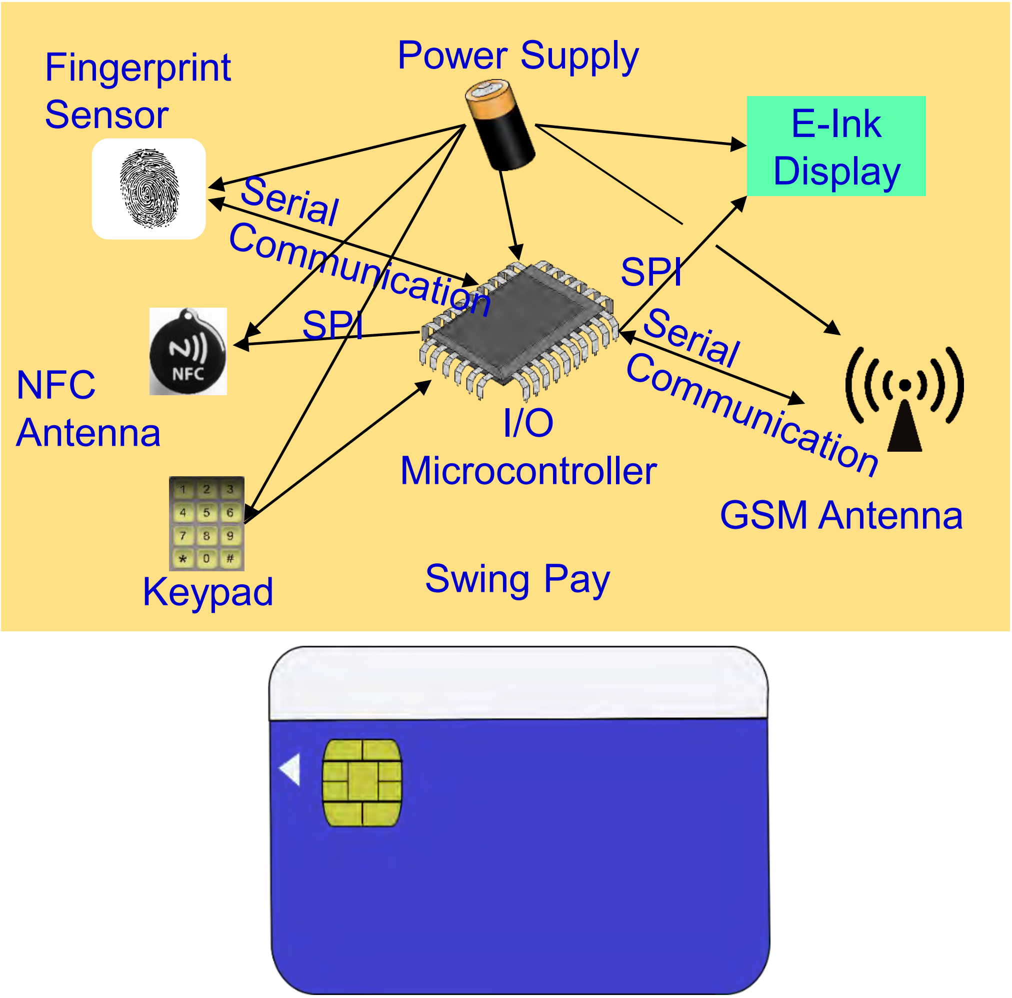


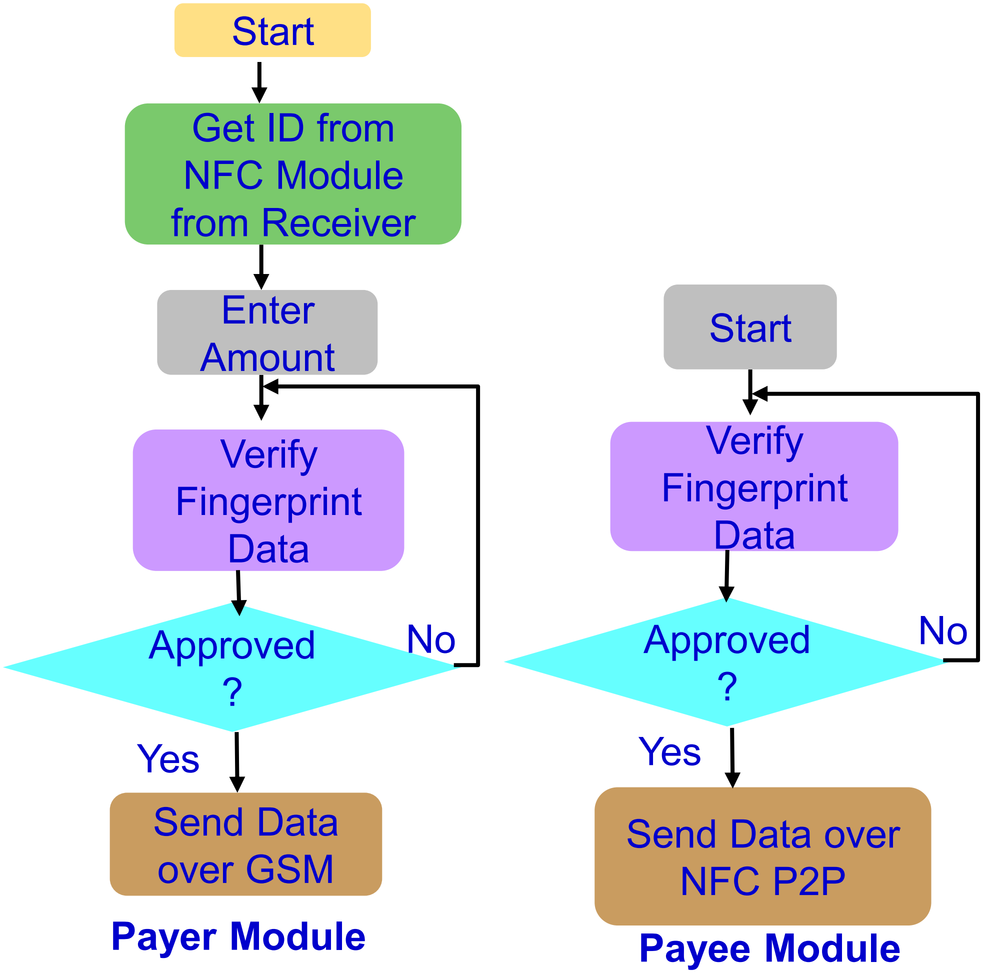
Security Methods (Authentication)

- Finger Vein
- Facial Recognition
- Fingerprint
- Personal Identification Number (PIN)
- Password
- Touch-Screen Pattern
- Online Signature
- Electrocardiography (ECG)
- Electroencephalography (EEG)

Source: Mohanty ISCT 2019 Keynote

Our Swing-Pay: NFC Cybersecurity Solution





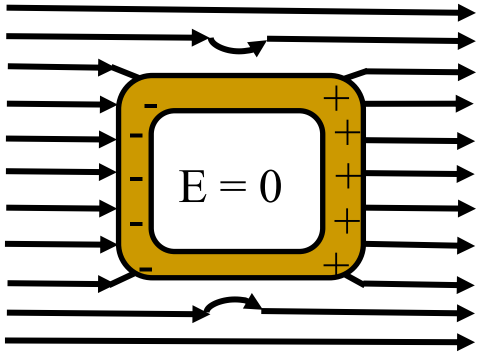
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

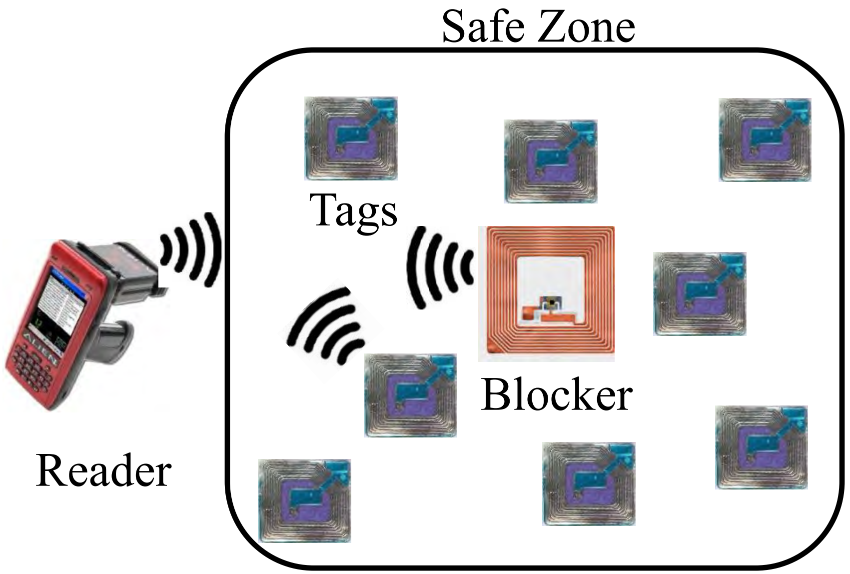
RFID Cybersecurity - Solutions

Selected RFID Security Methods

- Killing Tags
- Sleeping Tags
- Faraday Cage
- Blocker Tags
- Tag Relabeling
- Minimalist Cryptography
- Proxy Privacy Devices

Faraday Cage

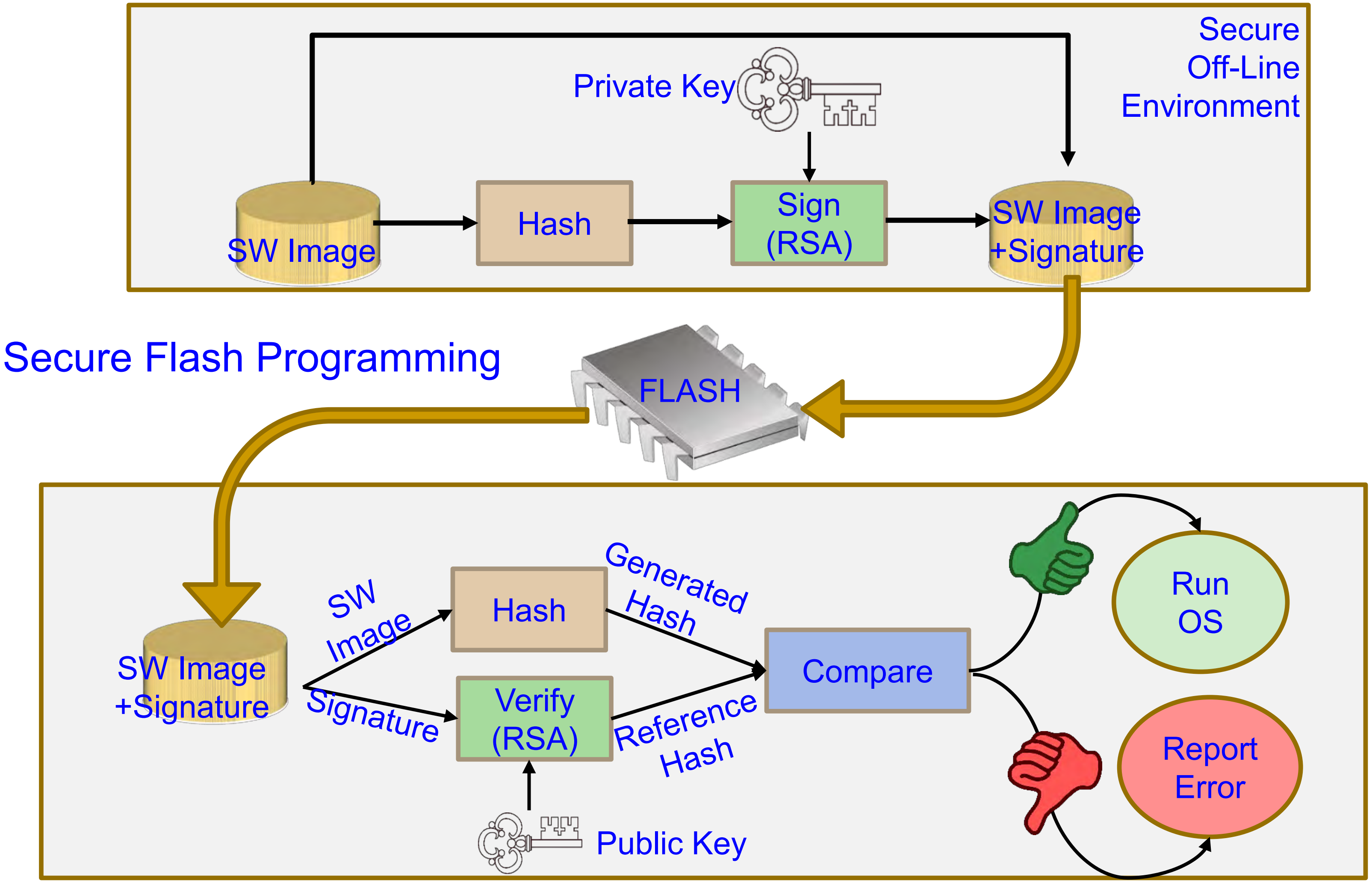




Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

Firmware Cybersecurity - Solution



Source: https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

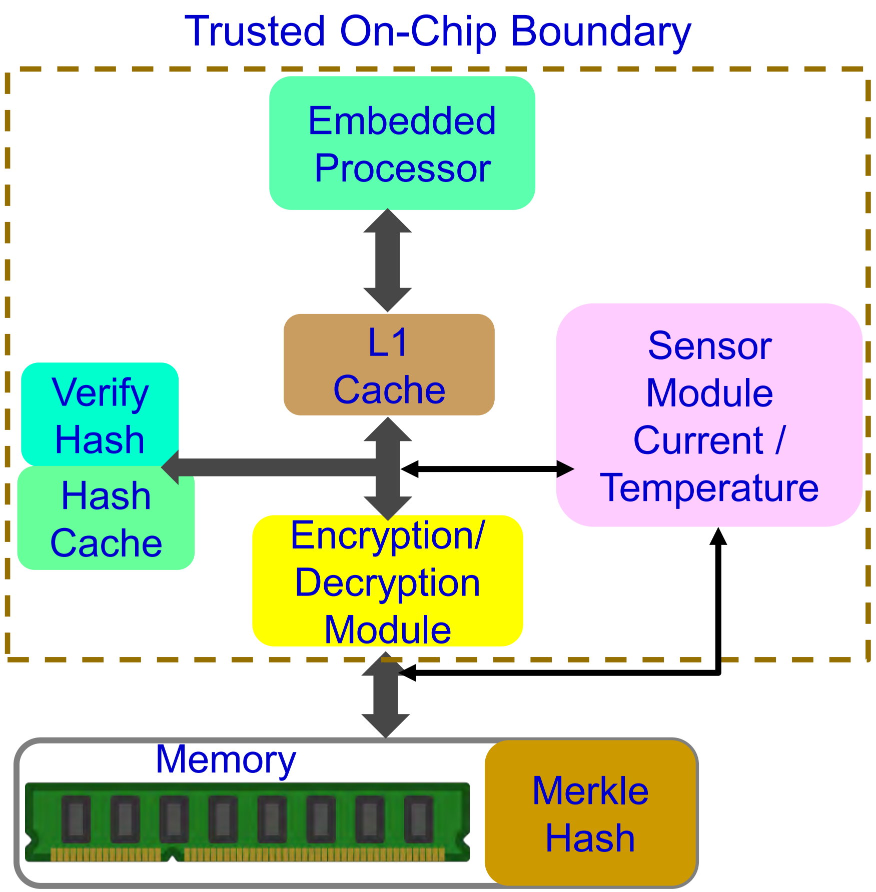
Nonvolatile / Harddrive Storage

Hardware-based encryption of data secured/protected by strong password/PIN authentication.

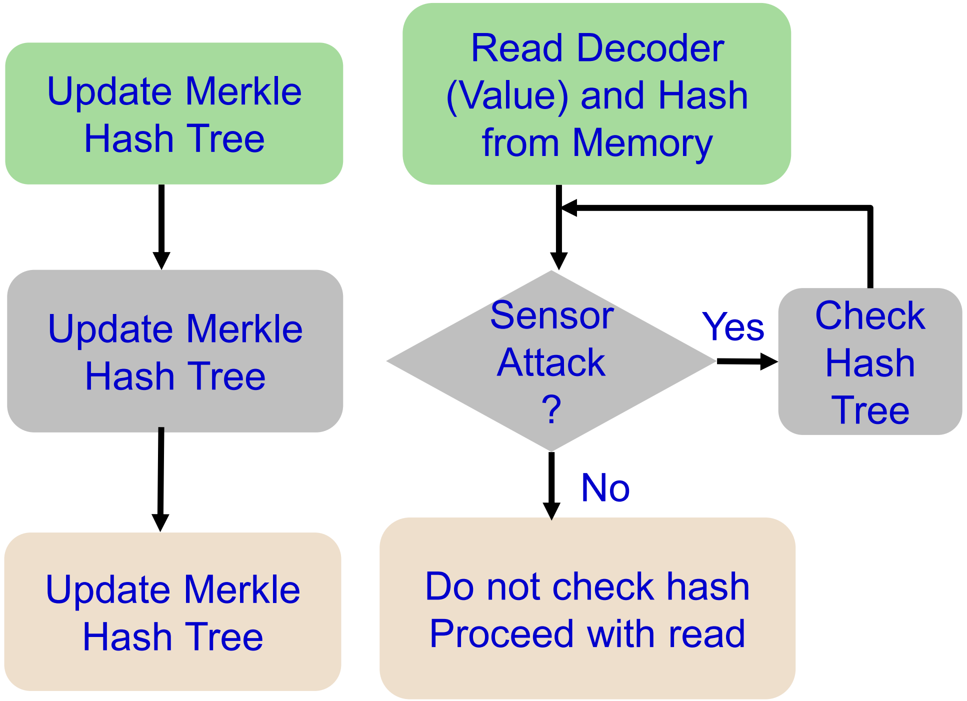
Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

Embedded Memory Security



On-Chip/On-Board Memory Protection



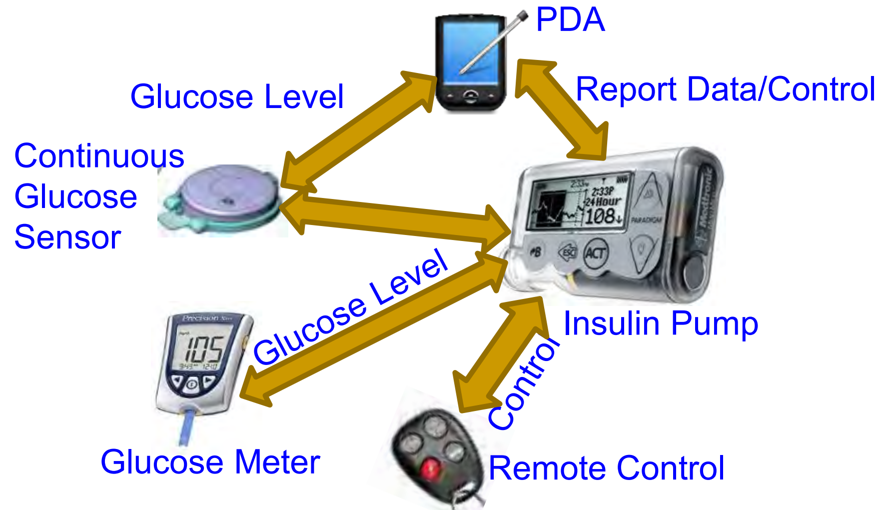
Write Operation

Read Operation

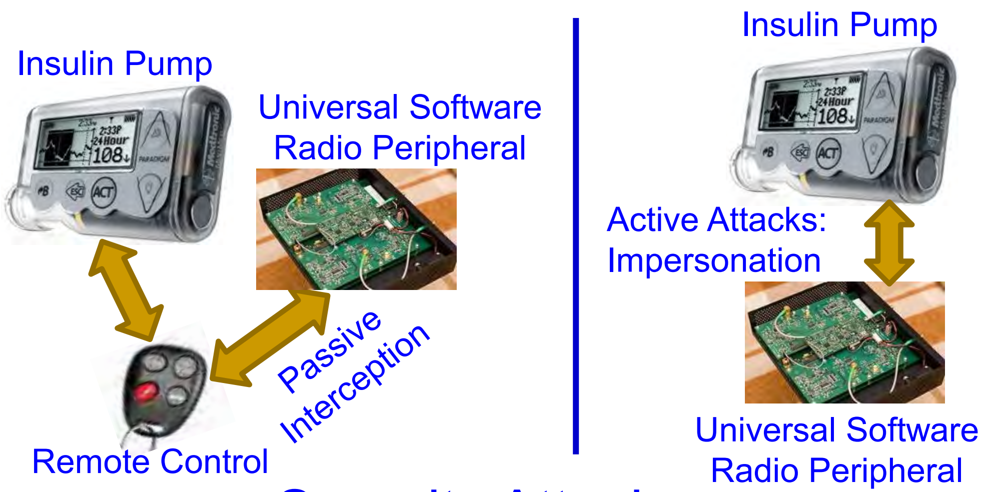
Memory integrity verification with 85% energy savings with minimal performance overhead.

Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "MEM-DnP: A Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems", *Springer Circuits, Systems, and Signal Processing Journal (CSSP)*, Volume 32, Issue 6, December 2013, pp. 2581--2604.

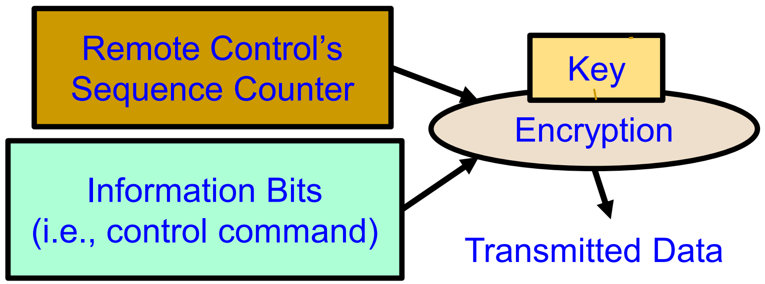
Smart Healthcare Cybersecurity



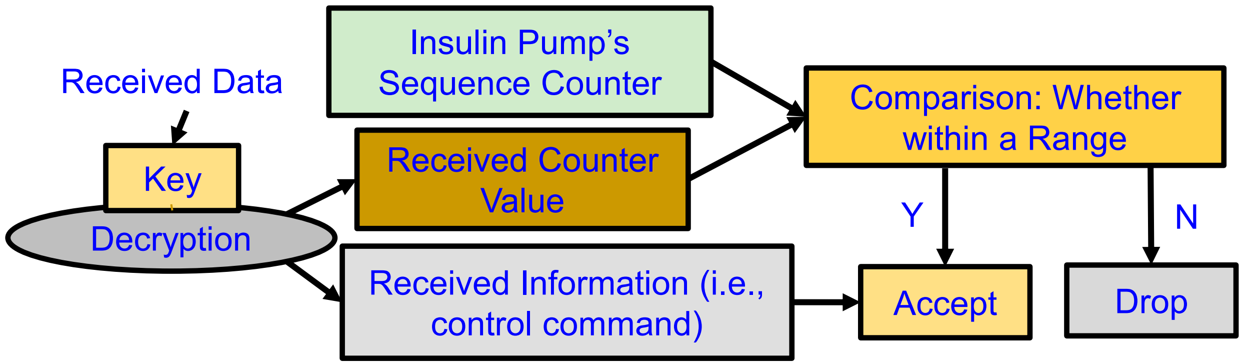
Insulin Delivery System



Security Attacks



Rolling Code Encoder in Remote Control



Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

Drawbacks of Existing Cybersecurity Solutions

IoT/CPS Cybersecurity Solutions – Advantages and Disadvantages

Analysis of selected approaches to security and privacy issues in CE.

Category	Current Approaches	Advantages	Disadvantages
Confidentiality	Symmetric key cryptography	Low computation overhead	Key distribution problem
	Asymmetric key cryptography	Good for key distribution	High computation overhead
Integrity	Message authentication codes	Verification of message contents	Additional computation overhead
Availability	Signature-based authentication	Avoids unnecessary signature computations	Requires additional infrastructure and rekeying scheme
Authentication	Physically unclonable functions (PUFs)	High speed	Additional implementation challenges
	Message authentication codes	Verification of sender	Computation overhead
Nonrepudiation	Digital signatures	Link message to sender	Difficult in pseudonymous systems
Identity privacy	Pseudonym	Disguise true identity	Vulnerable to pattern analysis
	Attribute-based credentials	Restrict access to information based on shared secrets	Require shared secrets with all desired services
Information privacy	Differential privacy	Limit privacy exposure of any single data record	True user-level privacy still chal-lenging
	Public-key cryptography	Integratable with hardware	Computationally intensive
Location privacy	Location cloaking	Personalized privacy	Requires additional infrastructure
Usage privacy	Differential privacy	Limit privacy exposure of any single data record	Recurrent/time-series data challenging to keep private

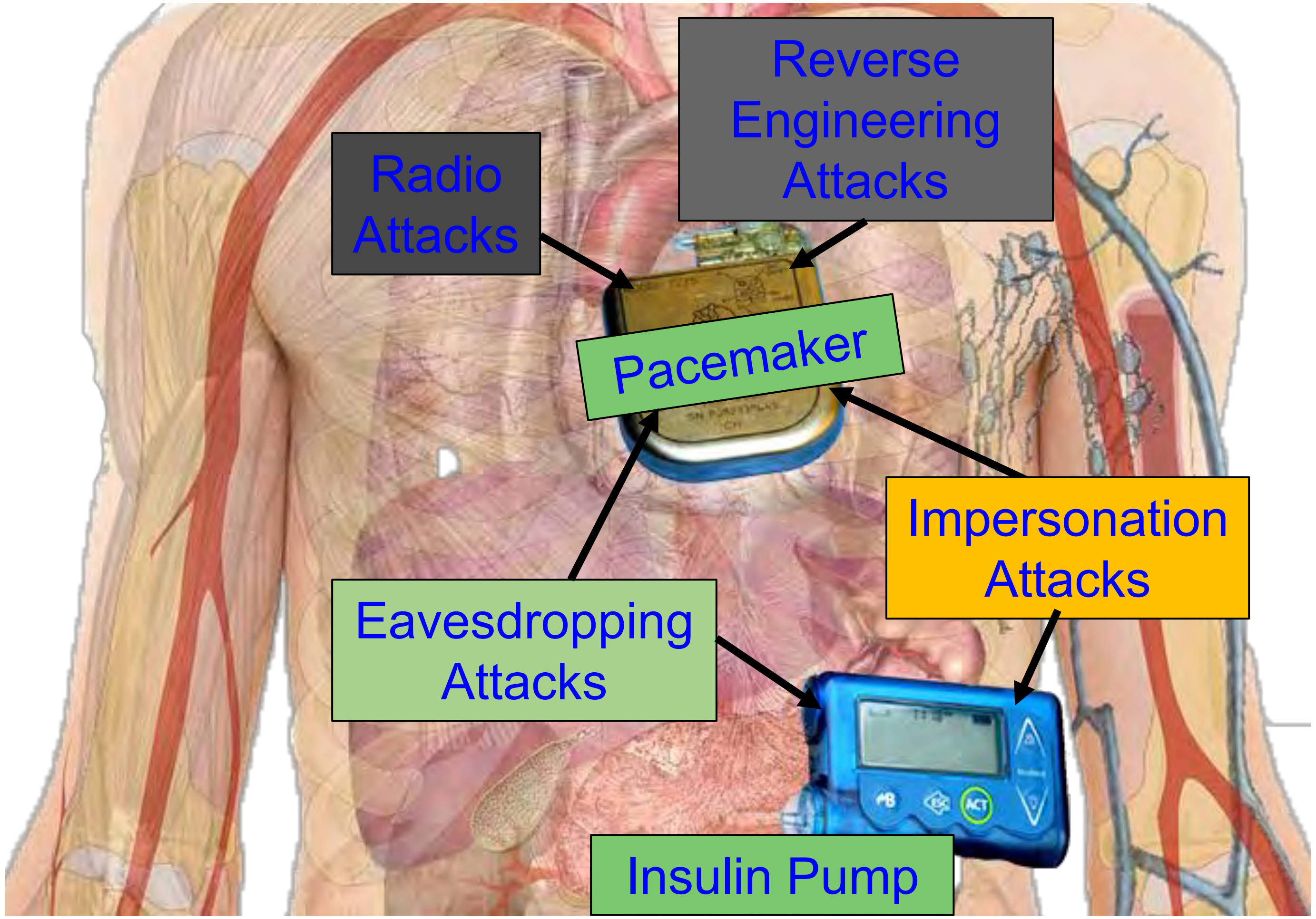
Source: D. A. Hahn, A. Munir, and S. P. Mohanty, "Security and Privacy Issues in Contemporary Consumer Electronics", *IEEE Consumer Electronics Magazine*, Vol 8, No. 1, Jan 2019, pp. 95--99.

IT Cybersecurity Solutions Can't be Directly Extended to IoT/CPS Cybersecurity

IT Cybersecurity	IoT Cybersecurity
IT infrastructure may be well protected rooms	IoT may be deployed in open hostile environments
Limited variety of IT network devices	Significantly large variety of IoT devices
Millions of IT devices	Billions of IoT devices
Significant computational power to run heavy-duty security solutions	May not have computational power to run security solutions
IT security breach can be costly	IoT security breach (e.g. in a IoMT device like pacemaker, insulin pump) can be life threatening

Maintaining of Cybersecurity of Electronic Systems, IoT, CPS, needs Energy, and affects performance.

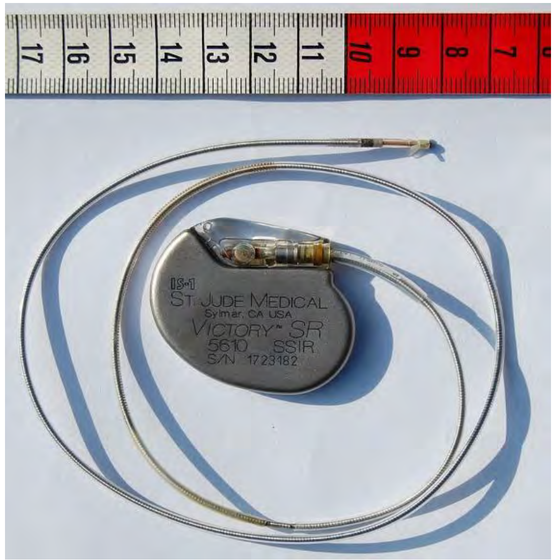
Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard



Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

Implantable and Wearable Medical Devices (IWMDs):
- → Longer Battery life
- → Safer device
- → Smaller size
- → Smaller weight
- → Not much computational capability

H-CPS Cybersecurity Measures is Hard - Energy Constrained



Pacemaker
Battery Life
- 10 years

Neurostimulator
Battery Life
- 8 years

- Implantable Medical Devices (IMDs) have integrated battery to provide energy to all their functions → Limited Battery Life depending on functions
- Higher battery/energy usage → Lower IMD lifetime
- Battery/IMD replacement → Needs surgical risky procedures

Source: C. Camara, P. Peris-Lopeza, and J. E.Tapiadora, “Security and privacy issues in implantable medical devices: A comprehensive survey", *Elsevier Journal of Biomedical Informatics*, Volume 55, June 2015, Pages 272-289.

Smart Car Cybersecurity - Latency Constrained

Protecting Communications
Particularly any Modems for In-vehicle Infotainment (IVI) or in On-board Diagnostics (OBD-II)

Over The Air (OTA) Management
From the Cloud to Each Car

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive cybersecurity issues.

Protecting Each Module
Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

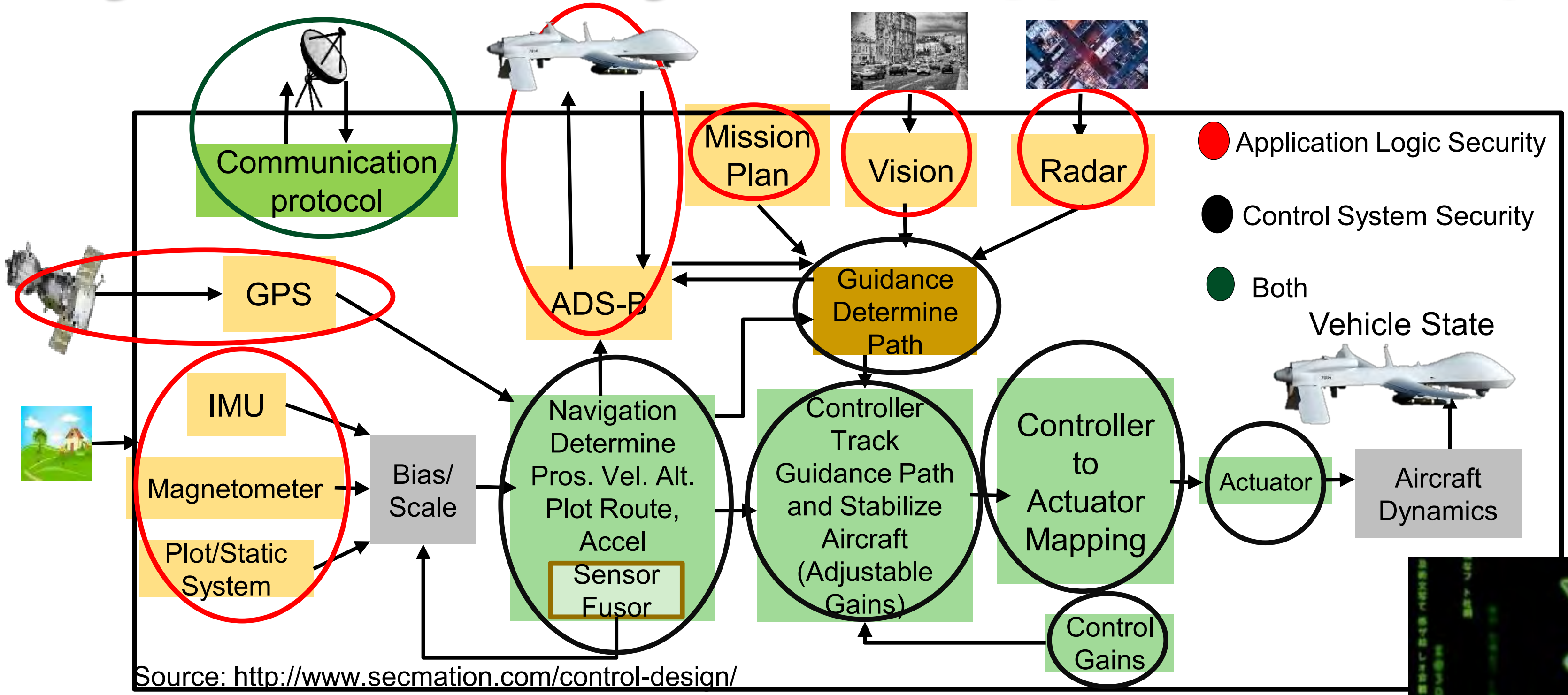
Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Car Cybersecurity – Latency Constrained

UAV Cybersecurity - Energy & Latency Constrained



Source: http://www.secmation.com/control-design/

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Cybersecurity Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

Smart Grid Security Constraints

Smart Grid – Security Objectives

- Availability
- Integrity
- Confidentiality

Smart Grid – Security Requirements

- Identification
- Authentication
- Authorization
- Trust
- Access Control
- Privacy

Smart Grid – Security Solution Constraints

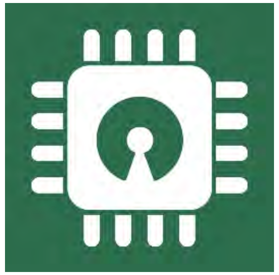
- Transactions Latency
- Communication Latency
- Transactions Computational Overhead
- Energy Overhead on Embedded Devices
- Security Budget

Source: R. K. Pandey and M. Misra, "Cyber security threats - Smart grid infrastructure," in *Proc. National Power Systems Conference (NPSC)*, 2016, pp. 1-6.

Cybersecurity Attacks – Software Vs Hardware Based

Software Based

- Software attacks via communication channels
- Typically from remote
- More frequent
- Selected Software based:
  - Denial-of-Service (DoS)
  - Routing Attacks
  - Malicious Injection
  - Injection of fraudulent packets
  - Snooping attack of memory
  - Spoofing attack of memory and IP address
  - Password-based attacks



Hardware Based

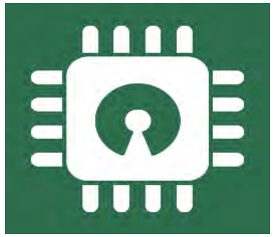
- Hardware or physical attacks
- Maybe local
- More difficult to prevent
- Selected Hardware based:
  - Hardware backdoors (e.g. Trojan)
  - Inducing faults
  - Electronic system tampering/ jailbreaking
  - Eavesdropping for protected memory
  - Side channel attack
  - Hardware counterfeiting

Source: Mohanty ICCE Panel 2018

Cybersecurity Solutions – Software Vs Hardware Based

Software Based

- Introduces latency in operation
- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can't stop hardware reverse engineering

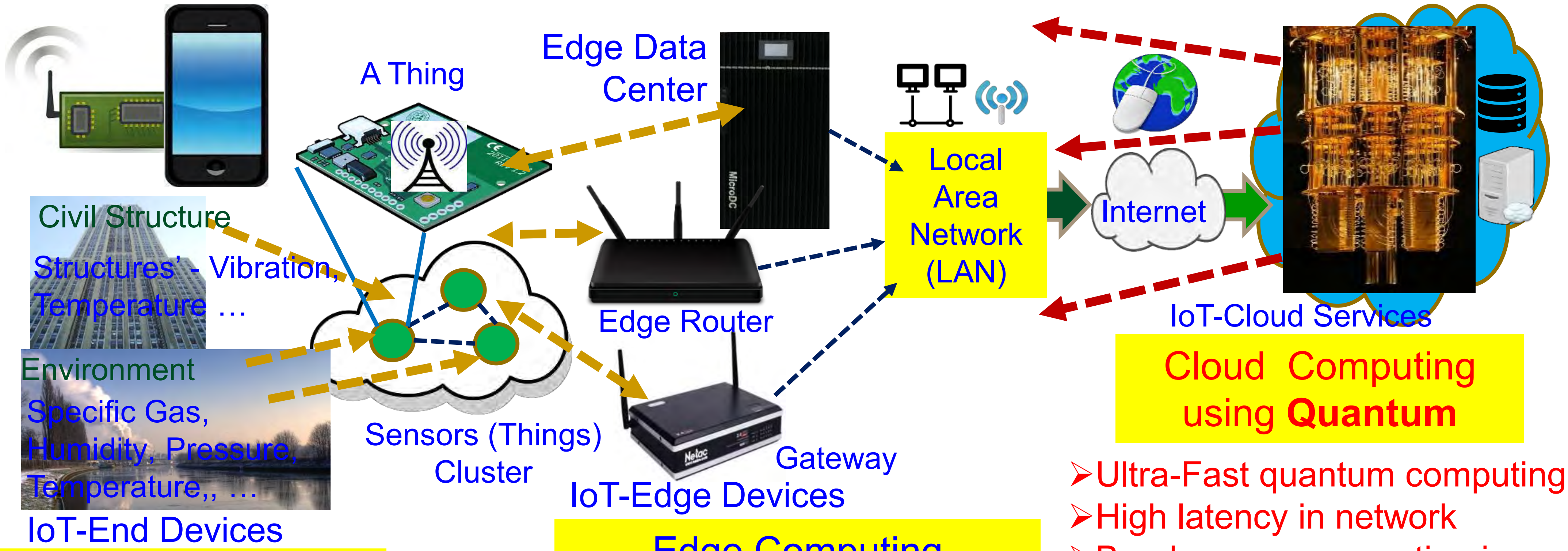


Hardware Based

- High-Speed operation
- Energy-Efficient operation
- Low-cost using ASIC and FPGA
- Tasks of encryption easy compared to software – bit permutation
- Easy integration in CE systems
- Possible security at source-end like sensors, better suitable for IoT
- Susceptible to side-channel attacks
- Can't stop software reverse engineering

Source: Mohanty ICCE Panel 2018

Cybersecurity Nightmare ← Quantum Computing



Cloud Computing using Quantum

- Ultra-Fast quantum computing resources
- High latency in network
- Breaks every encryption in no time

In-Sensor/End-Device Computing

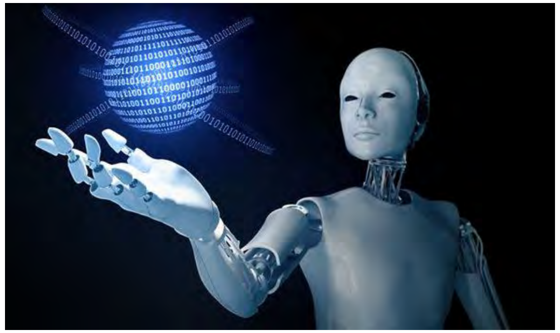
- Minimal computational resource
- Negligible latency in network
- Very lightweight security

Edge Computing

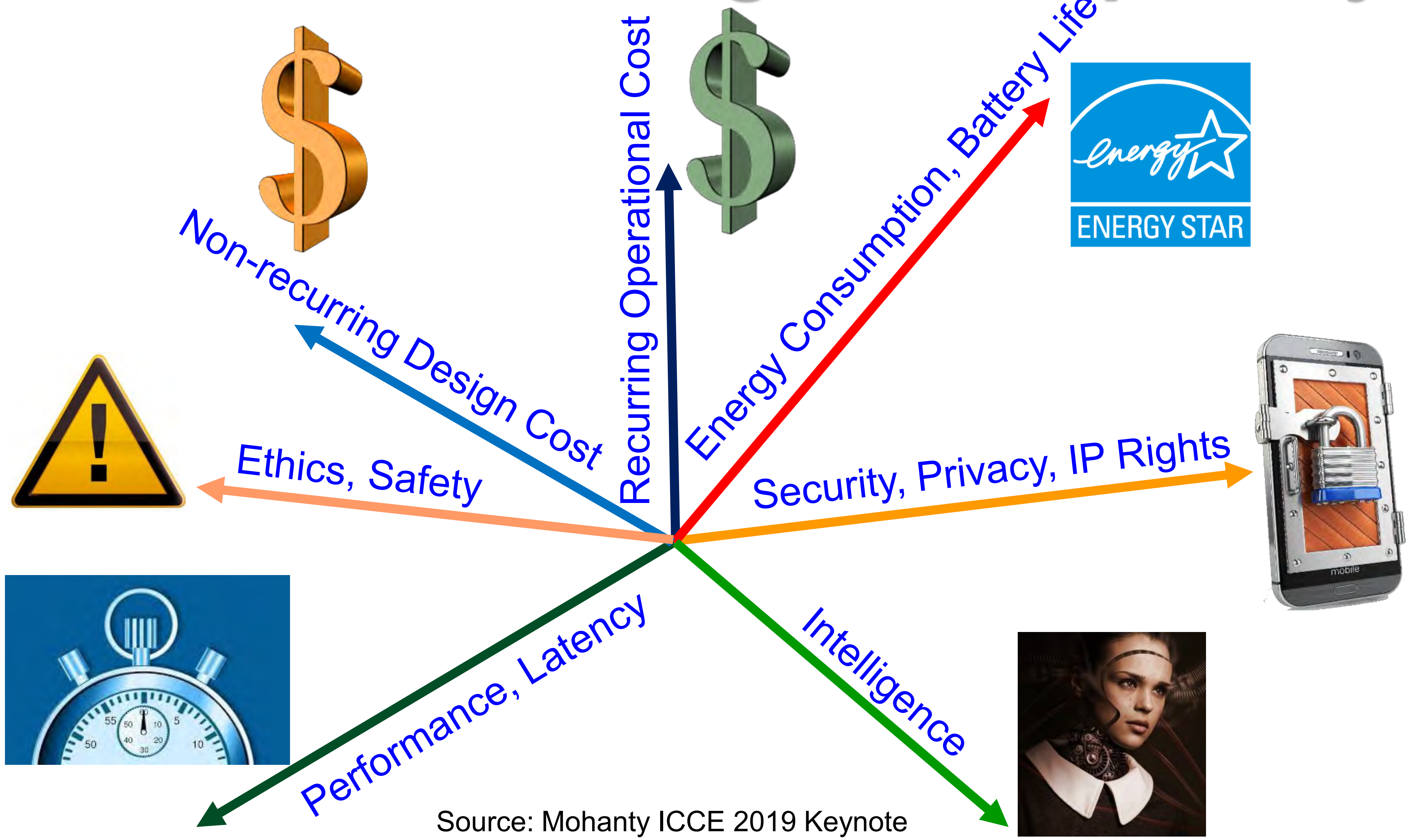
- Less computational resource
- Minimal latency in network
- Lightweight security

A quantum computer could break a 2048-bit RSA encryption in 8 hours.

Security-by-Design (SbD) – The Principle



IoT/CPS Design – Multiple Objectives



Source: Mohanty ICCE 2019 Keynote

Smart Cities
Vs
Smart Villages

Privacy by Design (PbD) → General Data Protection Regulation (GPDR)

1995
Privacy by Design (PbD)

- Treat privacy concerns as design requirements when developing technology, rather than trying to retrofit privacy controls after it is built

2018
General Data Protection Regulation (GDPR)

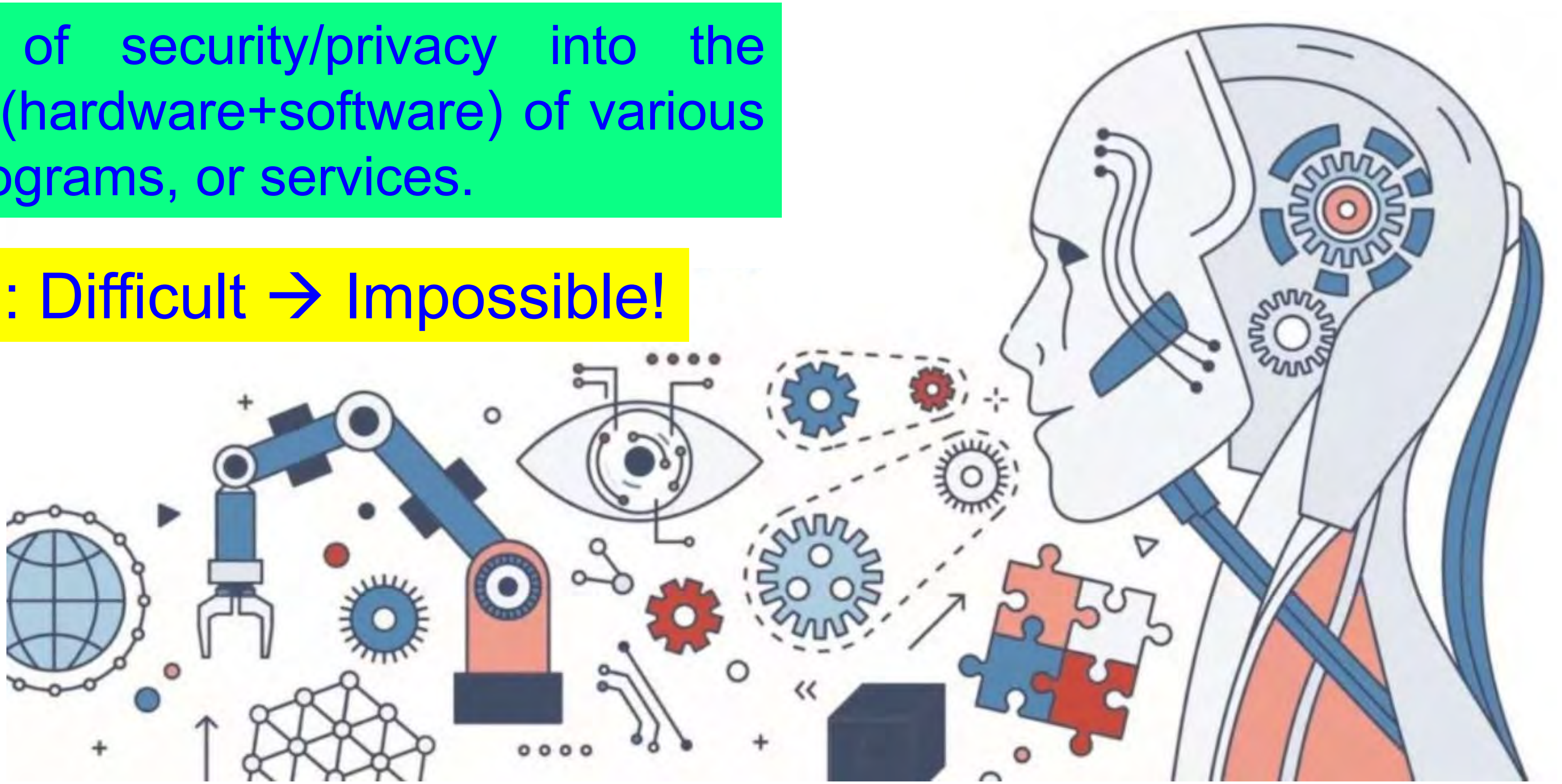
- GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design
aka
Secure by Design (SbD)

Security by Design (SbD) and/or Privacy by Design (PbD)

Embedding of security/privacy into the architecture (hardware+software) of various products, programs, or services.

Retrofitting: Difficult → Impossible!



Source: https://teachprivacy.com/tag/privacy-by-design/

Security by Design (SbD) and/or Privacy by Design (PbD)

7 Fundamental Principles

- Proactive not Reactive
- Security/Privacy as the Default
- Security/Privacy Embedded into Design
- Full Functionality - Positive-Sum, not Zero-Sum
- End-to-End Security/Privacy - Lifecycle Protection
- Visibility and Transparency
- Respect for Users

Source: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

CEI Tradeoffs for Smart Electronic Systems

Security of systems and data.

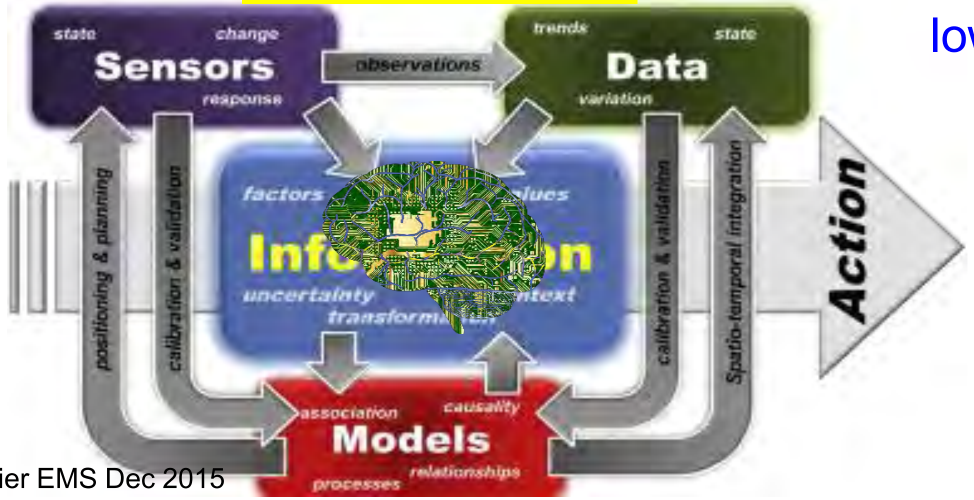
Cybersecurity

Energy

Source: https://mashable.com/2012/10/05/energy-efficient-smartphone/

Energy consumption is minimal and adaptive for longer battery life and lower energy bills.

Intelligence



Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

Source: Mohanty iSES 2018 Keynote

Hardware-Assisted Security (HAS)

- Software based Security:
  - A general purposed processor is a deterministic machine that computes the next instruction based on the program counter.
  - Software based security approaches that rely on some form of encryption can't be full proof as breaking them is just matter of time.
  - It is projected that quantum computers that use different paradigms than the existing computers will make things worse.
- Hardware-Assisted Security (HAS): Security/Protection provided by the hardware: for information being processed by an electronic system, for hardware itself, and/or for the system.

Hardware-Assisted Security (HAS)

- Hardware-Assisted Security: Security provided by hardware for:
  - (1) information being processed,
  - (2) hardware itself,
  - (3) overall system

Privacy by Design (PbD)

Security/Secure by Design (SbD)

- Additional hardware components used for cybersecurity.
- Hardware design modification is performed.
- System design modification is performed.

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

Bluetooth Hardware Security

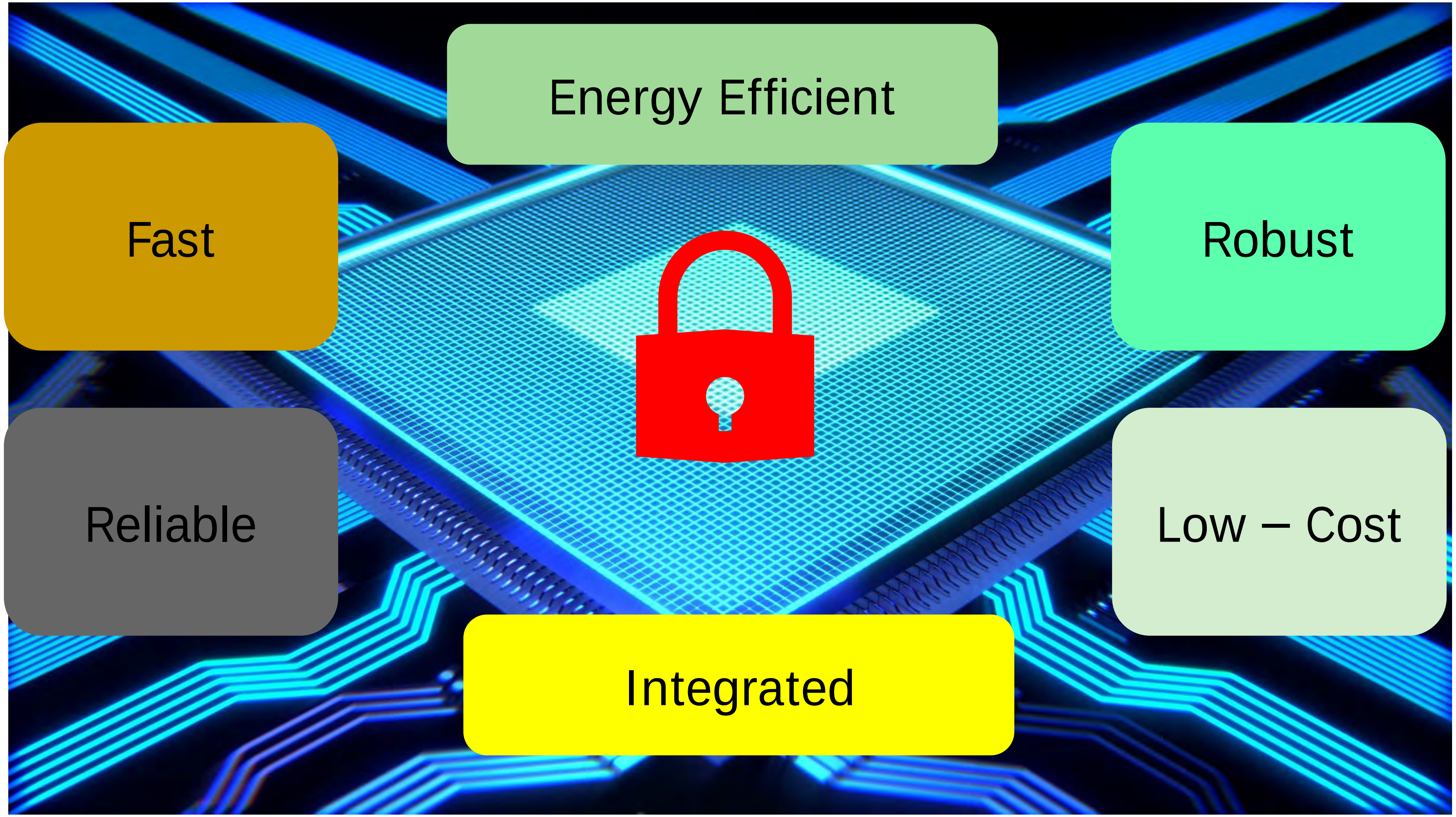
Memory Protection

Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

Source: E. Kougianos, S. P. Mohanty, and R. N. Mahapatra, "Hardware Assisted Watermarking for Multimedia", Special Issue on Circuits and Systems for Real-Time Security and Copyright Protection of Multimedia, Elsevier International Journal on Computers and Electrical Engineering, Vol 35, No. 2, Mar 2009, pp. 339-358..

Hardware Assisted Security (HAS)



Secure SoC Design: Alternatives

- Addition of security and AI features in SoC:
  - Algorithms
  - Protocols
  - Architectures
  - Accelerators / Engines – Cybersecurity and AI Instructions
- Consideration of security as a dimension in the design flow:
  - New design methodology
  - Design automation or computer aided design (CAD) tools for fast design space exploration.

Secure SoC - Alternatives

Development of hardware amenable algorithms.

Building efficient VLSI architectures.

Hardware-software co-design for security, power, and performance tradeoffs.

SoC design for cybersecurity, power, and performance tradeoffs.

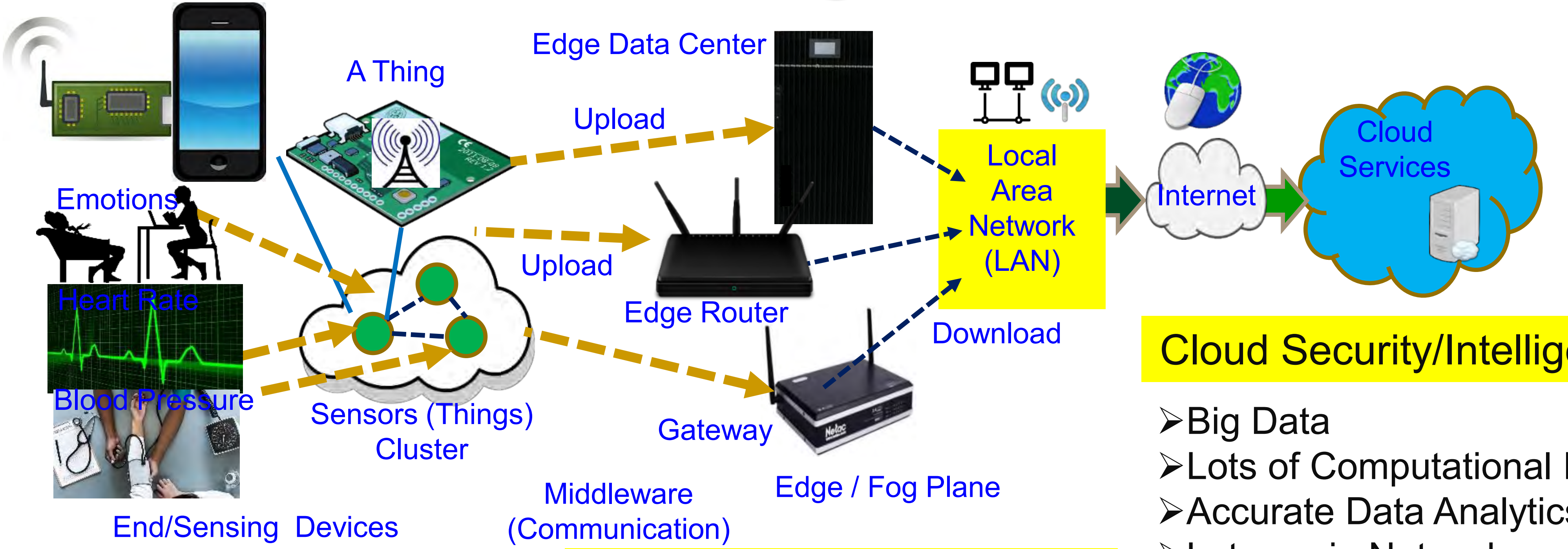
Secure SoC: Different Design Alternatives

- New CMOS sensor with security.
- New data converters with security.
- Independent security and AI processing cores.
- New instruction set architecture for RISC to support security at micro-architecture level.

Trustworthy Electronic System

- A selective attributes of electronic system to be trustworthy:
  - It must maintain integrity of information it is processing.
  - It must conceal any information about the computation performed through any side channels such as power analysis or timing analysis.
  - It must perform only the functionality it is designed for, nothing more and nothing less.
  - It must not malfunction during operations in critical applications.
  - It must be transparent only to its owner in terms of design details and states.
  - It must be designed using components from trusted vendors.
  - It must be built/fabricated using trusted fabs.

CPS – IoT-Edge Vs IoT-Cloud



End Security/Intelligence

- ➢ Minimal Data
- ➢ Minimal Computational Resource
- ➢ Least Accurate Data Analytics
- ➢ Very Rapid Response

Edge Security/Intelligence

- ➢ Less Data
- ➢ Less Computational Resource
- ➢ Less Accurate Data Analytics
- ➢ Rapid Response

Cloud Security/Intelligence

- ➢ Big Data
- ➢ Lots of Computational Resource
- ➢ Accurate Data Analytics
- ➢ Latency in Network
- ➢ Energy Overhead in Communications

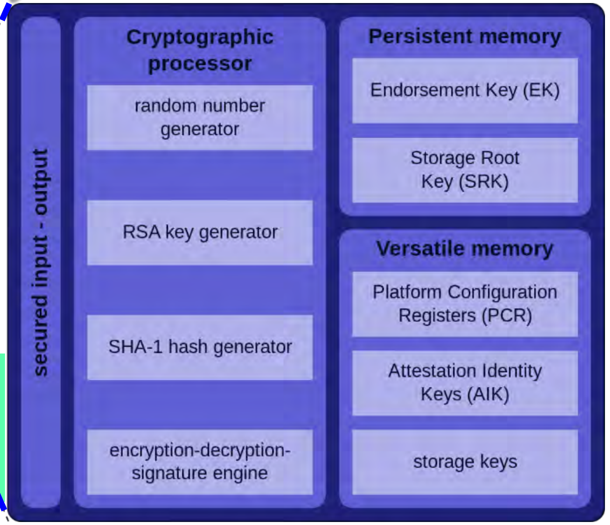
TinyML at End and/or Edge is key for smart villages.

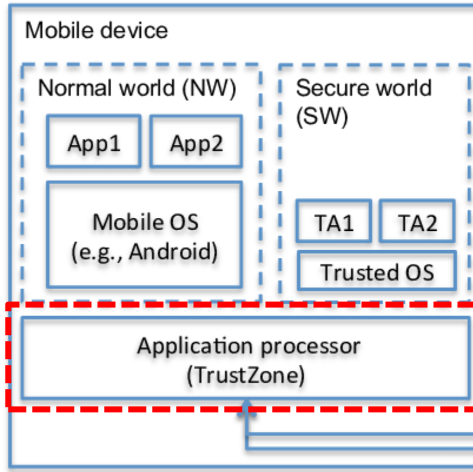
Heavy-Duty ML is more suitable for smart cities

Hardware Cybersecurity Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)

Trusted Platform Module (TPM)





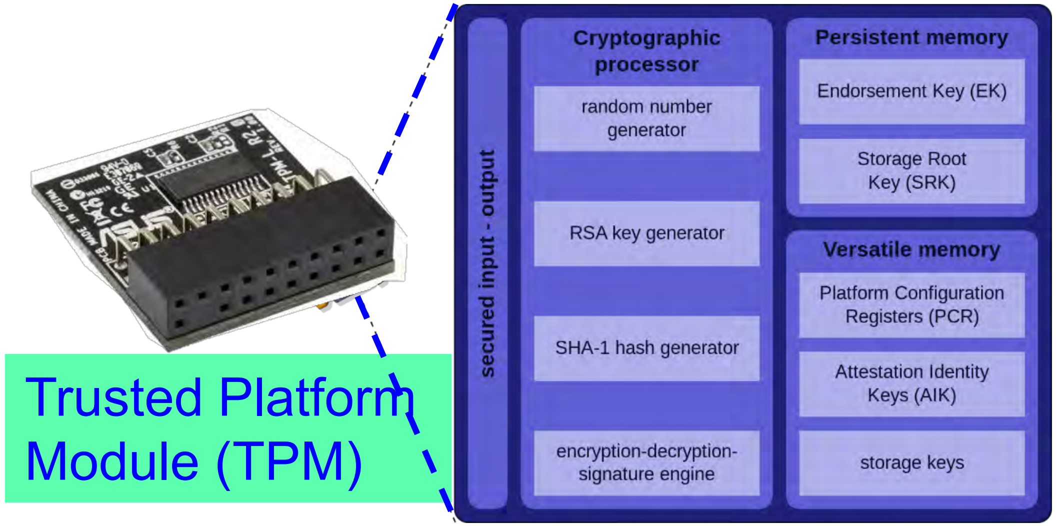
Source: C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun, *Smartphones as Practical and Secure Location Verification Tokens for Payments*. 2014.

Keep It Simple Stupid (KISS) → Keep It Isolated Stupid (KIIS)

Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

PUF versus TPM



Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

TPM:
1) The set of specifications for a secure crypto- processor and
2) The implementation of these specifications on a chip

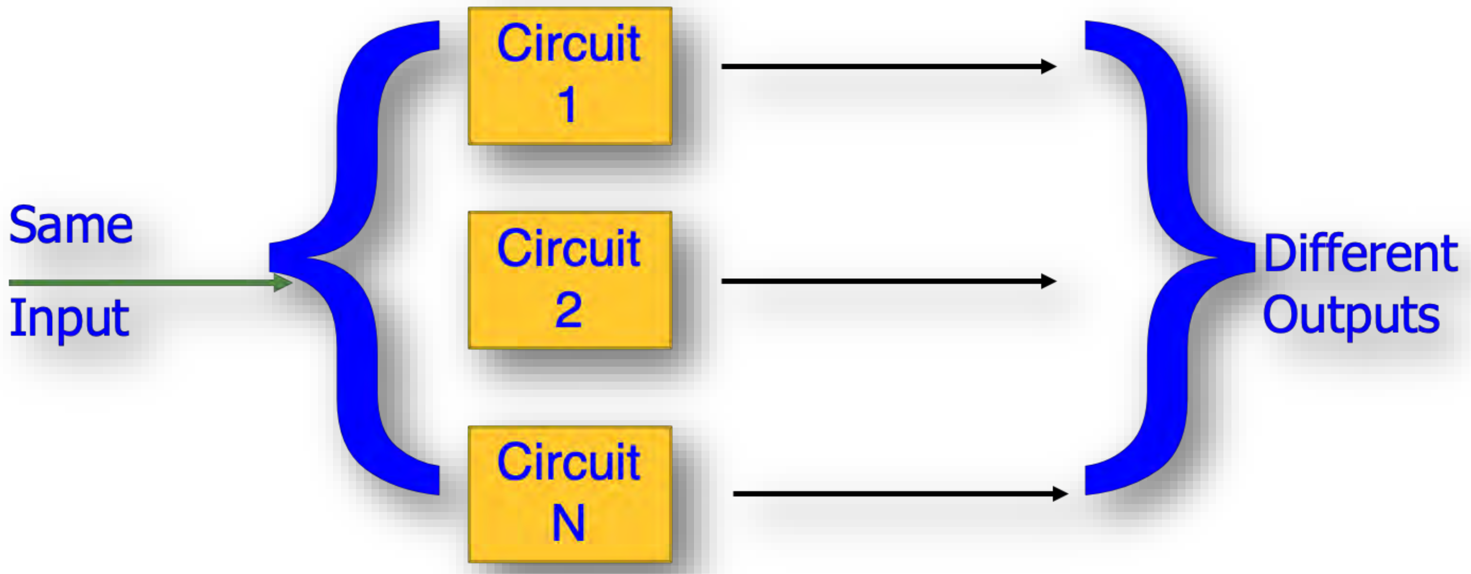
PUF:
1) Based on a physical system
2) Generates random output values

Why PUFs?

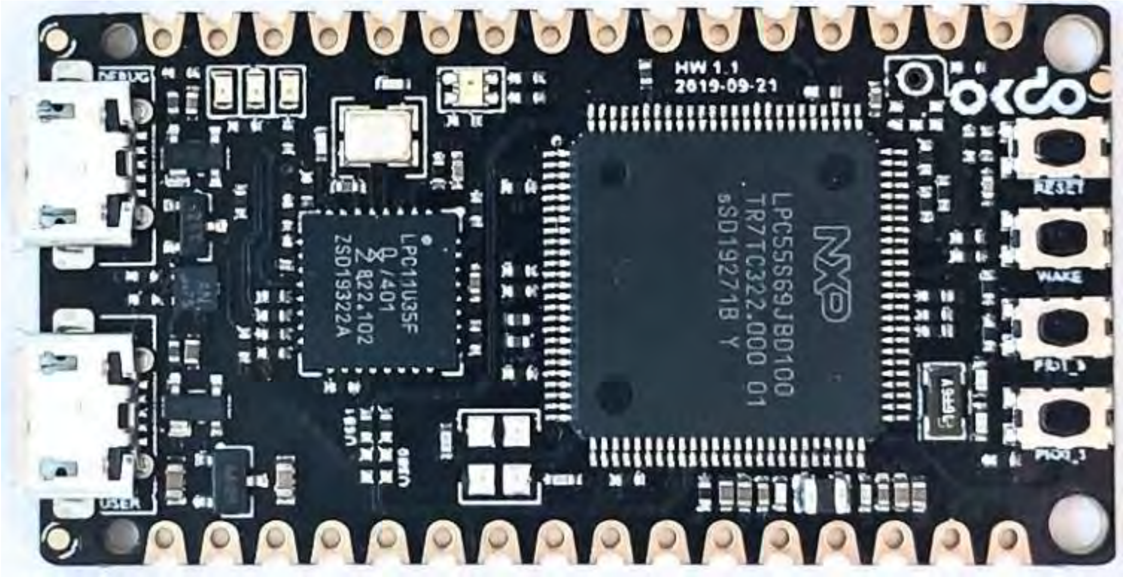
- Hardware-assisted security.
- Key not stored in memory.
- Not possible to generate the same key on another module.
- Robust and low power consuming.
- Can use different architectures with different designs.

Physical Unclonable Functions (PUF)

- Uses manufacturing variations for generating unique set of keys for cryptographic applications.
- Input of PUF is a challenge and output from PUF is response.

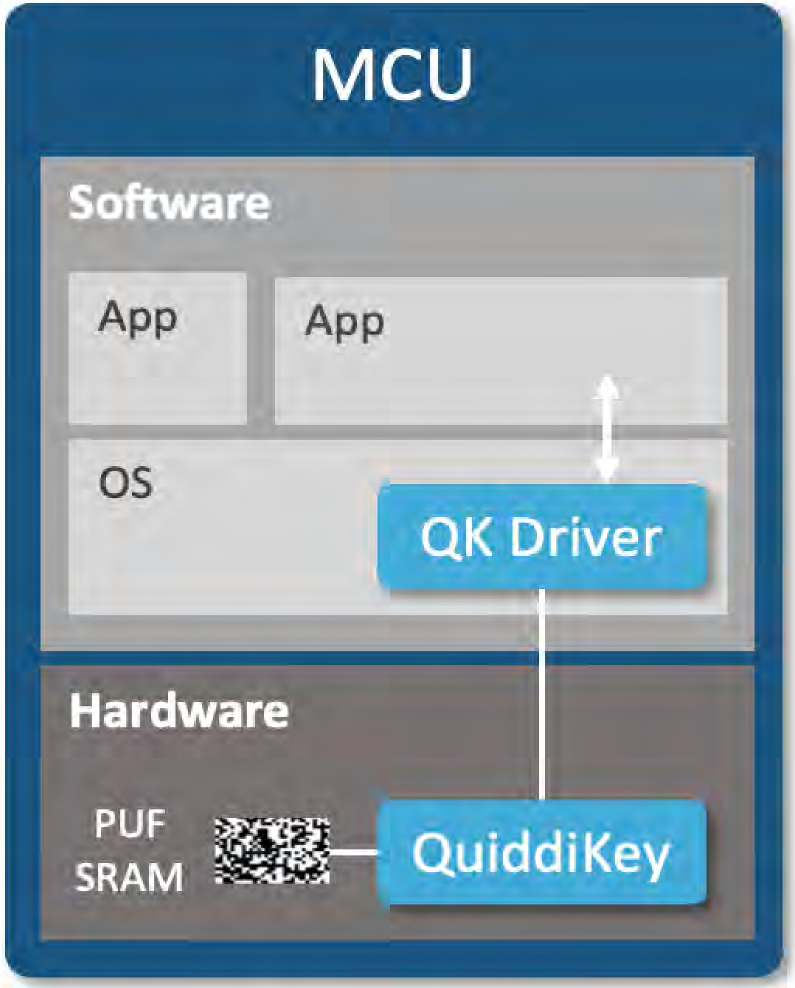


PUF Hardware Modules



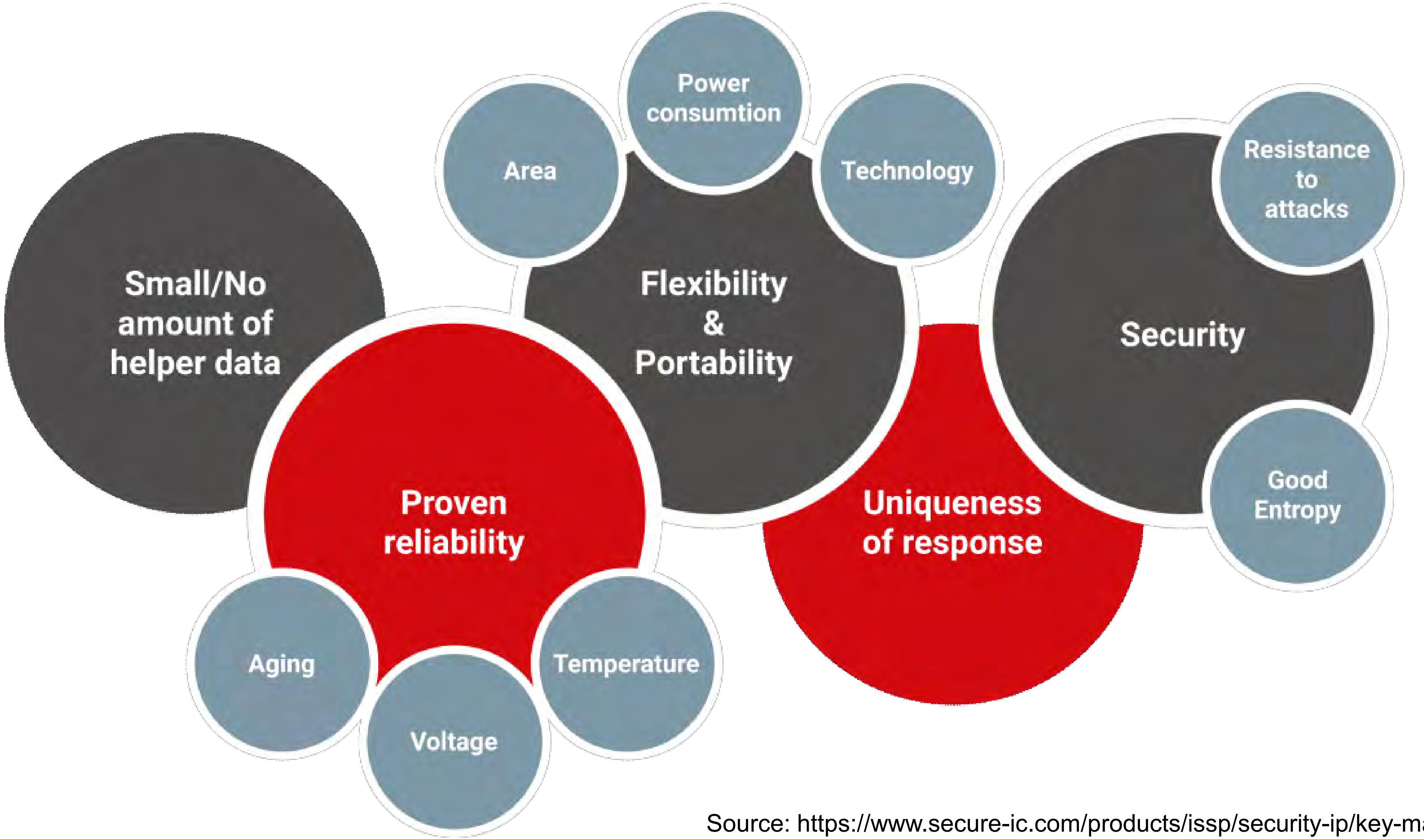
Source: https://asvin.io/physically-unclonable-function-setup/

- This development board is based on LPC55S69xx microcontroller from NXP.
- The microcontroller contains onboard PUF using dedicated SRAM.



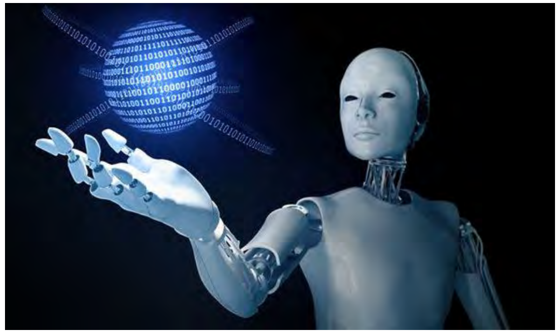
Source: https://www.intrinsic-id.com/products/quiddikey/

PUF: Advantages

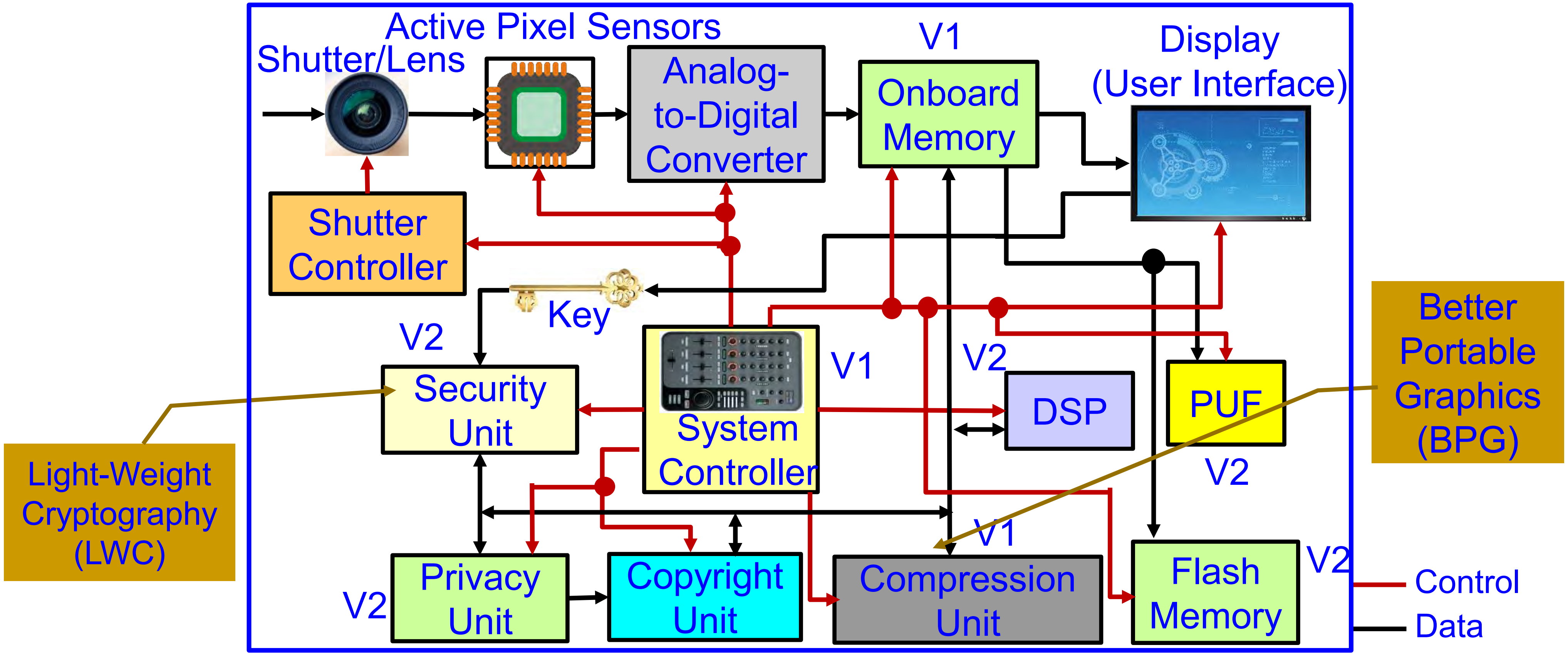


Source: https://www.secure-ic.com/products/issp/security-ip/key-management/puf-ip/

Security-by-Design (SbD) – Specific Examples



Secure Digital Camera (SDC) – My Invention

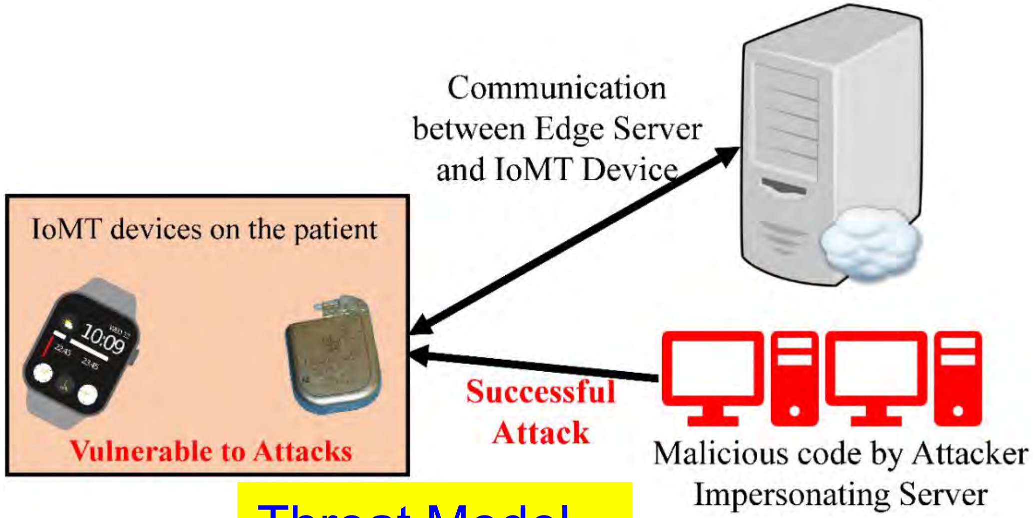


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

Security and/or Privacy by Design (SbD and/or PbD)

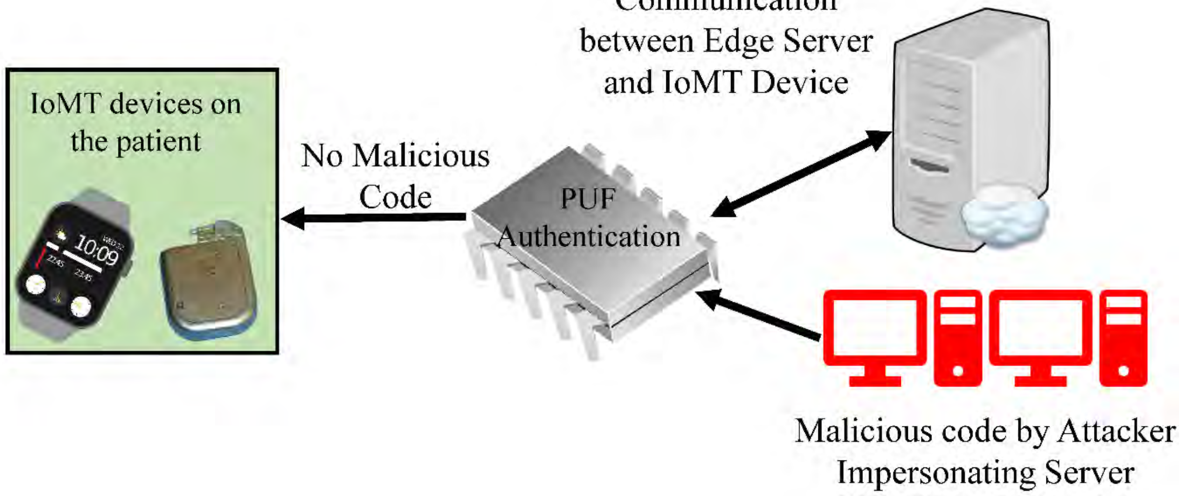
Source: S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", *Elsevier Journal of Systems Architecture (JSA)*, Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



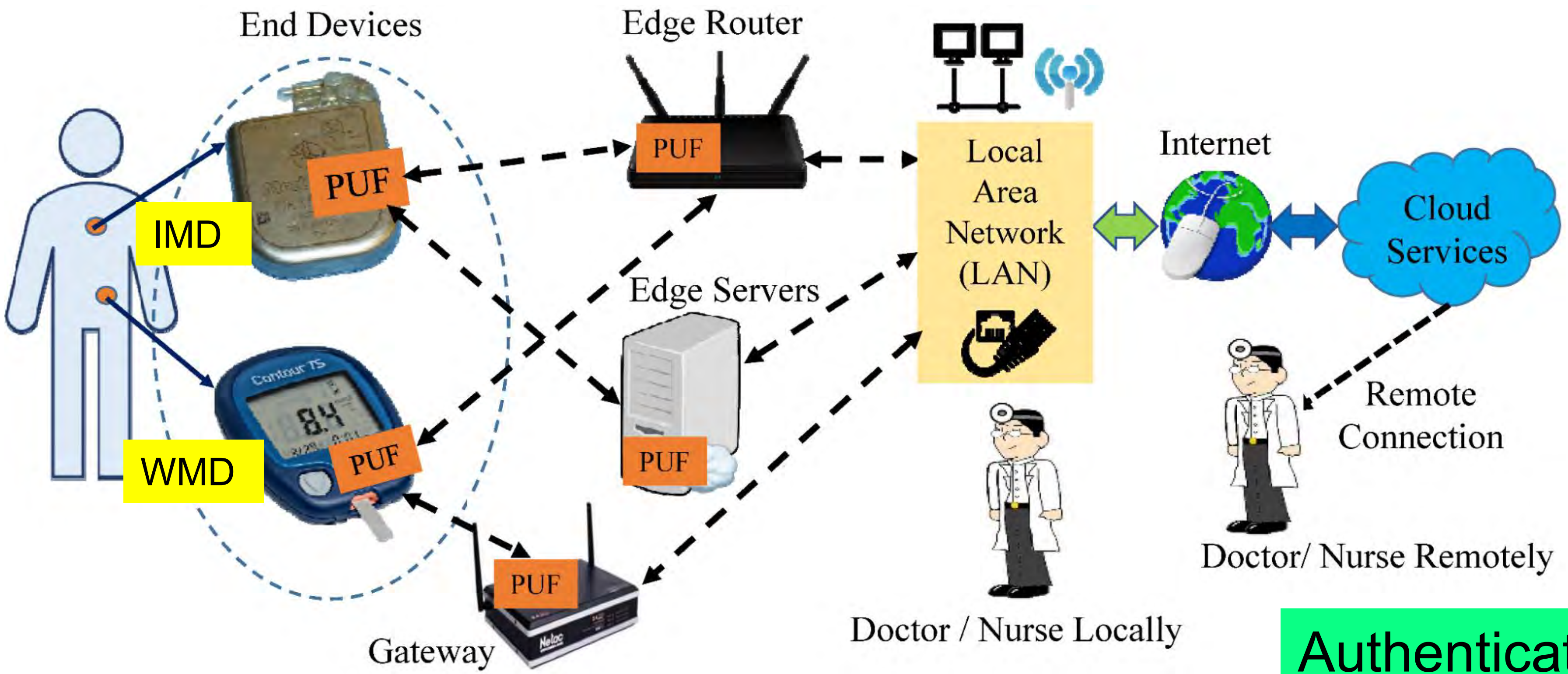
Threat Model

PUF based Solution



Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

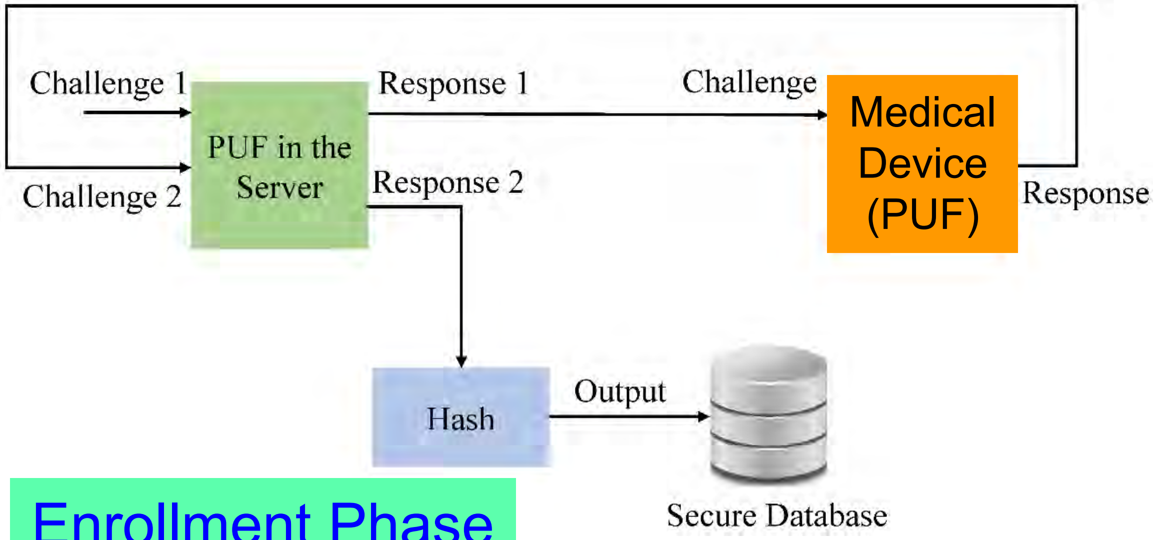
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec

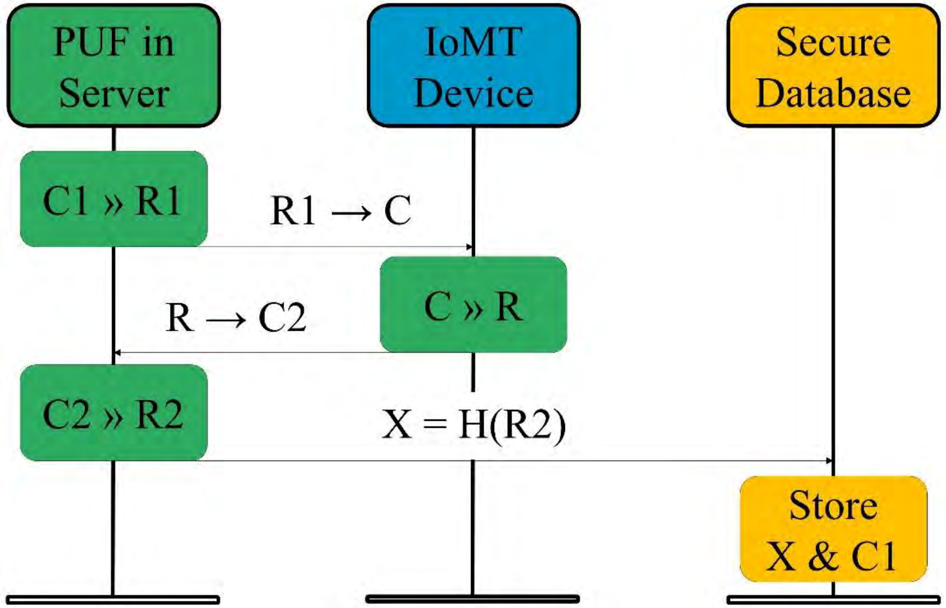


Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

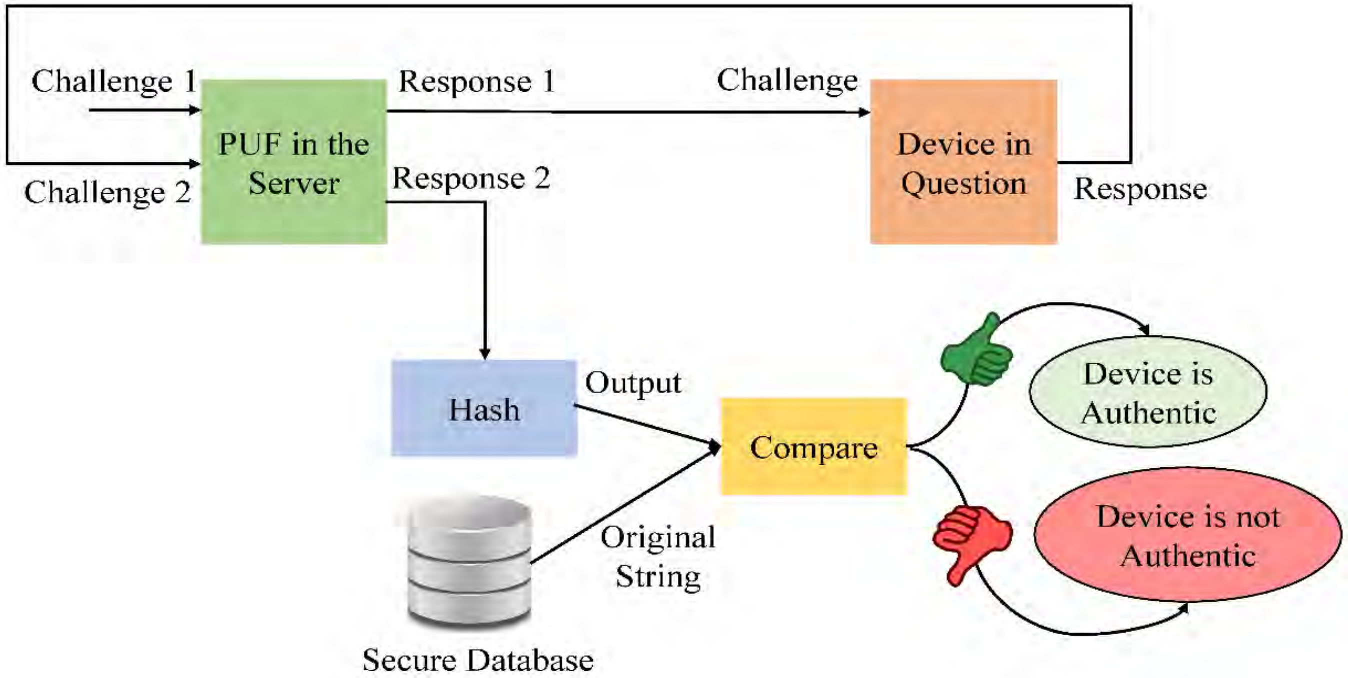


PUF Security Full Proof:

- Only server PUF Challenges are stored, not Responses
- Impossible to generate Responses without PUF

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec

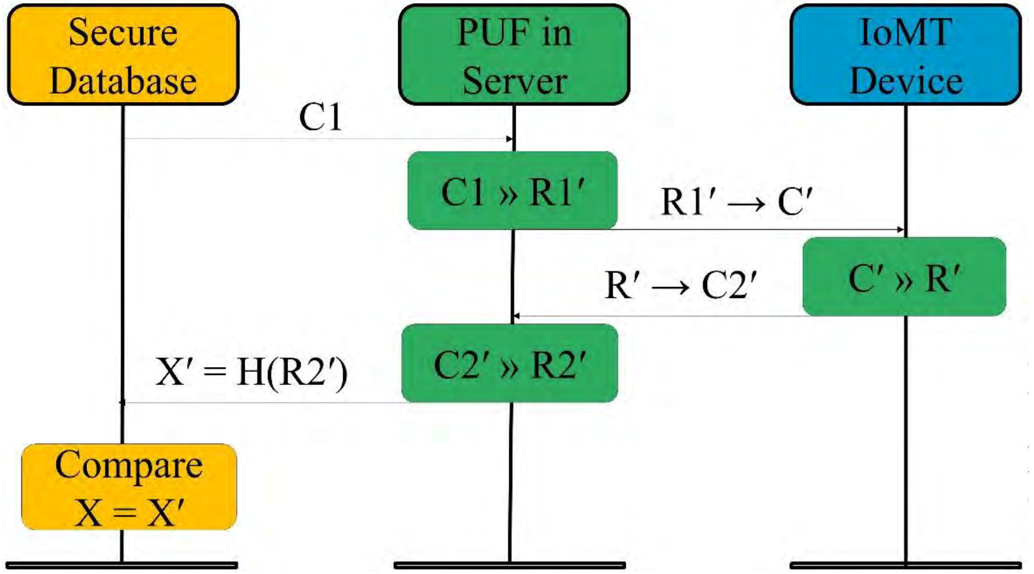


Authentication Phase

At the Doctor

- When doctor needs to access an existing IoMT-device

Device Authentication Procedure



Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our PMsec in Action

Output from IoMT-Server during Enrollment

```
------------Enrollment Phase------------
Generating the Keys
Sending the keys to the Client
Receiving the Keys from the client
Saving the database
>>>
```

Output from the IoMT-Device

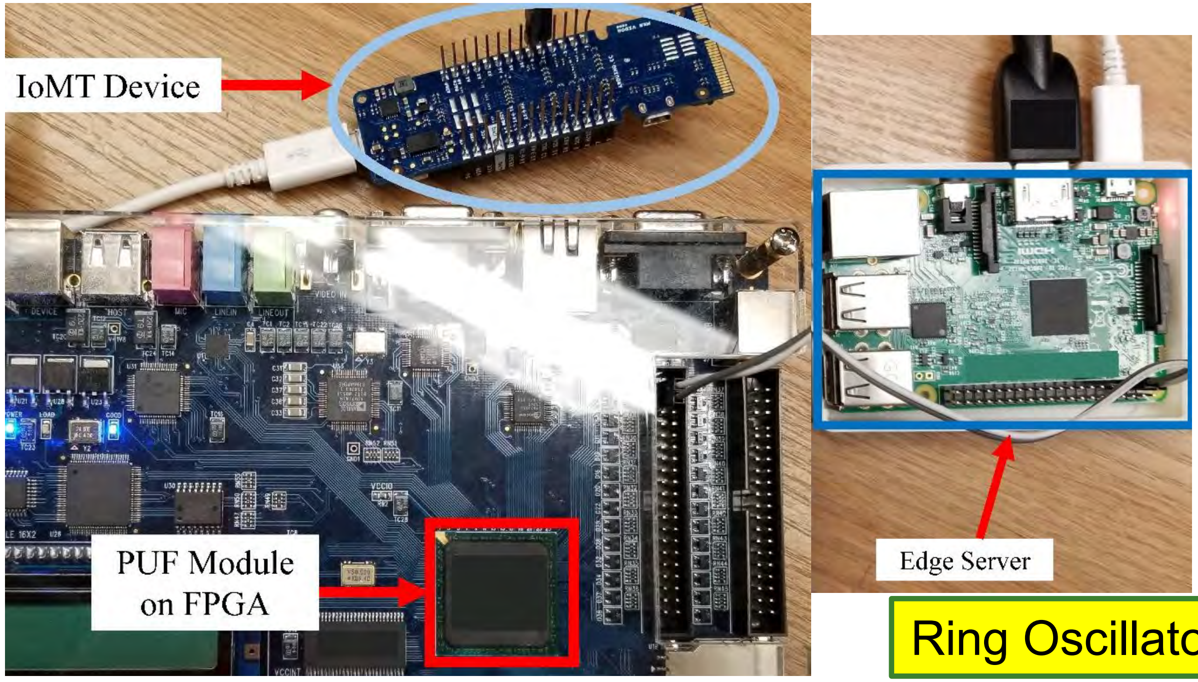
```
COM4
Hello
Received Key from the Server
Generating PUF Key
PUF Key : 1011100001011100101111000101111000101101001101110010100101000011
Sending key for authentication
```

Output from IoMT-Server during Authentication

```
>>>
Hello
------------Authentication Phase------------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  1011100001011100101111000101111000101101001101110010100101000011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76
Authentication Successful
>>> |
```

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec



Average Power Overhead – 200 μW

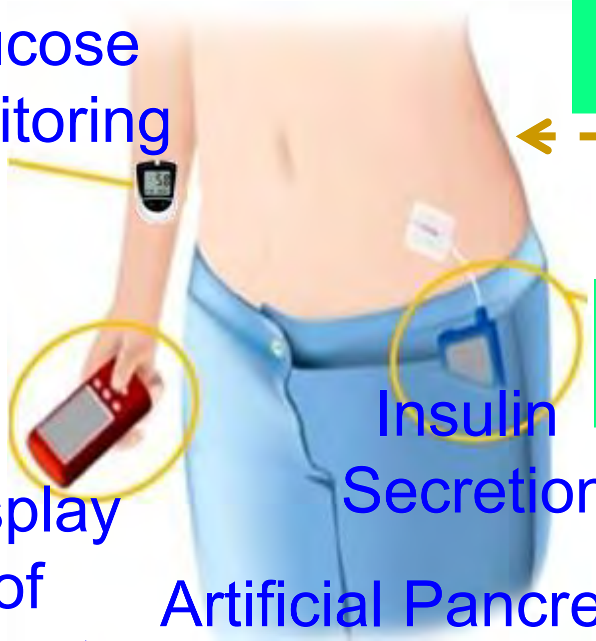
Ring Oscillator PUF – 64-bit, 128-bit, …

Proposed Approach Characteristics	Value (in a FPGA / Raspberry Pi platform)
Time to Generate the Key at Server	800 ms
Time to Generate the Key at IoMT Device	800 ms
Time to Authenticate the Device	1.2 sec - 1.5 sec

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics*, Vol 65, No 3, Aug 2019, pp. 388--397.

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery

Continuous Glucose Monitoring



Privacy-Assured Health Data Storage

Security-Assured System

Cloud Storage

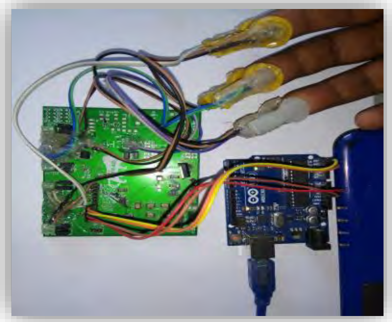
Hospital

Doctor

Insulin Secretion

Display of Parameters

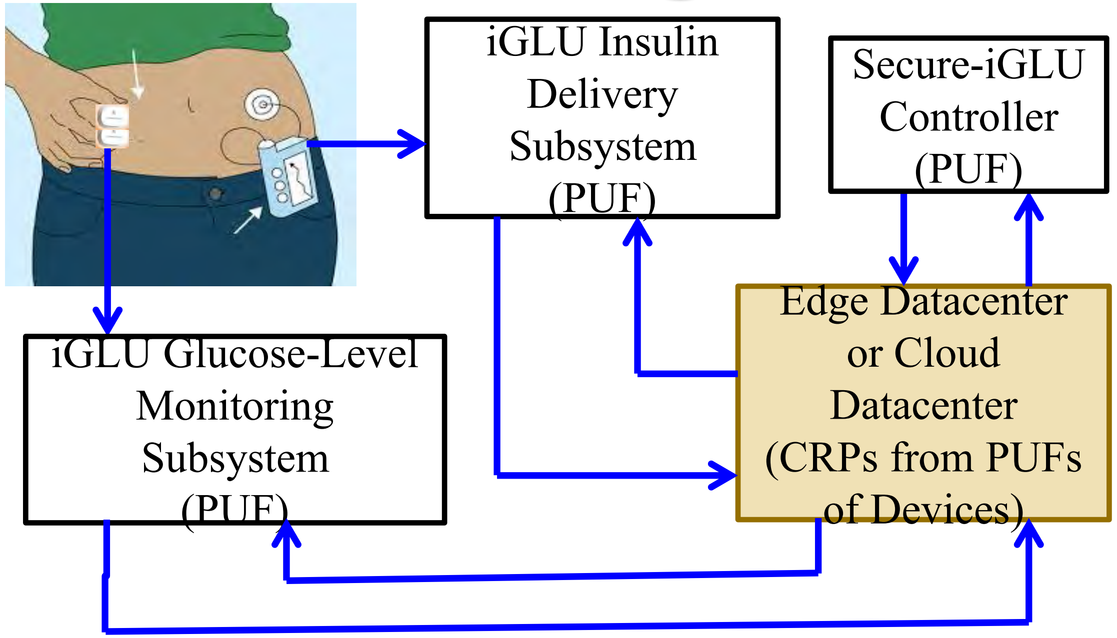
Artificial Pancreases System (APS)

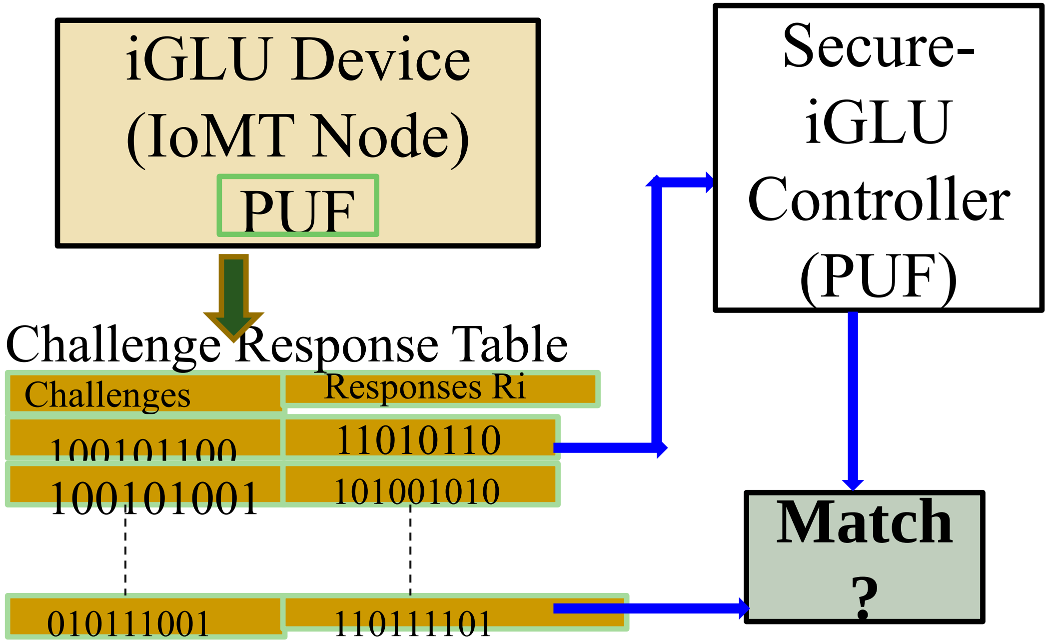


Near Infrared (NIR) based Noninvasive, Accurate, Continuous Glucose Monitoring

P. Jain, A. M. Joshi, and S. P. Mohanty, "iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare", *IEEE Consumer Electronics Magazine (MCE),* Vol. 9, No. 1, January 2020, pp. 35–42.

Secure-iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery





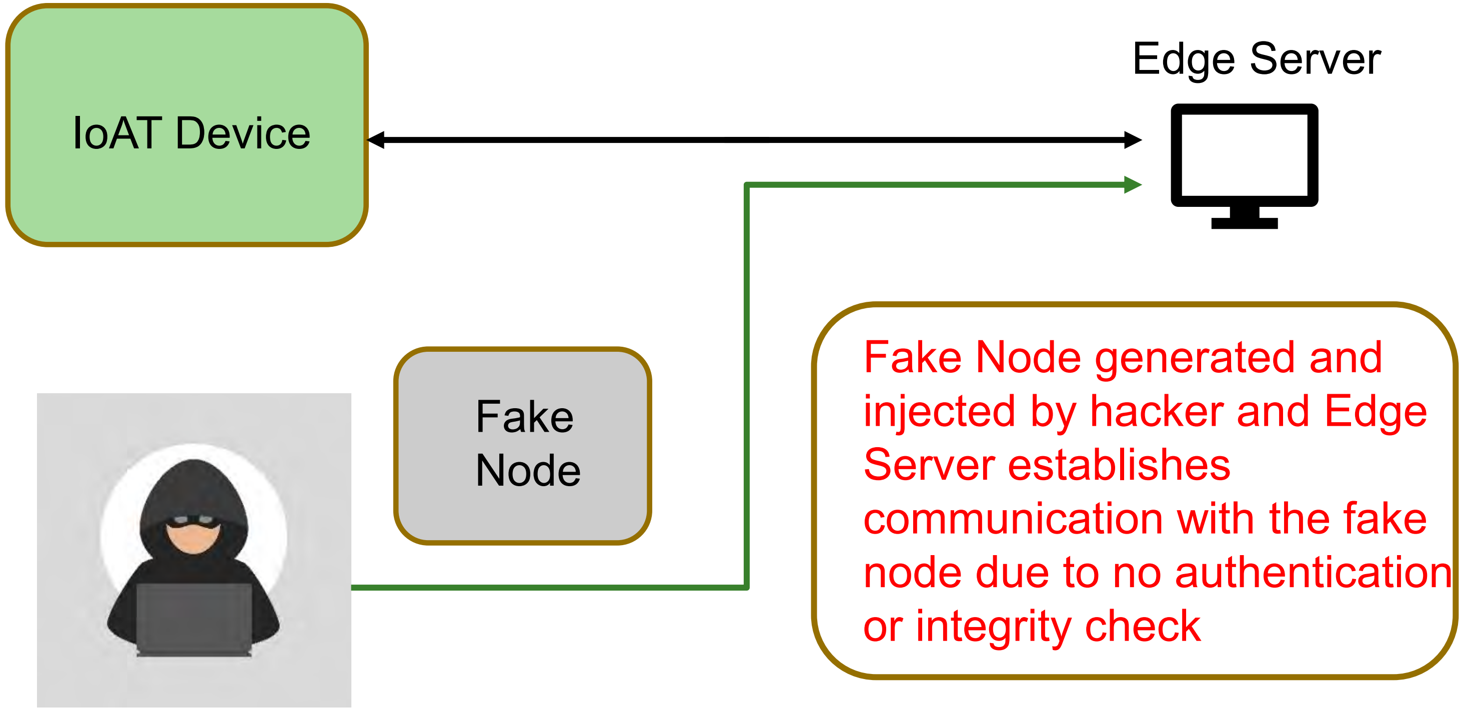
Arbiter PUF – 64-bit, 128-bit, 256 bit …

Source: A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440-445.

Smart Agriculture Cybersecurity - Solutions

- Developing a cloud centric network model
- Using Intrusion detection systems
- Blockchain based solutions for data and device integrity
- Physical countermeasures
  - Machine learning based countermeasures
- Constant security analysis

Smart Agriculture - Threat Model



Malicious Node Generation and replacement

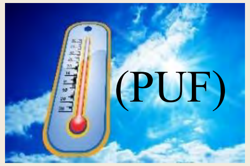
Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Secure Design Approach for Robust IoAT

IoAT Devices

Air Hygrometer

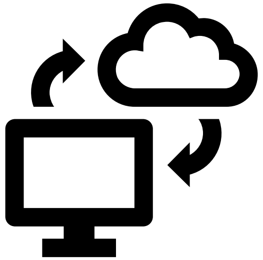
Drone



Temperature Sensor

Secure Communication between PUF Embedded IoAT device and Edge Server

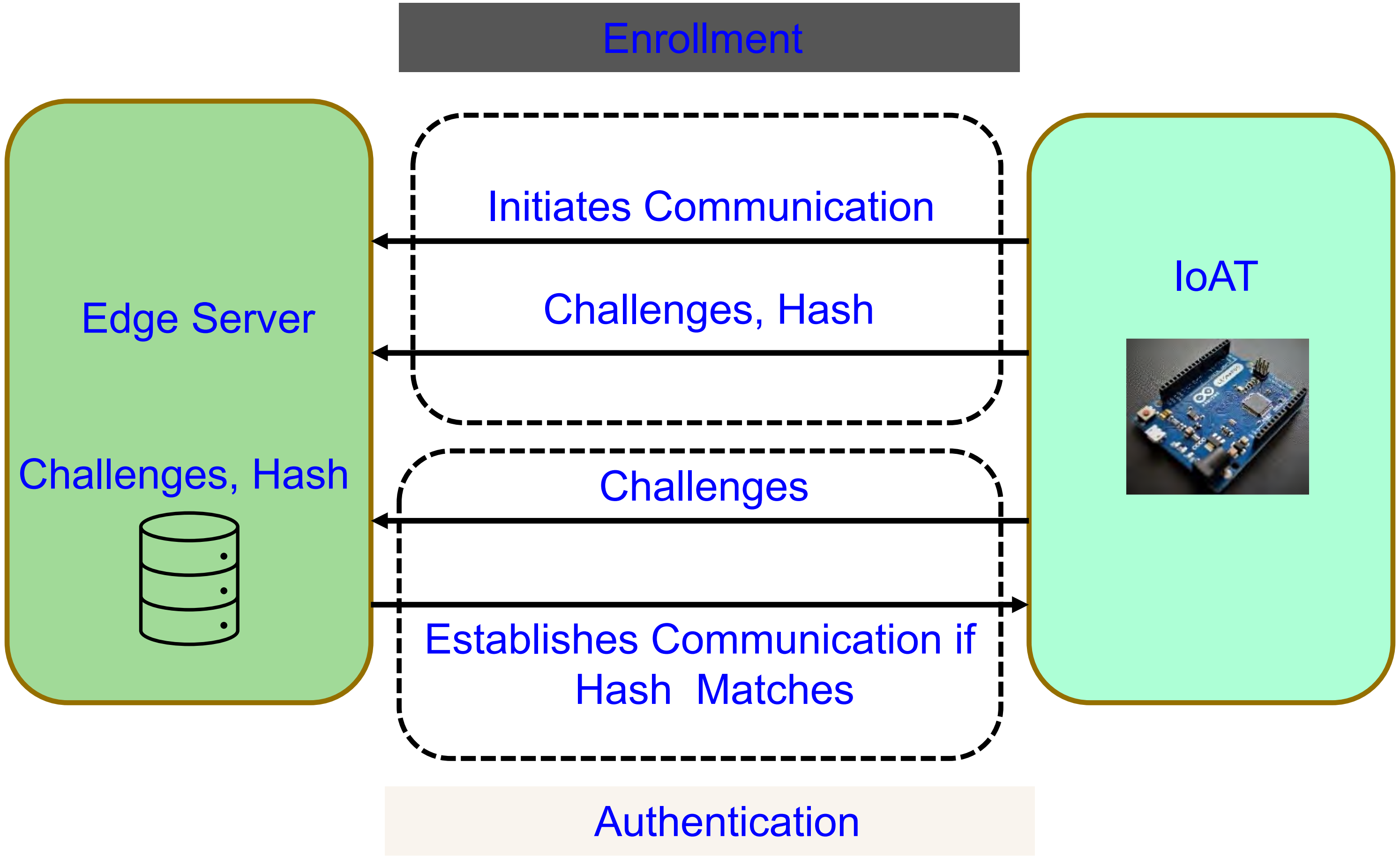
Edge Server



Edge Server authenticates the devices using the PUF key of each electronic device which is the fingerprint for that device

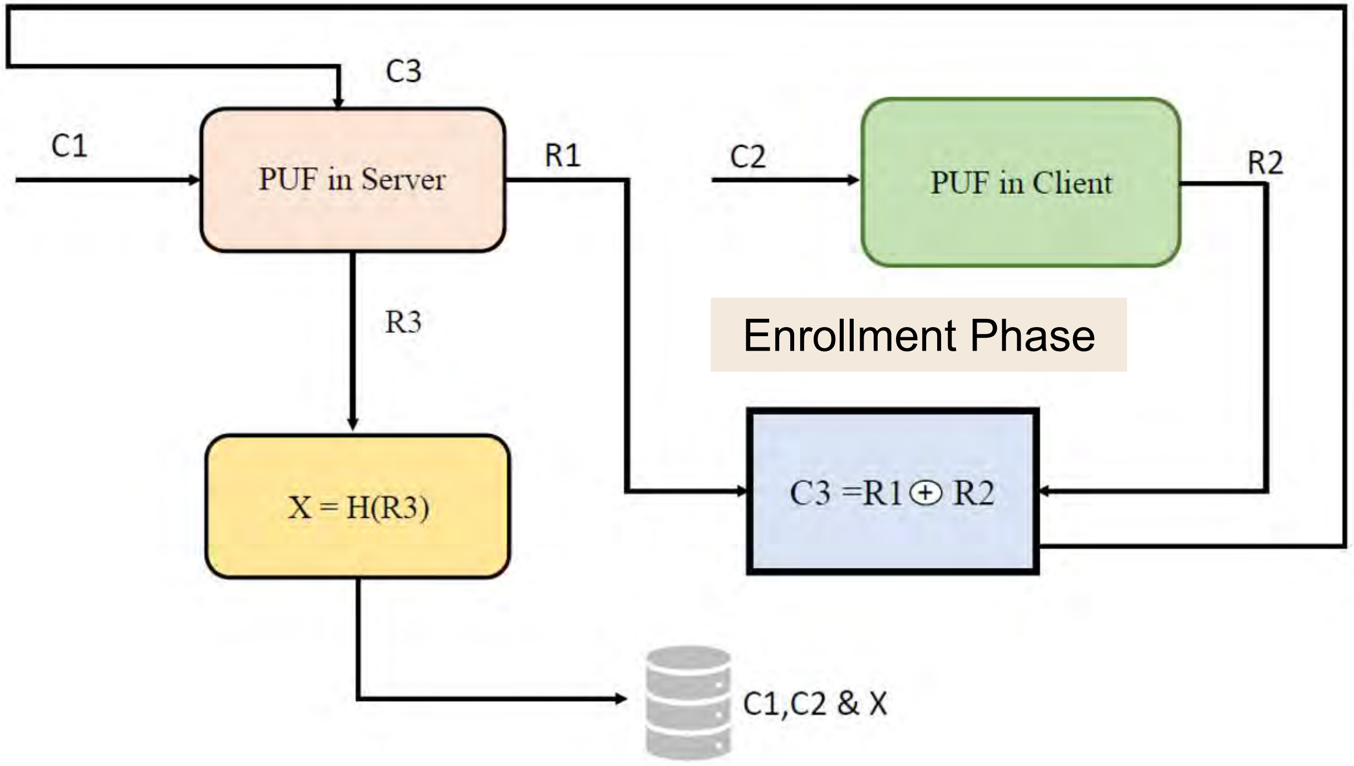
Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Authentication Process for IoAT



Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

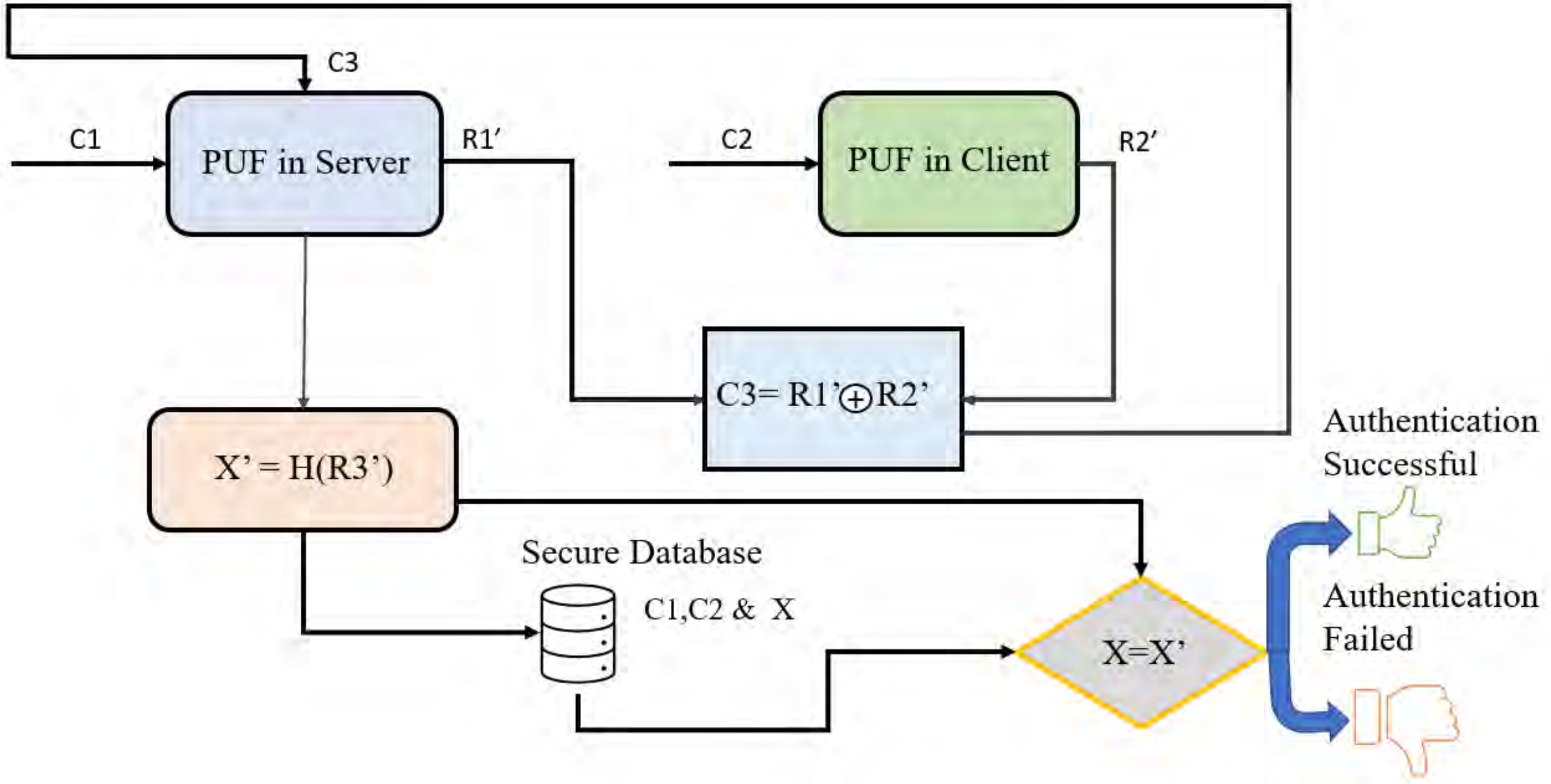
Enrollment Phase of the Proposed Security Protocol



C1 => R1
C2 => R2
C3 = R1 XOR R2
C3 => R3
X = H(R3)
X, C1,C2 are stored in Database

Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture,“ in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

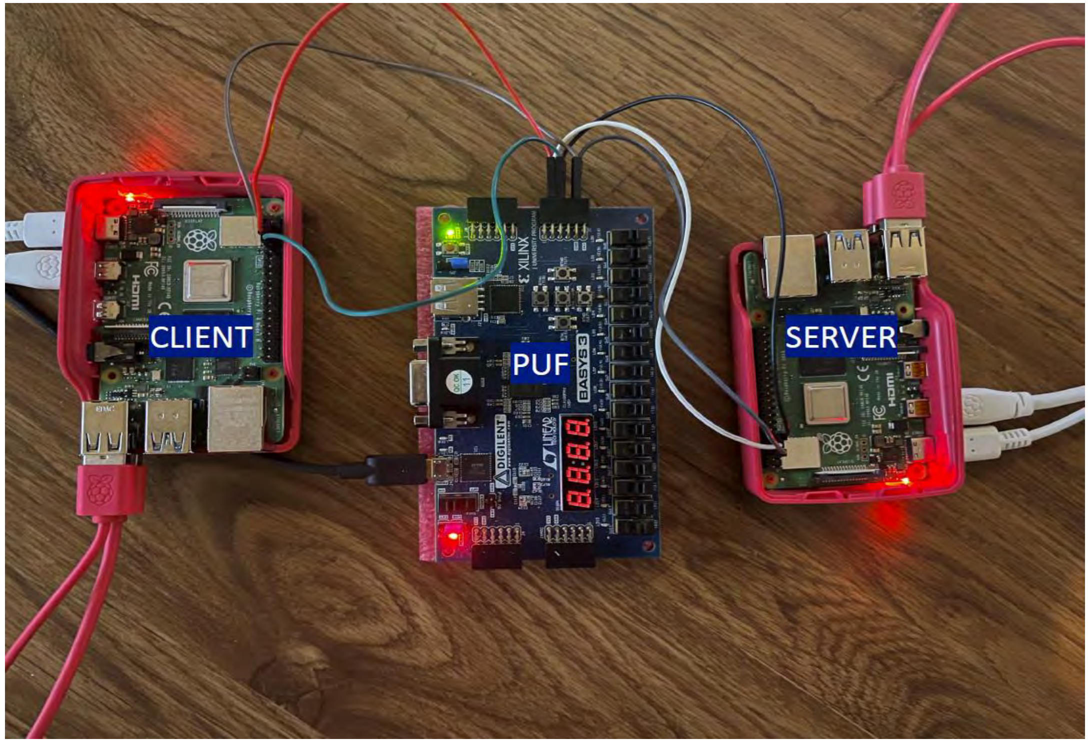
Authentication Phase of the Proposed Security Protocol



Only C1 and C2 are retrieved and given as inputs to the PUF module. The final Hash value X is compared with the stored hash value X to authenticate the device

Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Prototype of the Proposed Security Scheme



Parameter	Value
Hamming Distance	48%
Randomness	41.07%
Time Taken to Authenticate the Device in Seconds	0.16 to 2.93 Seconds
FPGA	Basys 3, Artix-7

Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Experimental Results

```
Python 3.7.3 (/usr/bin/python3)
>>> %Run server1pufauthenticatio.py
 The Server Challenge input
 [39, 33, 33, 81, 83, 82, 62, 61]
 The Server PUF Key
 1100111100000111000001110000011100000111000001110000011100000111
 Client PUF Key
 1001001110010011100100111001001110010011100100111001001110010011
 The XOR Output of Client and Server key
 0101110010010100100101001001010010010100100101001001010010010100
 The XOR ed Challenge input to Server
 [92, 148, 148, 148, 148, 148, 148, 148]
 The Response output from Server
 1000101010111100101111001011110010111100101111001011110010111100
 The Hash Output
 ed7f6d9edc9a6e8437f1fe386cfc2fa80815fb79a3fcb00debf96d1e843e5fa3
 Device Authenticated
 Time taken to Authenticate the Device in seconds
 2.9331398010253906
```

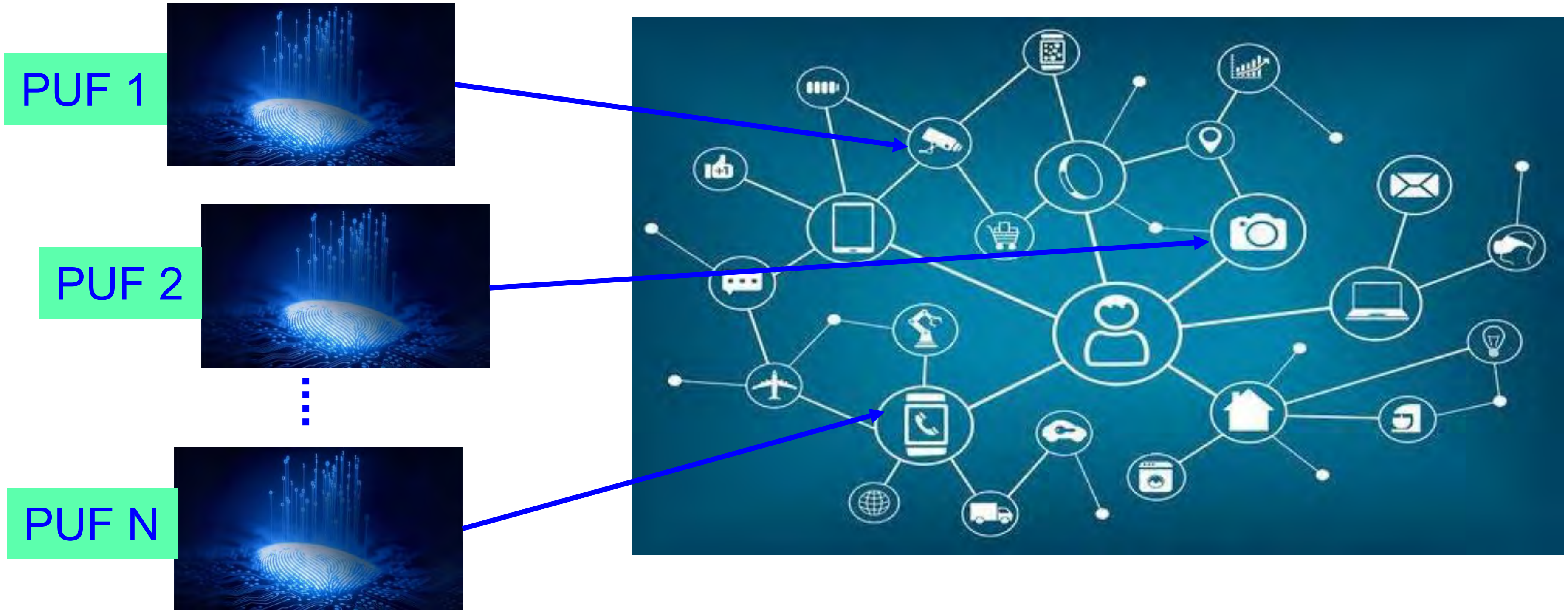
Server Output

```
Python 3.7.3 (/usr/bin/python3)
>>> %Run client_puf.py
 The Client Challenge input
 [66, 52, 17, 7, 2, 24, 89, 6]
 The Client PUF Key
 1001000110010011100100111001001110010011100100111001001110010011
 Time taken to Generate the key at Client in seconds
 0.07773900032043457
```

Client Output

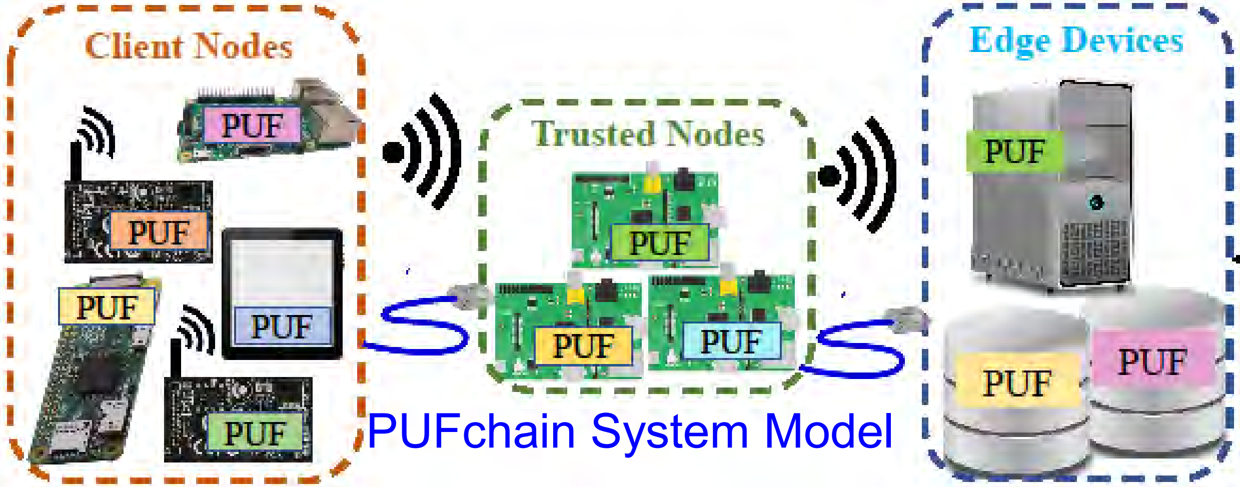
Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

We Proposed World's First Hardware-Integrated Blockchain (PUFchain) that is Scalable, Energy-Efficient, and Fast



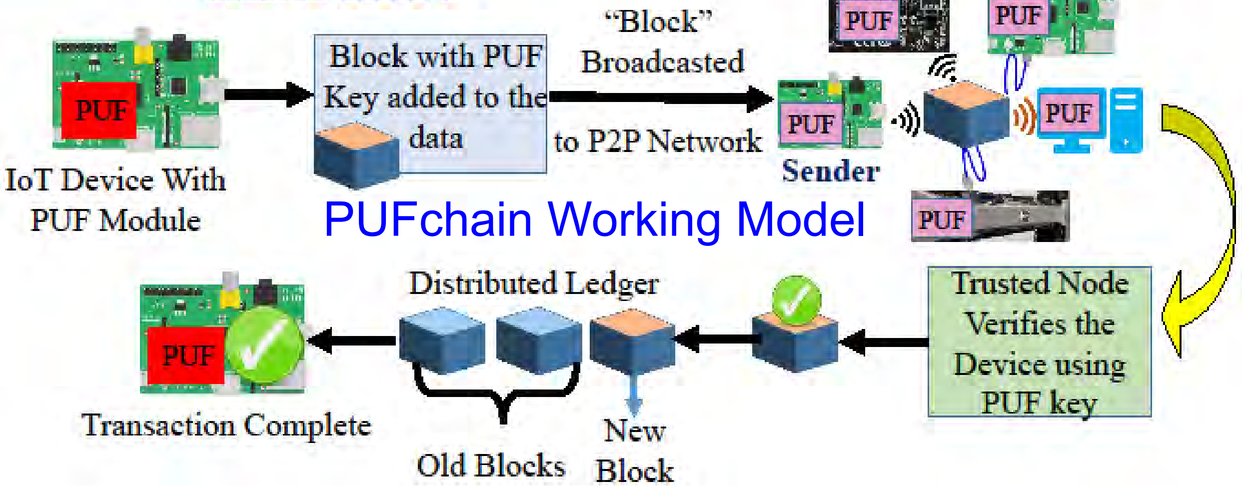
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and
Data Security



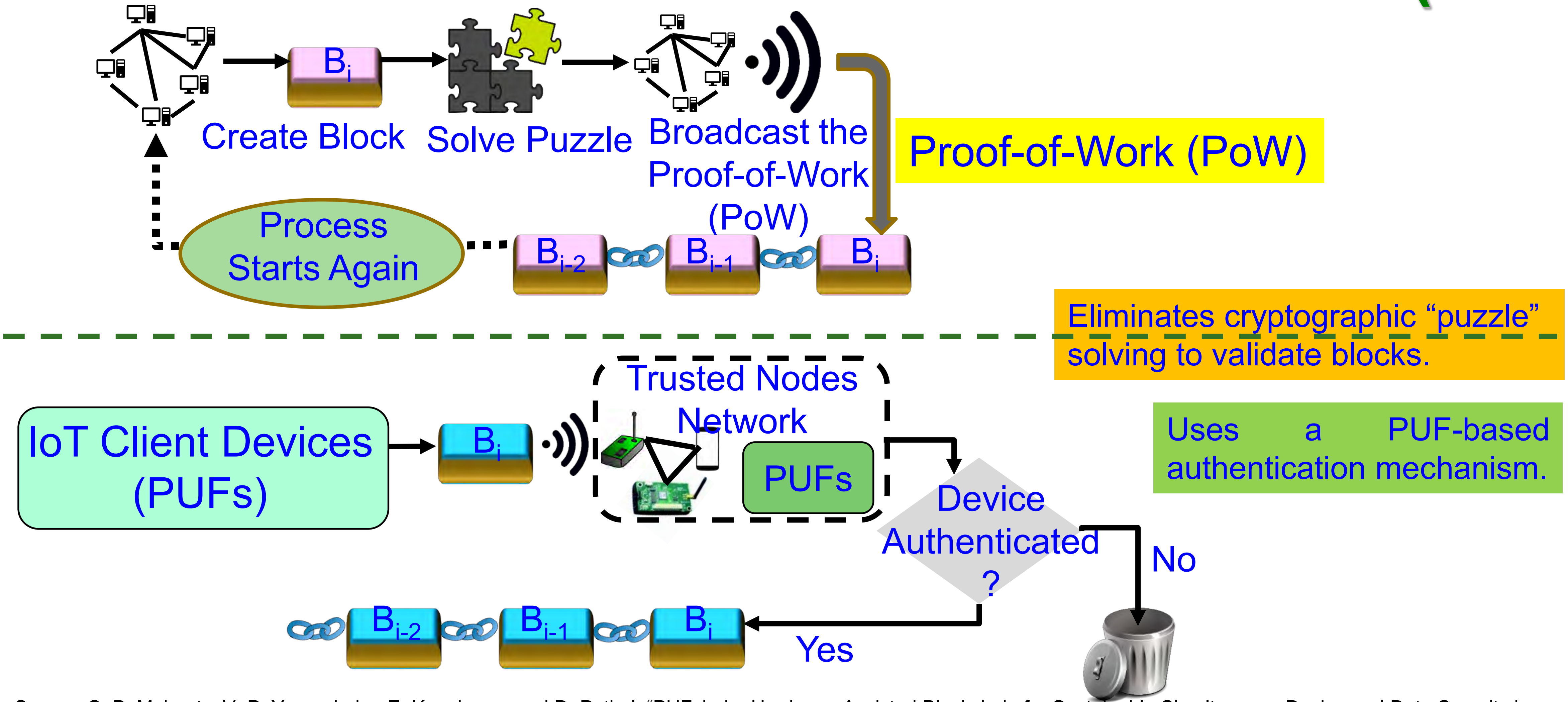
PUFchain Working Model

PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode

- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

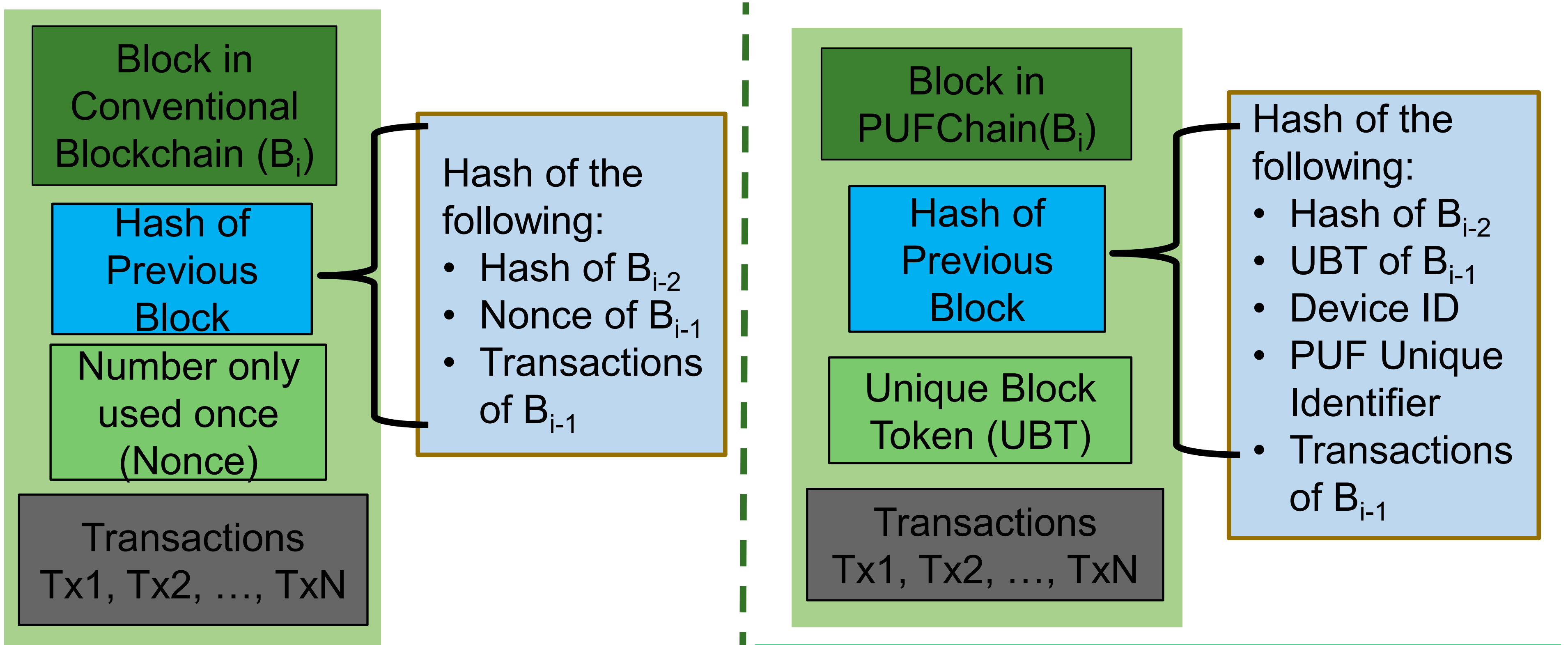
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

Our Proof-of-PUF-Enabled-Authentication (PoP)



Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

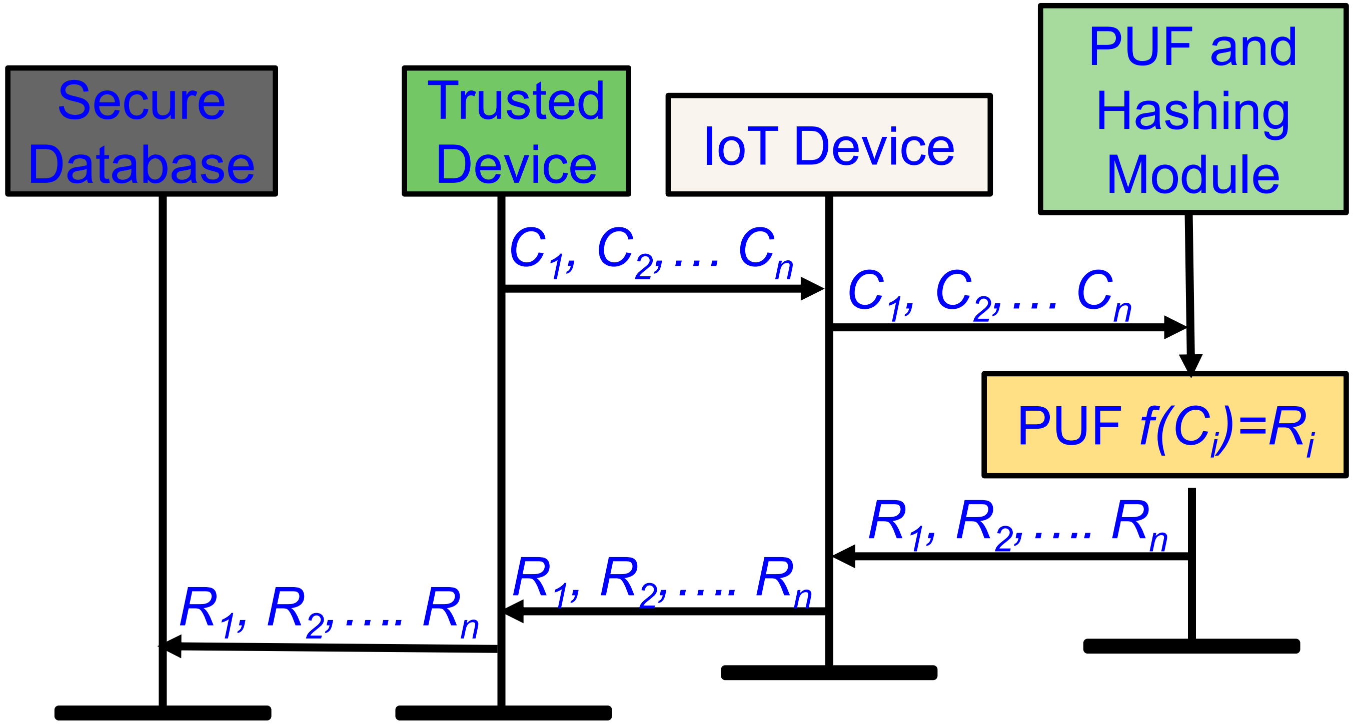
PUFchain: Proposed New Block Structure



Conventional Block Structure

Proposed Block Structure for PUFchain

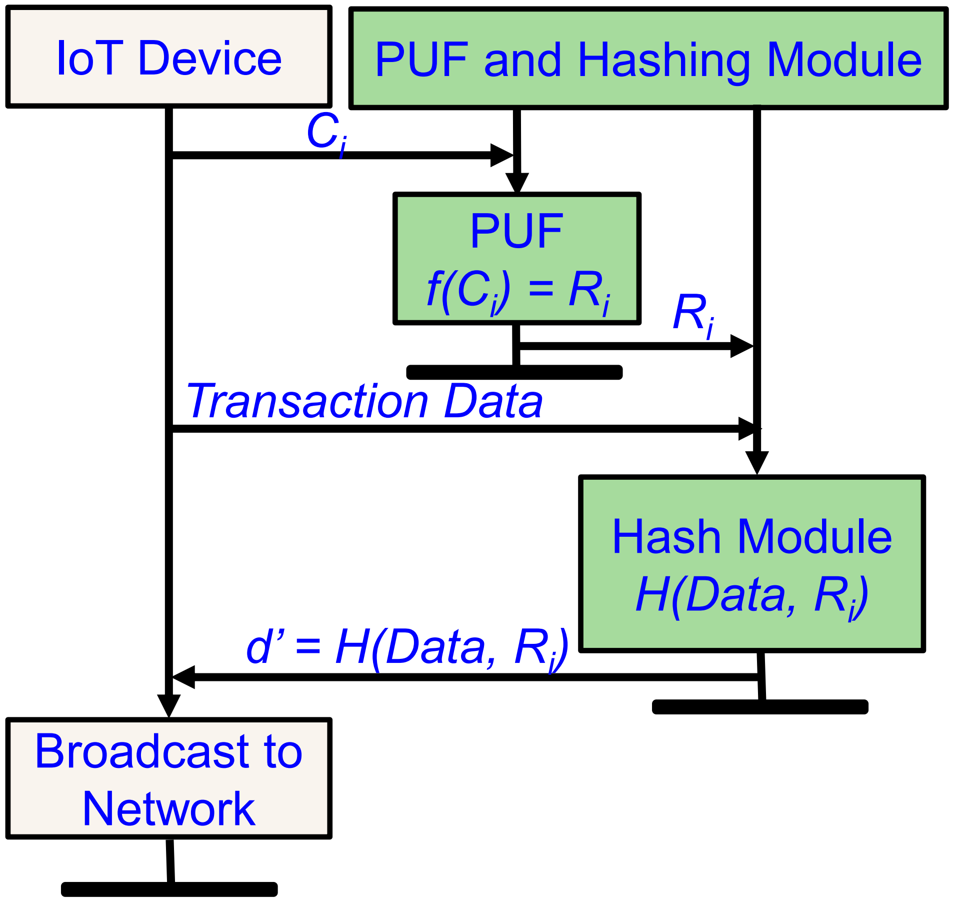
PUFchain: Device Enrollment Steps



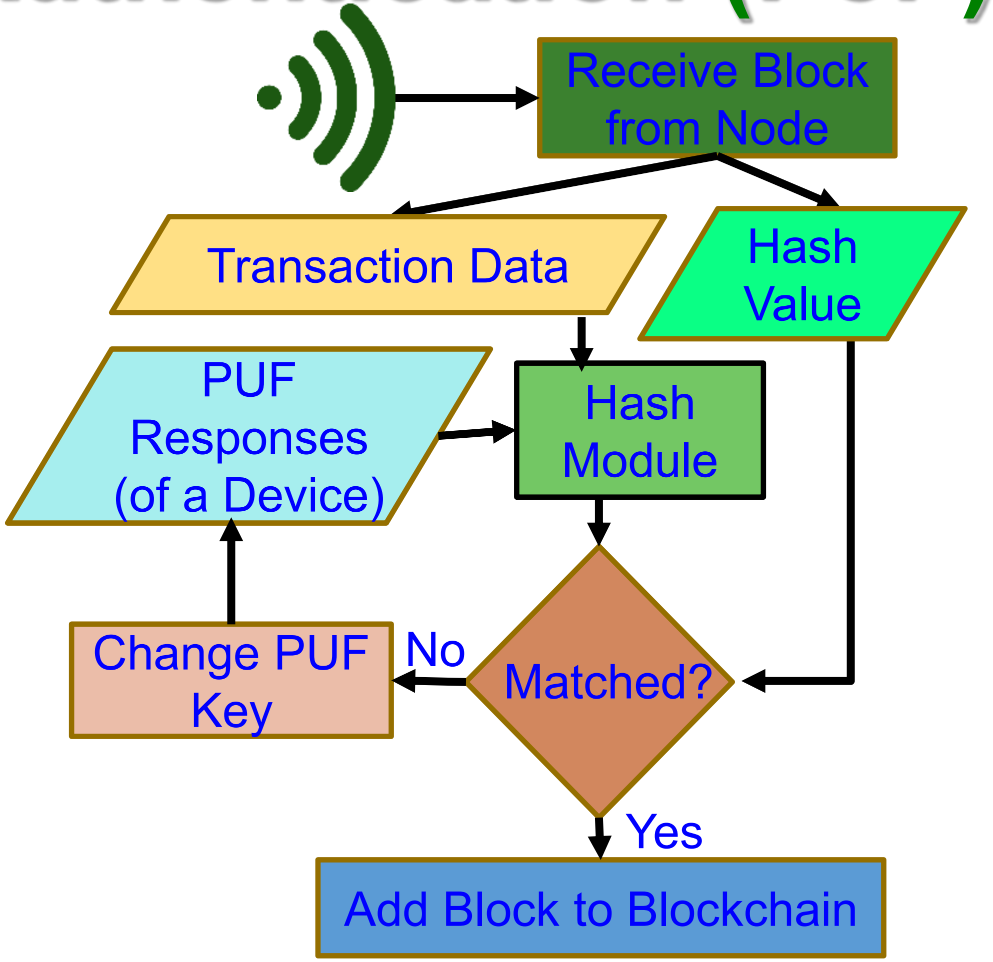
Device Enrollment Steps

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

Proof-of-PUF-Enabled-Authentication (PoP)



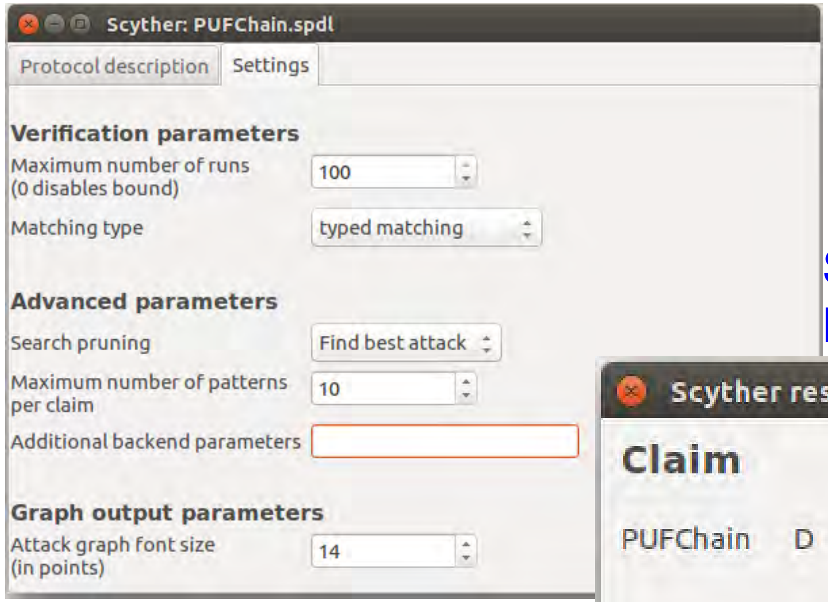
Steps for Transactions Initiation



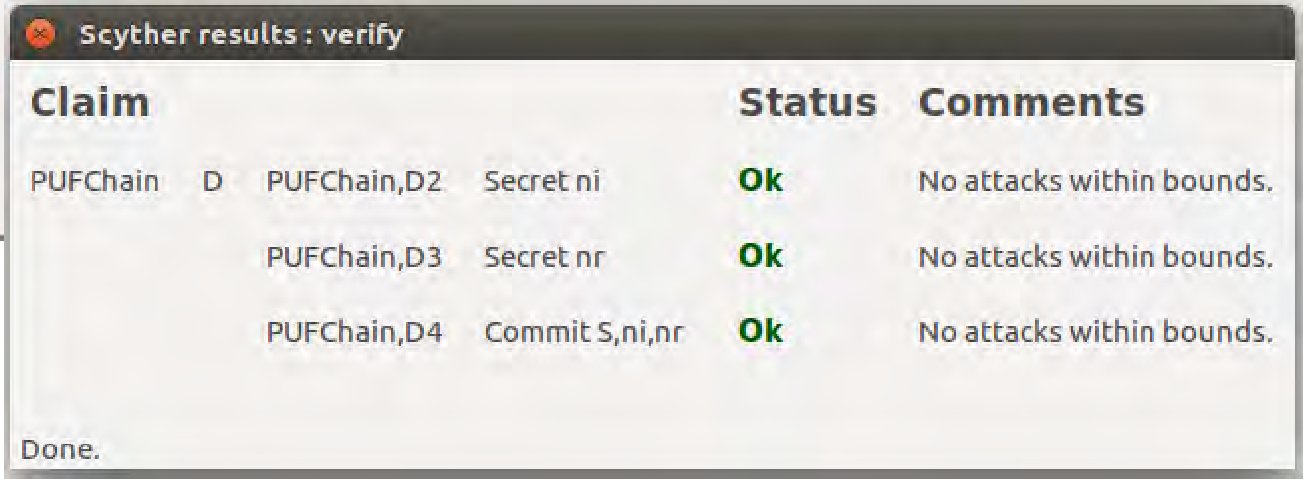
Steps for Device Authentication

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain Security Validation



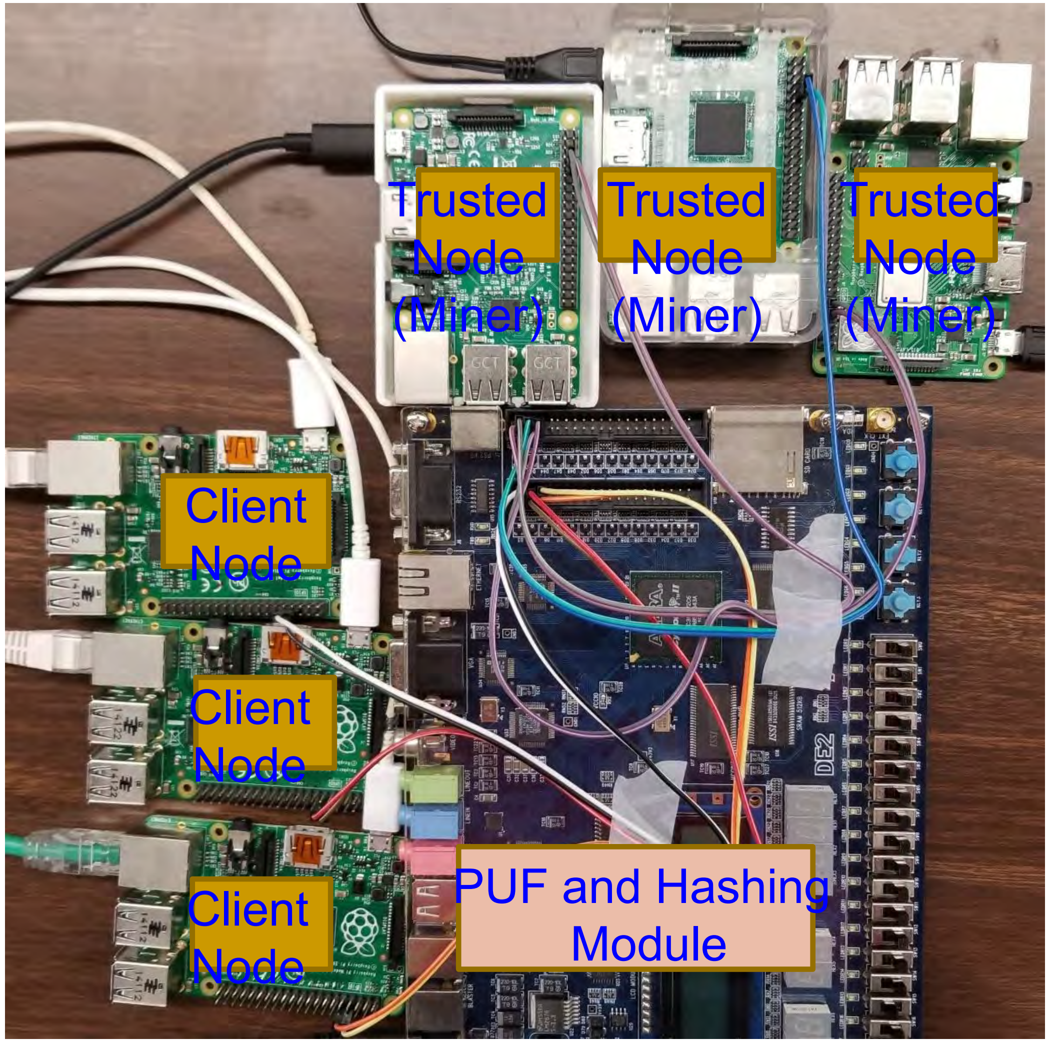
S - the source of the block
D - the miner or authenticator node in the networks



PUFchain Security Verification in Scyther simulation environment proves that PUFChain is secure against potential network threats.

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

Our PoP is 1000X Faster than PoW

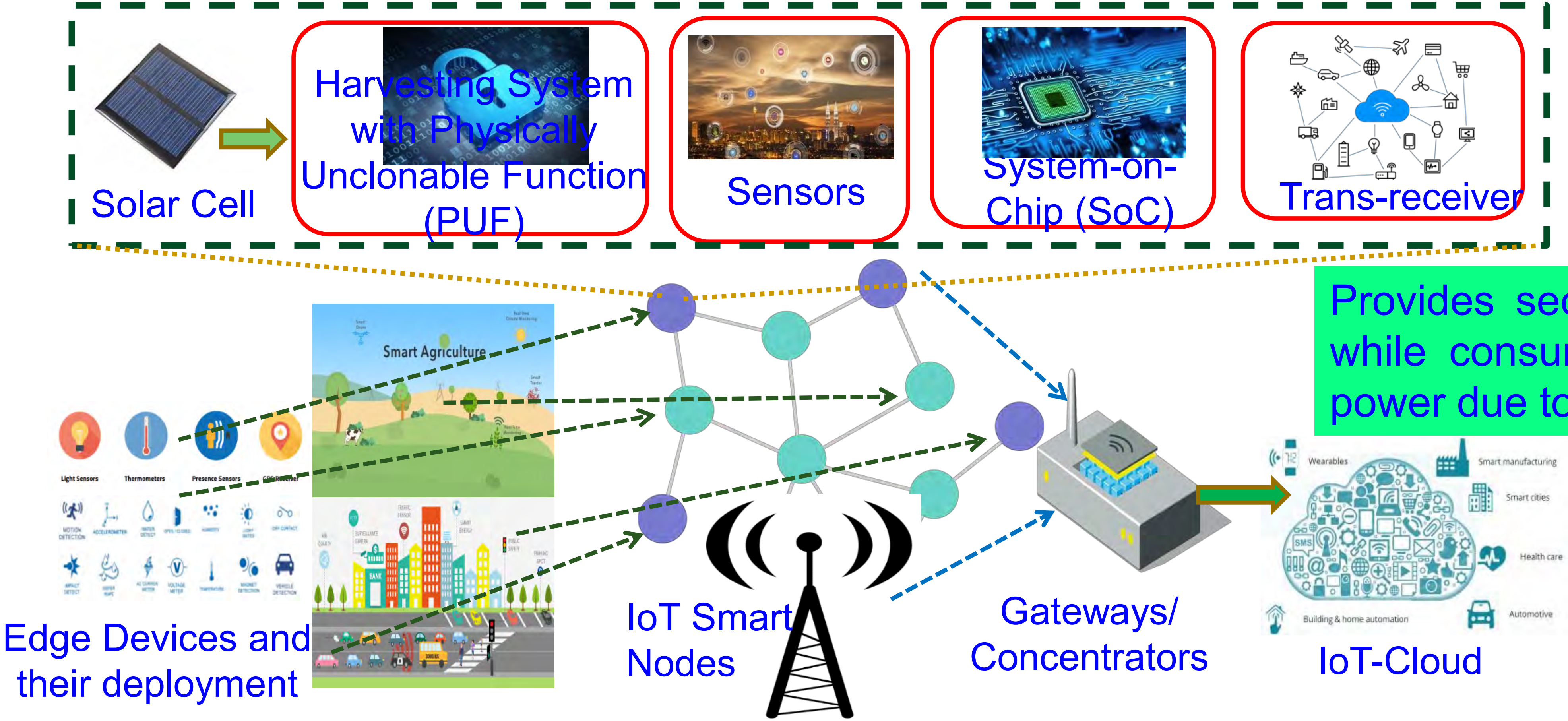


PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

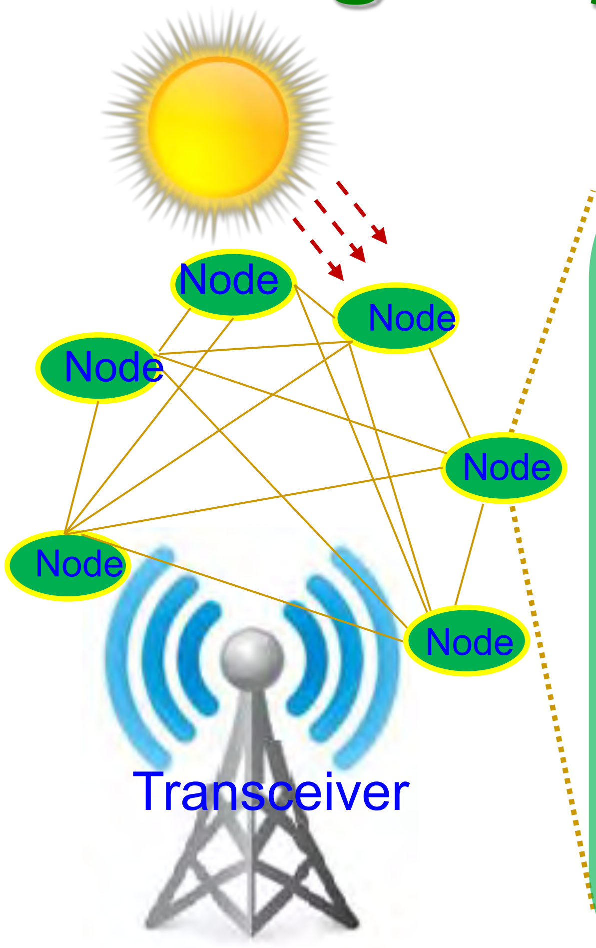
Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge

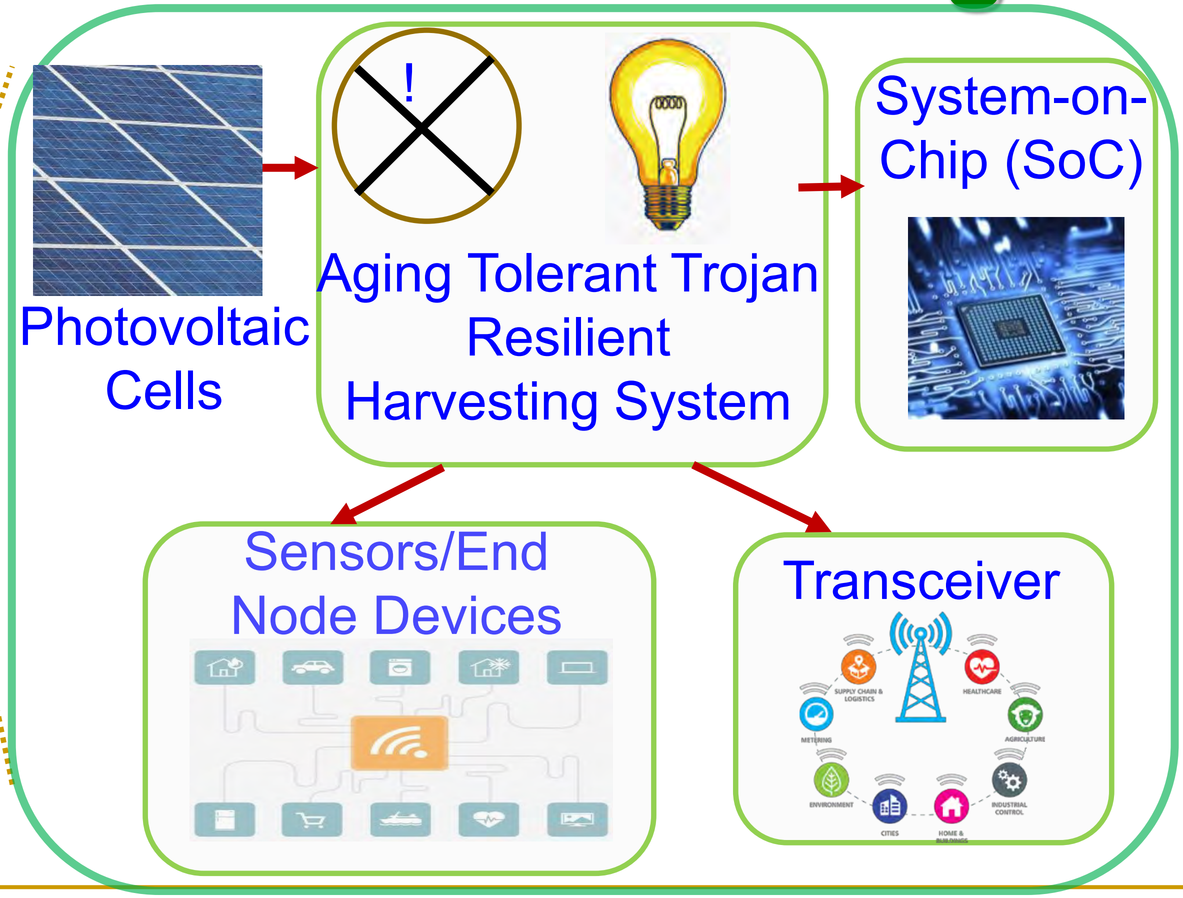


Provides security using PUFs while consuming only 22 μW power due to harvesting.

Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, “Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT”, *IEEE Transactions on Sustainable Computing*, Vol. 6, No. 2, April 2021, pp. 320--333.

Our SbD based Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the IoT-Edge





Provides security against analog-Trojan while consuming only 22 µW power due to harvesting.

Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, "Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT", arXiv Computer Science, arXiv:2103.05615, March 2021, 24-pages.

Smart Grid Cybersecurity - Solutions

Smart Grid – Security Solutions

- Network Security
- Data Security
- Key Management
- Network Security Protocol

Smart Meter

Smart Grid Cybersecurity - Strategies

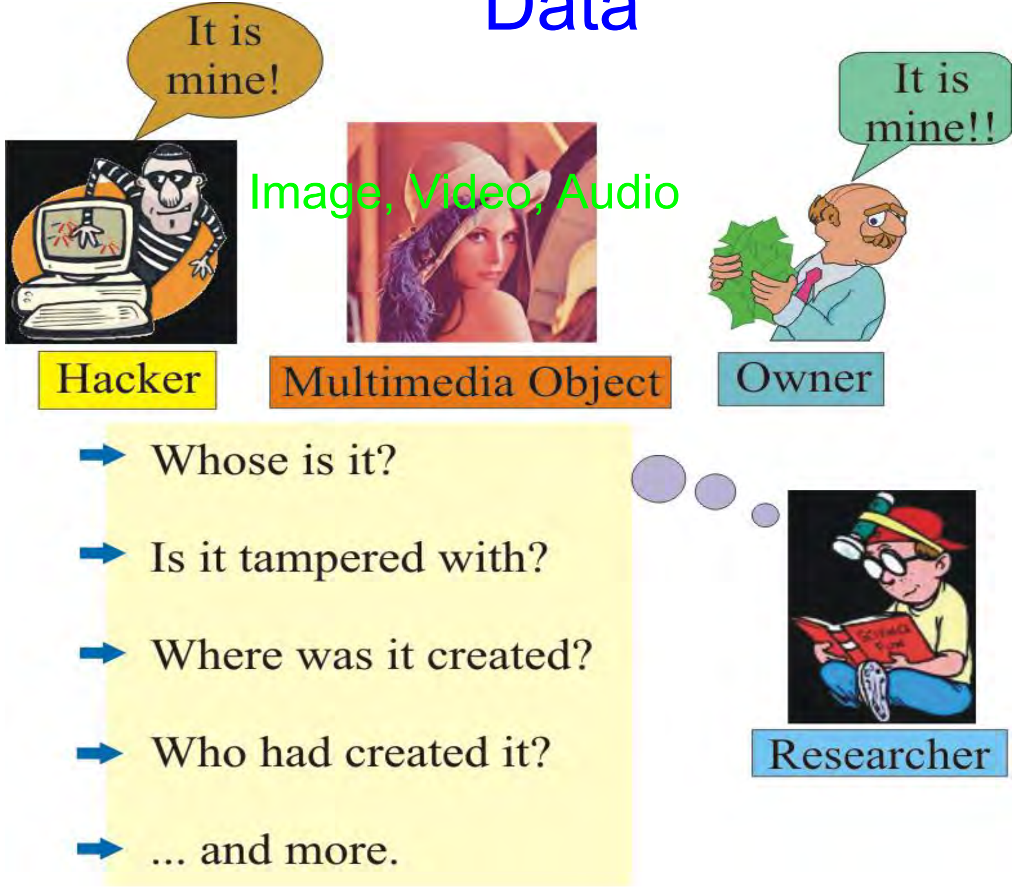
- Make Smart Grids Survivable
- Use Scalable Security Measures
- Integrate Security and Privacy by Design
- Deploy a Defense-in-Depth Approach
- Enhance Traditional Security Measures

Phasor Measurement Unit (PMU)

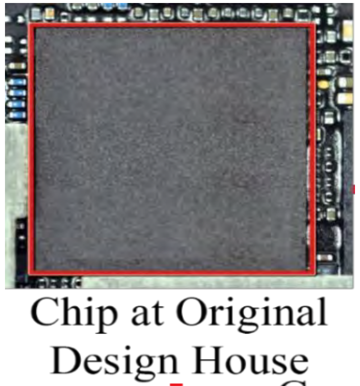
Source: S. Conovalu and J. S. Park. "Cybersecurity strategies for smart grids", *Journal of Computers*, Vol. 11, no. 4, (2016): 300-310.

Data and System Authentication and Ownership Protection – My 20 Years of Experiences

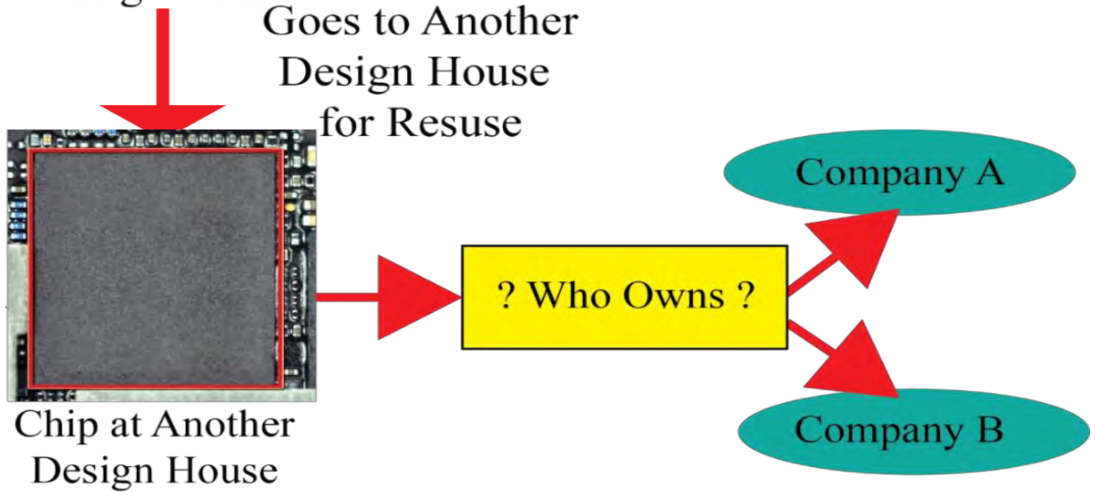
Data



System

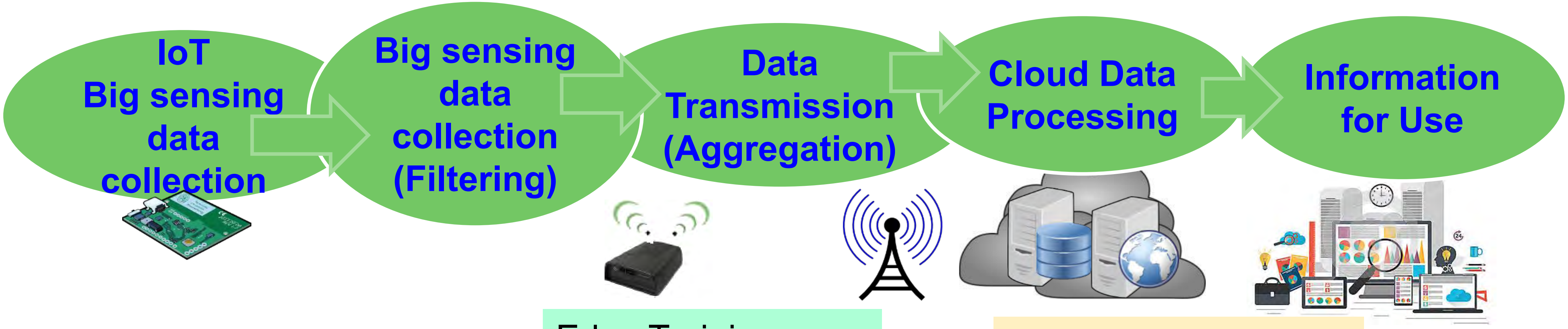


IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.



Source: S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything You Want to Know About Watermarking", *IEEE Consumer Electronics Magazine (CEM),* Volume 6, Issue 3, July 2017, pp. 83--91.

Data Quality Assurance in IoT/CPS



Edge Training:
- Data Signature
- Model Signature

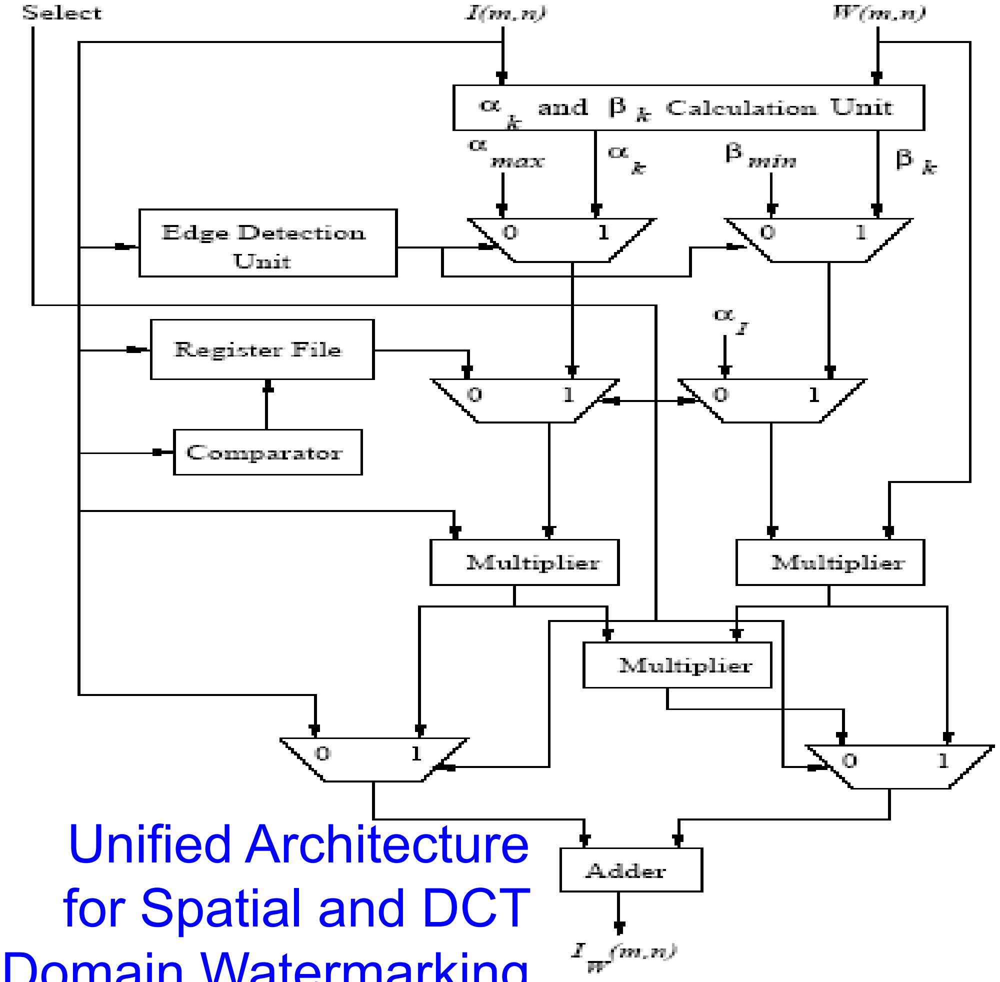
Cloud Training:
- Data Signature
- Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

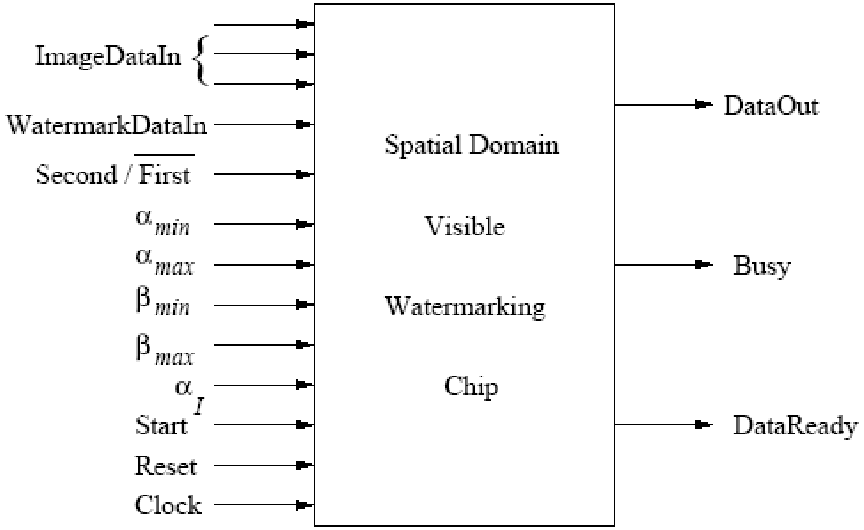
Secure data curation a solution for fake data?

Source: C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, “Big-Sensing-Data Curation for the Cloud is Coming”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 6, Issue 4, October 2017, pp. 48--56.

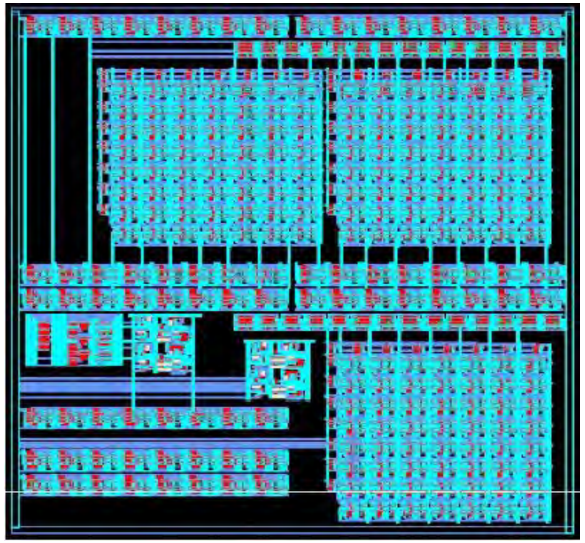
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

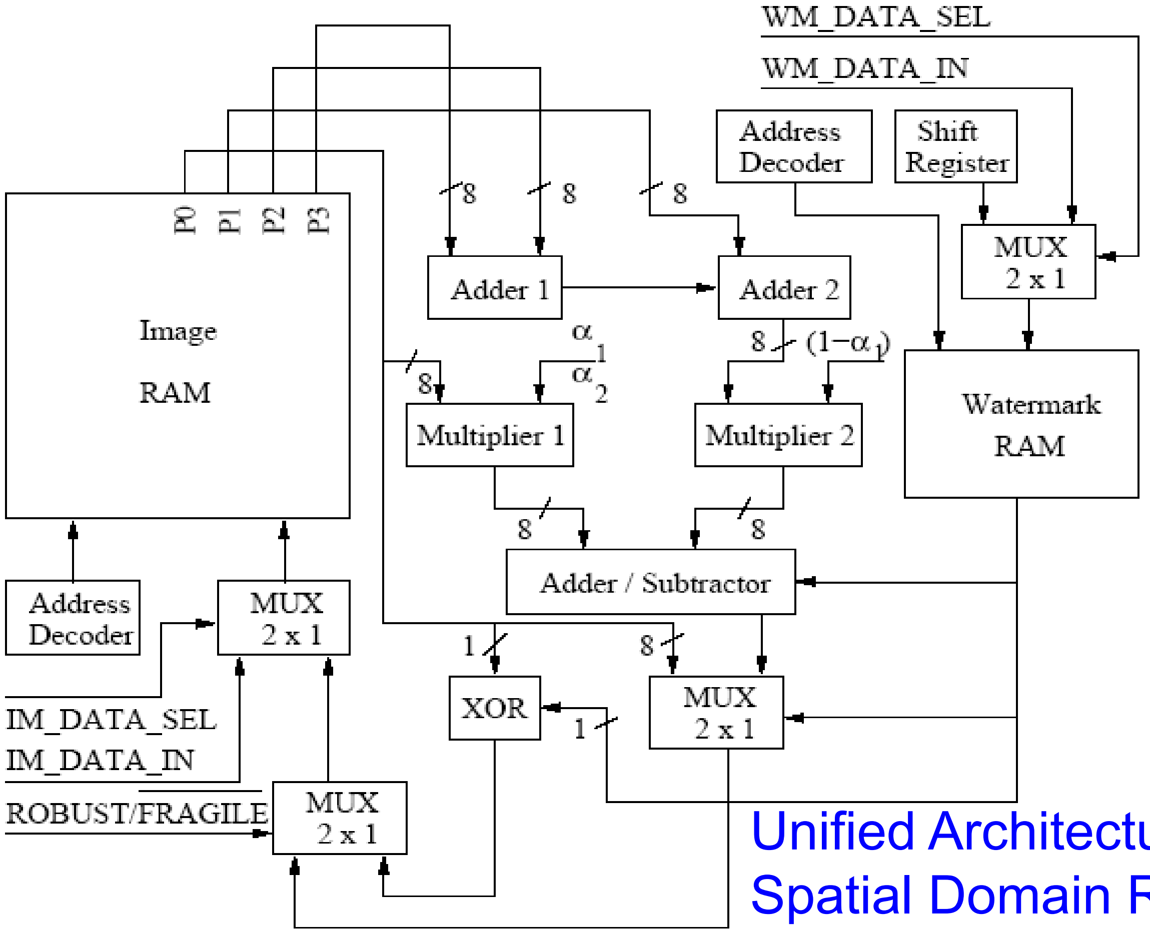
Chip Design Data

Total Area : 9.6 sq mm, No. of Gates: 28,469

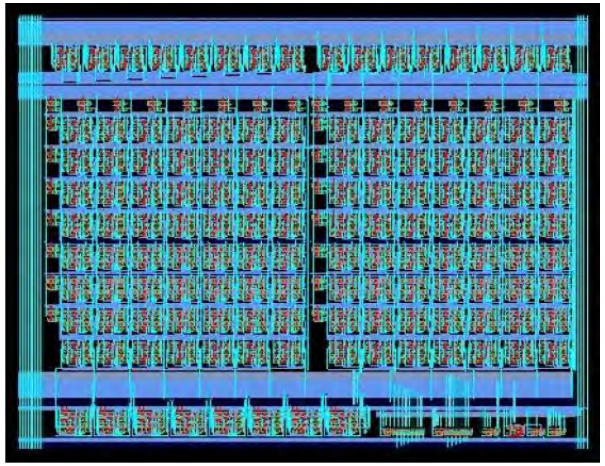
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

Source: **S. P. Mohanty**, N. Ranganathan, and R. K. Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S^{2}DC) Design", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 13, No. 8, August 2005, pp. 1002-1012.

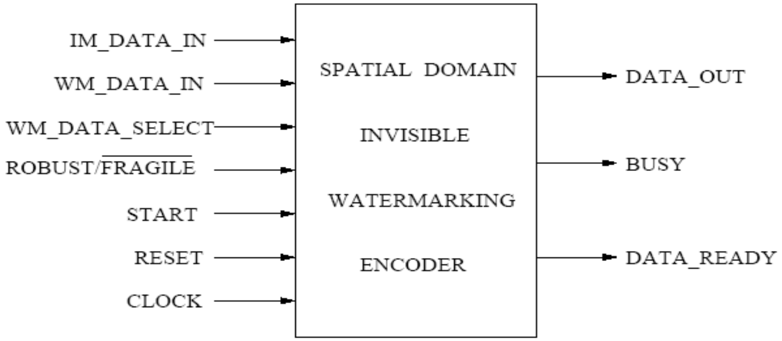
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout



Pin Diagram

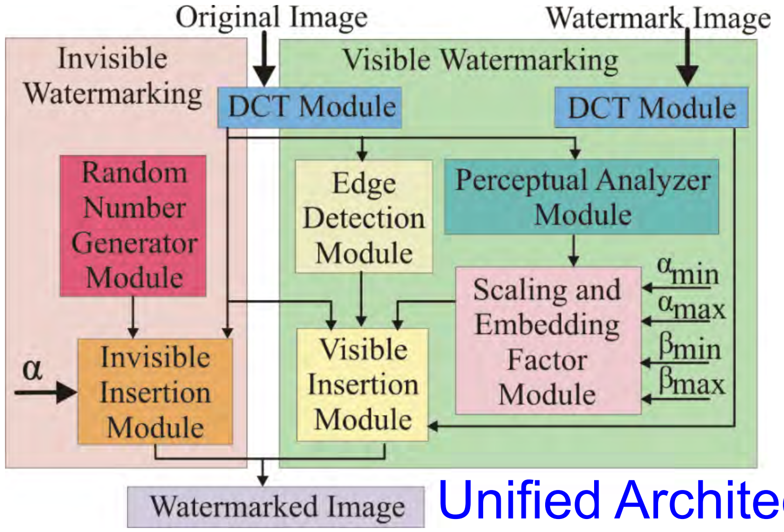
Chip Design Data

Total Area : 0.87 sq mm, No. of Gates: 4,820

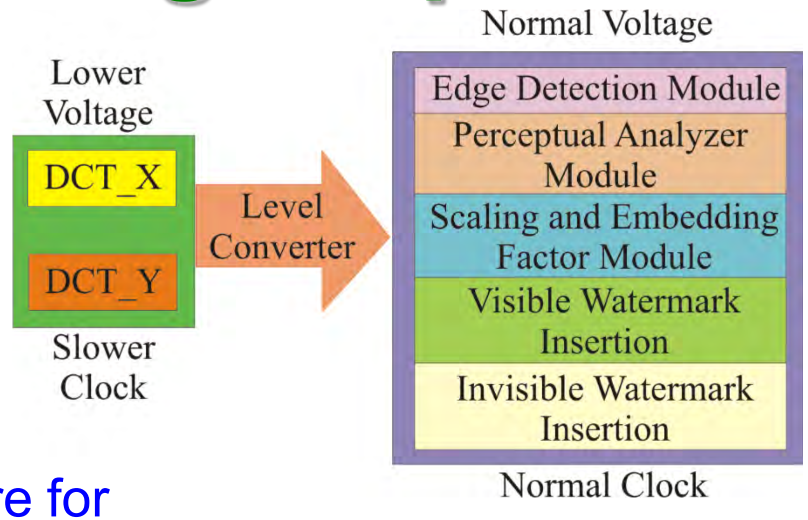
Power Consumption: 2.0 mW, Frequency: 500 MHz

Source: S. P. Mohanty, E. Kougianos, and N. Ranganathan, "VLSI Architecture and Chip for Combined Invisible Robust and Fragile Watermarking", *IET Computers & Digital Techniques (CDT)*, Sep 2007, Vol. 1, Issue 5, pp. 600-611.

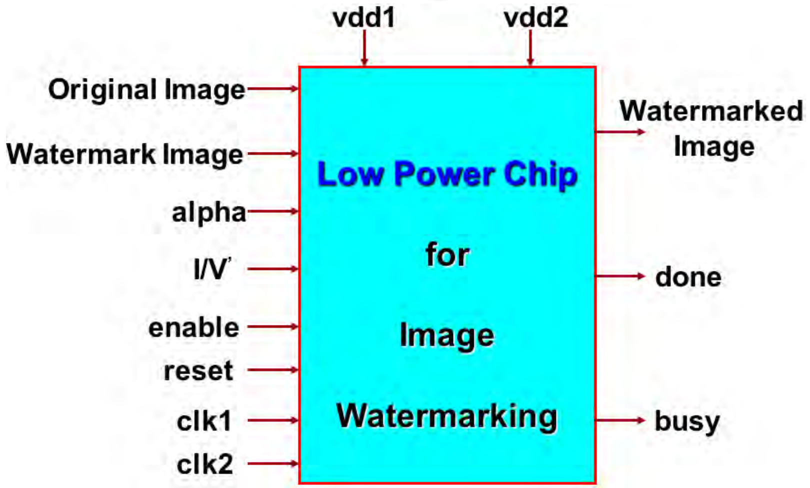
Our Design: First Ever Low-Power Watermarking Chip for Data Quality



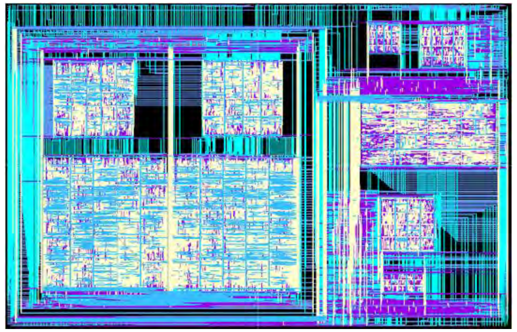
Unified Architecture for DCT Domain Watermarking



DVDF Low-Power Design



Pin Diagram



Chip Layout

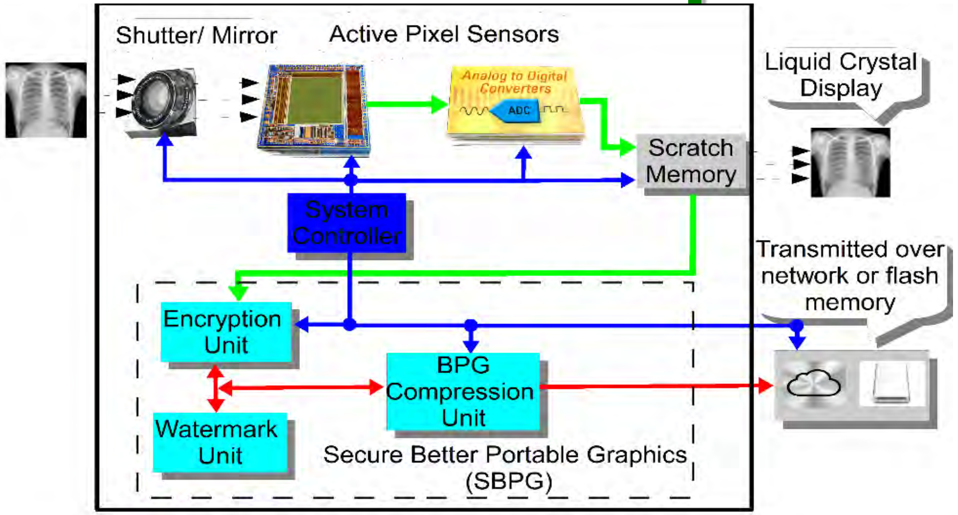
Chip Design Data

Total Area : 16.2 sq mm, No. of Transistors: 1.4 million

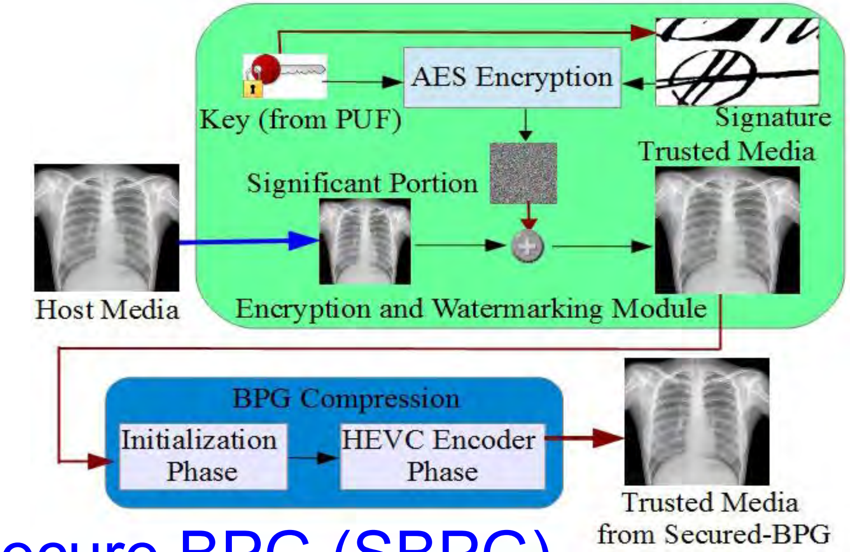
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V

Source: S. P. Mohanty, N. Ranganathan, and K. Balakrishnan, "A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain", *IEEE Transactions on Circuits and Systems II (TCAS-II)*, Vol. 53, No. 5, May 2006, pp. 394-398.

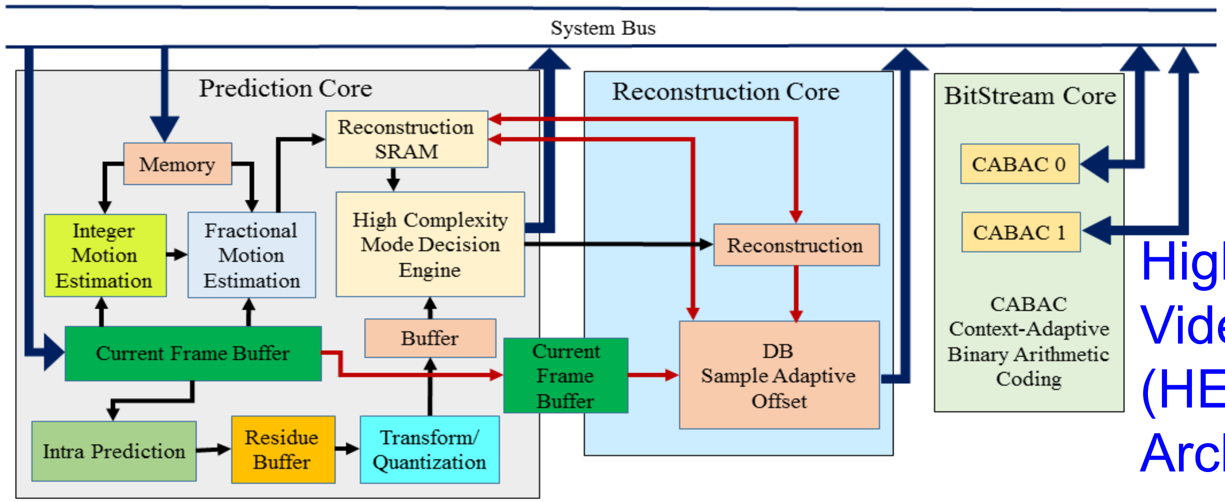
We Introduced First Ever Secure Better Portable Graphics (SBPG) Architecture



Secure Digital Camera (SDC) with SBPG



Secure BPG (SBPG)

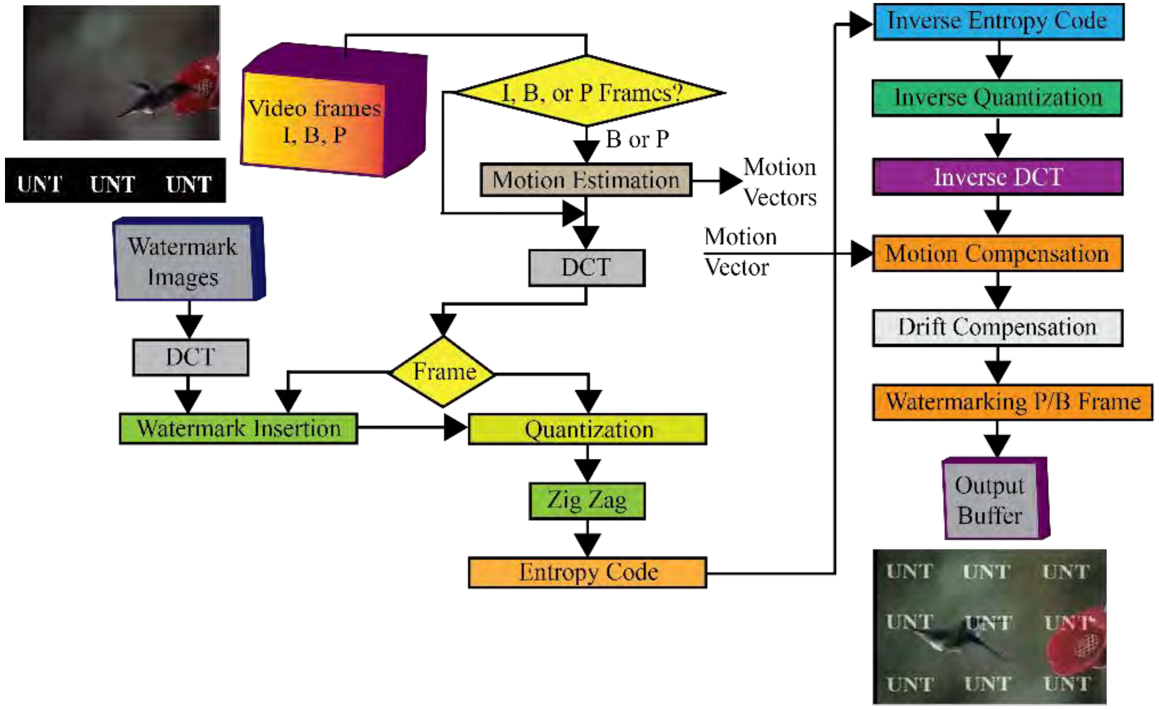


High-Efficiency Video Coding (HEVC) Architecture

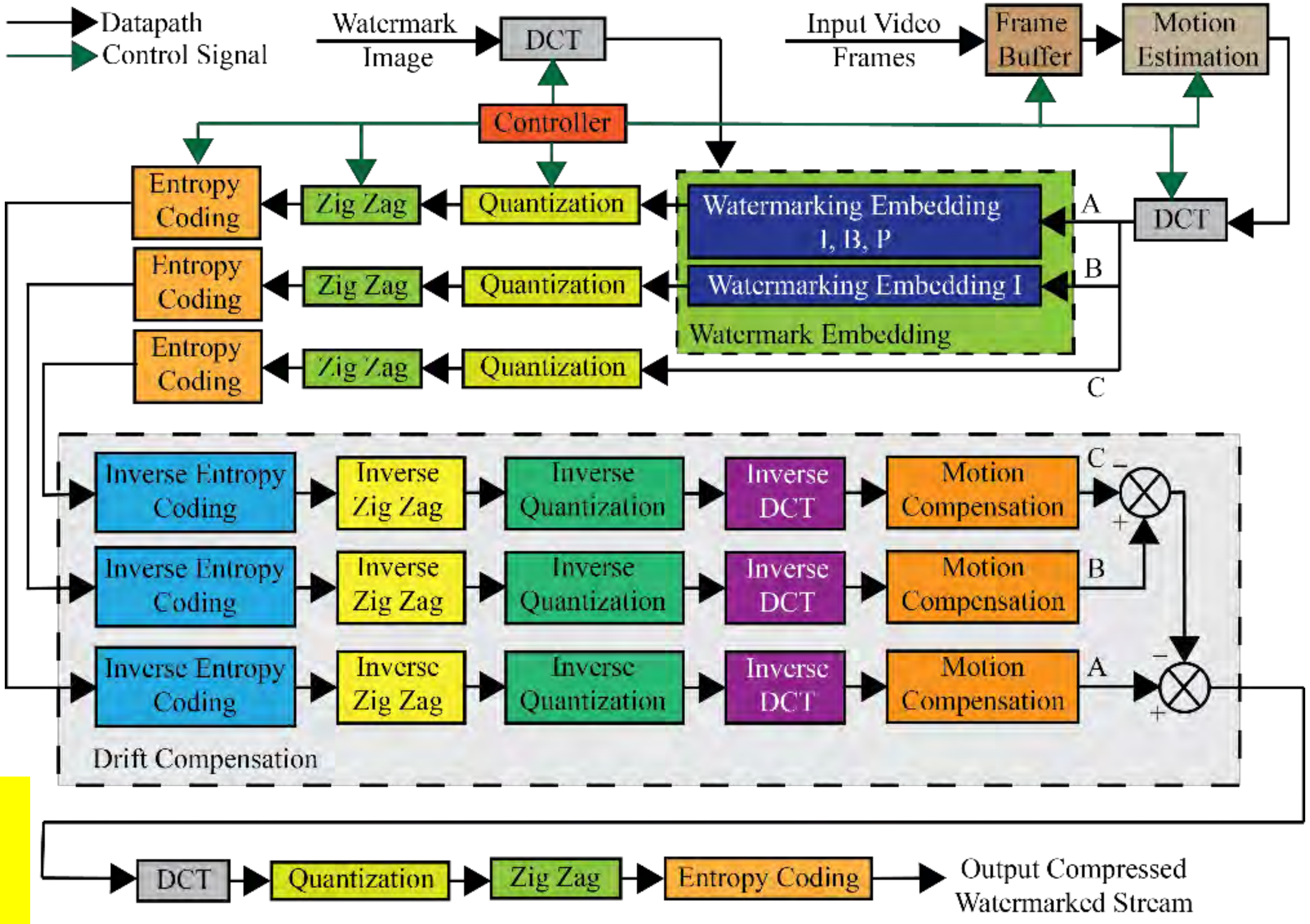
Simulink Prototyping
Throughput: 44 frames/sec
Power Dissipation: 8 nW

Source: S. P. Mohanty, E. Kougianos, and P. Guturu, "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT (Invited Paper)", *IEEE Access Journal*, Volume 6, 2018, pp. 5939--5953.

Our Hardware for Real-Time Video Watermarking



(a) Video Watermarking Algorithm as a Flow Chart

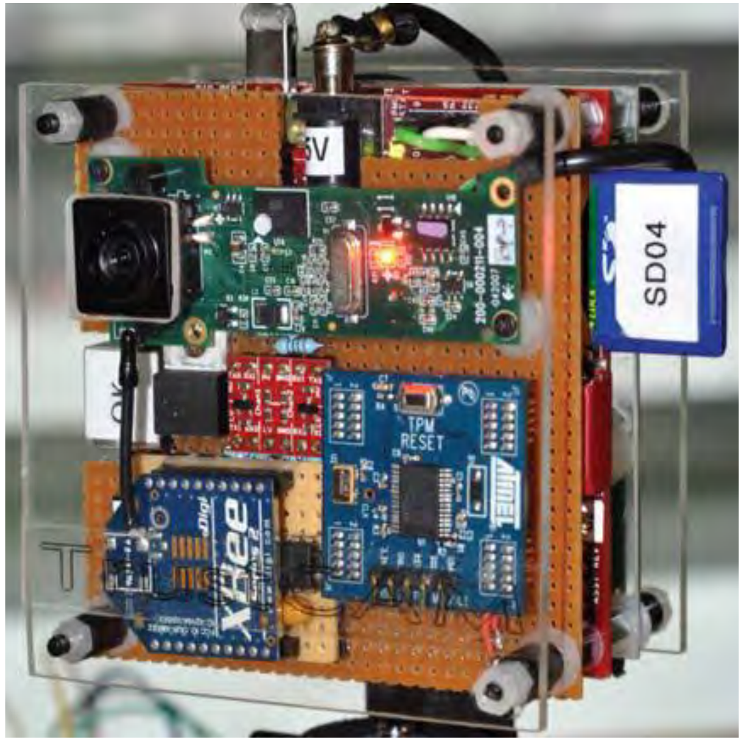


(b) Architecture of the Video Watermrking Algorithm

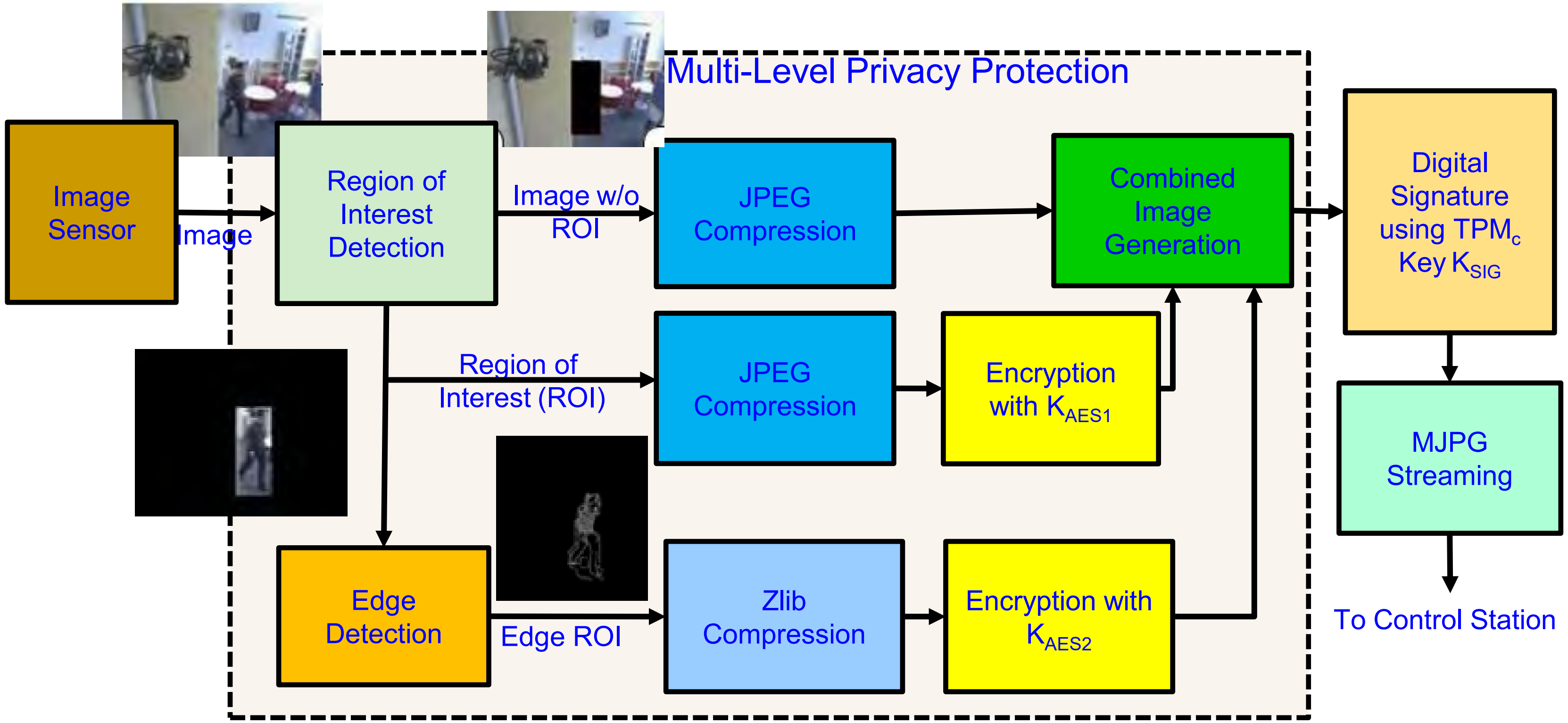
FPGA based Design Data
Resource: 28322 LE, 16532 Registers, 9 MUXes
Operating Frequency: 100 MHz
Throughput: 43 fps

Source: **S. P. Mohanty** and E. Kougianos, "Real-Time Perceptual Watermarking Architectures for Video Broadcasting", *Journal of Systems and Software*, Vol. 84, No. 5, May 2011, pp. 724--738.

My Watermarking Research Inspired - TrustCAM



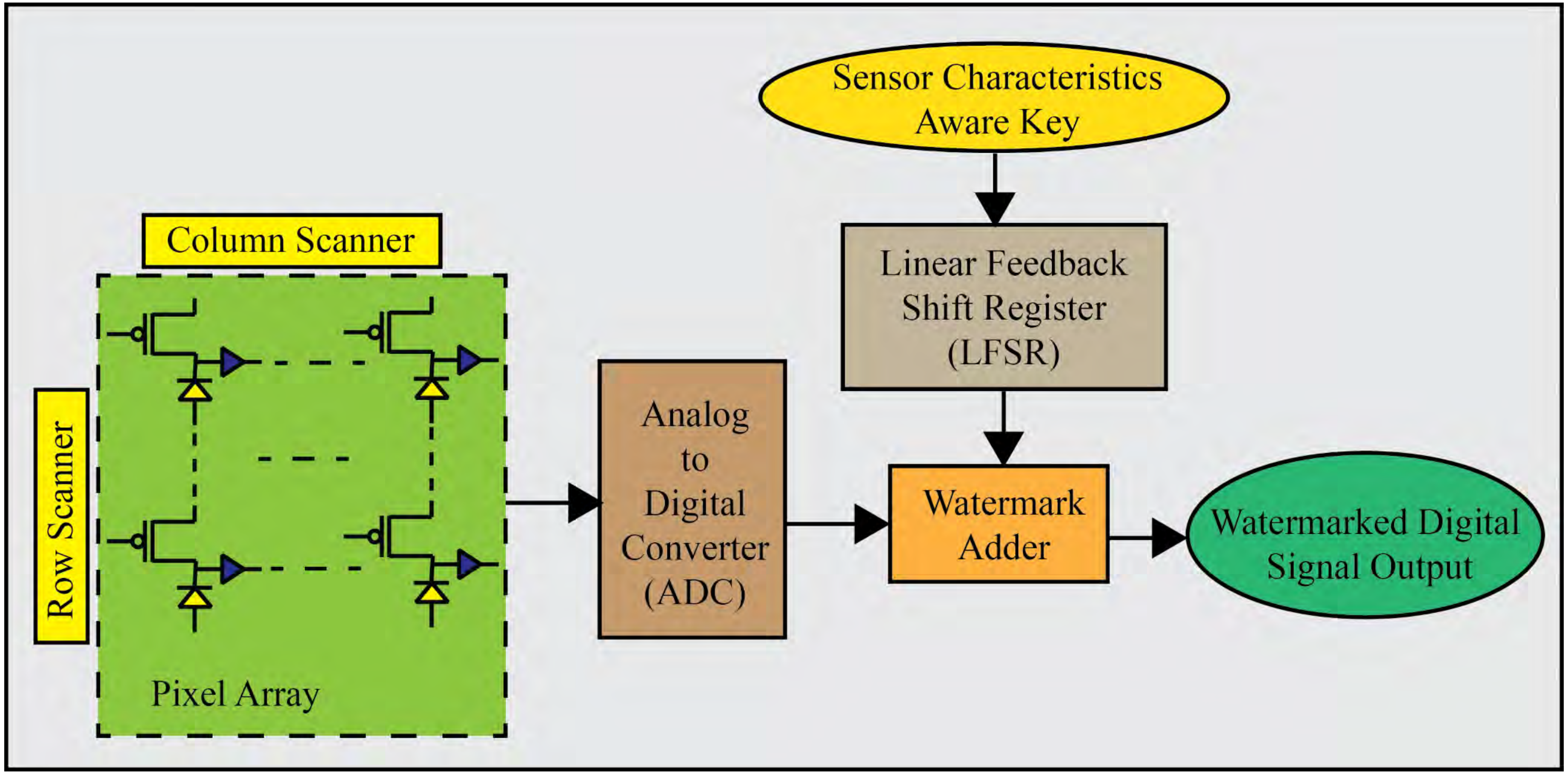
Source: https://pervasive.aau.at/BR/pubs/2010/Winkler_AVSS2010.pdf



For integrity protection, authenticity and confidentiality of image data.

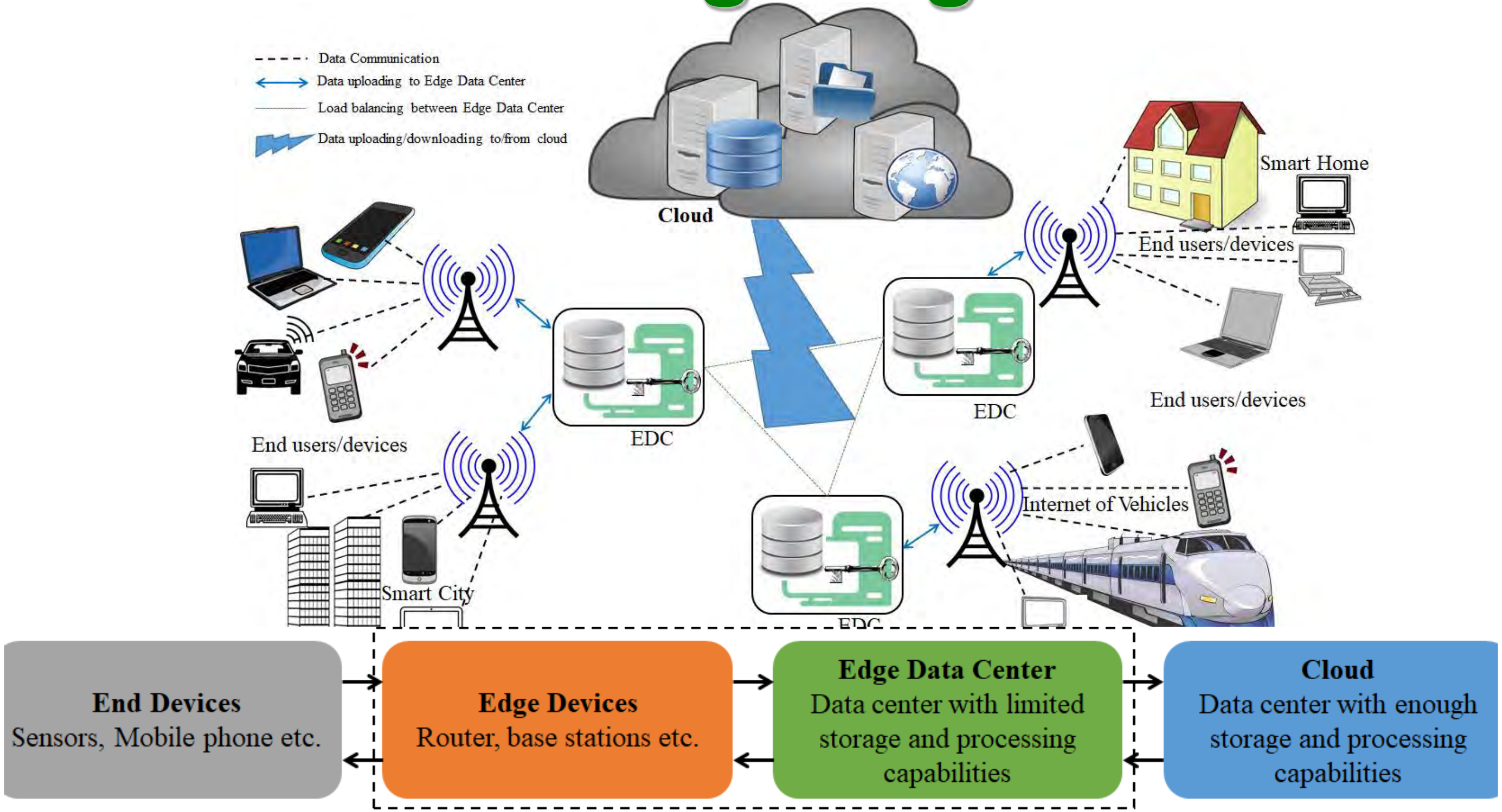
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

My Watermarking Research Inspired – Secured Sensor



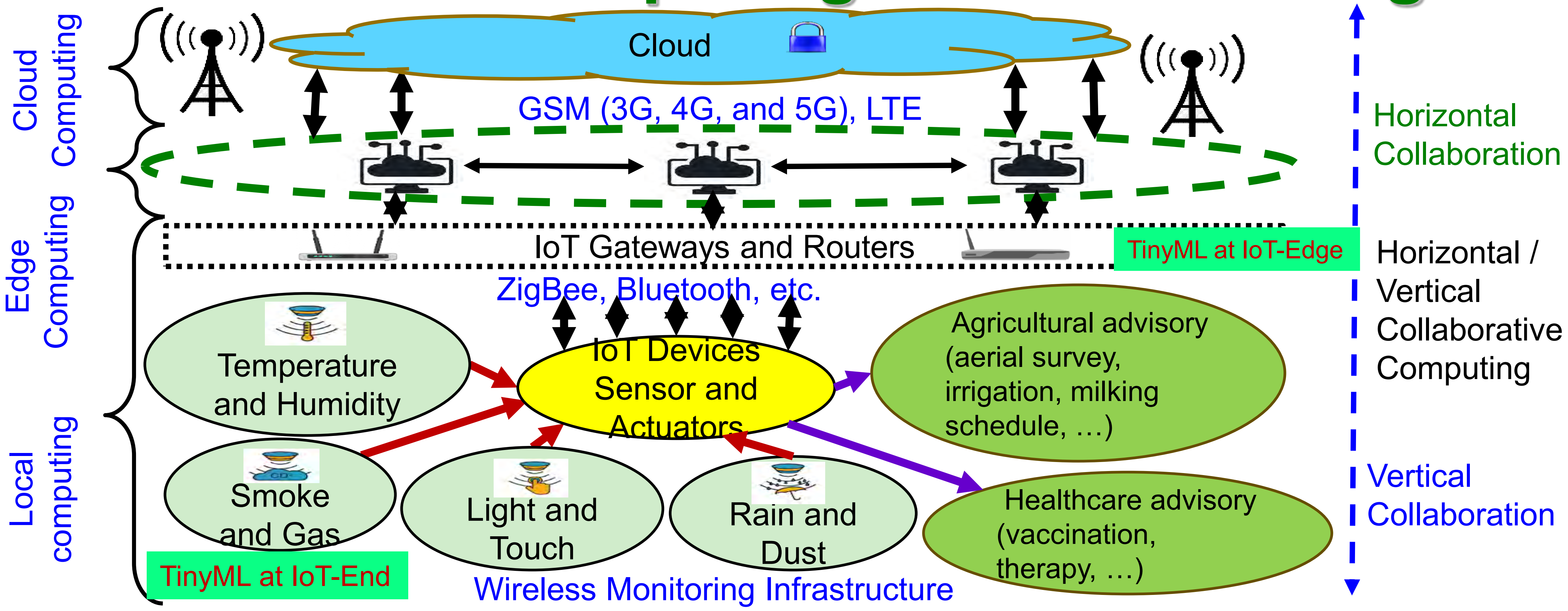
Source: G. R. Nelson, G. A. Jullien, O. Yadid-Pecht, "CMOS Image Sensor With Watermarking Capabilities", in *Proc. IEEE International Symposium on Circuits and Systems* (*ISCAS*), 2005, pp. 5326–5329.

Data and Security Should be Distributed using Edge Datacenter



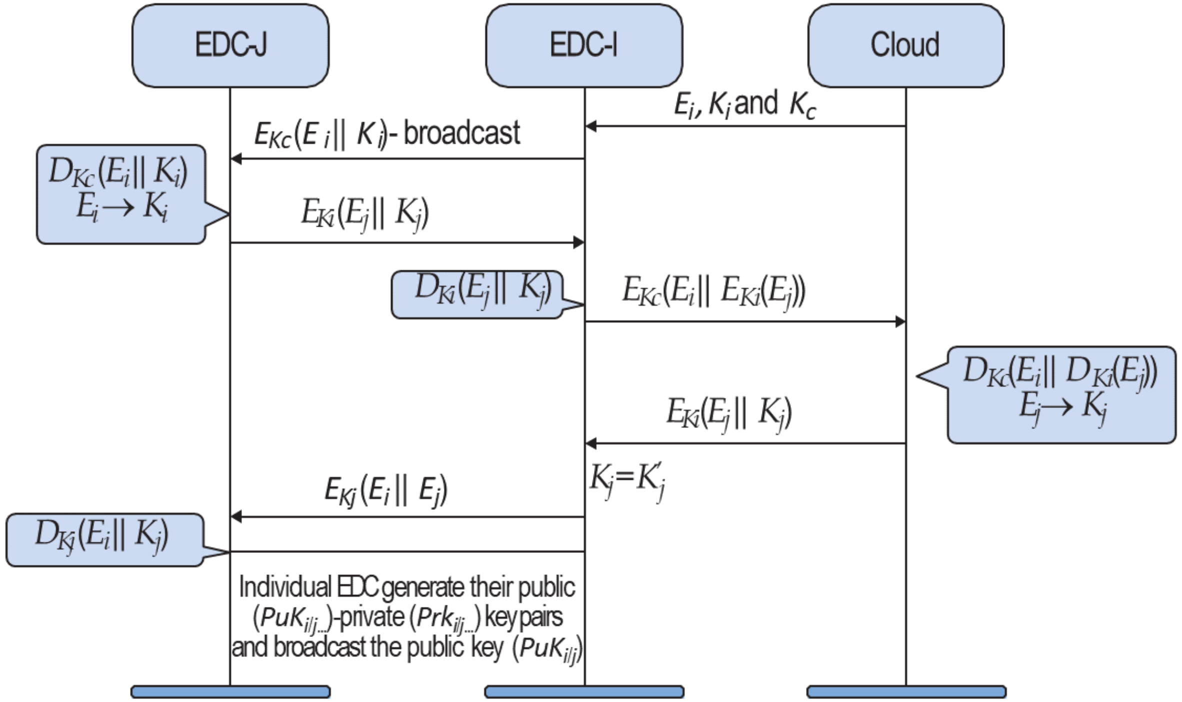
Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing”, *IEEE Communications Magazine*, Volume 56, Issue 5, May 2018, pp. 60--65.

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, "Collaborative Edge Computing for Smart Villages", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.

Our Proposed Secure Edge Datacenter



Secure edge datacenter –
- Balances load among the EDCs
- Authenticates EDCs

Algorithm 1: Load Balancing Technique

1. If (EDC-I is overloaded)
2. EDC-I broadcast (E_i, L_i)
3. EDC-J (neighbor EDC) verifies:
4. If (E_i is in database) & ($p \le 0.6$ & $L_i << (n-m)$)
5. Response $E_{Kpu_i}(E_j || K_j || p)$
6. EDC-I perform $D_{Kpr_i}(E_j || K_j || p)$
7. $k_j' \leftarrow E_j$
8. If ($k_j' = k_j$)
9. EDC-I select EDC-J for load balancing.

Response time of the destination EDC has reduced by 20-30% using the proposed allocation approach.

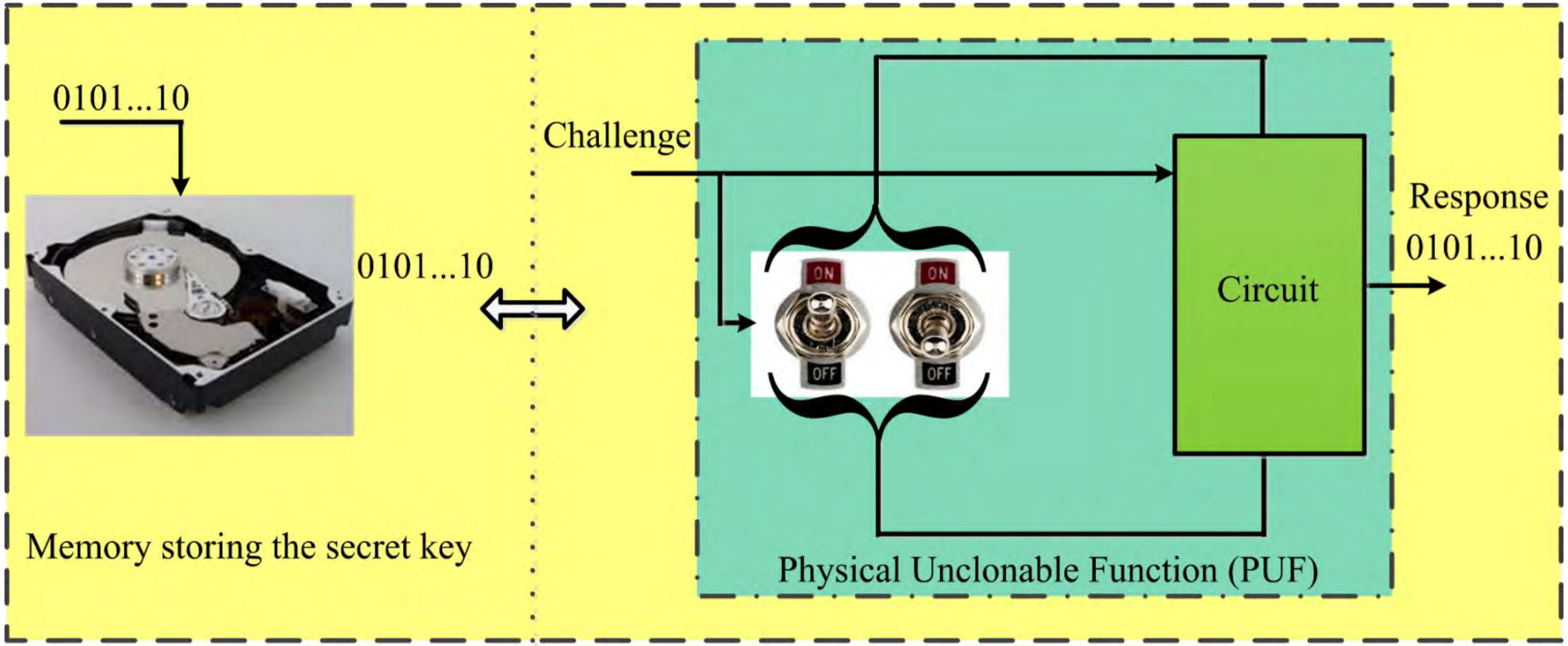
Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing”, *IEEE Communications Magazine*, Volume 56, Issue 5, May 2018, pp. 60--65.

Physical Unclonable Function – Introduction

Lock and Key

- Earliest mechanical lock found dates back 4000 years.
- Even today, we keep things under LOCK and KEY – but digitally.
- Digital keys are stored in Non – Volatile Memory (NVM) for cryptographic applications.

PUFs Don't Store Keys

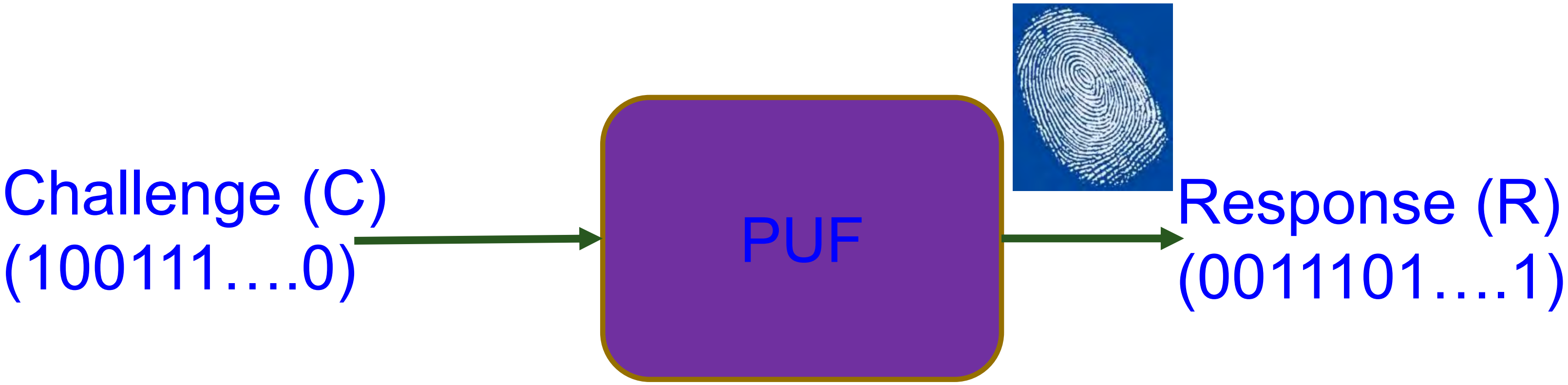


Source: S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

Physical Unclonable Functions (PUFs) - Principle

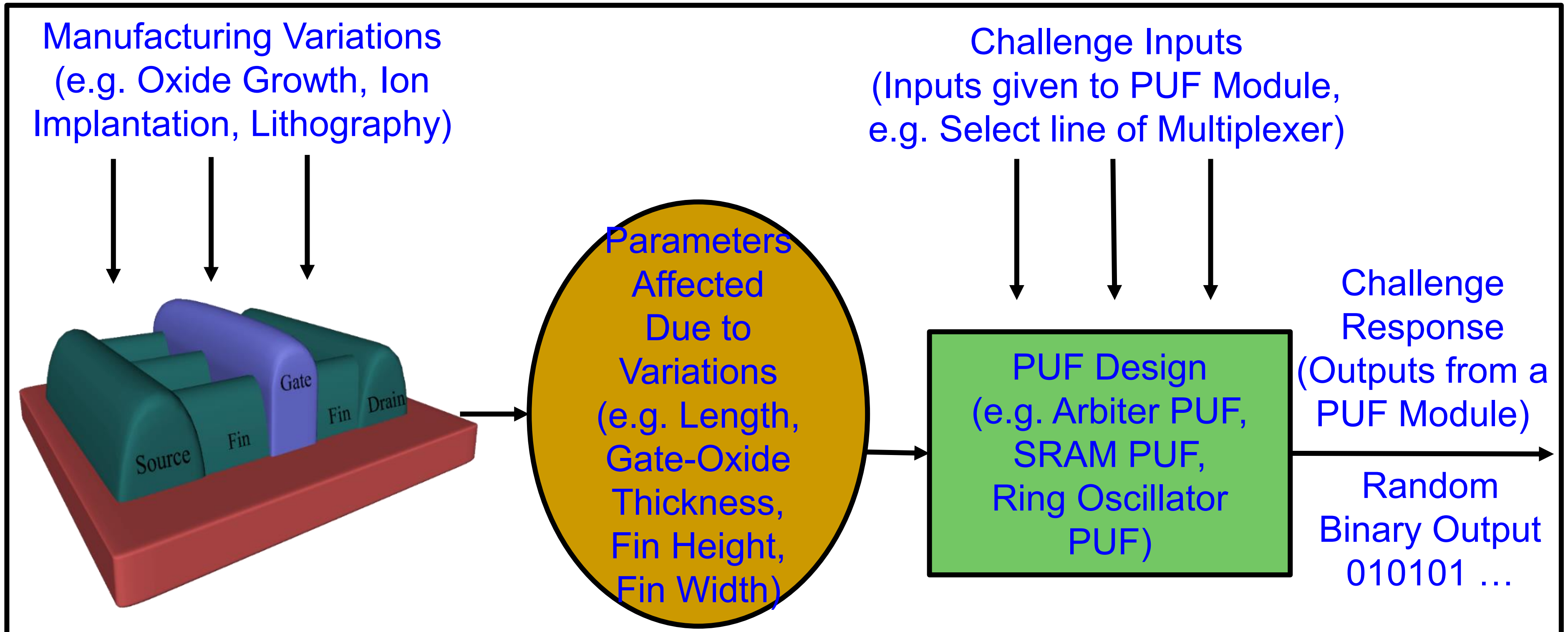
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

Source: S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

PUF - Principle



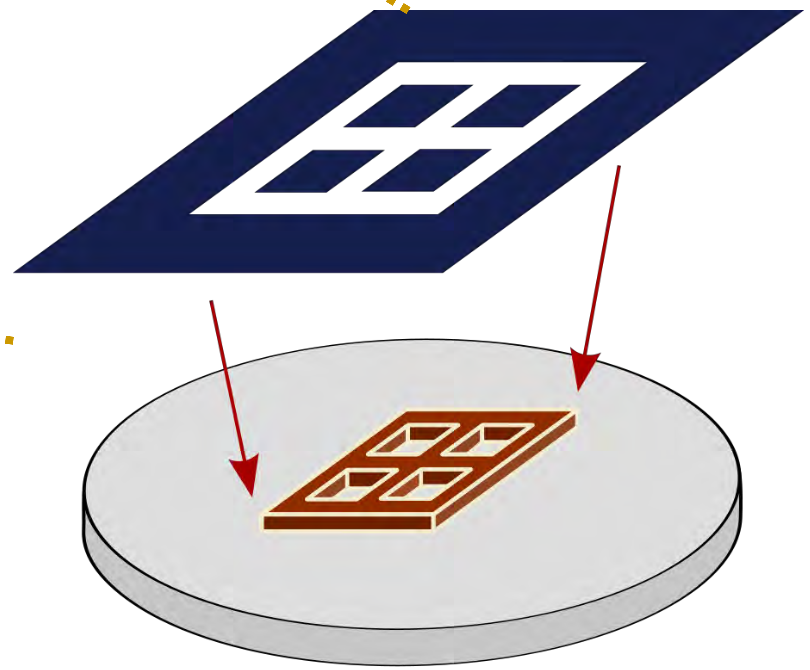
Silicon manufacturing process variations are turned into a feature rather than a problem.

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3, December 2017, pp. 429--441.

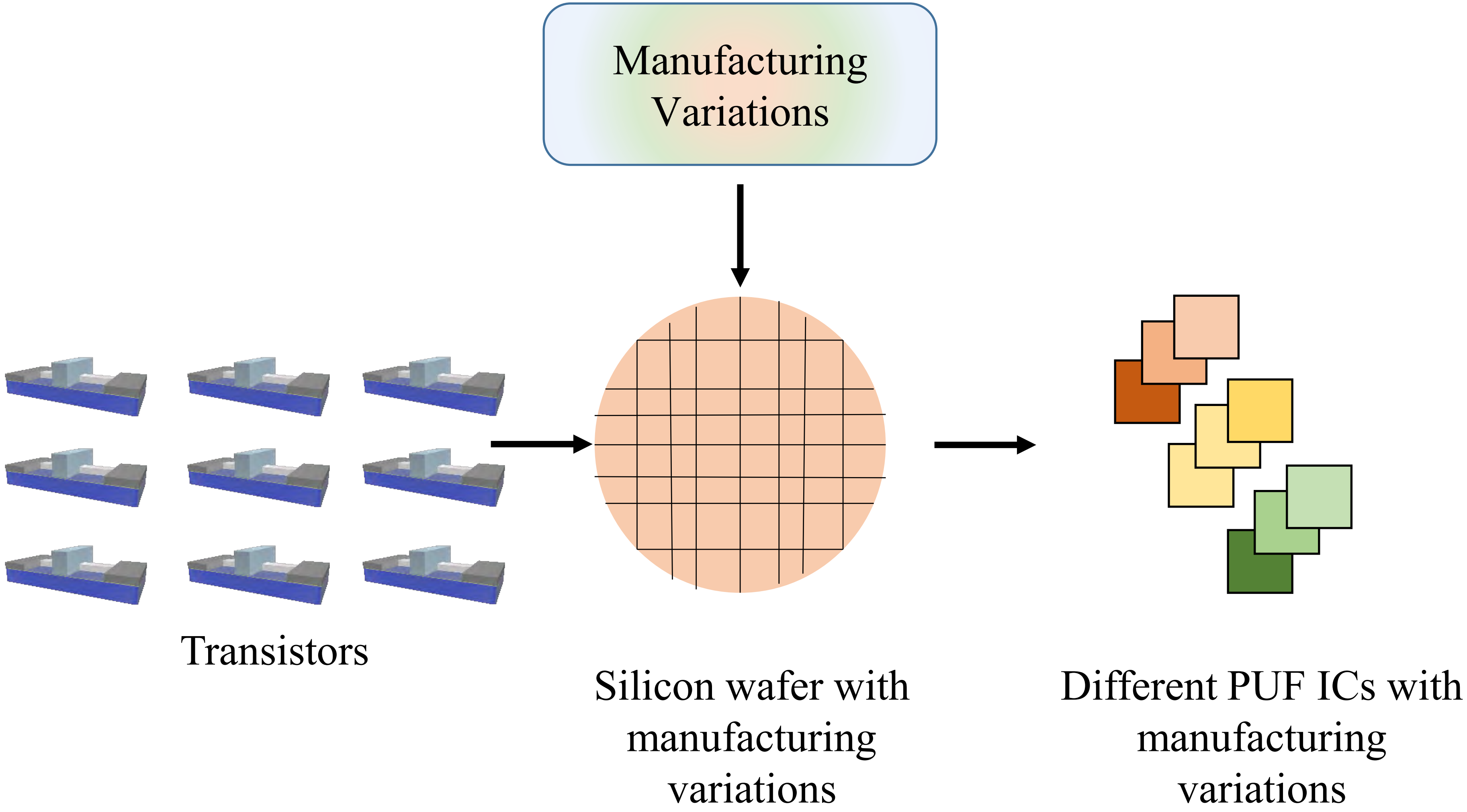
How PUF Works?

Process Variation

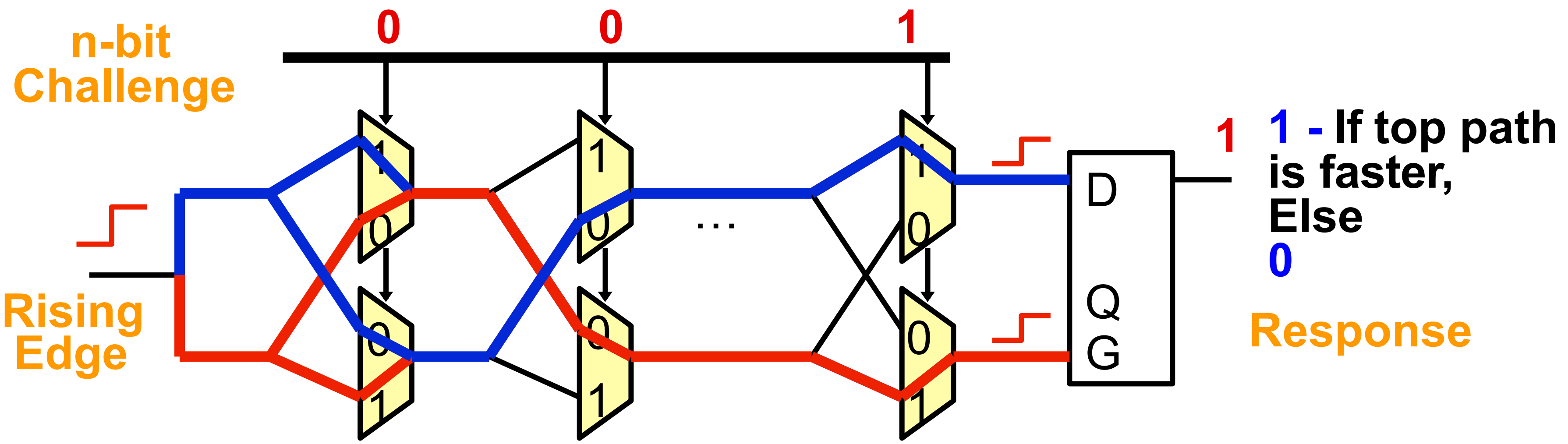
Mismatch Variation



How PUFs Work?



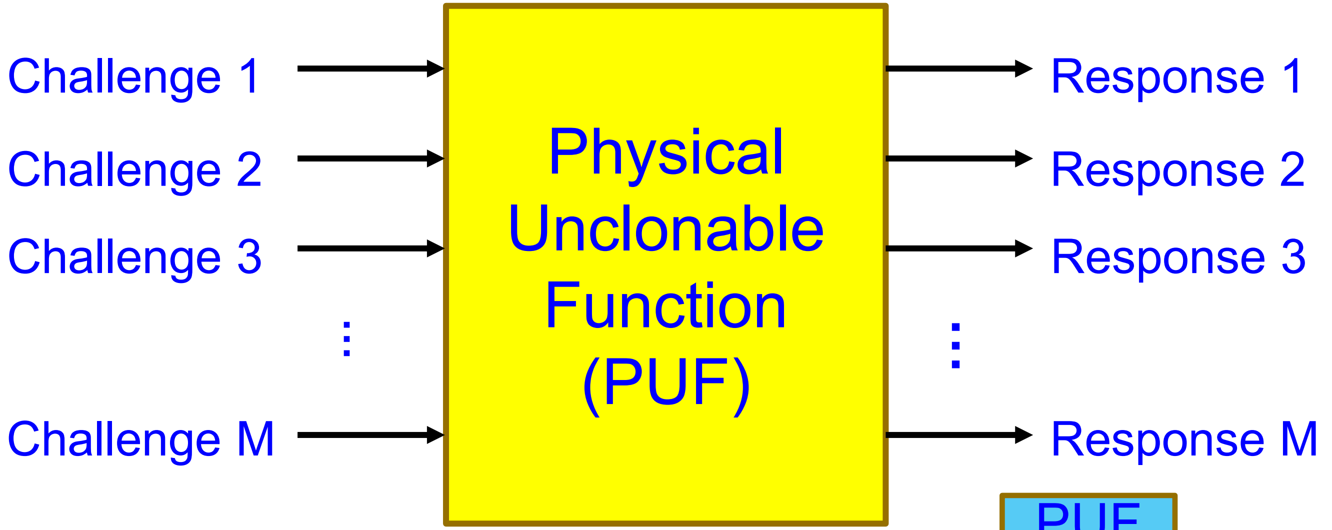
Principle of Generating Random Response using PUF

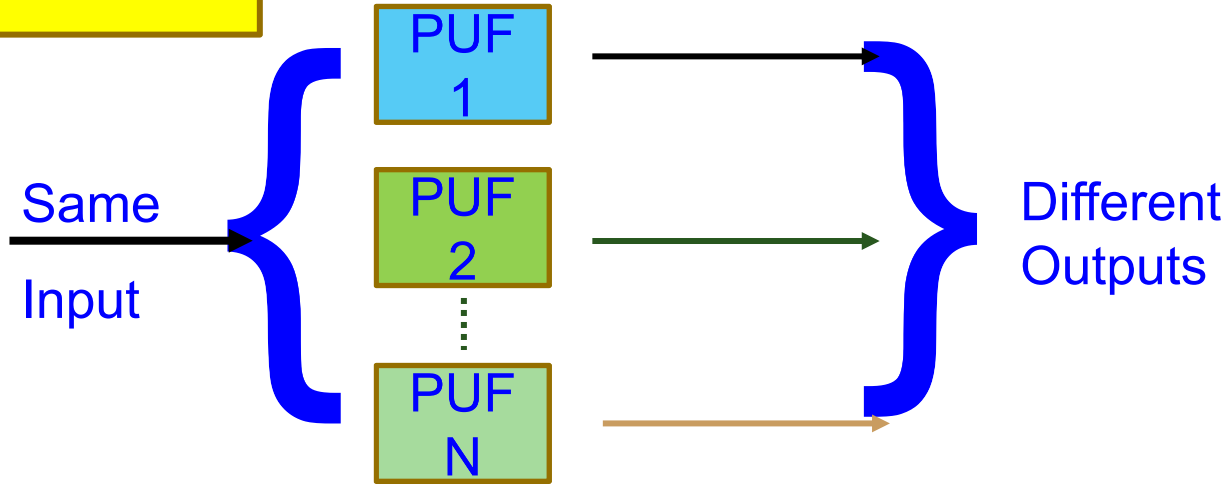


Compare two paths with an identical delay in design
- Random process variation determines which path is faster
- An arbiter outputs 1-bit digital response

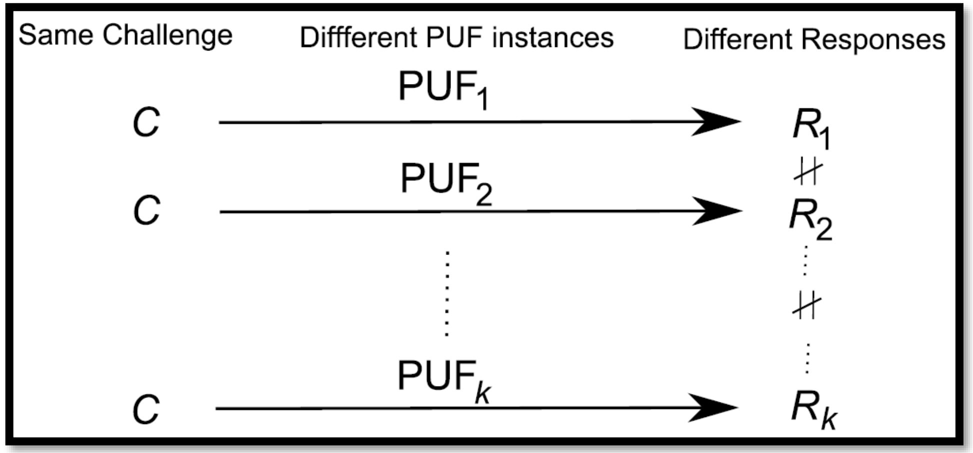
Source: Srini Devadas, Physical Unclonable Functions (PUFs) and Secure Processors, *Cryptographic Hardware and Embedded Systems*, 2009.

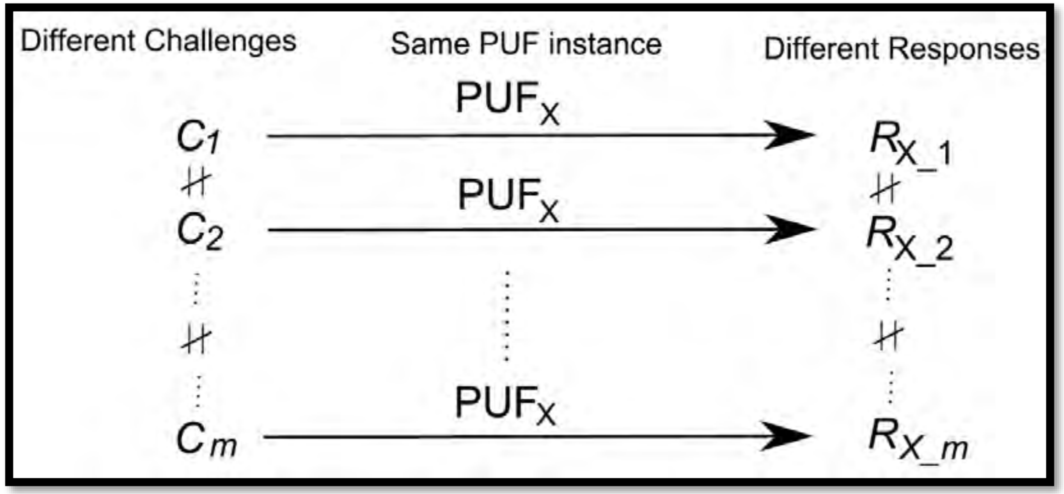
Principle of Generating Multiple Random Response using PUF





Principle of Generating Multiple Random Response using PUF





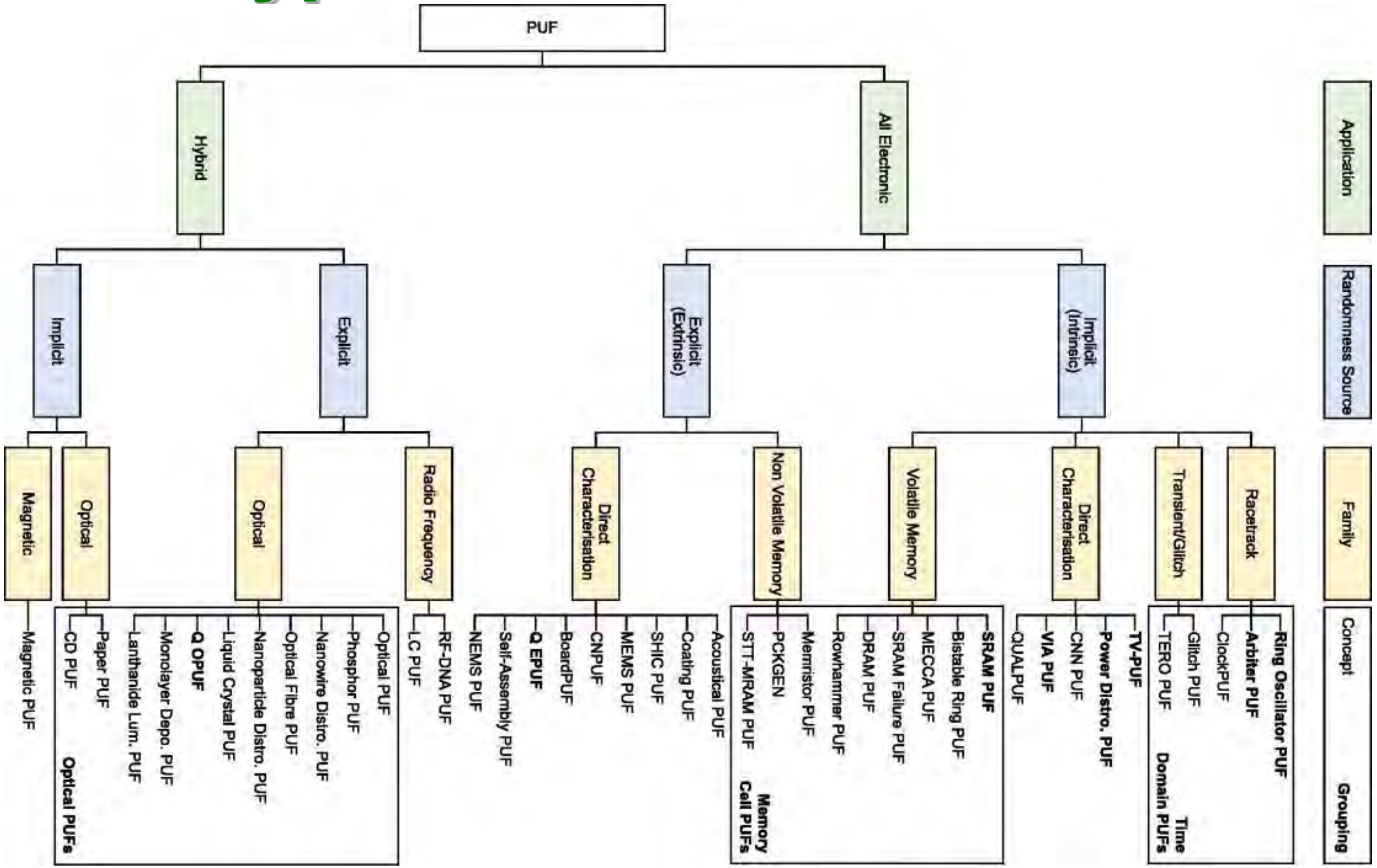
PUF Response is *not* Same as Encryption

PUF vs Encryption

- In classic encryption, decryption key is stored in memory.
- If memory gets attacked, key is compromised.
- Key generated by PUF is not stored in memory.
- PUF extracts manufacturing variations in an IC.
- So PUF generated key acts as fingerprint for the module.

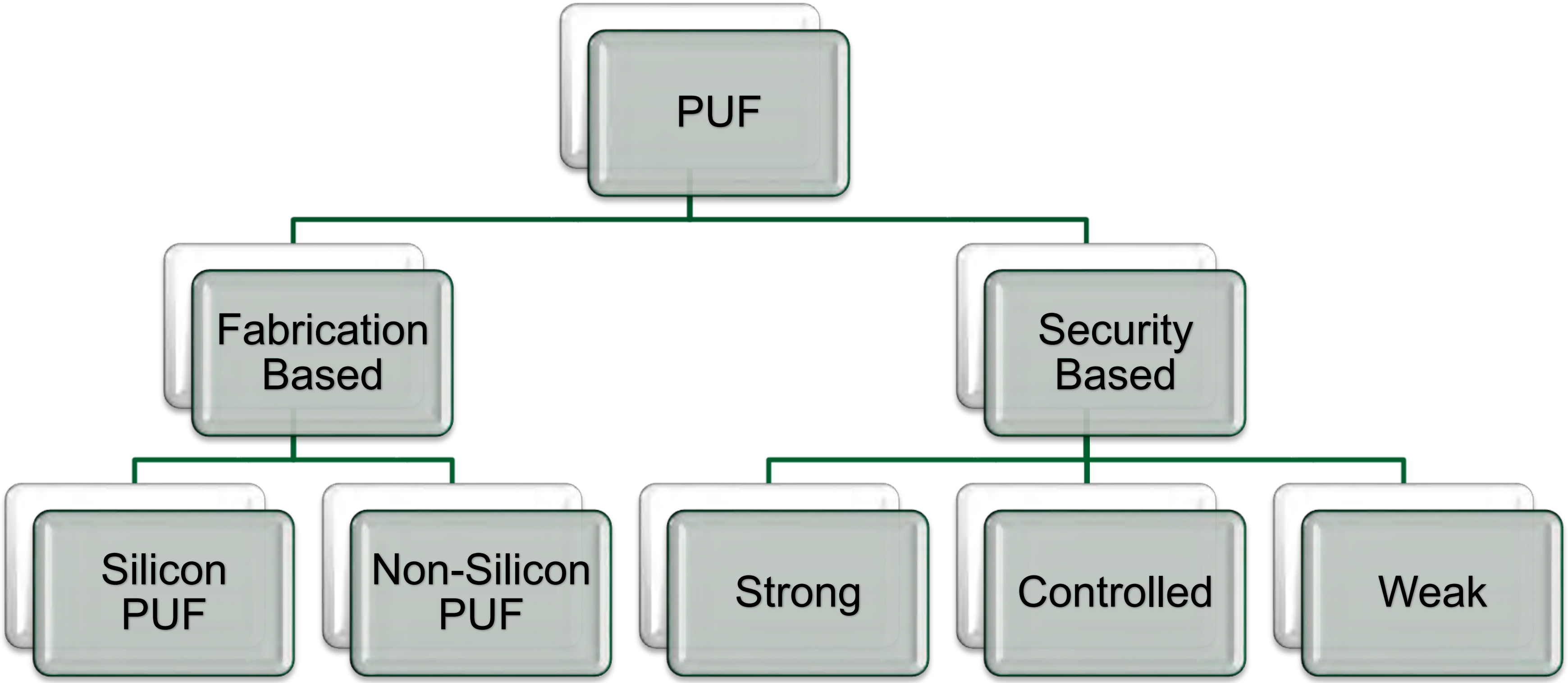
Physical Unclonable Function - Types and Topologies

PUF Types – At Least 40 Different



Source: Thomas McGrath, Ibrahim E. Bagci, Zhiming M. Wang, Utz Roedig, *and* Robert J. Young, "A PUF taxonomy", Applied Physics Reviews 6, 011303 (2019) https://doi.org/10.1063/1.5079407

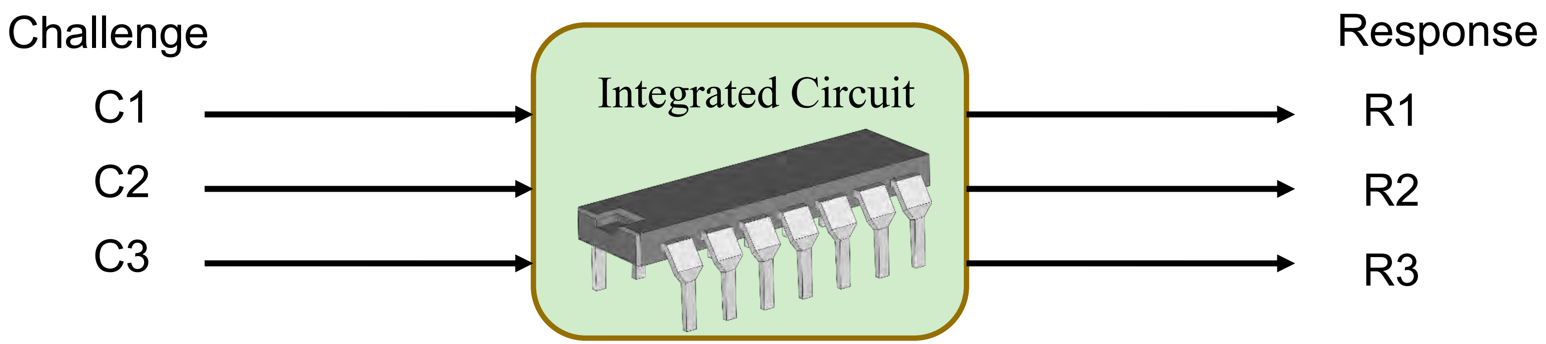
Classification of PUF

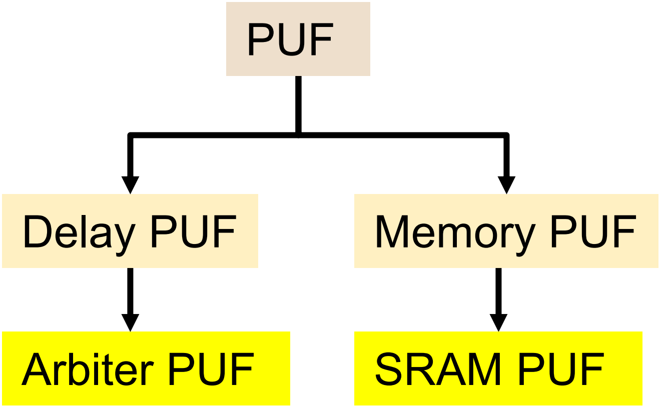


Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Classification of PUF …

- Input to a PUF is called as Challenge and Output from a PUF is called Response.





- A PUF generating large number of CRP is a strong PUF and PUF supporting small number of CRP is considered as Weak PUF.

- A PUF can be categorized as Delay and Memory based PUF. Delay PUF is based on the variations in wiring and variations at gates in silicon. Memory based PUF is based on the instability in the startup phase of SRAM cell.

Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Classification of PUF …

Fabrication Based :

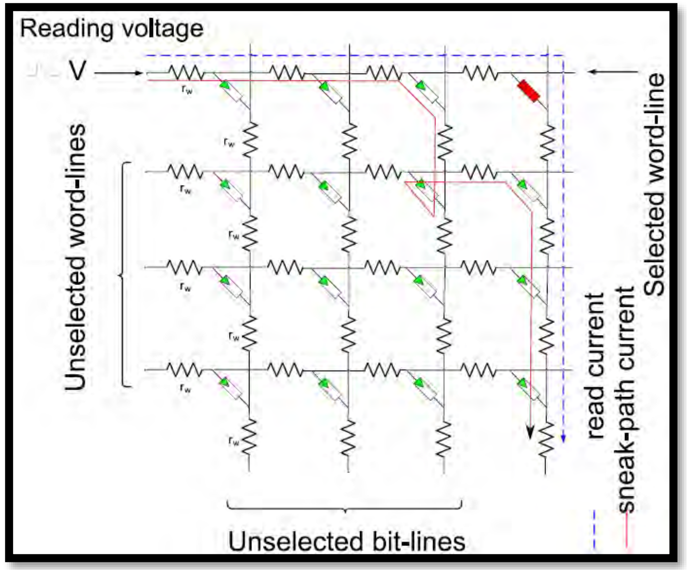
- Silicon based Integrated Circuits can be used for PUF.
- There are also Non-Silicon based PUF like optical PUF, RF PUF and so on.

Security Based :

- Strong PUF generates very high number of Challenge Response Pairs.
- Weak PUF generates low number of Challenge Response Pairs and lowest being ‘1’.
- In a Controlled PUF, inputs and outputs are processed.

Super High Information Content PUF (SHIC-PUF)

- A special nanocrossbar array of nanoscale diodes is capable of storing a significant number of bits.
- This is called a Super – High Information Content PUF.
- Full readout of all bits stored in an SHIC-PUF requires a long time (100 bits/s).



- Hence used in applications where readout time is not restricted.

Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

Carbon – Nanotube FET Based PUF

- A chain of CNT-FETs is built and given the same gate voltage .
- The comparator at the end produces a single bit comparing currents from the chain.

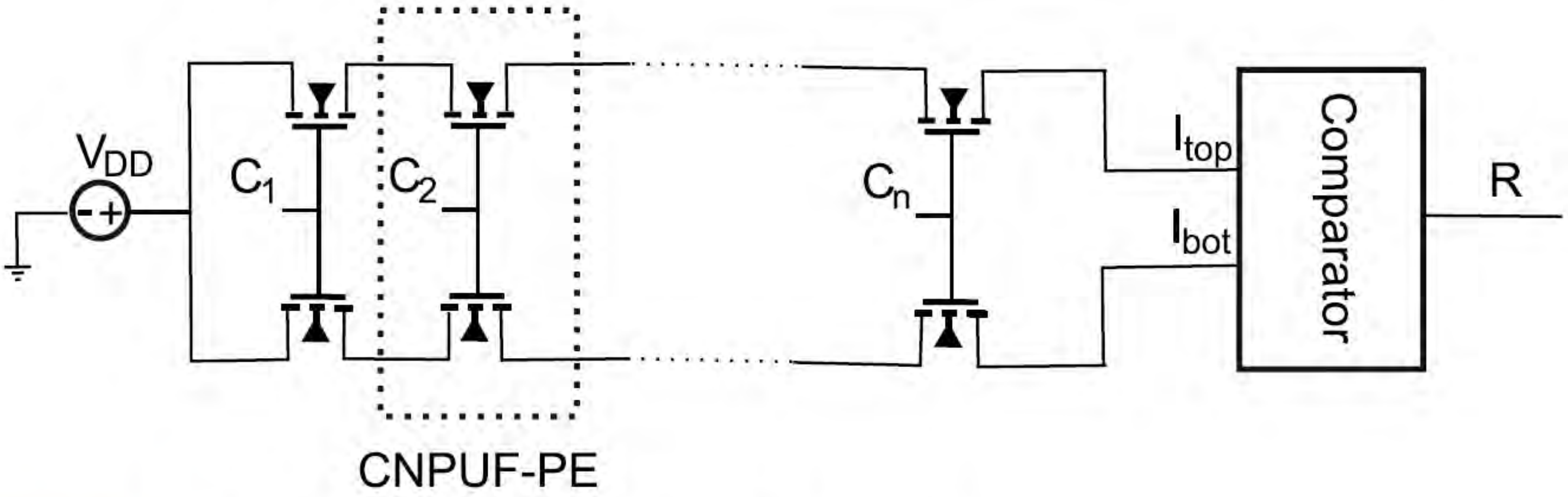


FIGURE 3. **CNFET based PUF design (CNPUF).**

Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

Carbon – Nanotube FET Based PUF

- CNPUF compares the sum of resistances compared to time delay in Arbiter PUF.
- 97% reliability achieved without any post processing.

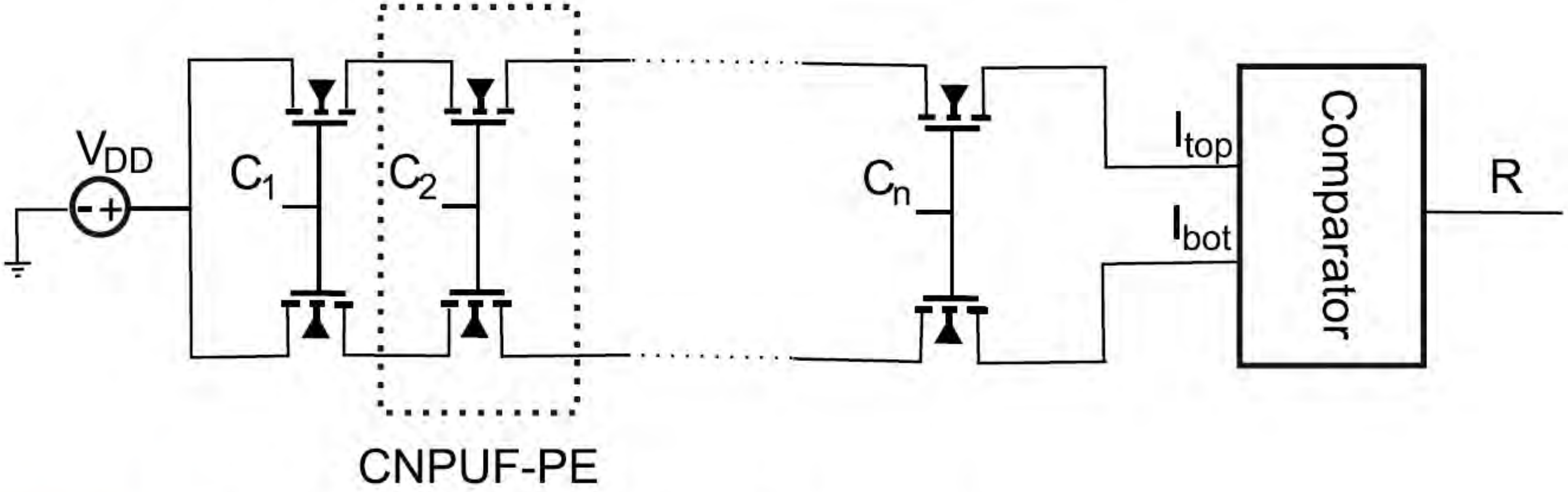


FIGURE 3. **CNFET based PUF design (CNPUF).**

Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

Phase Change Memory Based PUF

- PCM uses amorphous and crystalline nature of phase change materials.
- High amplitude, fast fall time pulse will set material in amorphous state.
- Moderate amplitude pulse with long period will set in it crystalline phase.

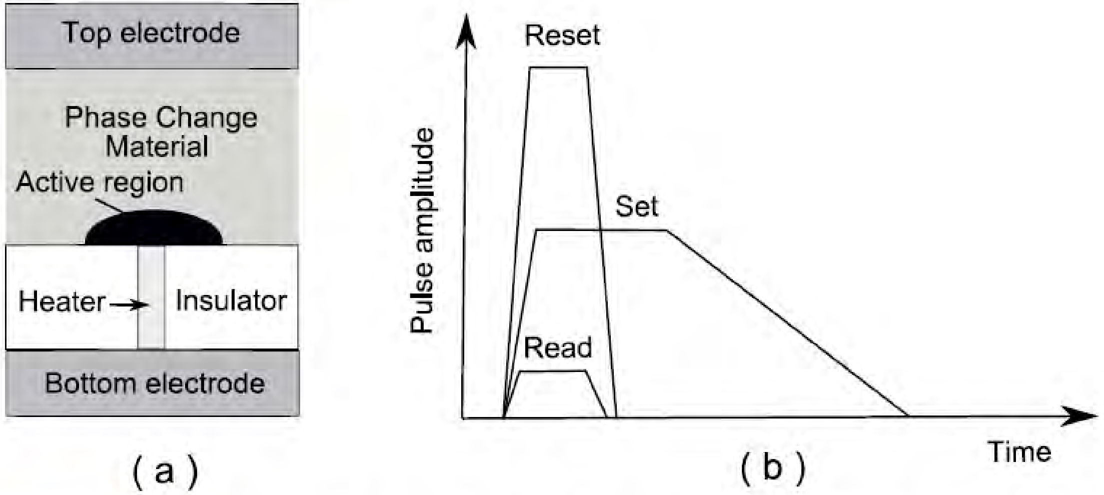
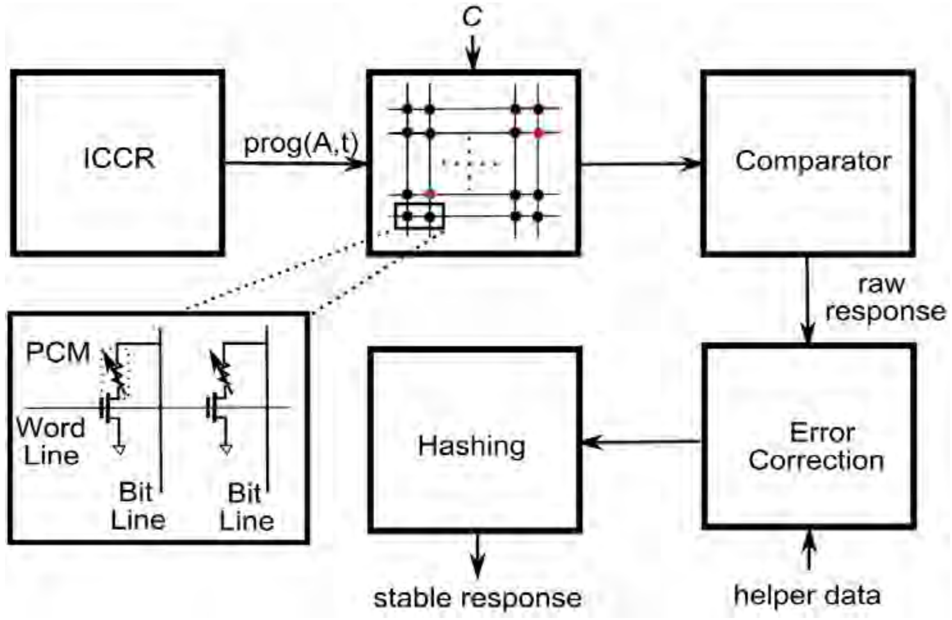


FIGURE 4. (a) A cross-sectional view of a conventional PCM cell. (b) The programming pulse passing through the PCM will change the temperature in the active region using the heater based on the pulse amplitude and duration. The resistance is read out by passing a small amplitude and short duration pulse without disturbing the resistance of the PCM.

Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

PCM Based PUF 2

- Two PCM modules are selected and the resistance is compared.
- The addresses of the two selected modules will be the challenge bit.
- The programming pulse that reconfigures the resistance ensures the reconfigurability.
- Variations of programming pulse width depend on intrinsic process variations of the block ICCR (imprecisely controlled current-pulse regulator).



Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

STT – MRAM Based PUF 1

- Magnetic tunnel junction is used in STT-MRAM whose resistance can be altered by changing the spin polarized current.
- PUF signature is extracted based on spin transfer switching (STS).
- Different MTJs due to variability require different voltages to switch between parallel and anti-parallel states.

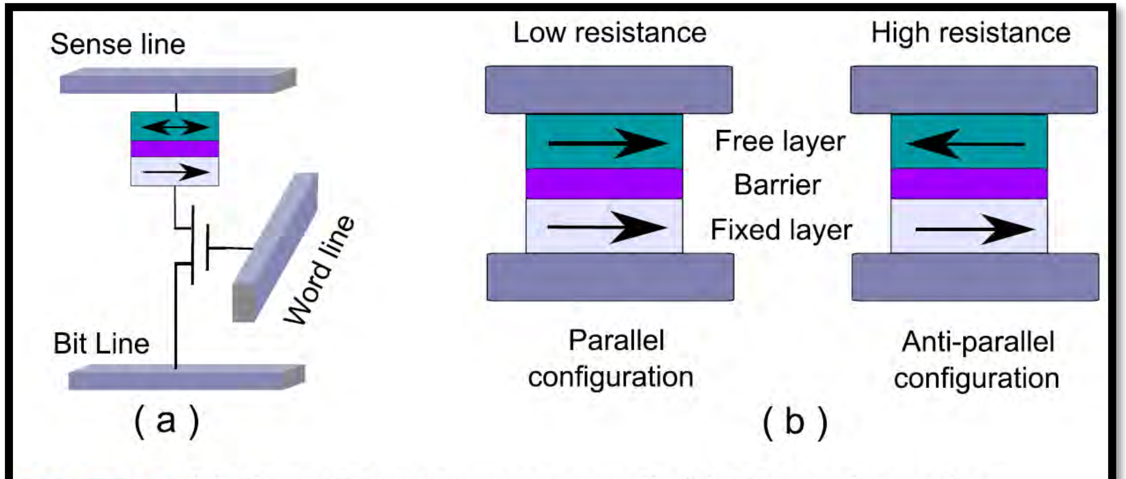
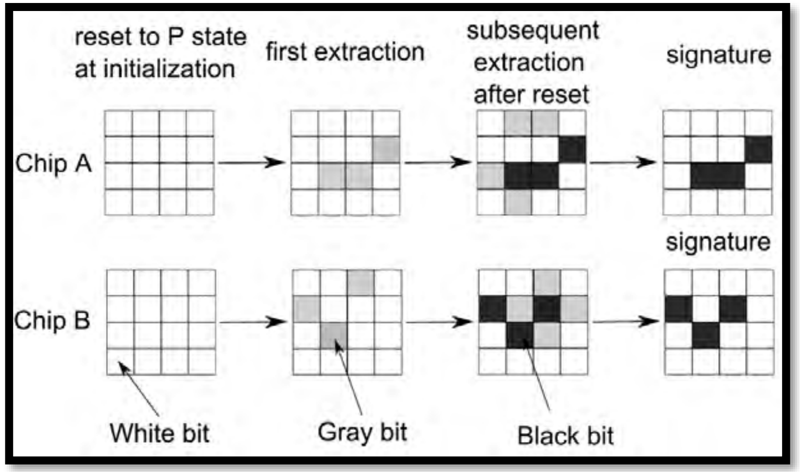
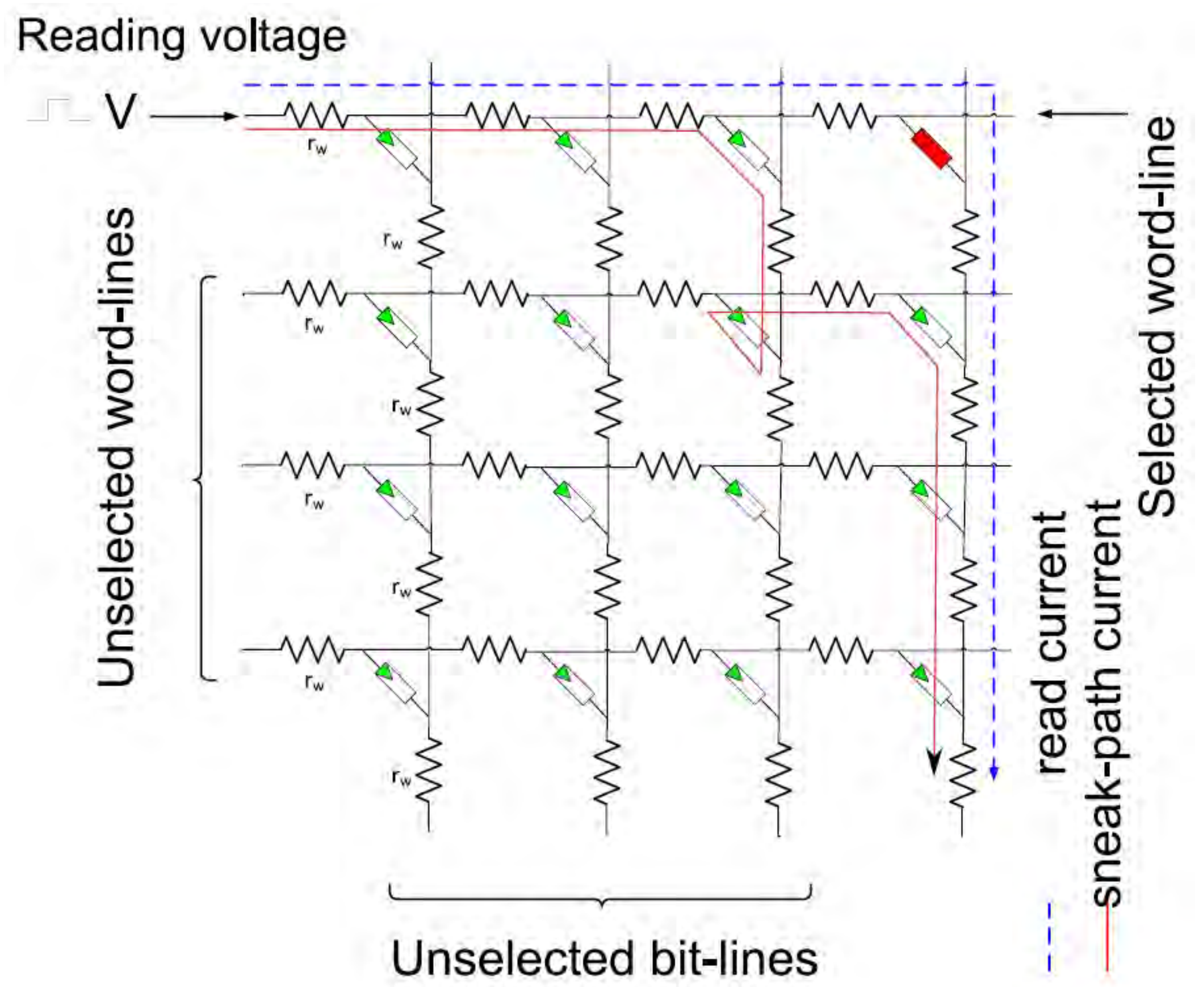


FIGURE 7. (a) The STT-MRAM memory cell. (b) MTJ configuration.



Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

Memristor PUF (Weak–Write–Based)



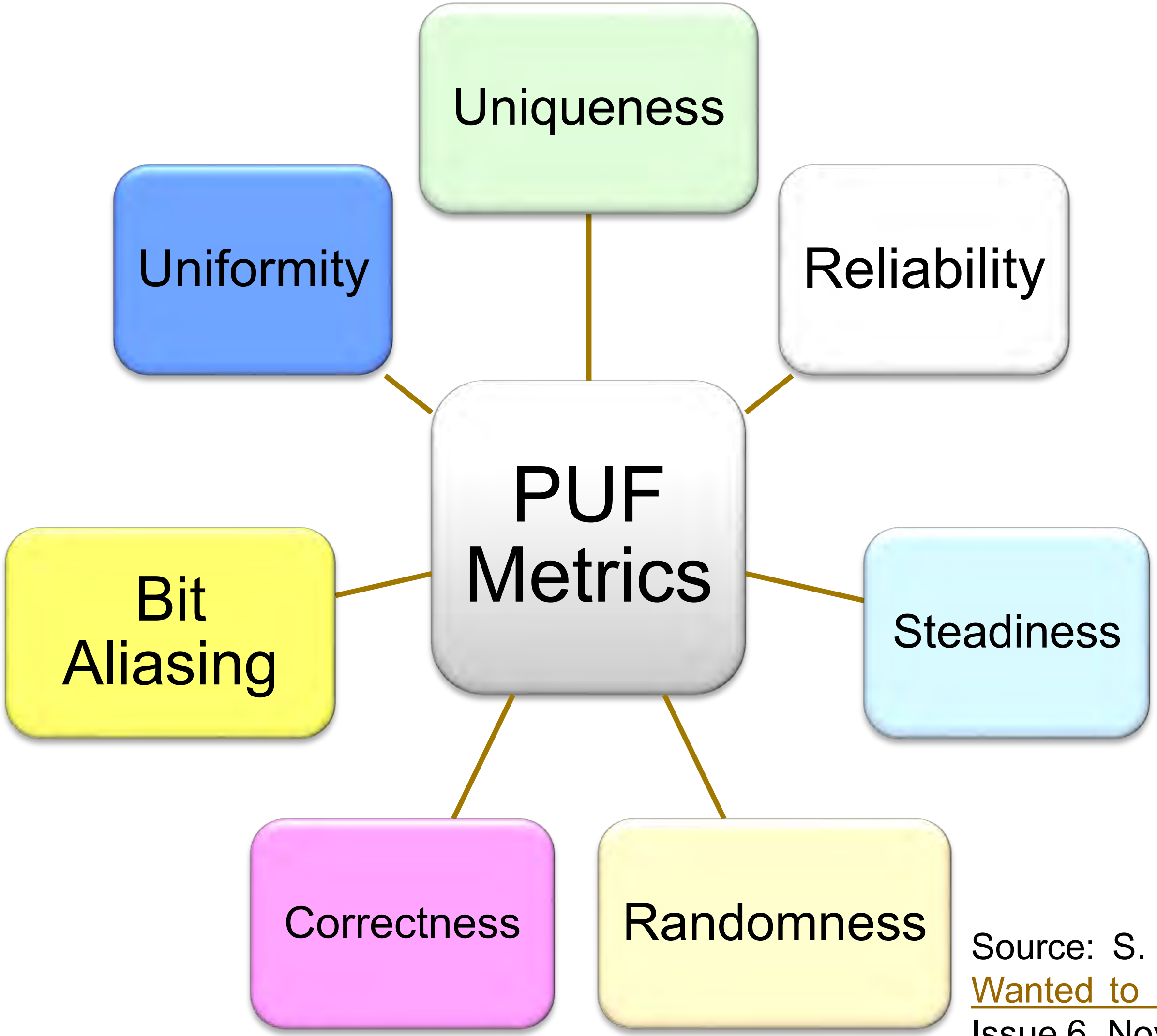
Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

Physical Unclonable Function - Characteristics

Performance Metrics …

Can any circuit become PUF?

PUF - Performance Metrics



AKA - Figure of Merits

Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Performance Metrics …

- Uniqueness:
  - Measure of average inter-chip Hamming Distance of response. Ideal is 50%.
- Reliability:
  - Measure of how much reliable CRP under noise and environmental variations. Ideal is 0% - Hamming Distance should be 0.
- Randomness:
  - Number of 0’s and 1’s in a PUF key. There should be 50% 1’s and 50% 0’s.

Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, “Everything You Wanted to Know about PUFs”, *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Performance Metrics …

- Correctness:
  - Measure of correctness of response under different operating conditions.
- Bit Aliasing:
  - It is measure of biasness of particular response bit across several chips. Ideal value is 50%. There should be no correlation between any of the outputs generated by different PUF modules.
- Steadiness:
  - Measure of biasness of response bit for a given number of 0's and 1's over total number of samples gives the steadiness. Ideal value is 100%.

Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

More Performance Metrics …

- Tamper Sensitivity:
  - The PUF module designed and deployed should be Tamper Resistant.
- Indistinguishability:
  - PUF key generated should not be similar to any random string of numbers
- Unpredictability:
  - PUF responses generated should not be predicted by any algorithm or machine learning.

Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

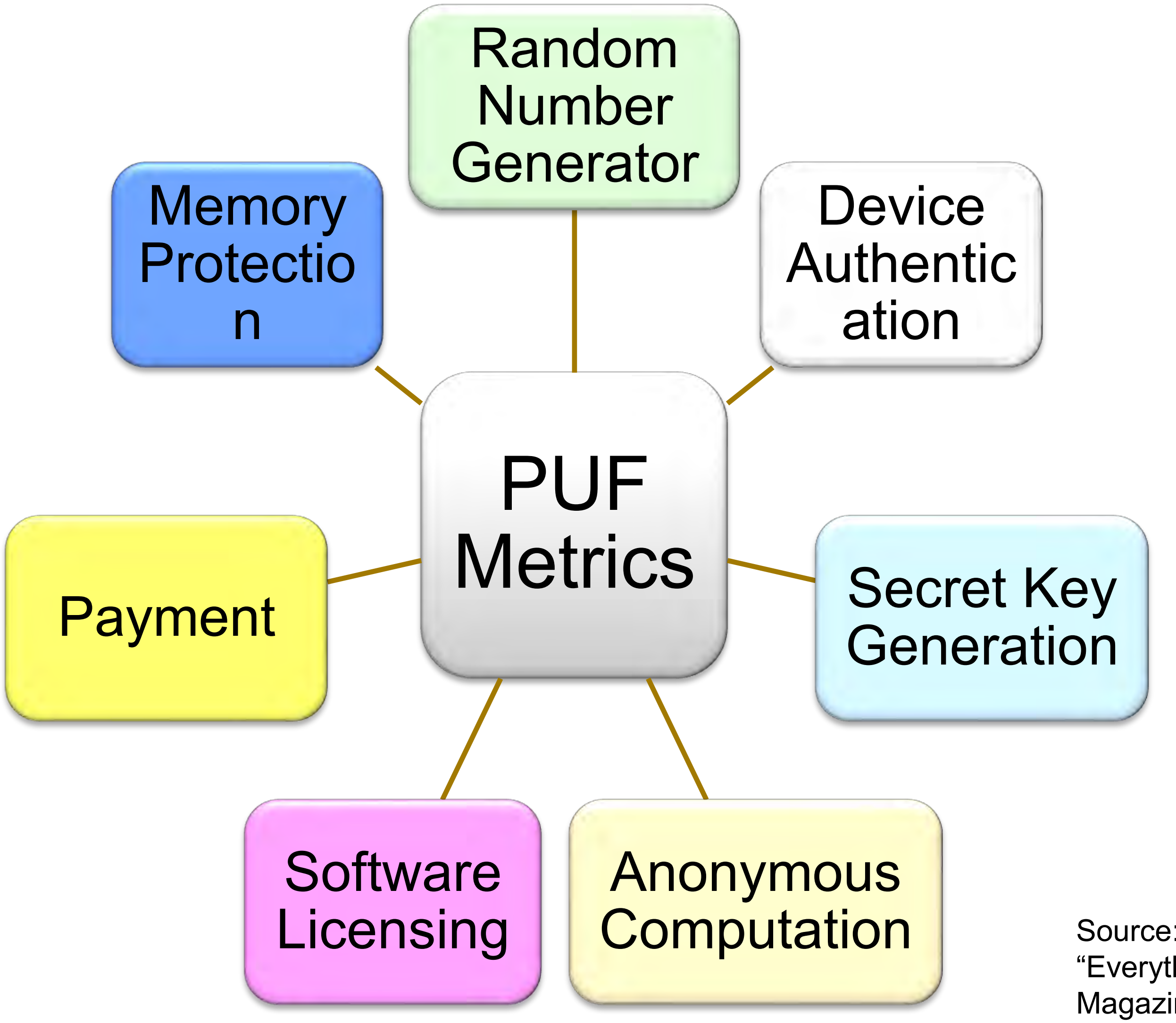
More Performance Metrics …

- Average Power consumption:
  - The average power consumed by the entire PUF module.
- Speed:
  - The output key generation latency should be low.

Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Physical Unclonable Function - Applications

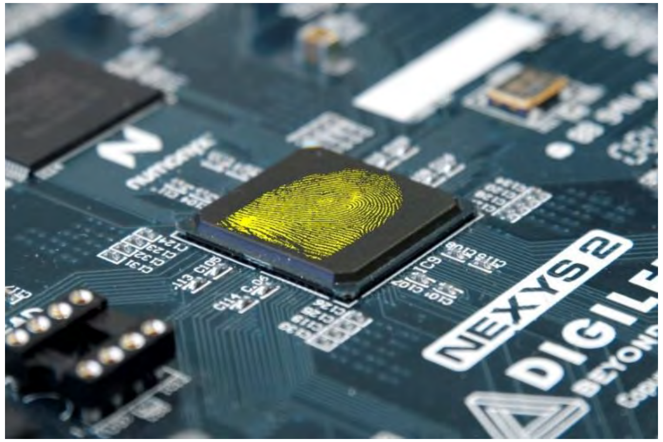
PUF -- Applications



Source: S. Joshi, S. P. Mohanty, and E. Kougianos, “Everything You Wanted to Know about PUFs”, IEEE Potentials Magazine, Volume 36, Issue 6, Nov-Dec 2017, pp. 38--46.

Protecting Hardware using PUF

- A countermeasure against electronics cloning is a physical unclonable function (PUF).
- It can potentially protect chips, PCBs, and even high-level products like routers.
- PUFs give each chip a unique “fingerprint.”



Source: https://phys.org/news/2011-02-fingerprint-chips-counterfeit-proof.html

An on-chip measuring circuit (e.g. a ring oscillator) can generate a characteristic clock signal which allows the chip’s precise material properties to be determined. Special electronic circuits then read these measurement data and generate the component-specific key from the data.

Source: http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

Applications of PUF

- The IoT has smart devices deployed in unmonitored and unsecure environments.
- Tractable cryptography which can be deployed on hardware with limited processing and storage capabilities is required.
- Low-cost tamper resistant system to prevent adversarial compromise of remote unmonitored devices.
- PUF is one of the simplest and cost-effective solutions.

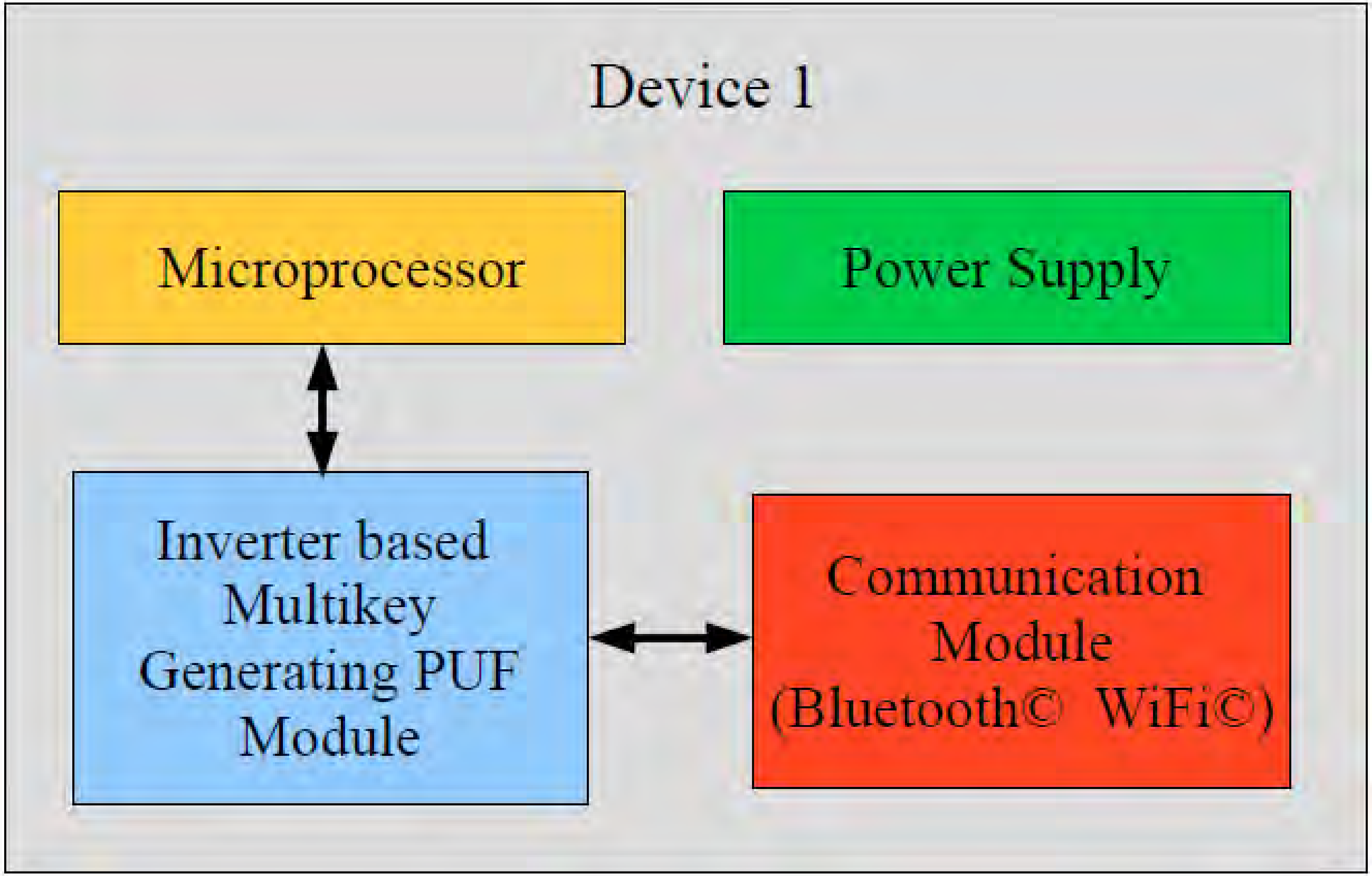
Applications

- Random Number Generator
  - Manufacturing variations in PUFs make the generated number truly random.
- Device Authentication
  - PUF generated keys can be used to authenticate a device being used or in networking.
- Anonymous Computation
  - Computations performed on anonymous computers can be authenticated with PUF.

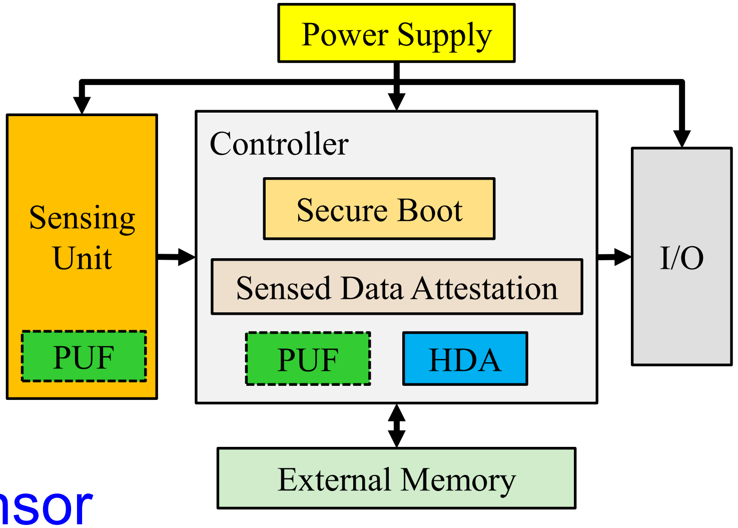
Applications

- Software Licensing
  - PUF keys generated are random and unique which can be used in giving as licenses for software.
- Payment
  - PUF plays important role in security of e-commerce transactions.
- Memory Protection
  - PUF keys generated can be used for encrypting an entire drive.

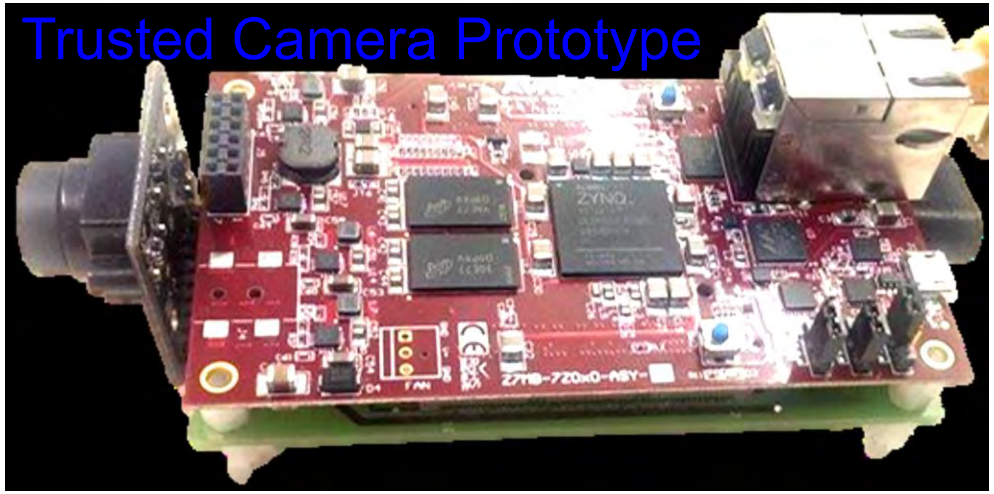
Applications



PUF-based Trusted Sensor



PUF-based Trusted Sensor



Source: https://pervasive.aau.at/BR/pubs/2016/Haider_IOTPTS2016.pdf

PUF-based Secure Key Generation and Storage module provides key:

- Sensed data attestation to ensure integrity and authenticity.
- Secure boot of sensor controller to ensure integrity of the platform at booting.

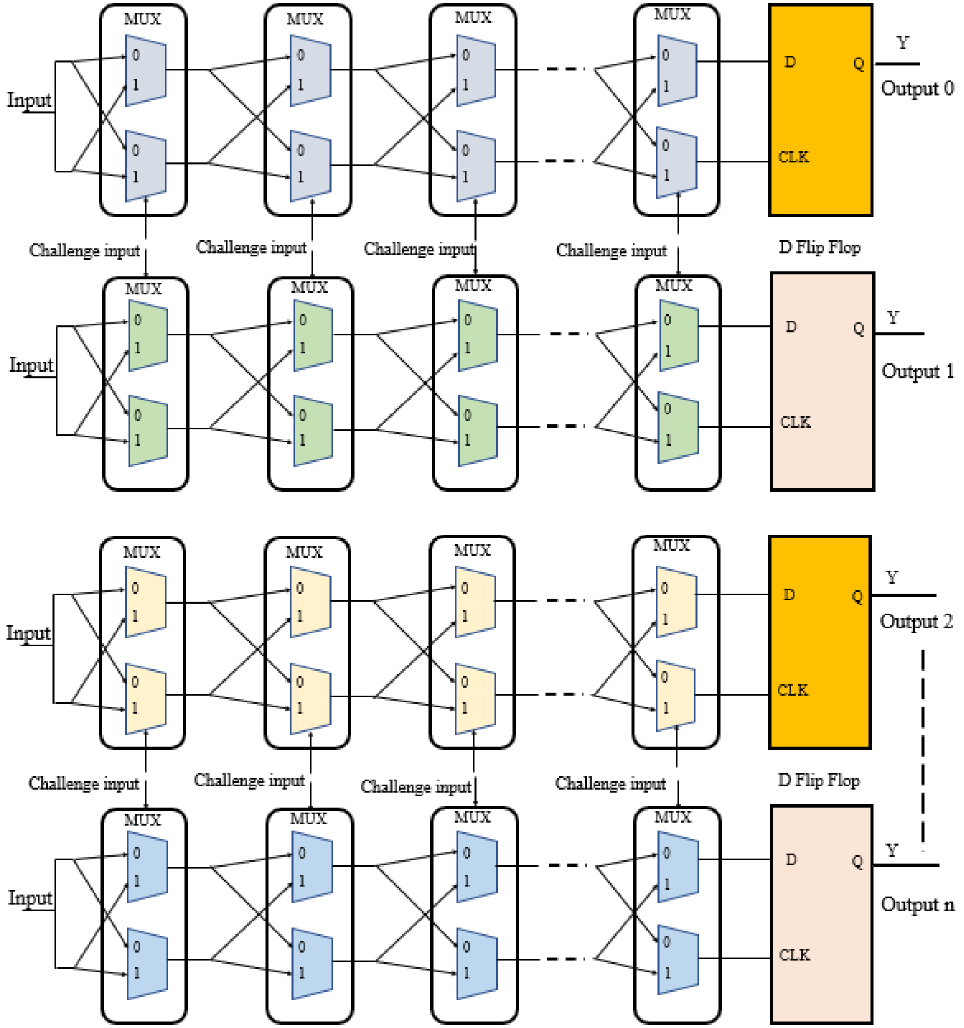
❖ On board SRAM of Xilinx Zynq7010 SoC cannot be used as a PUF.

❖ A total 1344 number of 3-stage Ring Oscillators were implemented using the Hard Macro utility of Xilinx ISE.

Process Speed: 15 fps
Key Length: 128 bit

PUF Design – Some Examples

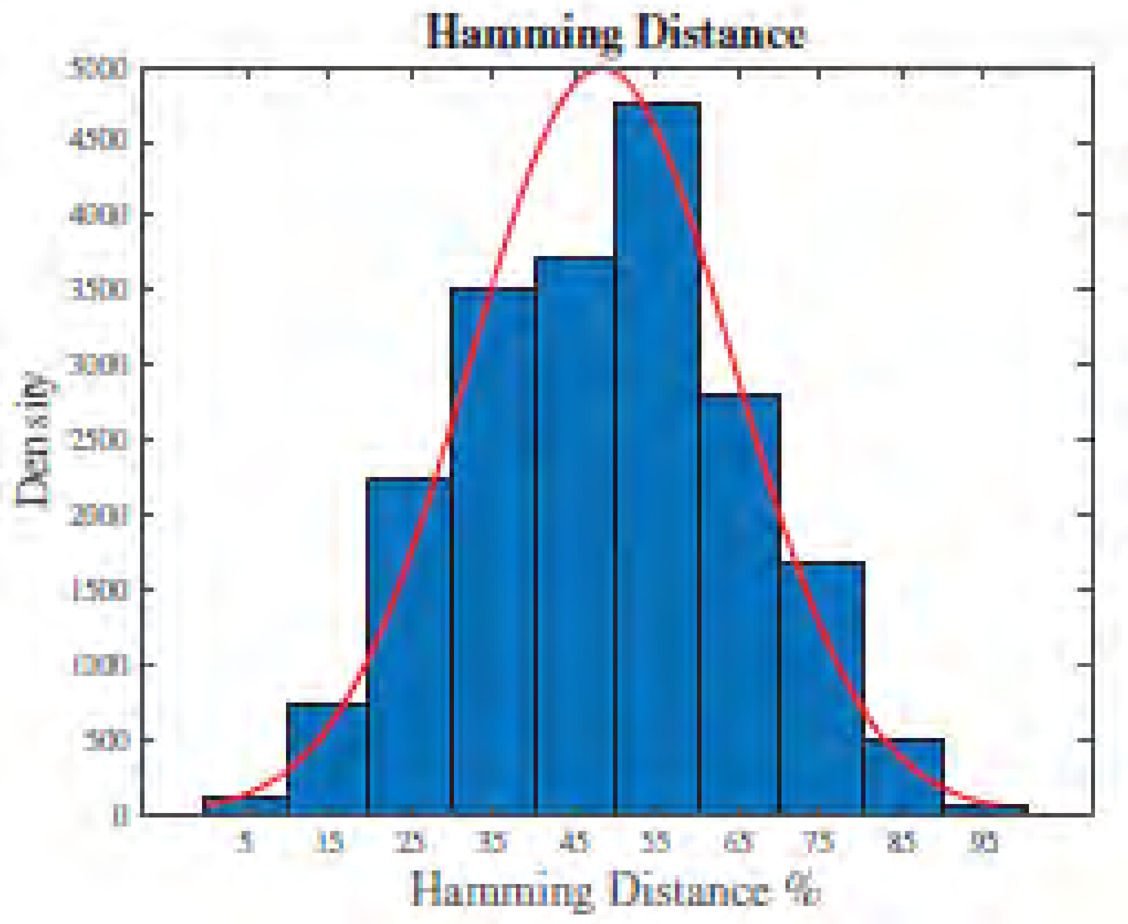
Arbiter PUF Design

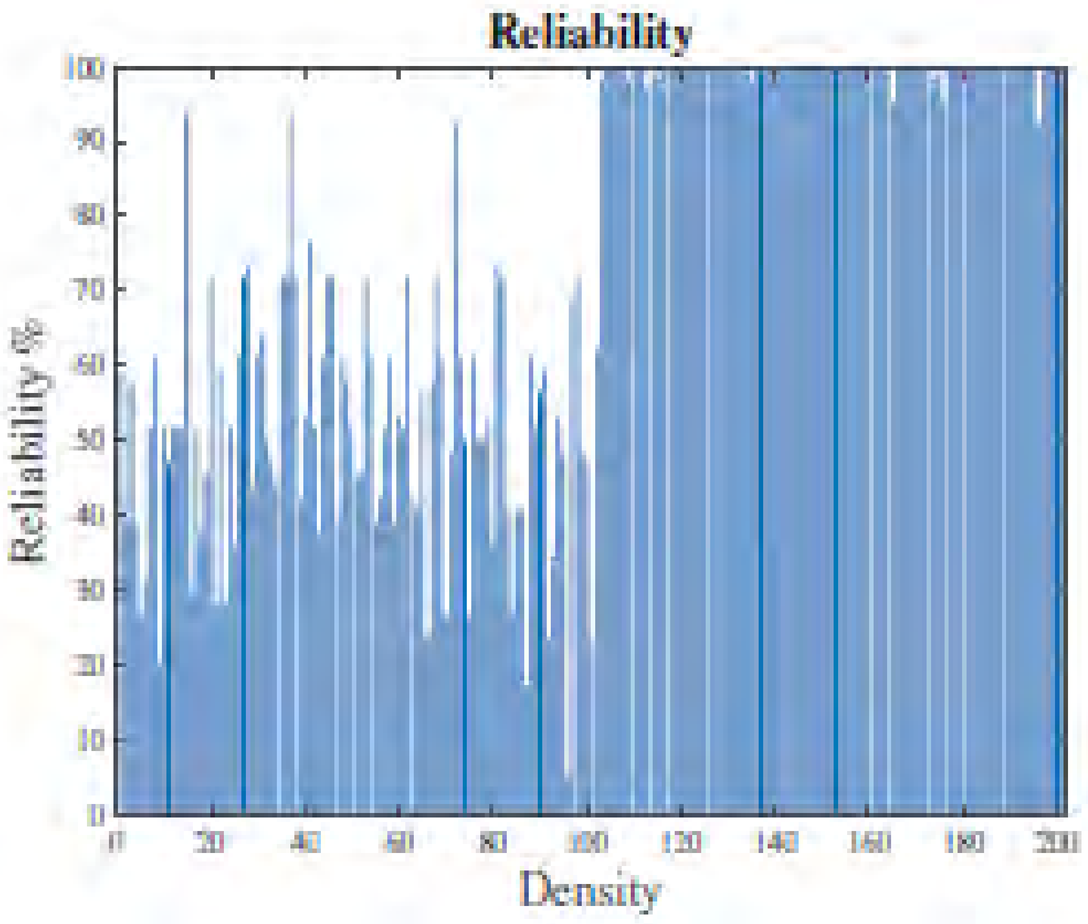


Strong PUF module which can be used for cryptographic purposes due to large number of CRP’s.

Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture,“ in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

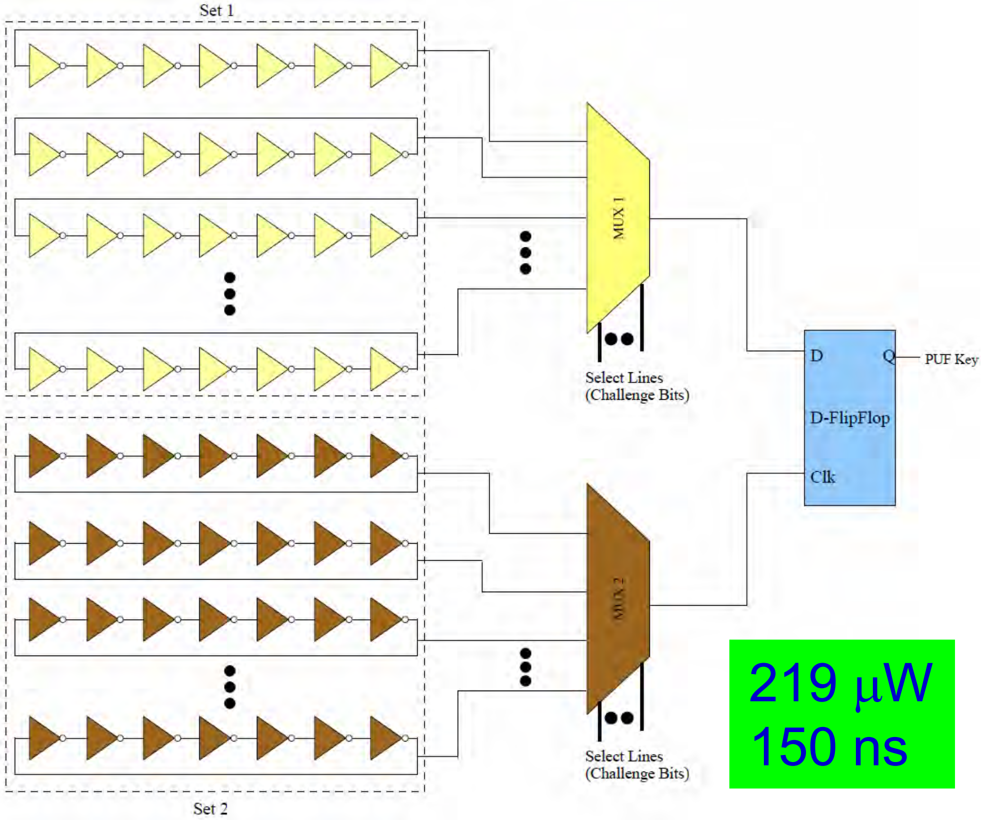
Arbiter PUF Metrics





Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

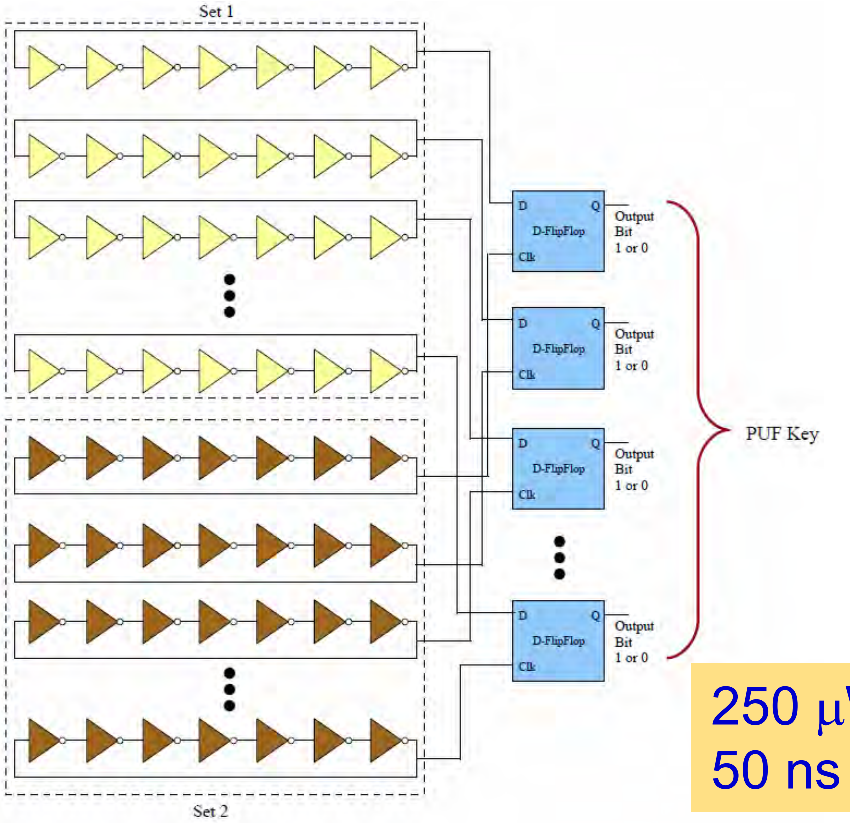
We Have Design a Variety of PUFs - FinFET based



219 µW
150 ns

Power Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS



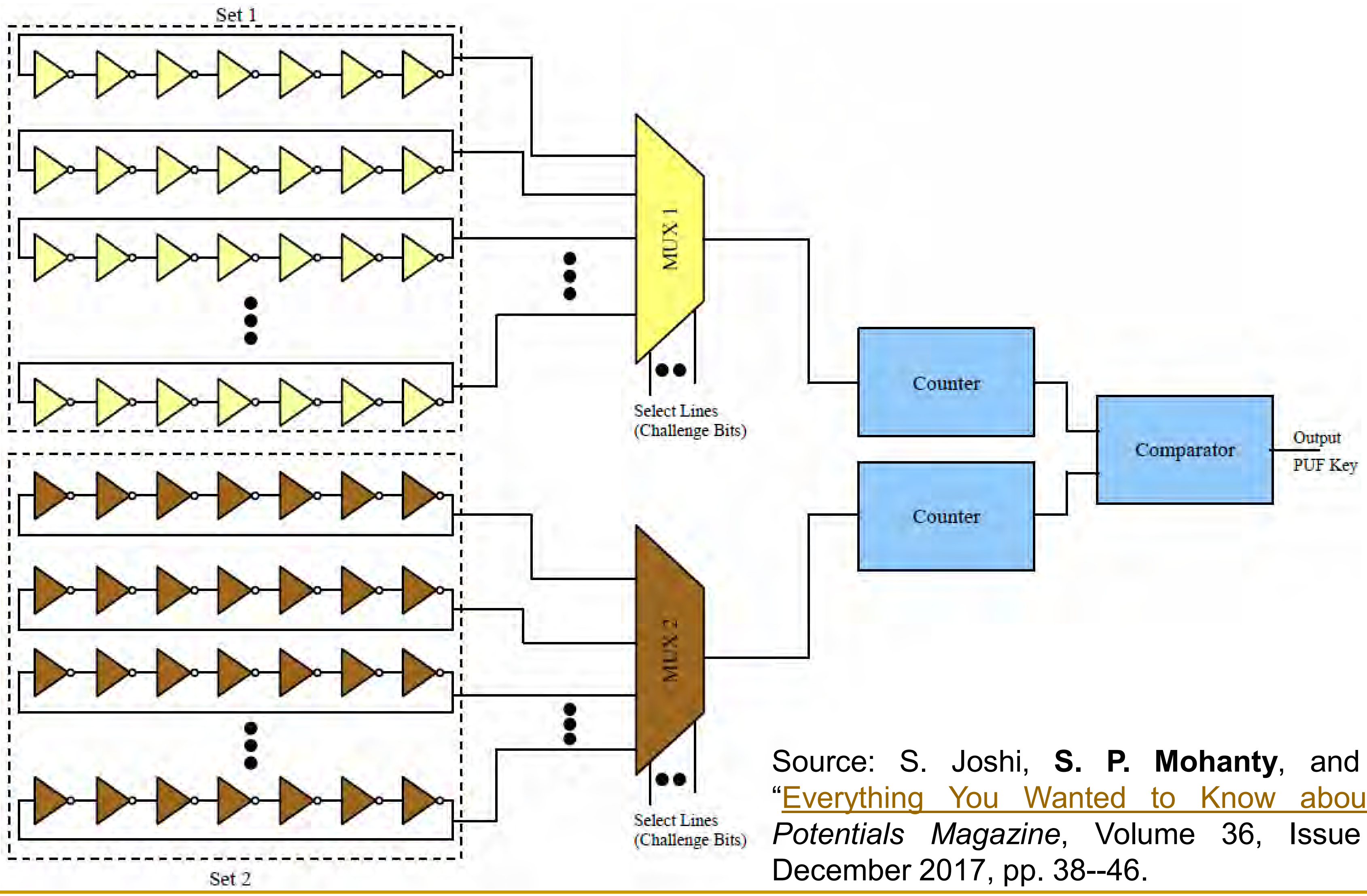
250 µW
50 ns

Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Transportation and Energy CPS

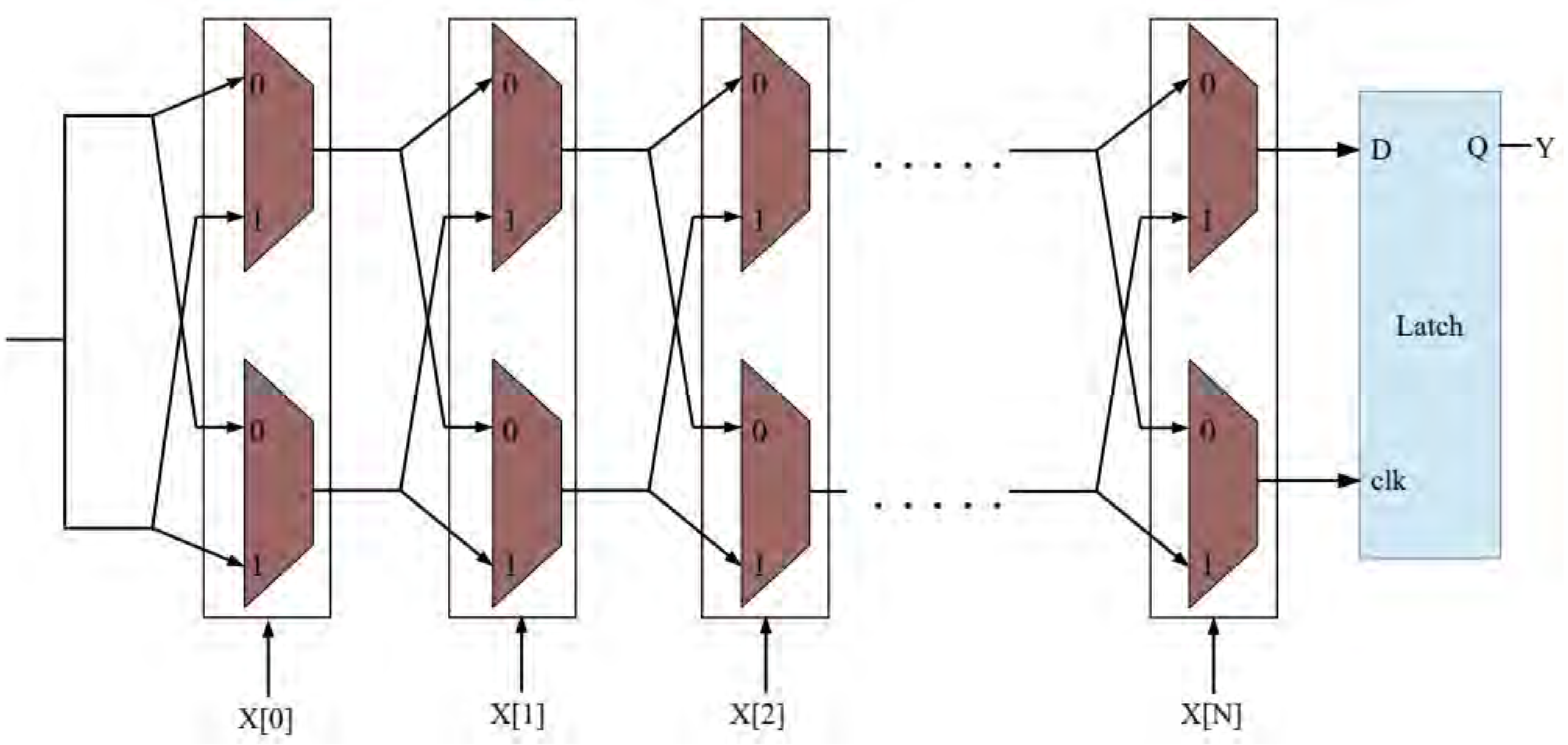
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3, December 2017, pp. 429--441.

Conventional Ring Oscillator PUF



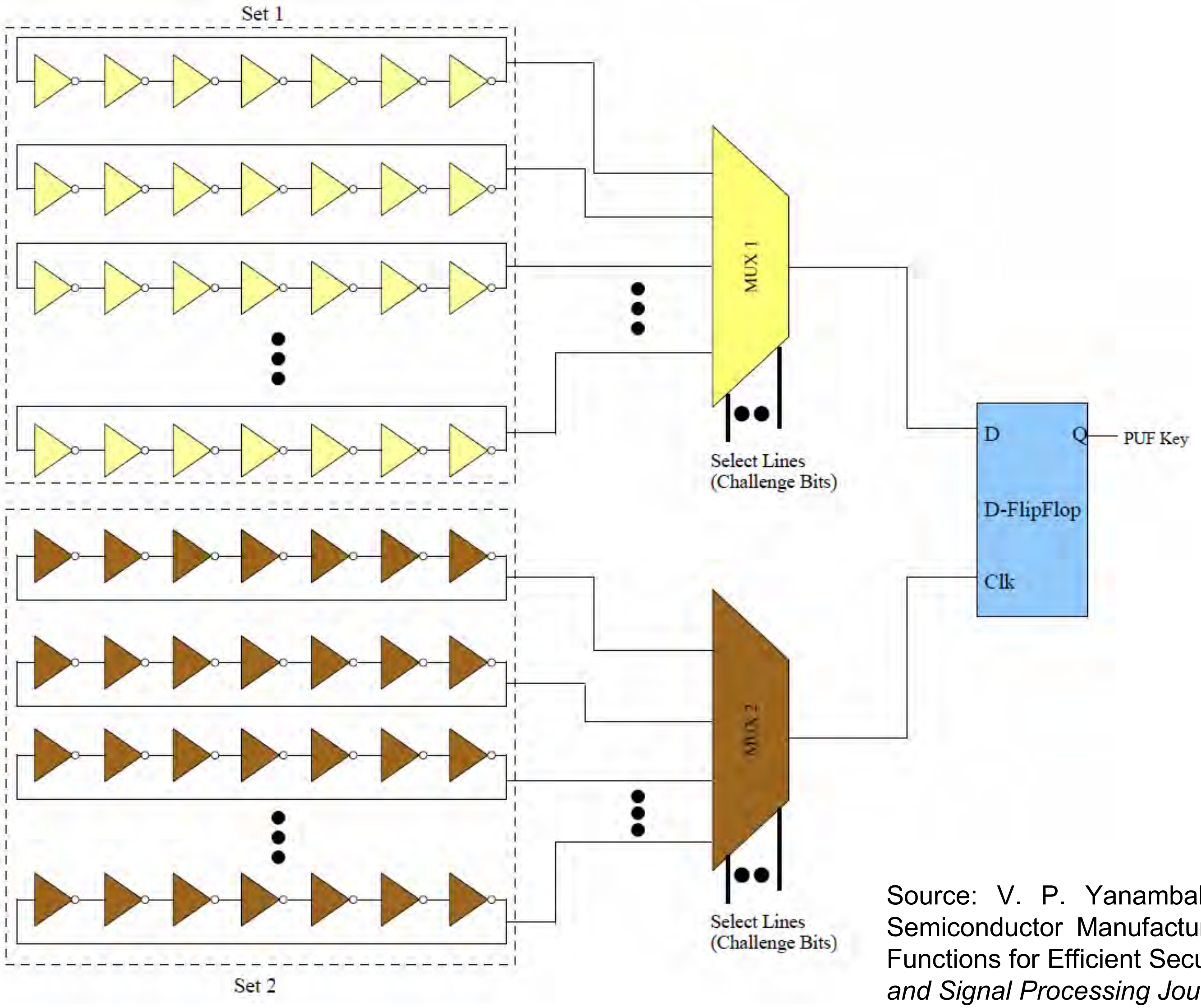
Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Conventional Arbiter PUF



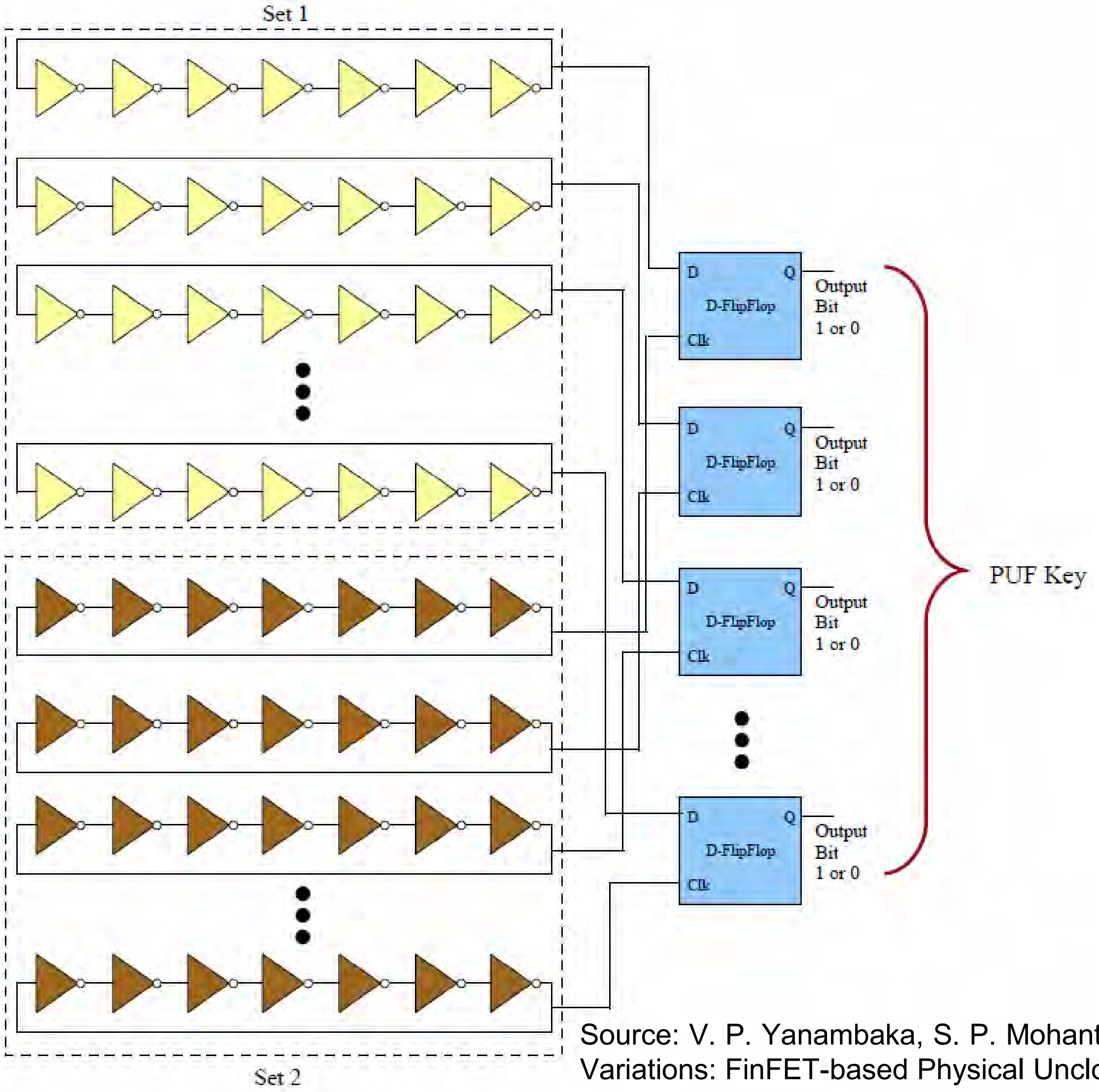
Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Power Optimized Hybrid Oscillator Arbiter PUF



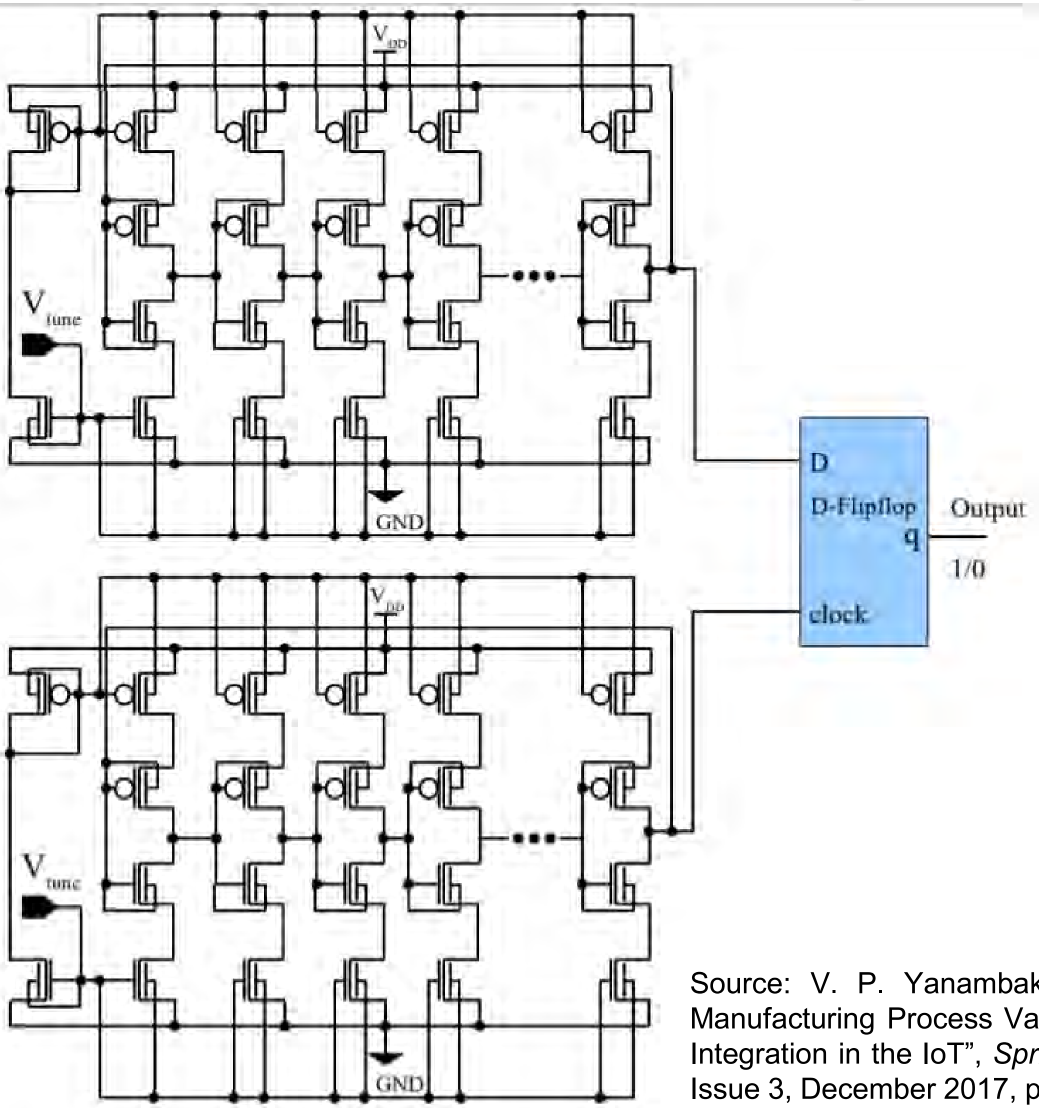
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT", *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3, December 2017, pp. 429--441.

Speed Optimized Hybrid Oscillator Arbiter PUF



Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3, December 2017, pp. 429--441.

FinFET – Based One Bit Hybrid Oscillator Arbiter PUF



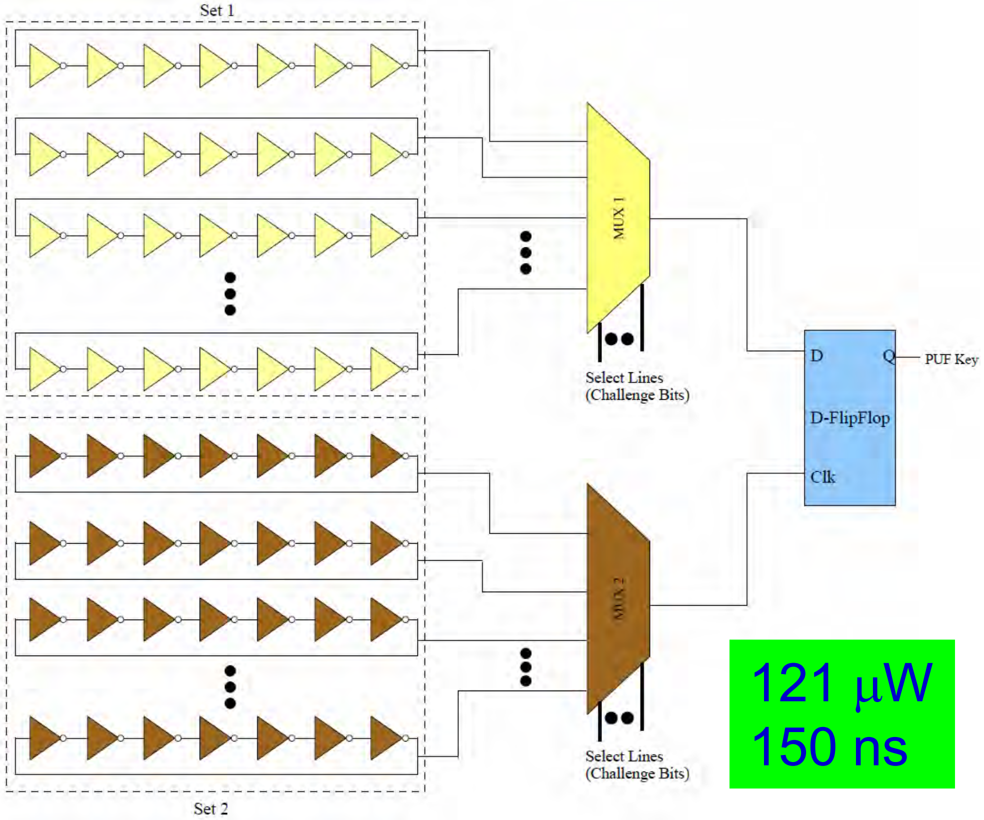
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT", *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3, December 2017, pp. 429--441.

Simulation Results

Research Work	Technology	Architecture Used	Power Consumption	Uniqueness (%)	Reliability (%)
Yanambaka et al. [1] (Power Optimized)	32 nm FinFET	Current Starved VCO Hybrid Oscillator Arbiter PUF	285.5 µW	50.9	0.79
Yanambaka et al. [1] (Speed Optimized)	32 nm FinFET	Current Starved VCO Hybrid Oscillator Arbiter PUF	310.8 µW	50.0	0.79
Yanambaka et al. [2] (Power Optimized)	32 nm FinFET	Ring Oscillator Multi-Key Generation PUF	175.5 µW	48.3	50
Yanambaka et al. [2] (Power Optimized)	32 nm FinFET	Ring Oscillator Multi-Key Generation PUF	251 µW	50.1	48.7

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3, December 2017, pp. 429--441.

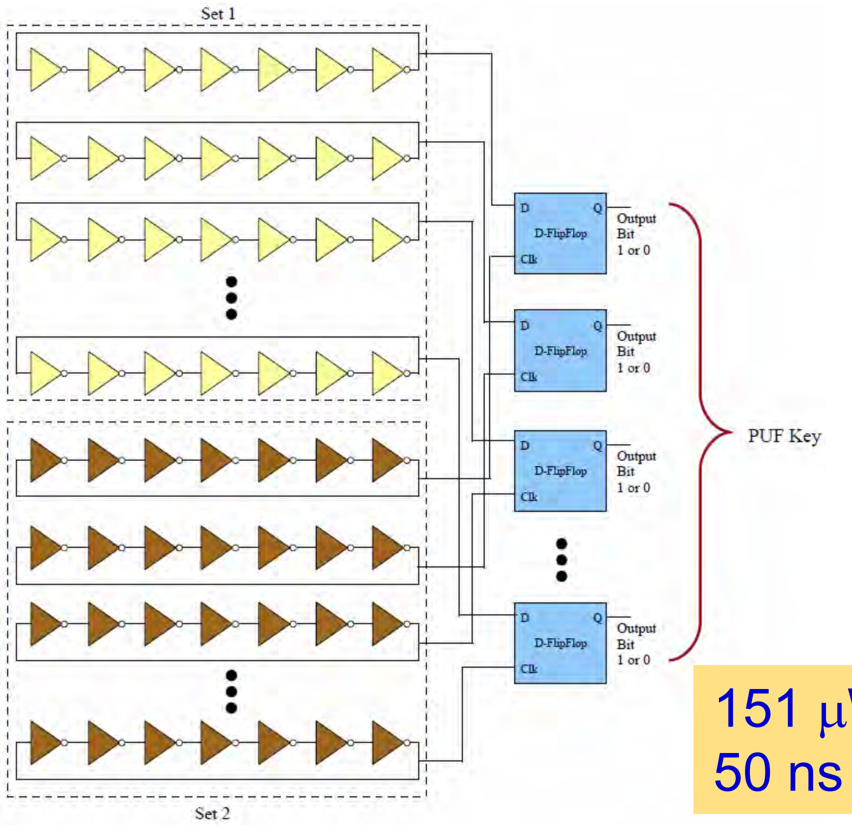
We Have Design a Variety of PUFs - DLFET Based



121 μW
150 ns

Power Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS



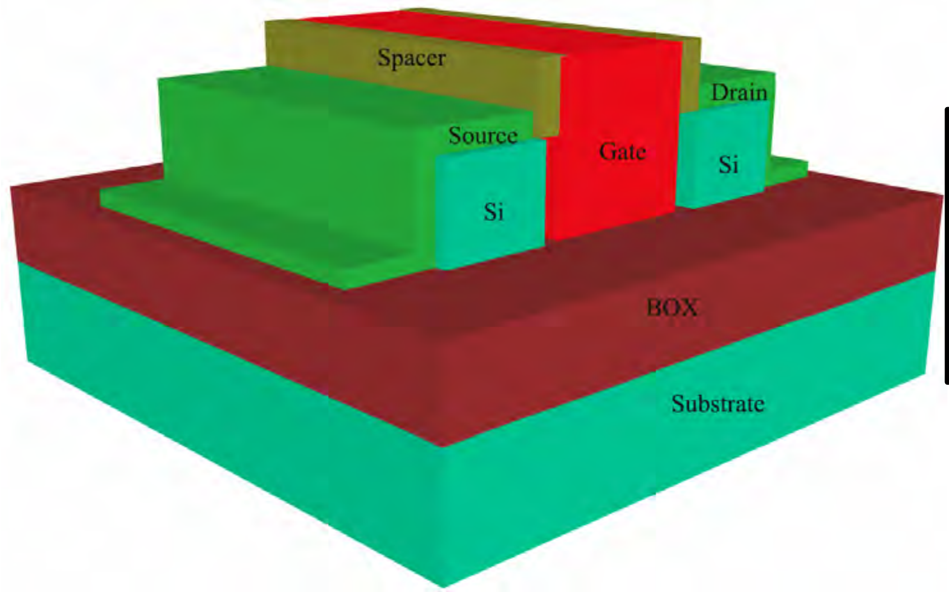
151 μW
50 ns

Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Transportation and Energy CPS

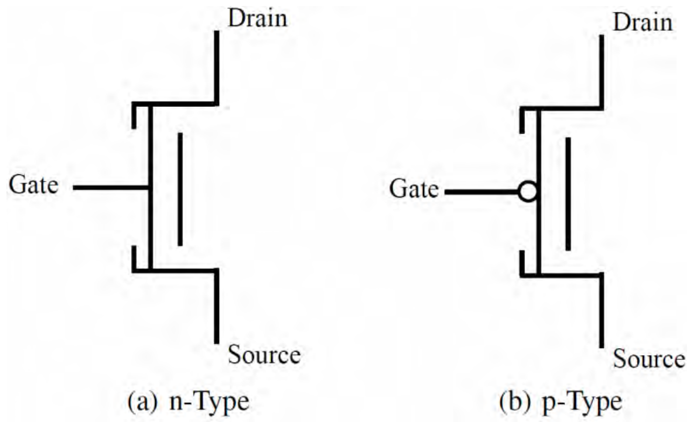
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Dopingless Transistor



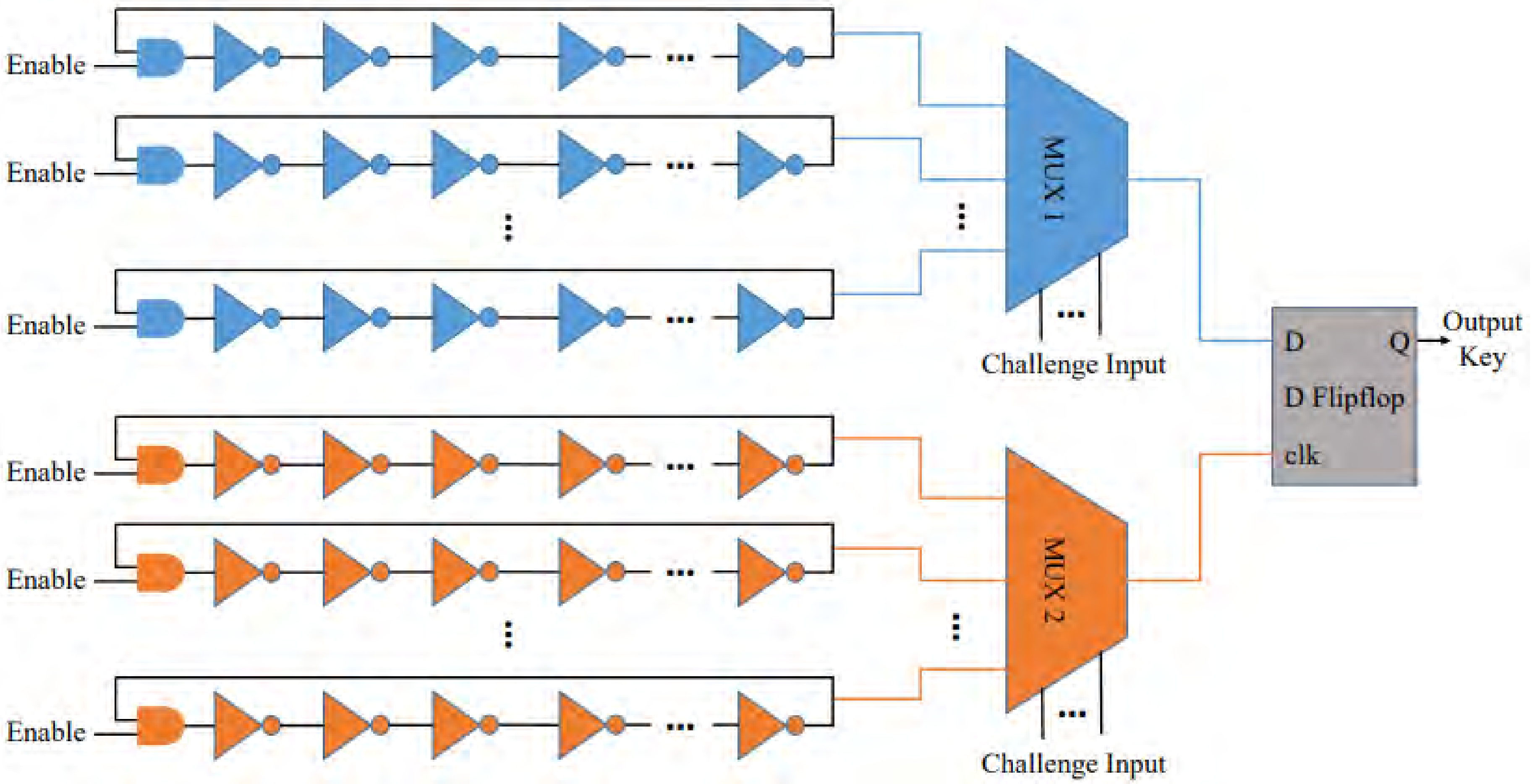
Structure of Dopingless FET

Symbols of n-type and p-type Dopingless FET



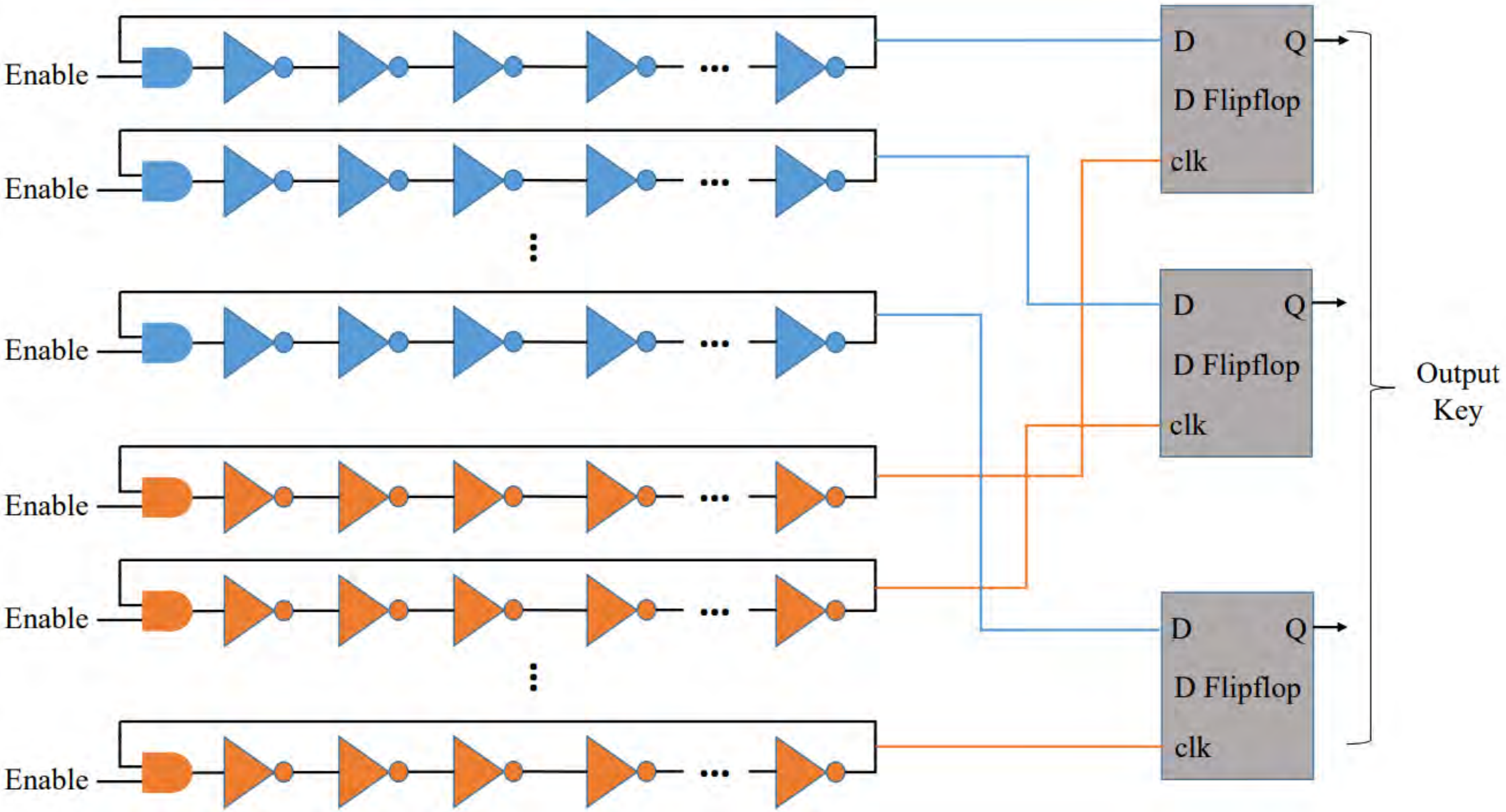
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

DLFET Based Power Optimized Hybrid Oscillator Arbiter PUF



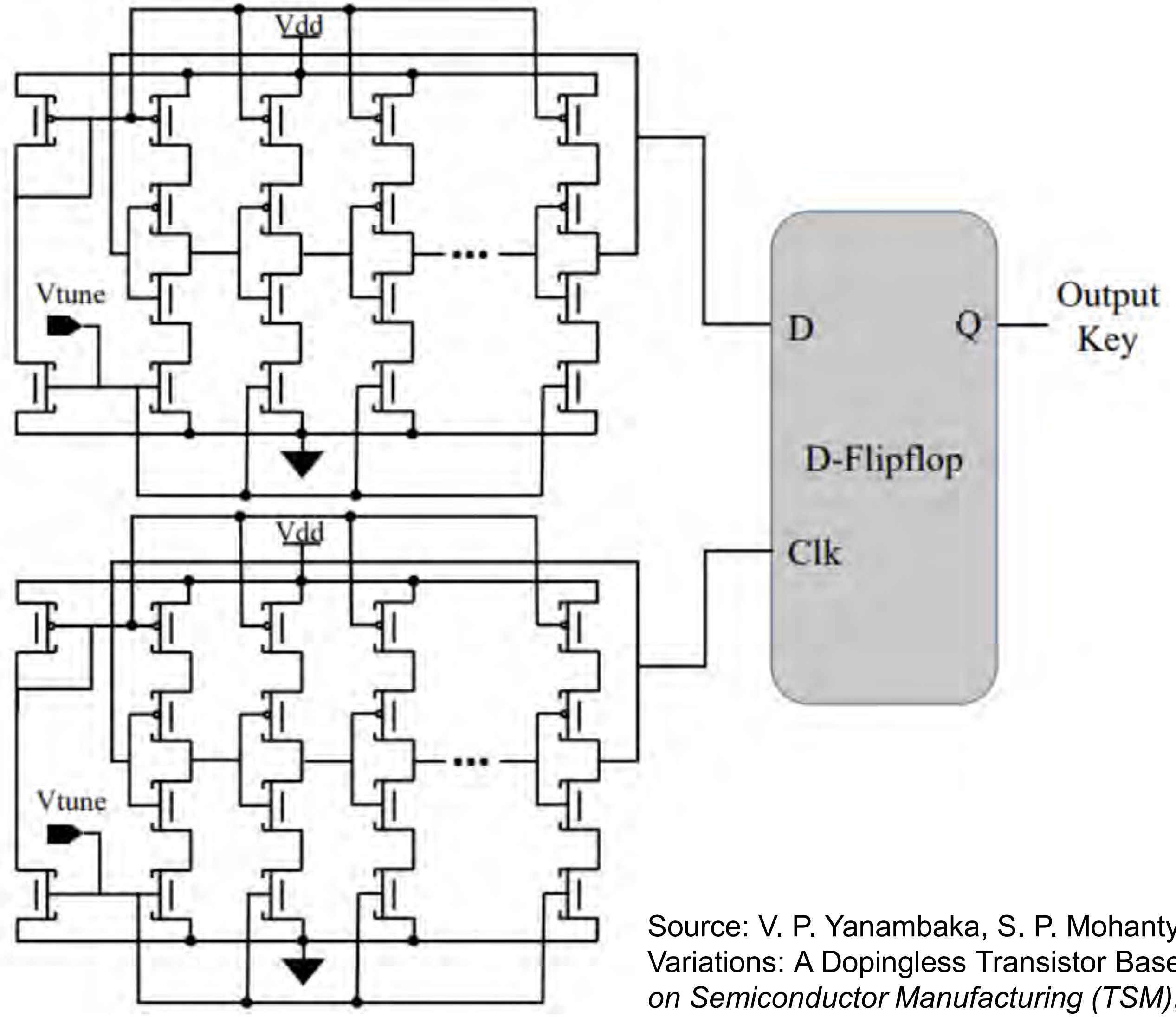
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

DLFET Based Speed Optimized Hybrid Oscillator Arbiter PUF



Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Dopingless Transistor Device Parameters



Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Dopingless Transistor Device Parameters

Parameters	Dopingless FET
Silicon Film Thickness (T_{si})	10 nm
Effective Oxide Thickness (EOT)	1 nm
Gate Length (L_g)	20 nm
Width (W)	1 μm
Source/Drain extension	10 nm
Metal work function/doping for source/drain	3.9 eV (Hafnium)
Metal work function/doping for gate	4.66 eV (TiN)
Doping	$10^{15}/cm^3$

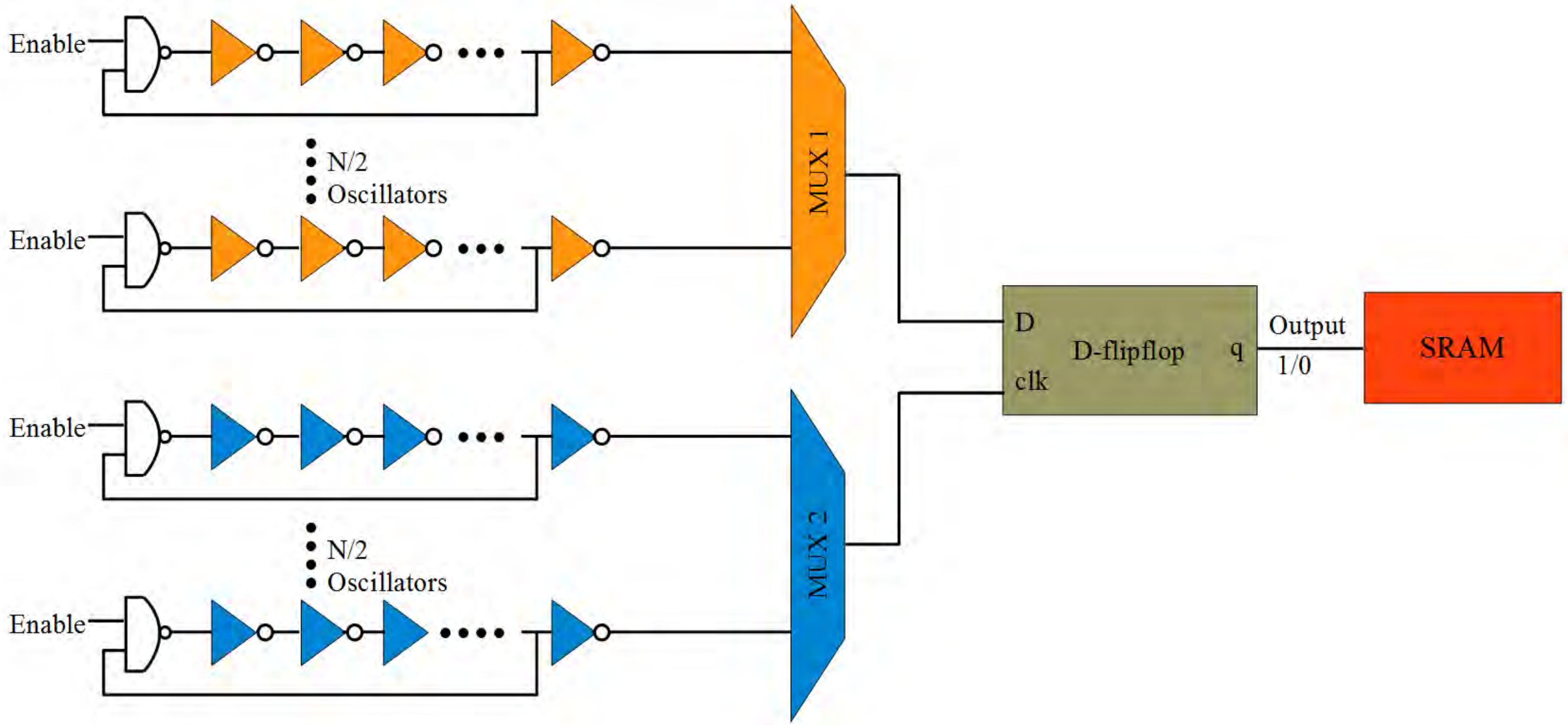
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Simulation Results

Research Work	Technology	Architecture Used	Power Consumption	Uniqueness (%)	Reliability (%)
Yanambaka et al. [3] (Power Optimized)	10 nm Dopingless FET	Current Starved VCO Hybrid Oscillator Arbiter PUF	121.3 μW	50.0	1.9
Yanambaka et al. [3] (Speed Optimized)	10 nm Dopingless FET	Current Starved VCO Hybrid Oscillator Arbiter PUF	310.8 μW	50.0	1.5
Yanambaka et al. [4] (Power Optimized)	10 nm Dopingless FET	Reconfigurable Hybrid Oscillator Arbiter PUF	143.3 μW	47.0	1.25
Yanambaka et al. [4] (Speed Optimized)	10 nm Dopingless FET	Reconfigurable Hybrid Oscillator Arbiter PUF	167.5 μW	48.0	2.1

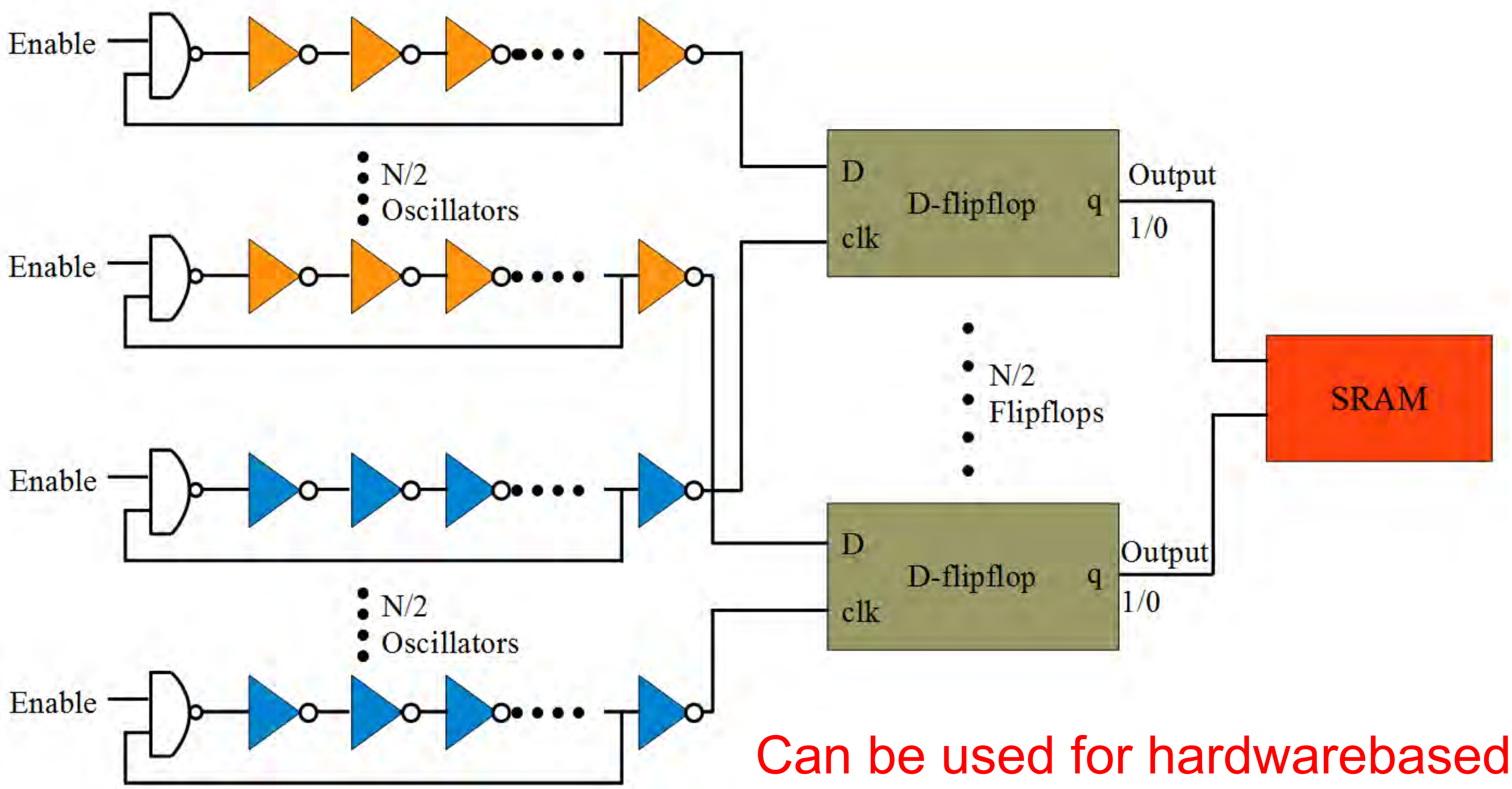
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Multikey Generating PUF



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, and J. Singh, "Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function", in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 200--205.

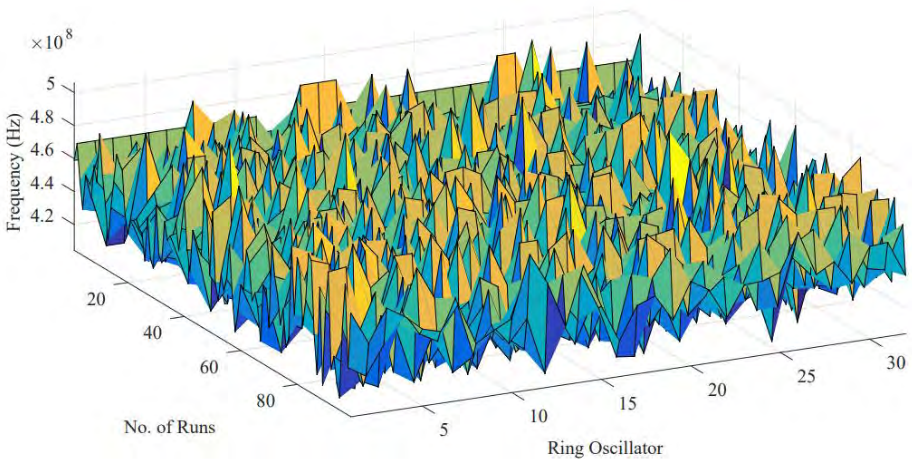
Multikey Generating PUF



Can be used for hardwarebased OTP generation.

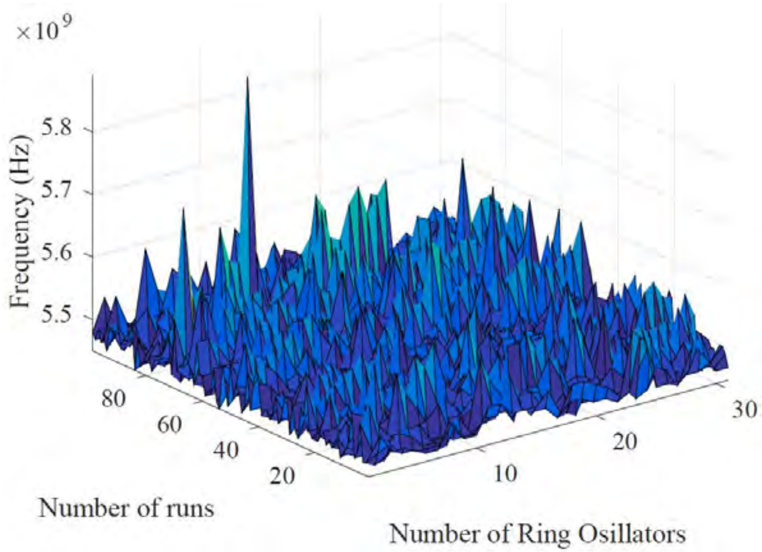
Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, and J. Singh, "Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function", in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 200--205.

Frequencies of Different Ring Oscillators



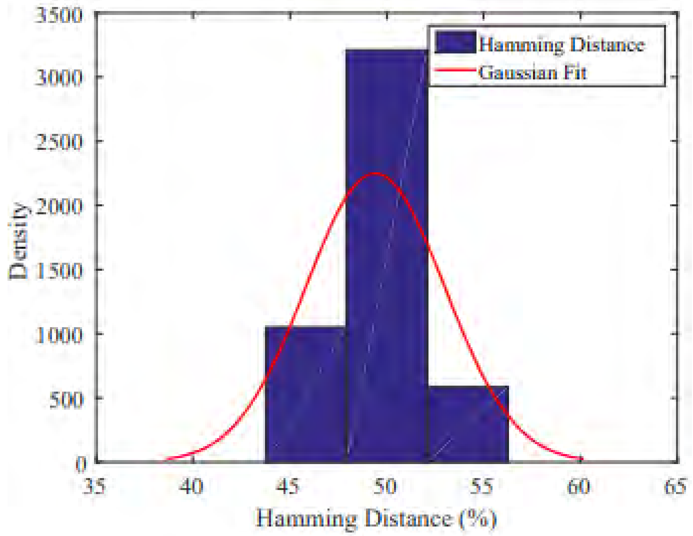
FinFET Based Ring Oscillators

DLFET Based Ring Oscillators

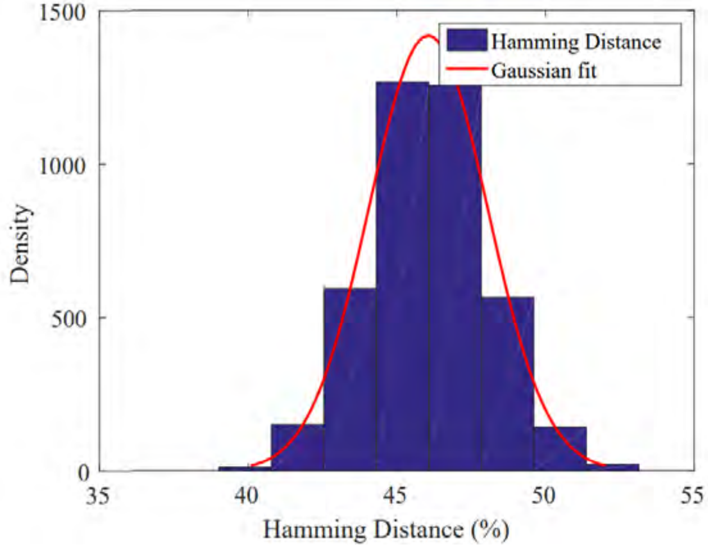


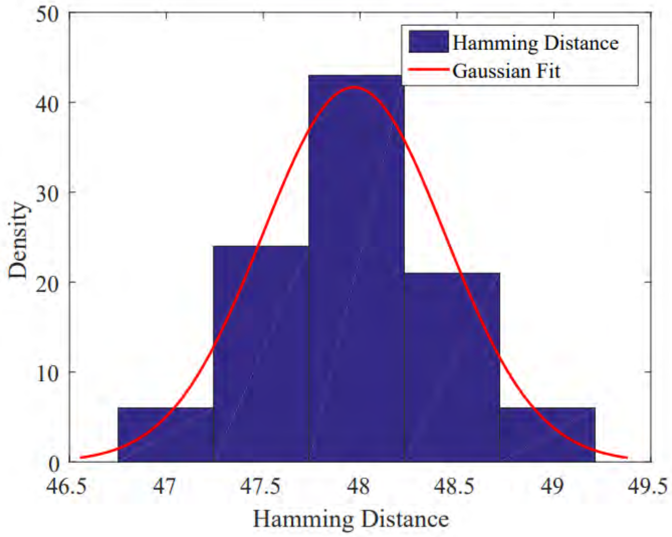
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Uniqueness of Power-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



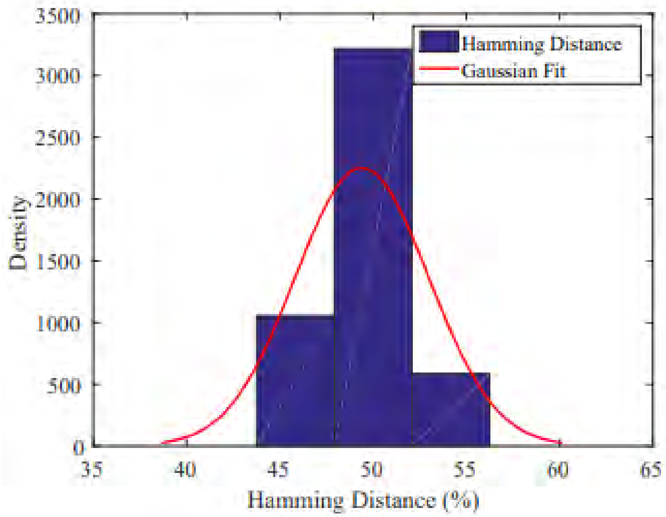


DLFET Based Hybrid Oscillator Arbiter PUF

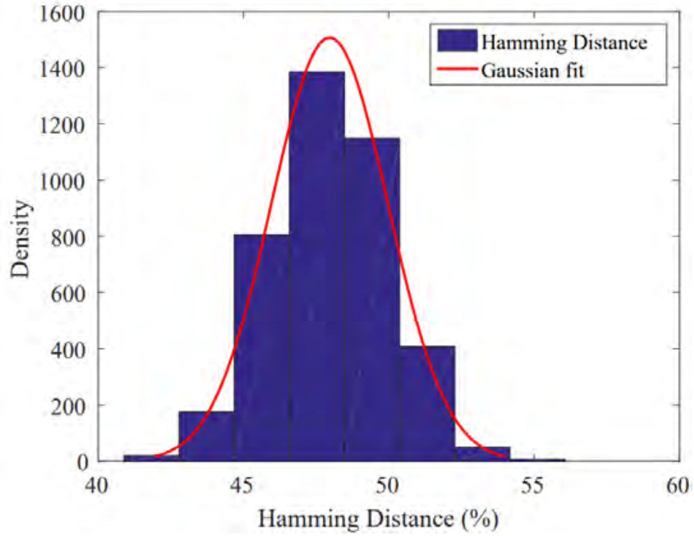
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

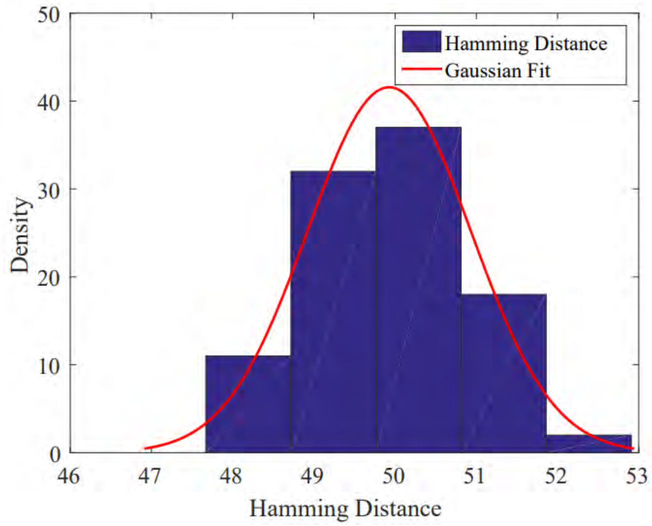
Uniqueness of Speed-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



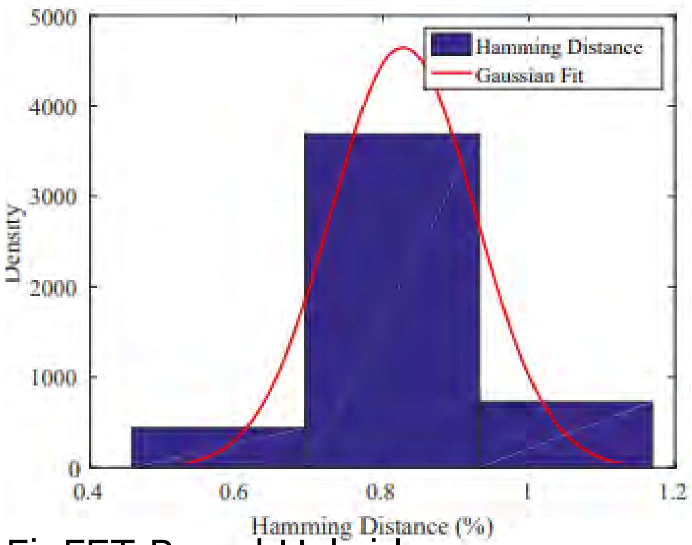
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF



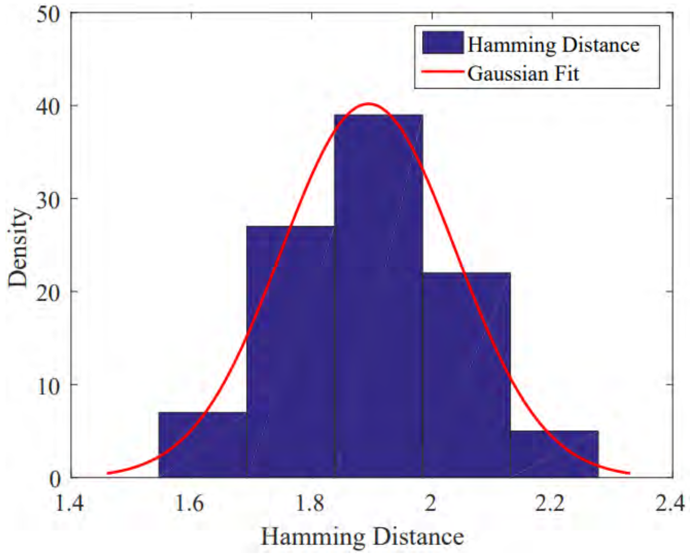
DLFET Based Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

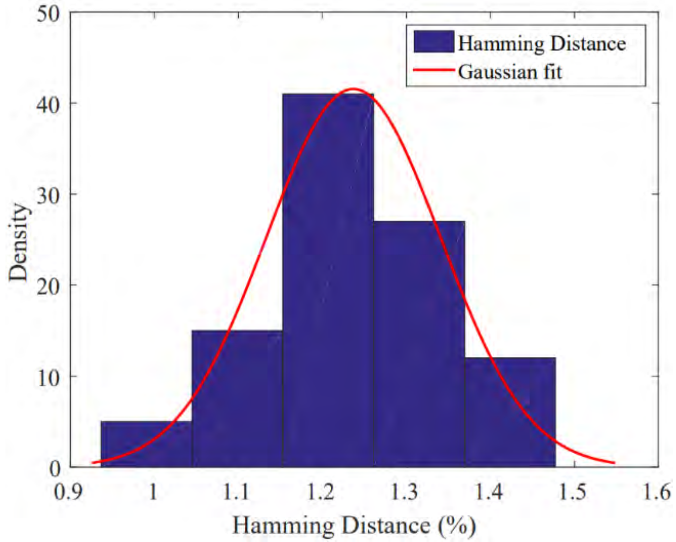
Reliability of Power-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



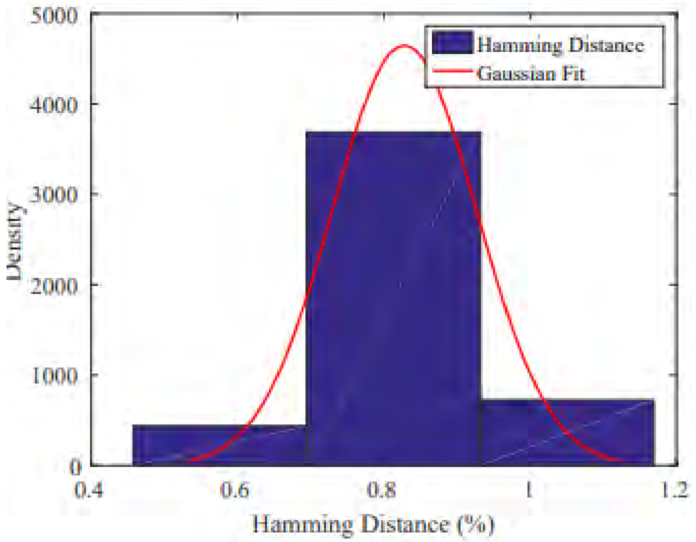
DLFET Based Hybrid Oscillator Arbiter PUF



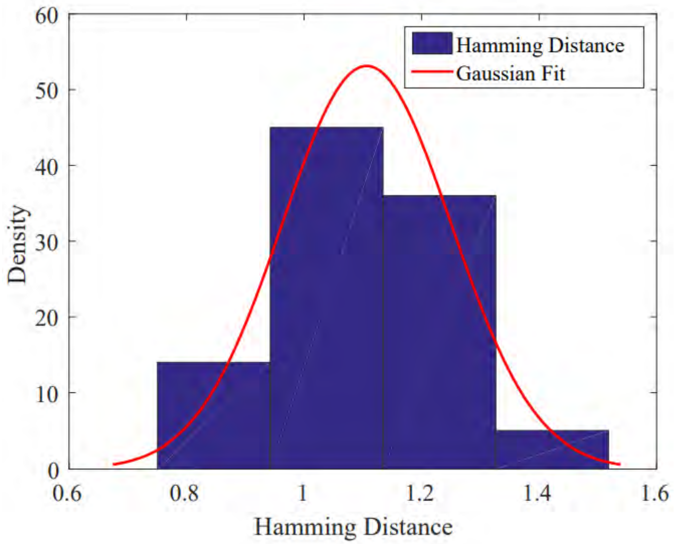
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

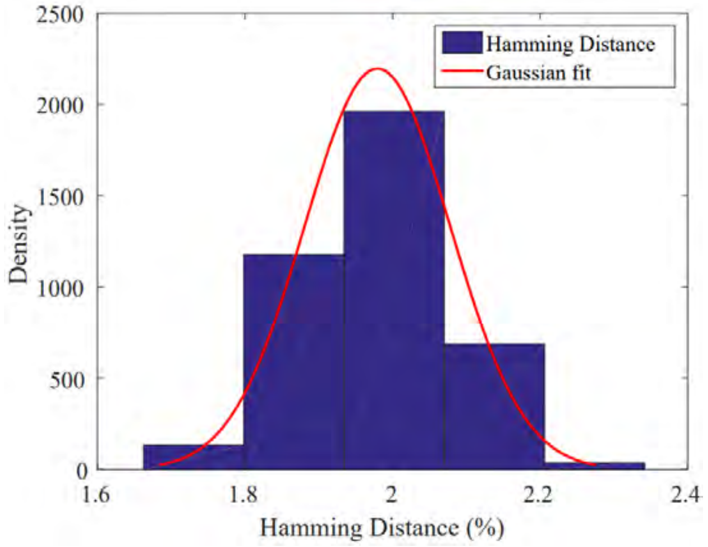
Reliability of Speed-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



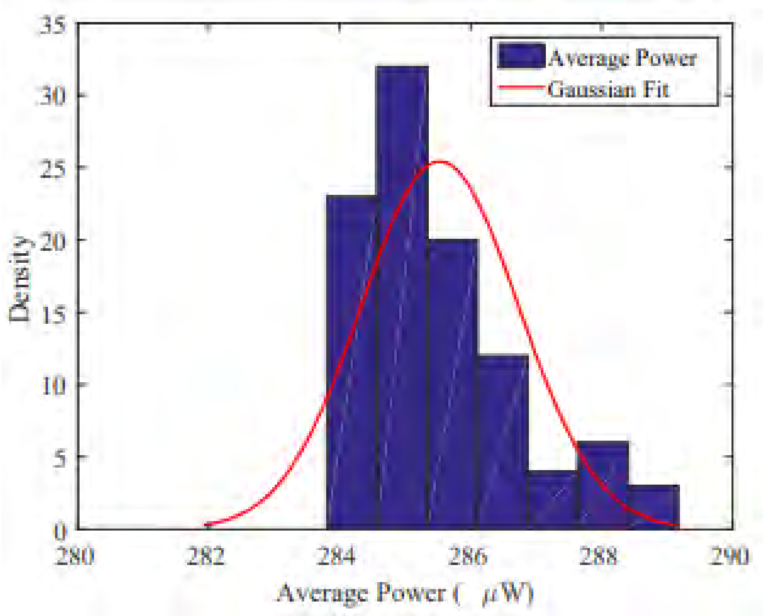
DLFET Based Hybrid Oscillator Arbiter PUF



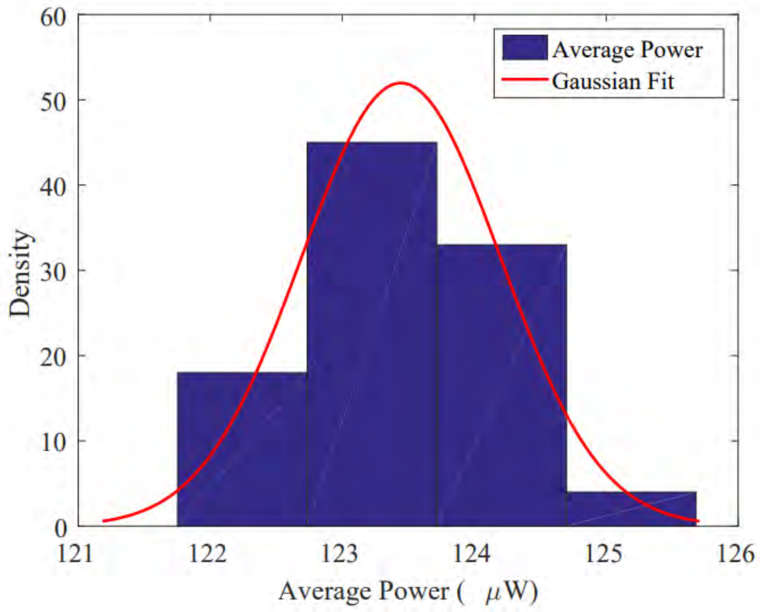
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Average Power of Power-Optimized PUF



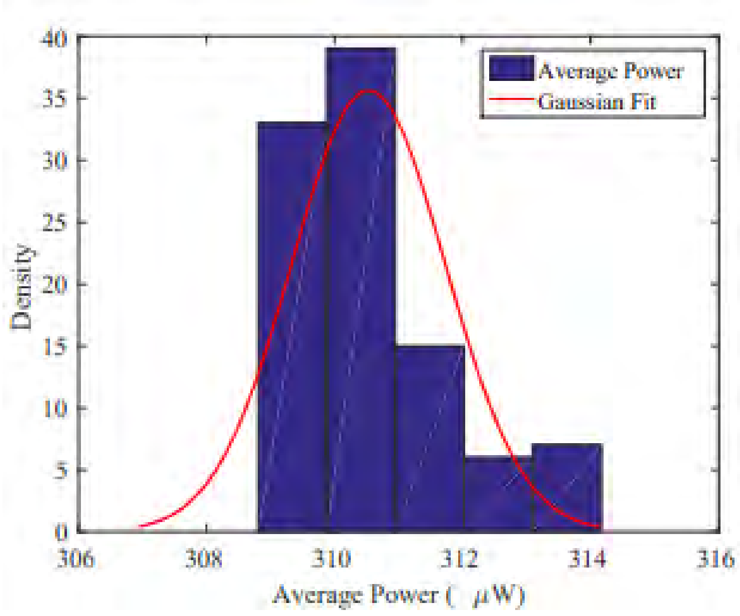
FinFET Based Hybrid Oscillator Arbiter PUF



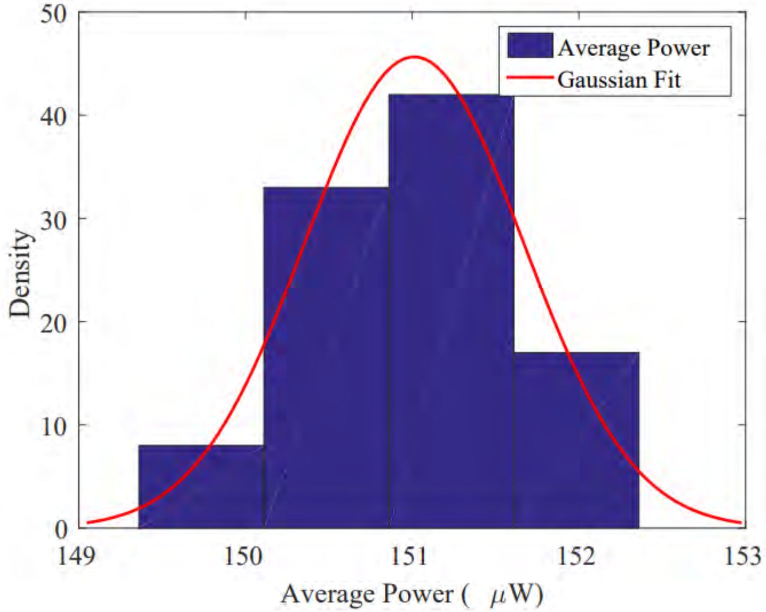
DLFET Based Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Average Power of Speed-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



DLFET Based Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Randomness of Hybrid Oscillator Arbiter PUF

	Power Optimized PUF	Speed Optimized PUF
32nm FinFET Based Hybrid Oscillator Arbiter PUF	42	42
DLFET Based Hybrid Oscillator Arbiter PUF	47.5	51.3
DLFET Based Reconfigurable PUF	48	46

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Time to Generate Keys

	Power Optimized PUF	Speed Optimized PUF
32nm FinFET Based Hybrid Oscillator Arbiter PUF	150 ns	50 ns
DLFET Based Hybrid Oscillator Arbiter PUF	150 ns	50 ns
DLFET Based Reconfigurable PUF	200 ns	100 ns

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Comparison of Results

Research Work	Technology	Architecture Used	Power Consumption	Uniqueness (%)	Reliability (%)
Yanambaka et al. [1] (Power Optimized)	32 nm FinFET	Current Starved VCO Hybrid Oscillator Arbiter PUF	285.5 µW	50.9	0.79
Yanambaka et al. [3] (Power Optimized)	10 nm Dopingless FET	Current Starved VCO Hybrid Oscillator Arbiter PUF	121.3 µW	50.0	1.9
Yanambaka et al. [4] (Power Optimized)	10 nm Dopingless FET	ReconfigurableHybrid Oscillator Arbiter PUF	143.3 µW	47.0	1.25
S. R. Sahoo, et al. [5]	90 nm CMOS	Ring Oscillator	-	45.78	-
Maiti, et al. [6]	90nm CMOS	Ring Oscillator	-	47.31	0.86
Cherkaoui, et al. [7]	350 nm CMOS	Transient Effect Ring Oscillator	-	49.7	0.6

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Vedas – Ancient Indian Scriptures

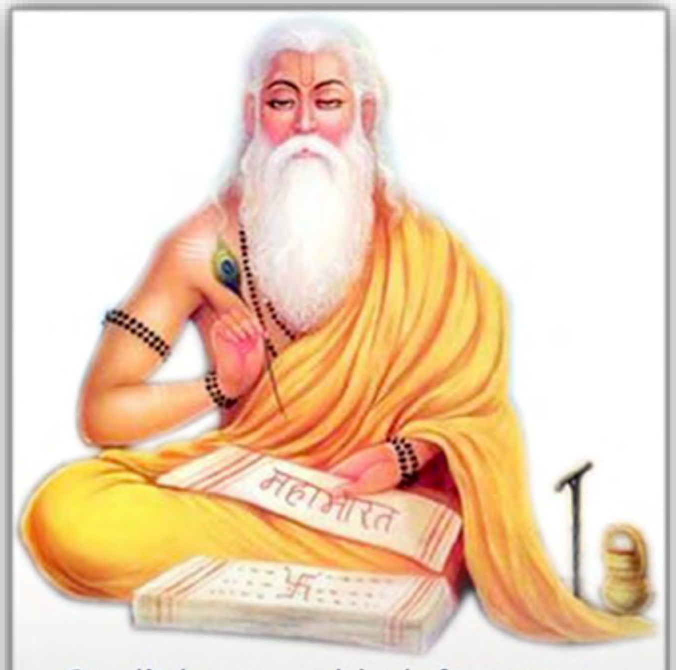
Rig Veda

Saama Veda

Vedic Scriptures

Yajur Veda

Adharva Veda



Credit by: www.hindufaqs.com

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Vedic Chanting

- Vedas were passed down through generations using mnemonic techniques.
- To ensure their integrity, two aspects were added to Vedas
  - Tones
    - Udaatta, Anudaatta, Svarita, Deergha Svarita
  - Pathas
    - Pada, Krama, etc.,

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Vedic Chanting Methods

- There are 11 *paathas* or methods to chant a vedic scripture.
- Words are repeated in each paatham using sequencing to ensure they are well memorized.
- Most popular are *Pada, Krama, Jata, Ghana,* ***Ghana Patham*** considered being the most difficult.
- Two words are repeated 6 times in Jata Paatham.
- Three words are repeated 13 times in Ghana Paatham.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Jata and Ghana Patham

- Consider three words – b1, b2, and b3.
- Following is the formula to recite the words in the Jata patham:
  - {b1, b2}, {b2, b1}, {b1, b2}
- Following is the formula to recite the words in the Ghana patham:
  - {b1, b2}, {b2, b1}, {b1, b2,b3}, {b3, b2,b1}, {b1, b2,b3}
- Using the formula above, a 128-bit key is transformed into a 2.5Kbit key in the processing algorithm.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Ghana Paatham

- Original Verse:
- gaṉānā̎ṃ tvā gaṉapa̍tigṃ havāmahē
- Ghana Paatham (considering first 3 words):
- gaṉānā̎ṃ tvā tvā gaṉānā̎ṃ gaṉānā̎ṃ tvā gaṉapa̍tiṃ gaṉapa̍tiṃ tvā gaṉānā̎ṃ gaṉānā̎ṃ tvā gaṉapa̍tim ||

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Ghana Paatham

- Original Verse:
- gaṇānā̍ṃ tvā gaṇapa̍tigṃ havāmahē
- Ghana Paatham (considering words 2, 3, and 4):
- tvā̲ gaṇapa̍tiṃ gaṇapa̍tiṃ tvā tvā gaṇapa̍tigṃ havāmahē havāmahē gaṇapa̍tiṃ tvā tvā gaṇapa̍tigṃ havāmahē

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

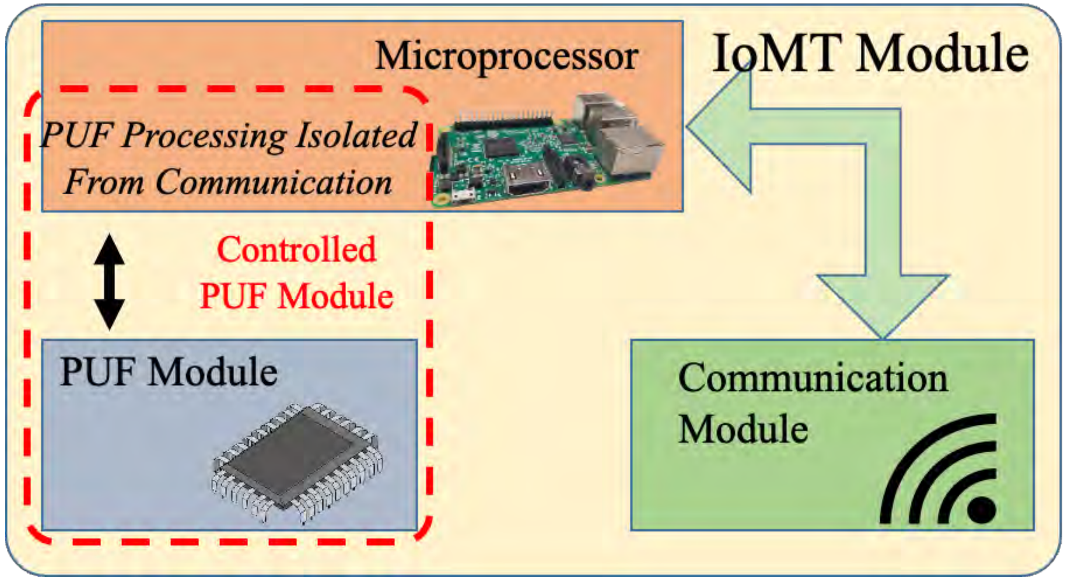
Why Veda for PUF?

- The key length increases significantly
- Number of keys around the ideal value increases significantly.
  - Keys around 54 % uniqueness decreased and 50 % increased.
  - Number of keys with randomness around 48 % increased significantly.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Proposed Veda – PUF Architecture

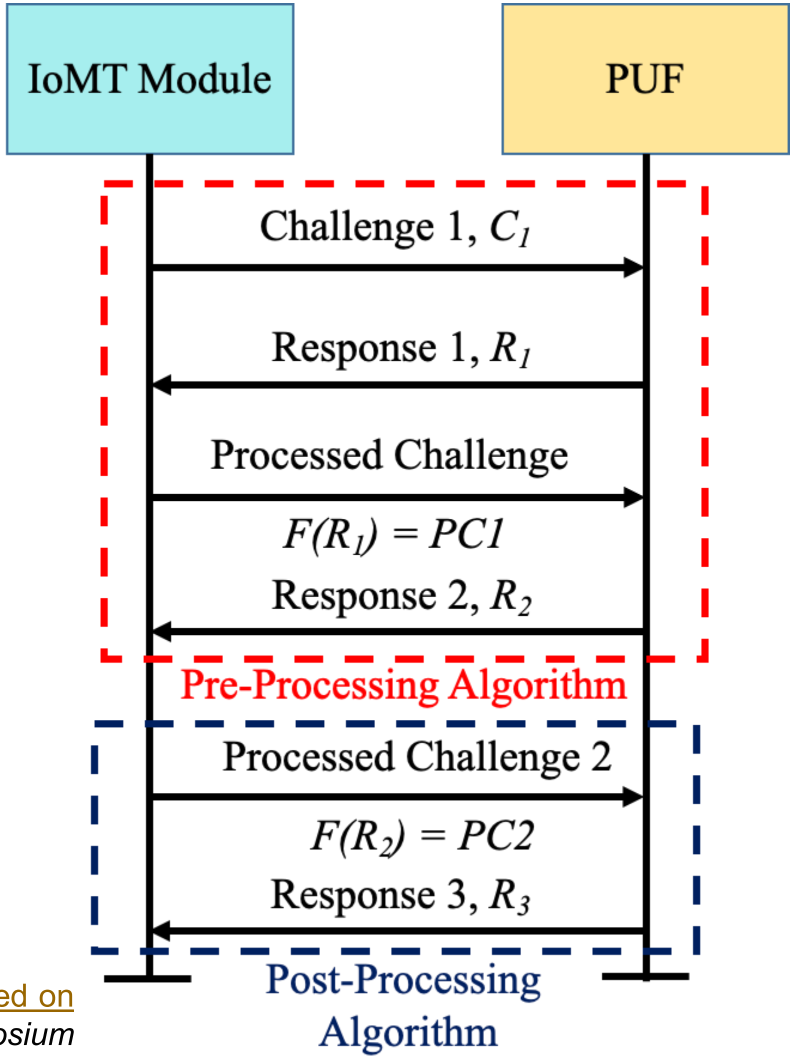
- Veda – PUF is a controlled PUF.
- Challenges and Responses are processed in the PUF.
- Communication module is isolated from the PUF.



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Proposed Controller Algorithm for Veda – PUF

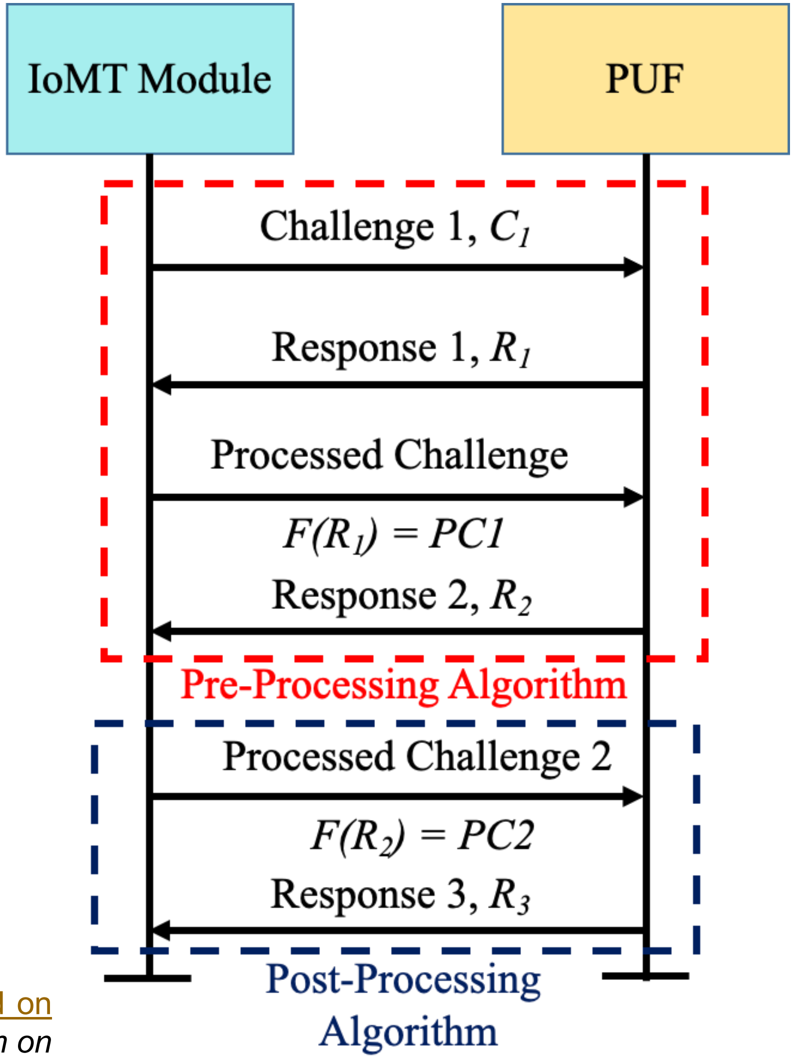
- Pre – Processing Algorithm
  - The first stage in key generation.
  - Generate the first response for a challenge and process it for the second stage.
- Post – Processing Algorithm
  - Generates the final response with increased key length.



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

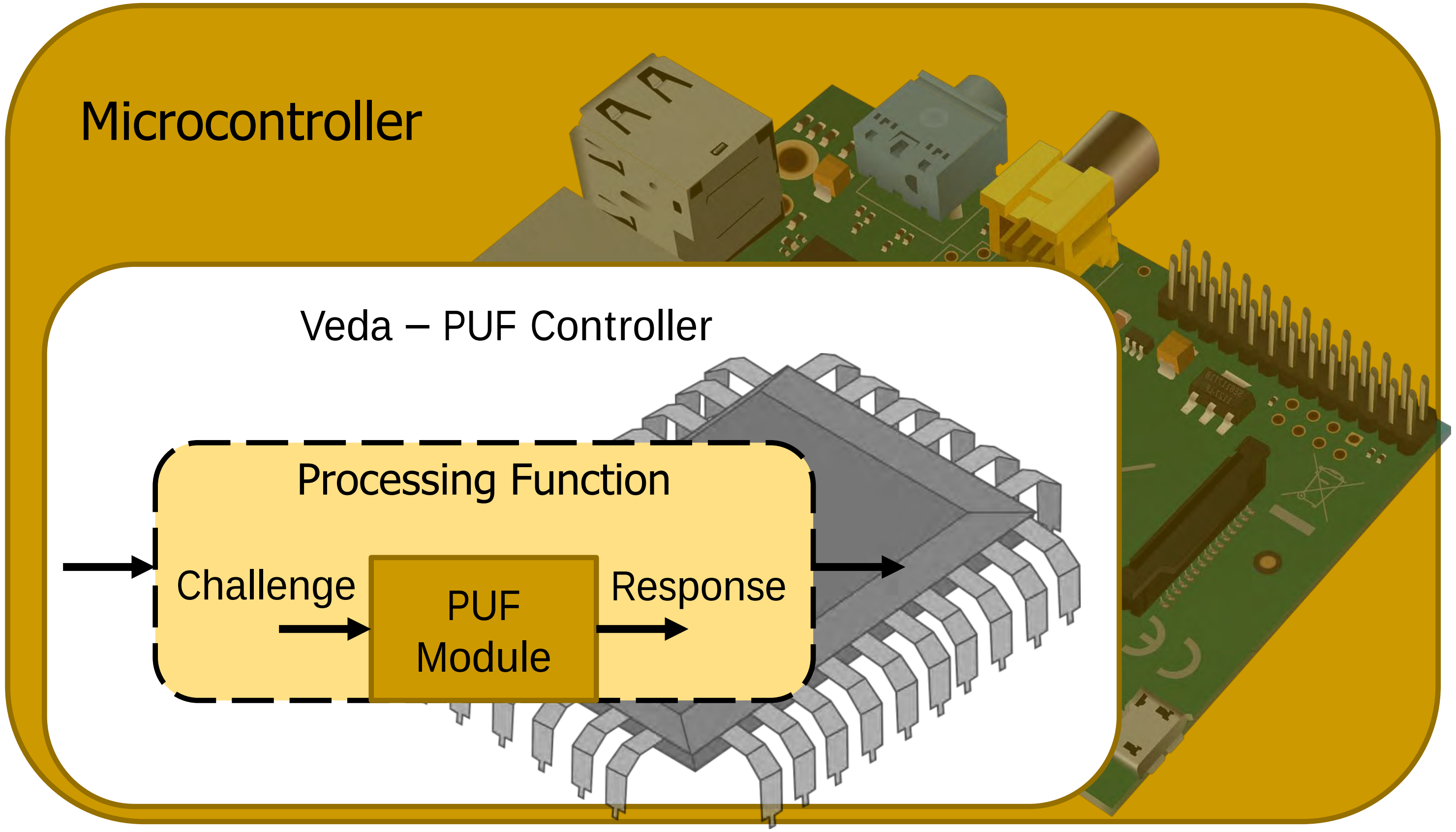
Key Processing Function Veda – PUF

- Considering the following binary key:
  - b1, b2,…. bn
- Ghana Paatha formula is used for the bits b1 -> bn-1.
- Jata Paatha formula is used for the last two bits.



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

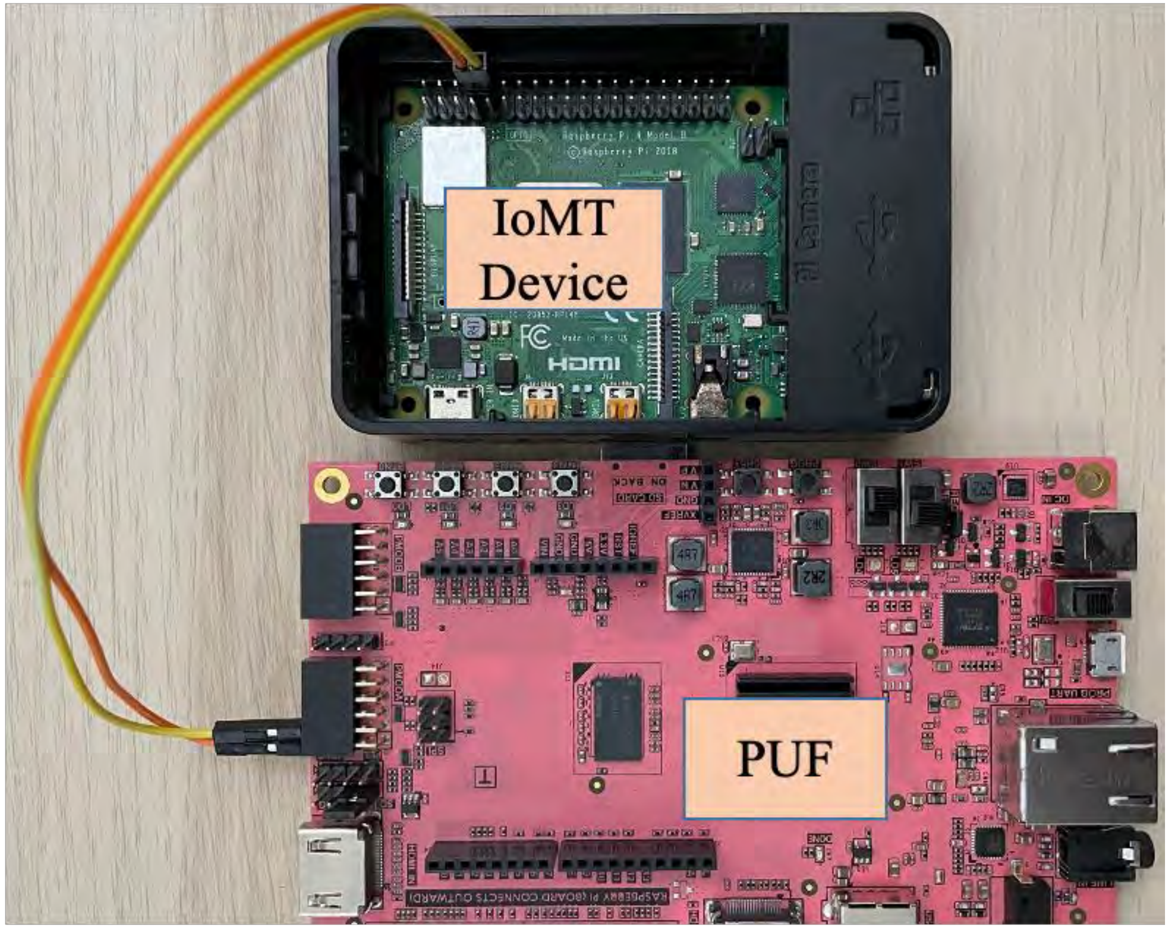
Veda-PUF Circuits



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

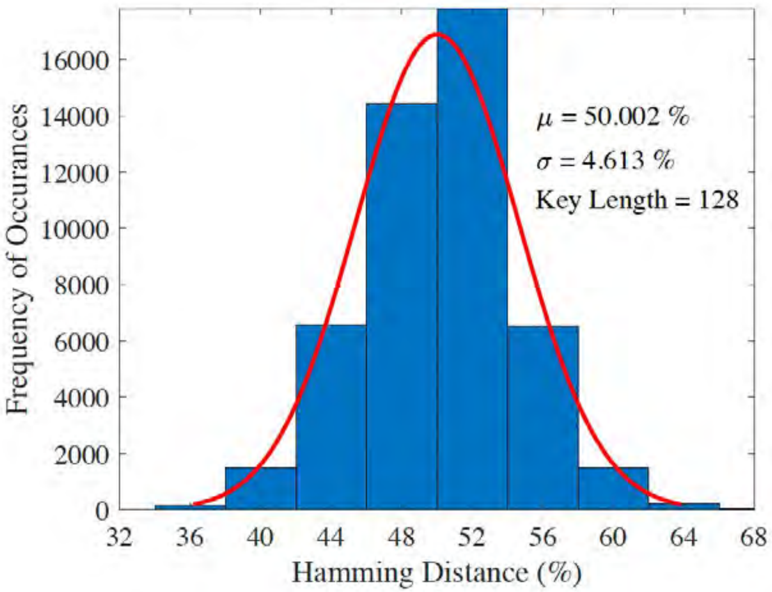
Experimental Setup

- Initial Considerations:
  - Initial challenge length is 128 – bits.
  - 1000 keys were generated.
  - Raspberry Pi– Key Generation IoMT device.
  - FPGA – PUF.

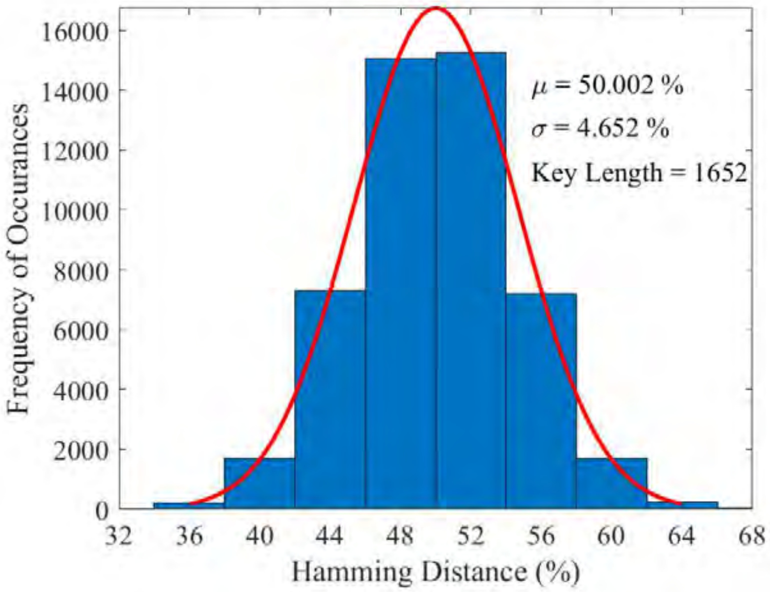


Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

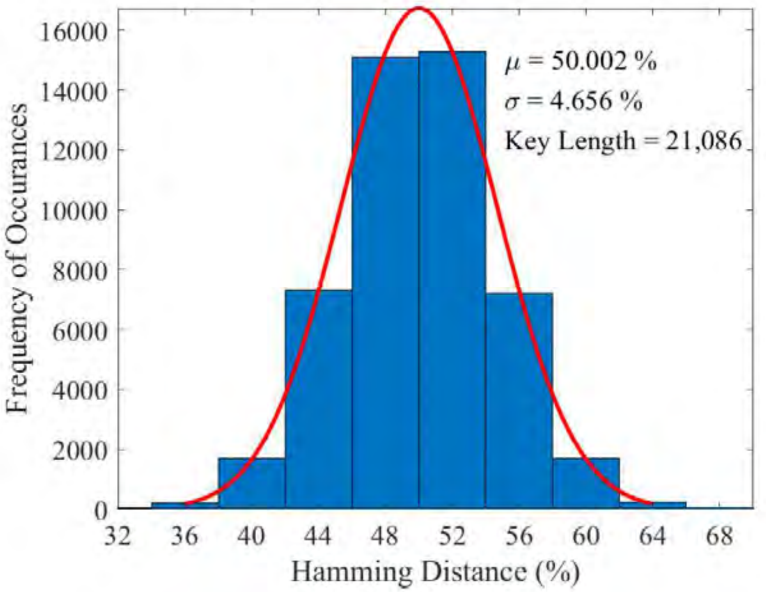
Characterization - Uniqueness



(a) Uniqueness of Original Keys



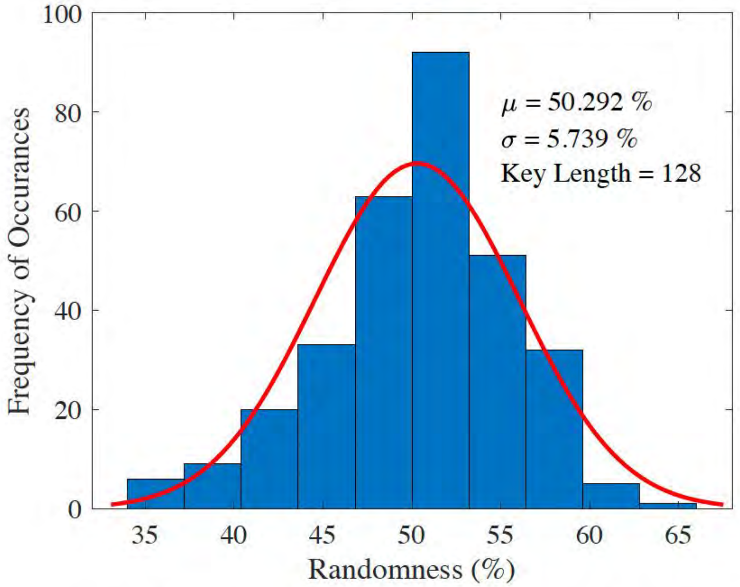
(b) Uniqueness of Processed Keys



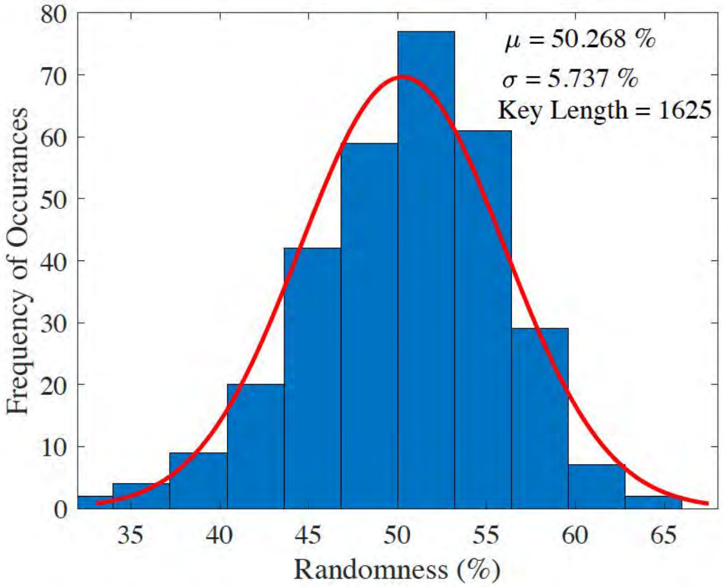
(c) Uniqueness of Keys Processed a Second Time

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

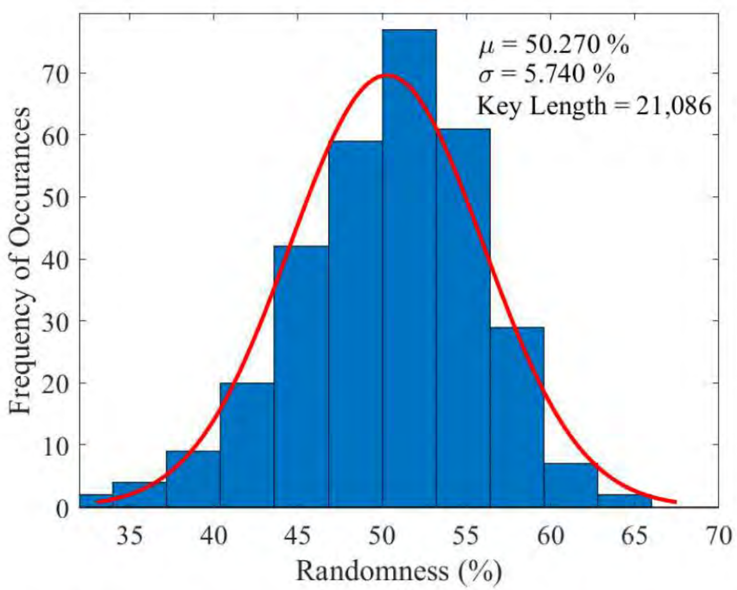
Characterization - Randomness



(a) Randomness of Original Keys



(b) Randomness of Processed Keys



(c) Randomness of Keys Processed a Second Time

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Reliability and Power Consumption

PUF Characteristic	Original Key	Processed Key
Uniqueness		
Mean	50.002 %	50.002 %
Standard Deviation	4.613 %	4.656 %
Reliability		
Mean	99.9 %	99.9 %
Standard Deviation	0 %	0 %
Randomness		
Mean	50.292 %	50.270 %
Standard Deviation	5.739 %	5.740 %
Power Consumption	3.1 W	3.25 W

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Veda-PUF: Conclusion and Future Research

- Key length increased significantly preserving the integrity.
  - 128 – bit key length increased to around 2.1 Kbits
- The number of keys at the ideal uniqueness and ideal randomness increased.
- Develop a machine learning resistant algorithm based on the Veda – PUF Architecture.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Physical Unclonable Function - Challenges and Research

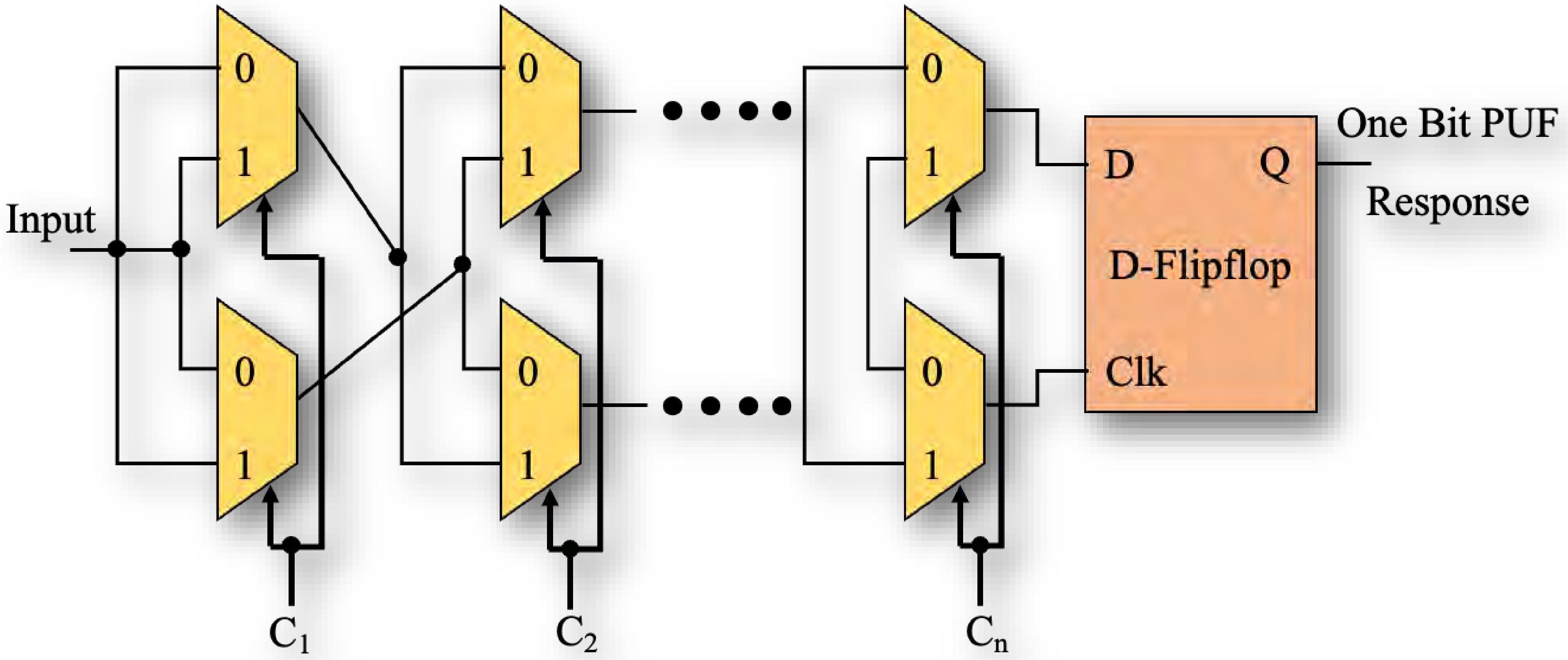
If PUF is So Great, Why Isn't Everyone Using It?

- PUF technology is difficult to implement well.
- In addition to security system expertise, one needs analog circuit expertise to harness the minute variances in silicon and do it reliably.
- Some PUF implementations plan for a certain amount of marginality in the analog designs, so they create a PUF field of 256 bits (for example), knowing that only 50 percent of those PUF features might produce reliable bits, then mark which features are used on each production part.
- PUF technology relies on such minor variances, long-term quality can be a concern: will a PUF bit flip given the stresses of time, temperature, and other environmental factors?
- Overall the unique mix of security, analog expertise, and quality control is a formidable challenge to implementing a good PUF technology.

Source: https://embeddedcomputing.com/technology/processing/semiconductor-ip/demystifying-the-physically-unclonable-function-puf

PUF Limitations – Larger Key Needs Large ICs

- Larger key requires larger chip circuit.



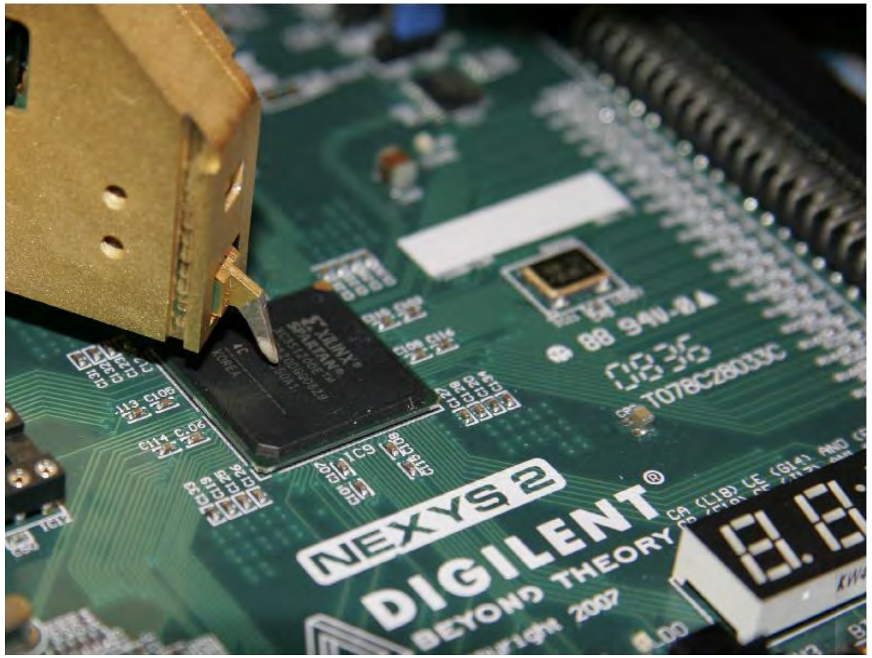
1 – Bit Arbiter PUF Architecture

PUF - Side Channel Leakage

- Cryptography and watermarking hardwares provide low-power consumption, real-time performance, higher reliability and low-cost along with easy integration in multimedia hardware.
- Cryptography and watermarking hardware which are implemented using CMOS technology are susceptible to side channel attacks which collects information from physical implementation rather than software weakness.
- DFX targeted for information leakage proof is very in the current information driven society.

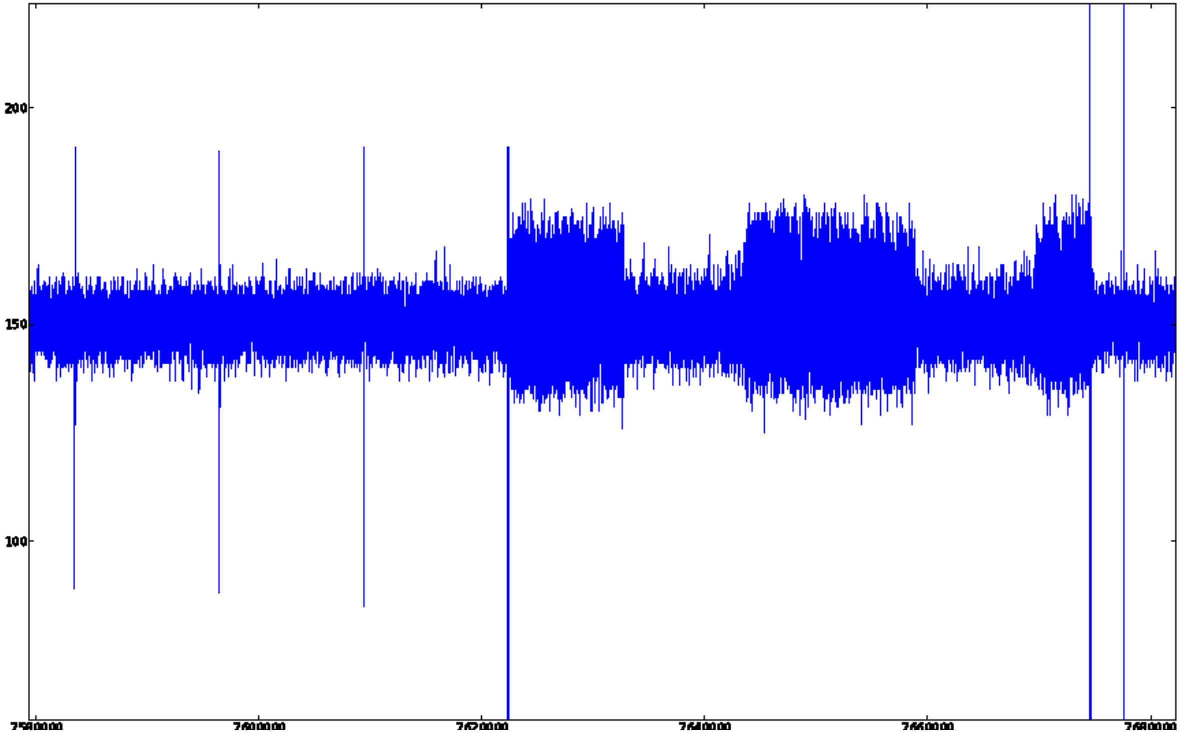
PUF - Side Channel Leakage

- Delay-based PUF implementations are vulnerable to side-channel attacks.



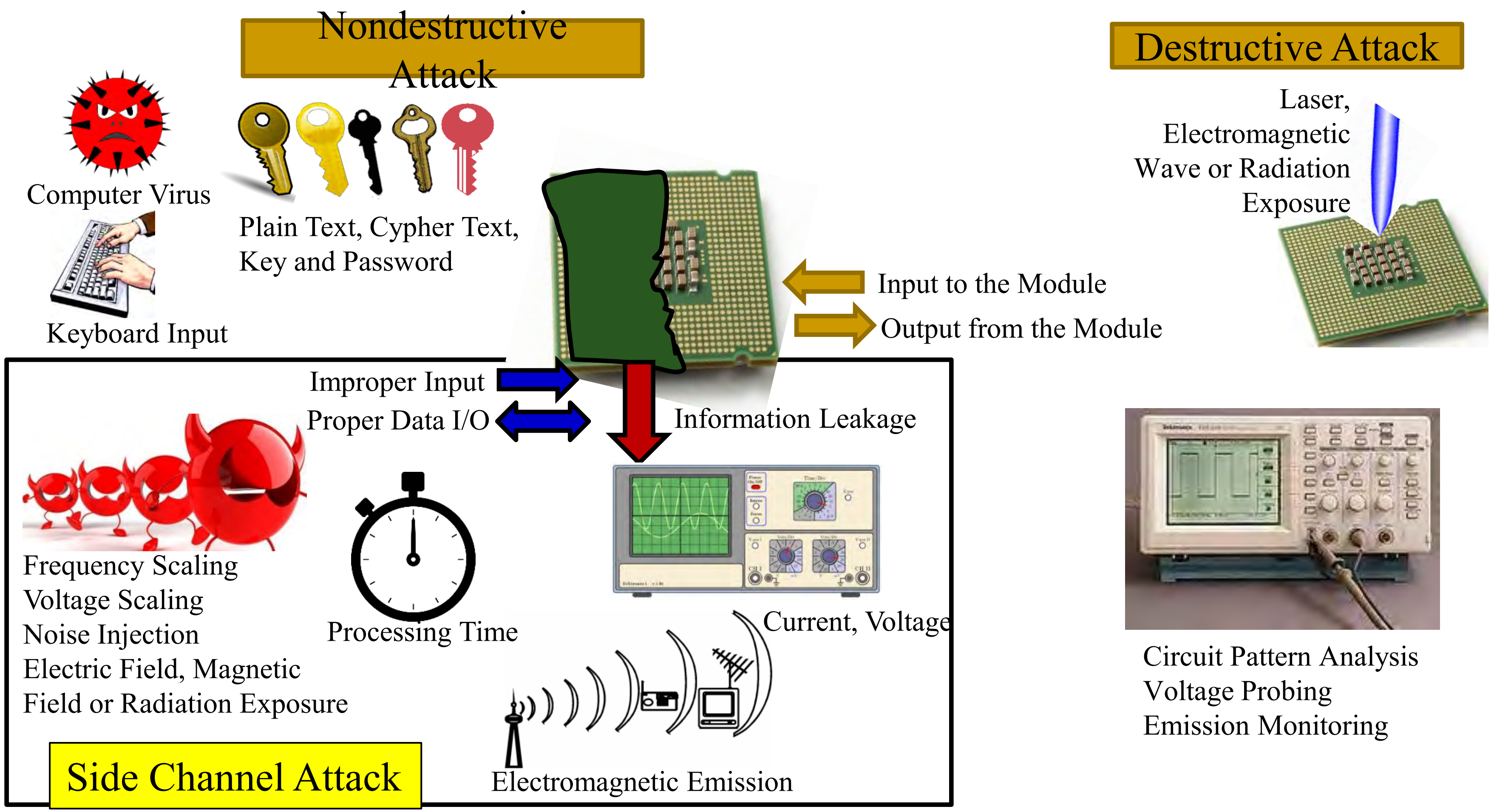
Langer ICR HH 150 probe over Xilinx Spartan3E-1200 FPGA

Source: Merli, D., Schuster, D., Stumpf, F., Sigl, G. (2011). Side-Channel Analysis of PUFs and Fuzzy Extractors. In: McCune, J.M., Balacheff, B., Perrig, A., Sadeghi, AR., Sasse, A., Beres, Y. (eds) Trust and Trustworthy Computing. Trust 2011. Lecture Notes in Computer Science, vol 6740. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21599-5_3



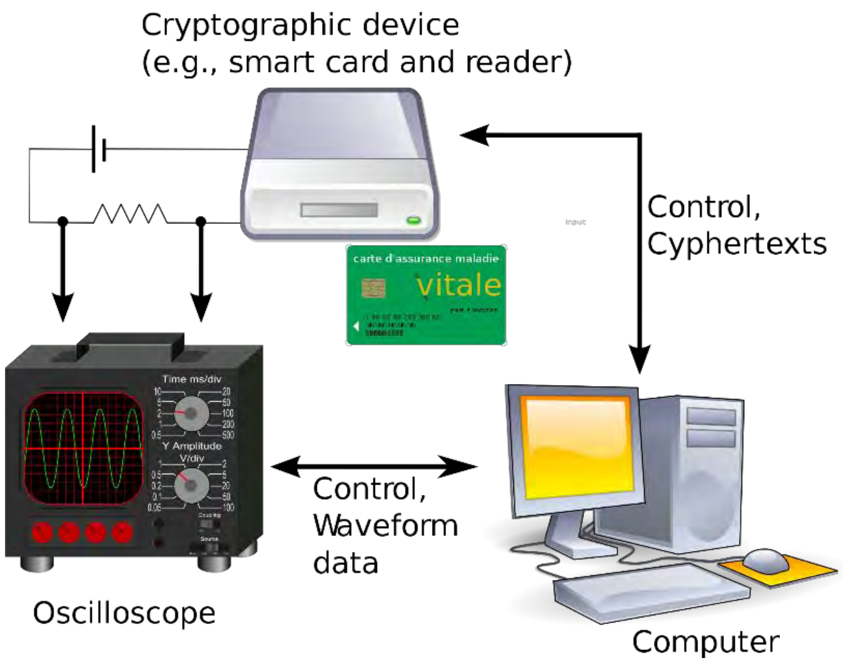
Magnification of the last part of the complete trace. Three trigger signals can be identified: (1) between oscillator phase and error correction phase, (2) between error correction and hashing, and (3) at the end of hashing.

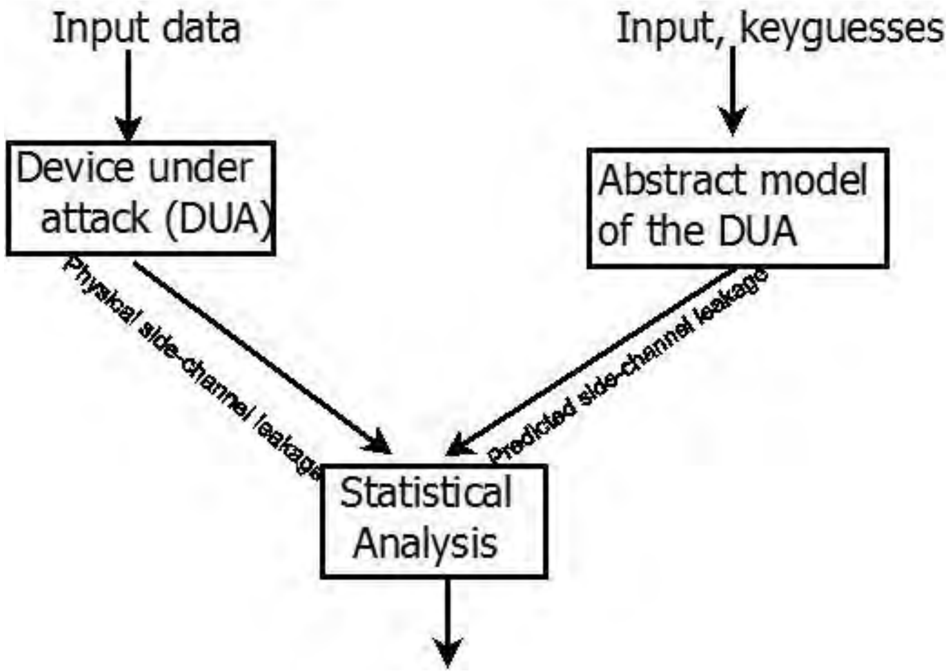
Side Channel Attacks



Source: http://www.keirex.com/e/Kti072_SecurityMeasure_e.html

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





Decision on key guess

Side Channel Attacks - Correlation Power Analysis (CPA)

- CPA analyzes the correlative relationship between the plaintext/ cipher-text and instantaneous power consumption of the cryptographic device.
- CPA is a more effective attacking method compared with DPA.

Differential Power Analysis (DPA)

- Attacks using relationship between data and power.
- Looks at difference of category averages for all key guess.
- Requires more power traces than CPA.
- Slower and less efficient than CPA.

Correlation Power Analysis (CPA)

- Attacks using relationship between data and power.
- Looks at correlation between all key guesses.
- Requires less power traces than DPA.
- Faster, more accurate than DPA.

Source: Zhang and Shi ITNG 2011

Differential Power Analysis (DPA) Attack Countermeasures

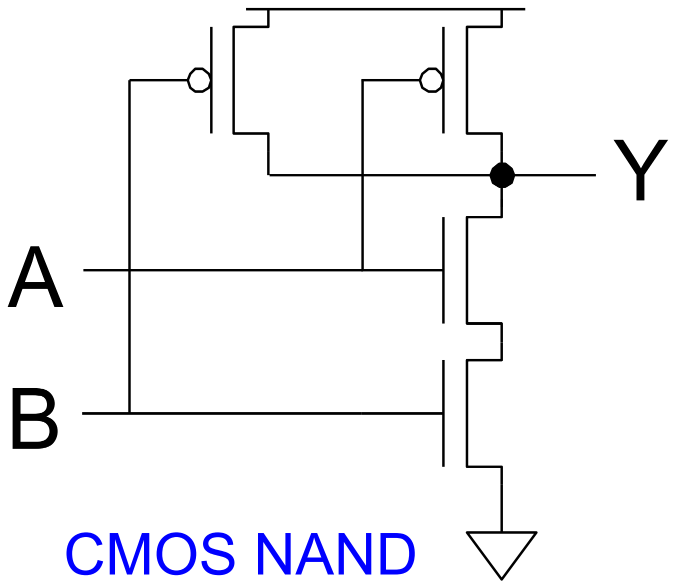
- DPA Attack Countermeasures
  - Hardware Measures
    - Power Randomization
    - Power Process Interrupts
    - Detached Power Supplies
    - Nondeterministic Execution
  - Software Measures
    - Desynchronization
    - Software Balancing
    - The Duplication Method
    - Random Masking
    - Secret-Sharing

Selected DPA and Correlation Power Analysis (CPA) Attack Resilience Methods

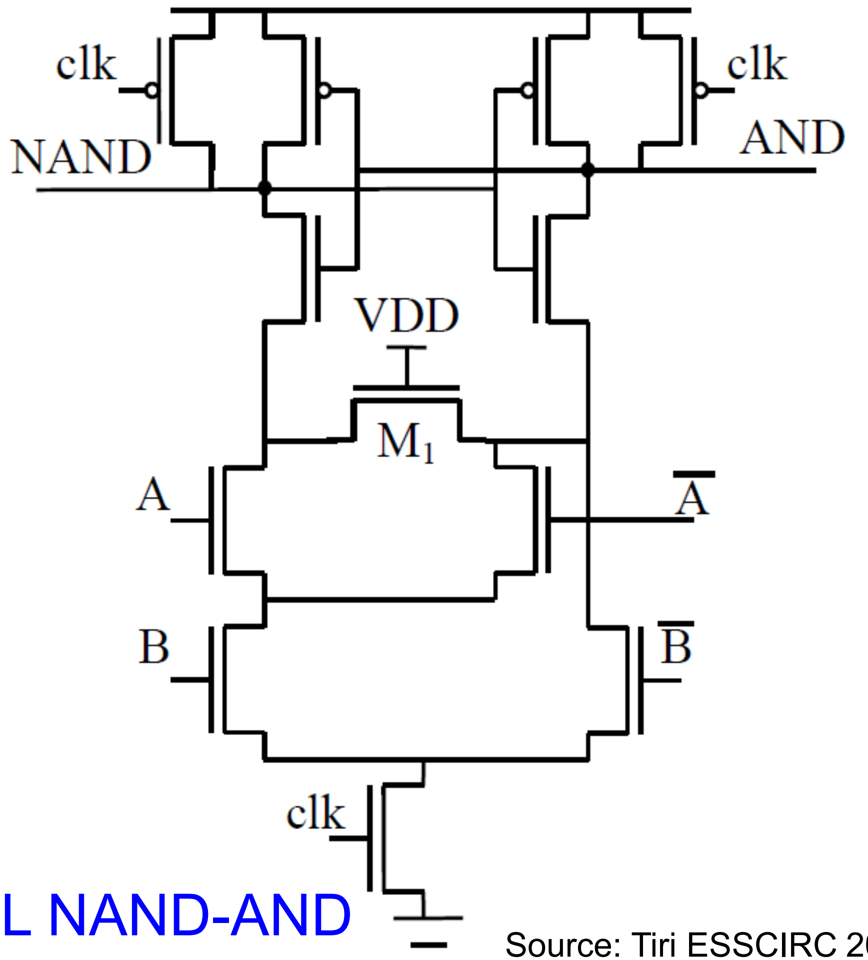
DPA and CPA Attack Resilience Methods

- Sense Amplifier Basic Logic (SABL)
- Wave Dynamic Differential Logic (WDDL)
- Two-Spacer Alternating Dual Rail Circuit
- Dynamic Voltage & Frequency Switching Approach
- Random Switching Logic (RSL)
- Return To Zero Protocols (RTZ)
- Masked Dual-Rail Pre-charged Logic (MDPL)

DPA Resilience Hardware: Sense Amplifier Basic Logic (SABL)



CMOS NAND



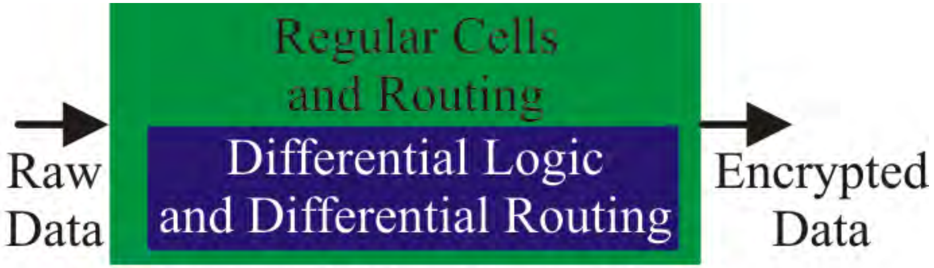
SABL NAND-AND

Source: Tiri ESSCIRC 2002

DPA Resilience Hardware: Differential Logic and Routing

- Develop logic styles and routing techniques such that power consumption per cycle is constant and capacitance charged at a node is constant.

(a) Standard SCMOS Logic

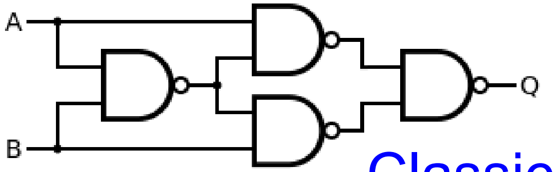


(b) Differential Logic and Routing

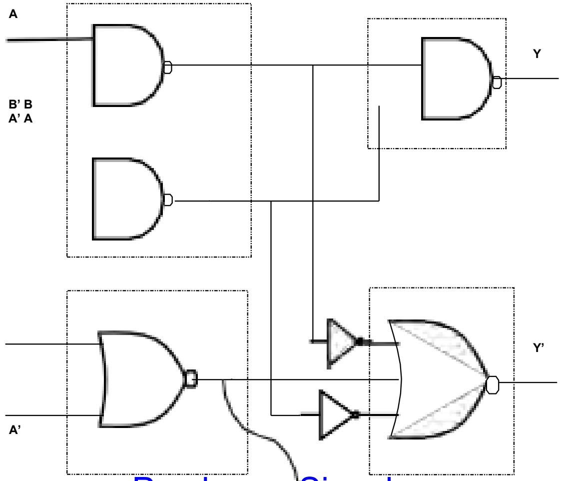
Vulnerable to side channel attack.

May abstract switching activity and reduce information leaking.

DPA Resilience Hardware: Differential Logic and Routing



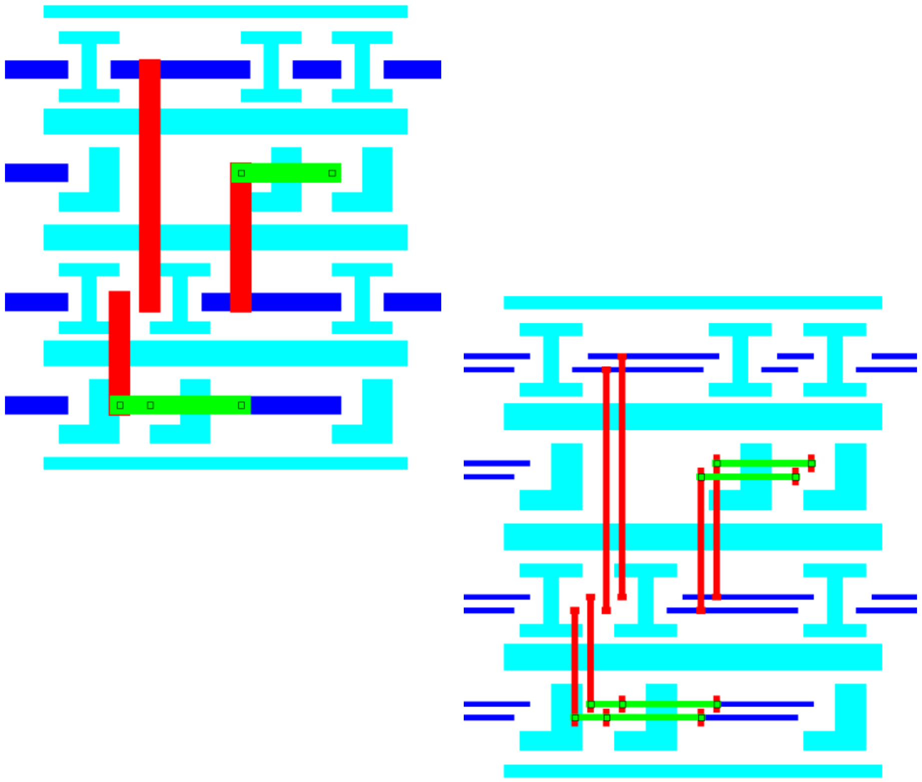
Classic XOR



Precharge Signal

Reduced Complementary Dynamic and Differential Logic (RCDDL) XOR

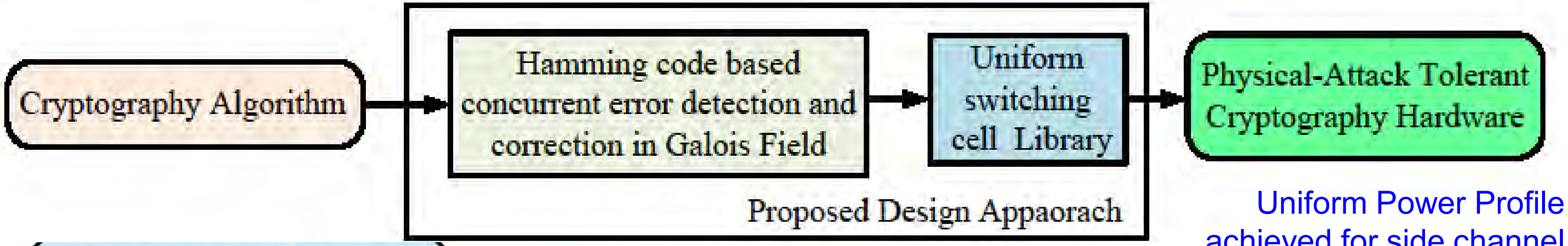
Source: Rammohan VLSID 2008



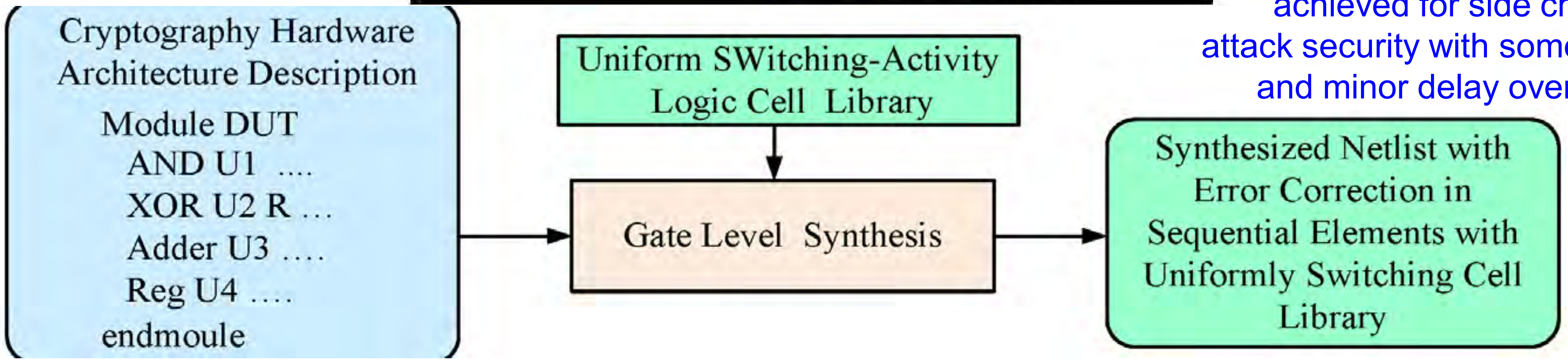
Differential Routing

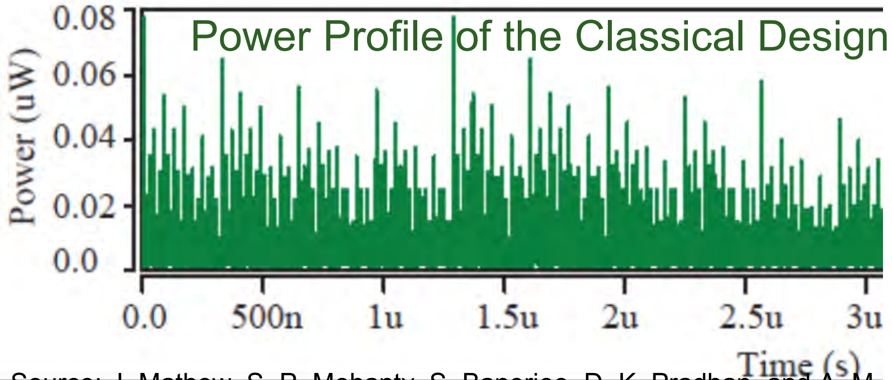
Source: Schaumont IWLS 2005

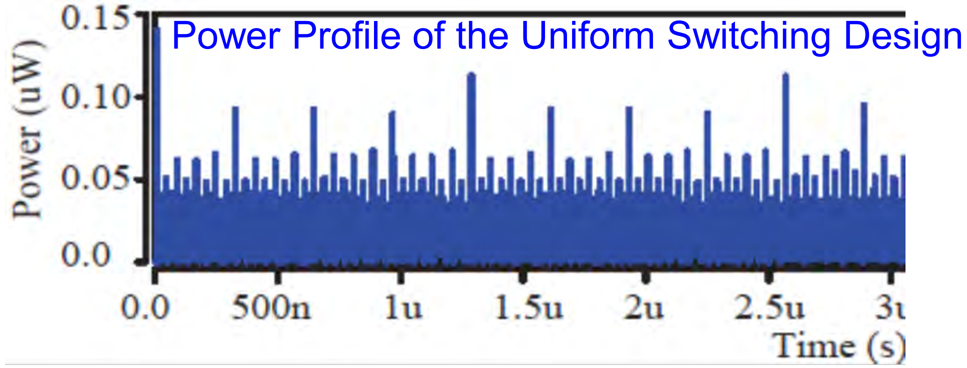
Our SdD: Approach for DPA Resilience Hardware



Uniform Power Profile achieved for side channel attack security with some area and minor delay overhead.







Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", *Elsevier Computers and Electrical Engineering*, Vol. 39, No. 4, May 2013, pp. 1077--1087.

PUF – Trojan Issue

- Improper implementation of PUF could introduce "backdoors" to an otherwise secure system.
- PUF introduces more entry points for hacking into a cryptographic system.

Provide backdoor to adversary.
Chip fails during critical needs.

Source: Rührmair, Ulrich; van Dijk, Marten (2013). *PUFs in Security Protocols: Attack Models and Security Evaluations* (PDF), in *Proc. IEEE Symposium on Security and Privacy*, May 19–22, 2013

PUF – Machine Learning Attack

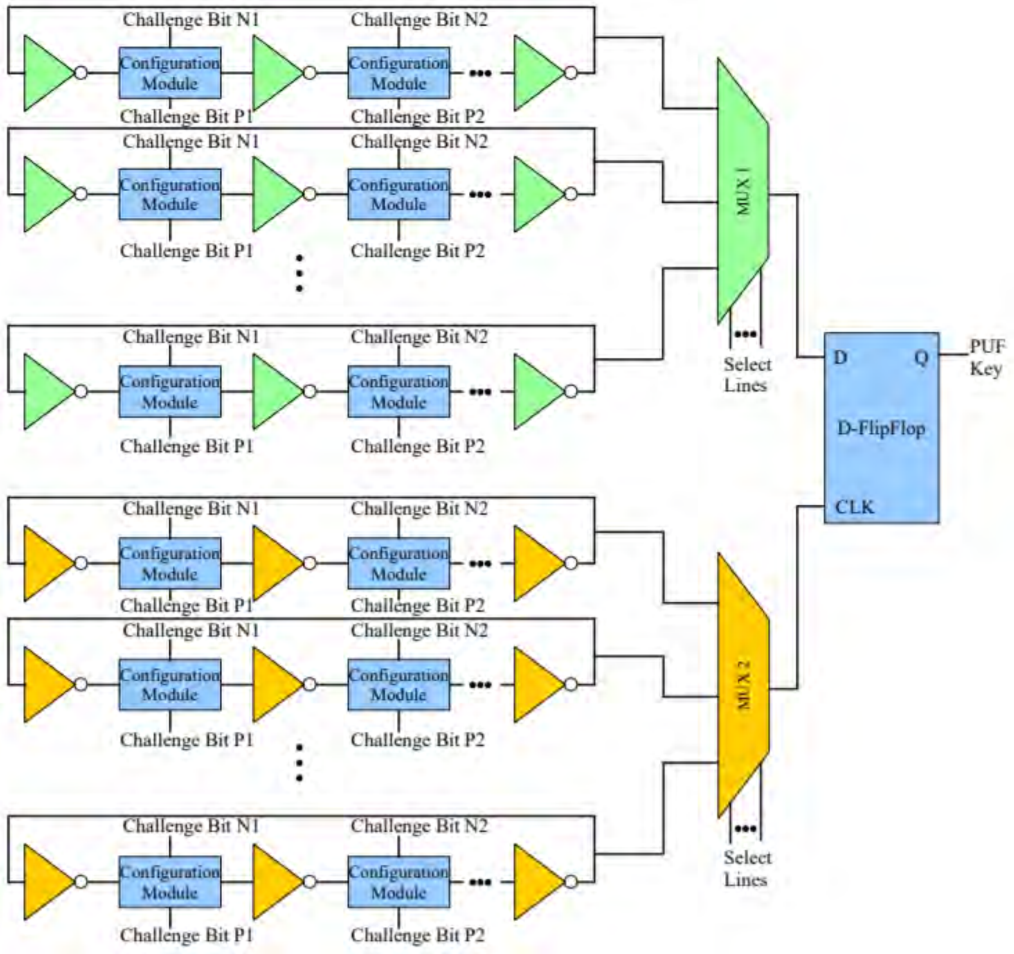
- One types of non-invasive attacks is machine learning (ML) attacks.
- ML attacks are possible for PUFs as the pre- and post-processing methods ignore the effect of correlations between PUF outputs.
- Many ML algorithms are available against known families of PUFs.

Source: Ganji, Fatemeh (2018), "On the learnability of physically unclonable functions", Springer. ISBN 978-3-319-76716-1.

Why Reconfigurability?

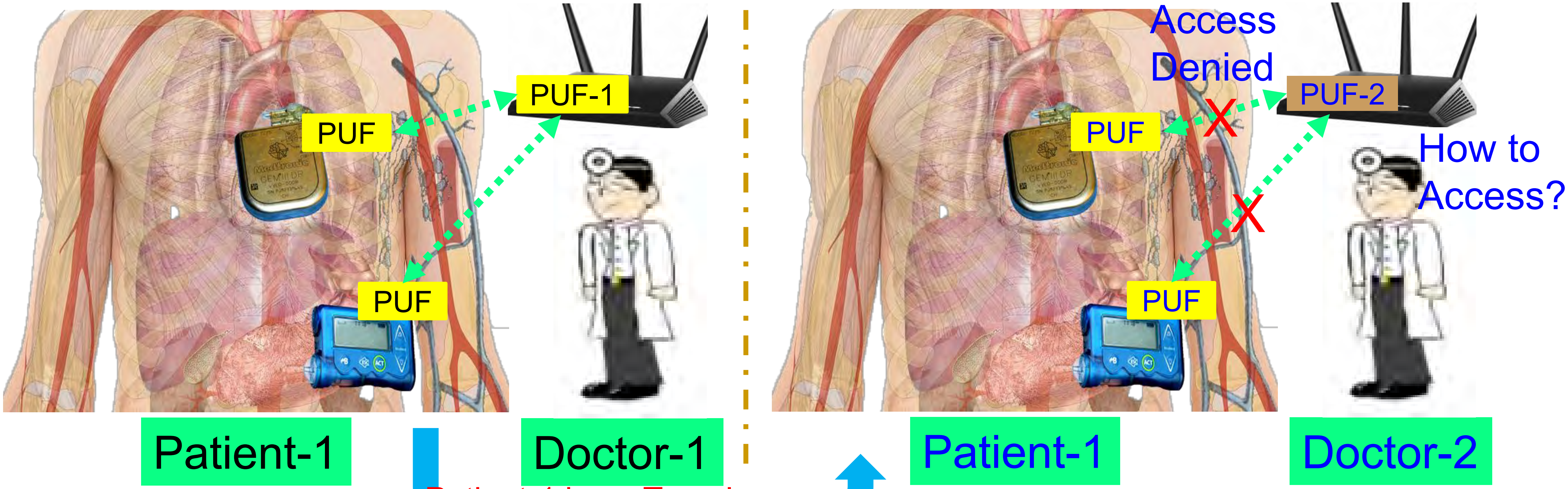
- Increased robustness.
- More Challenge Response Pairs.
- Lower chip area.

Reconfigurable Power Optimized Hybrid Oscillator Arbiter PUF



How to implement?

PUF based Cybersecurity in Smart Healthcare - Doctor's Dilemma

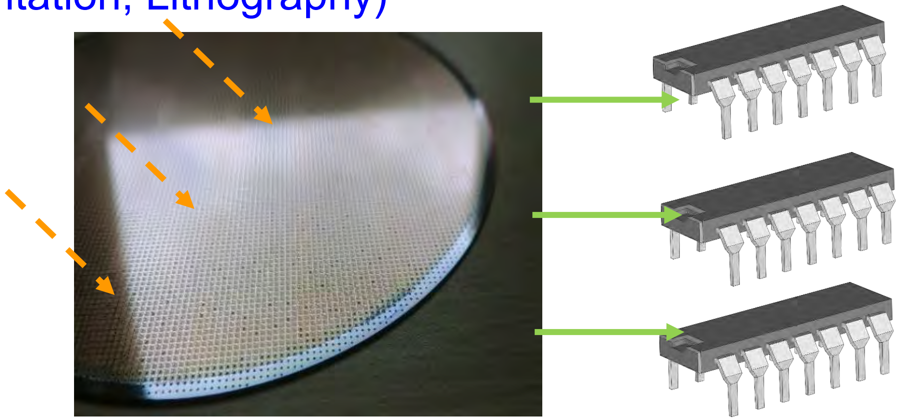


Patient-1 is on Travel
He/She has a Medical Emergency
He/She visits Doctor-2

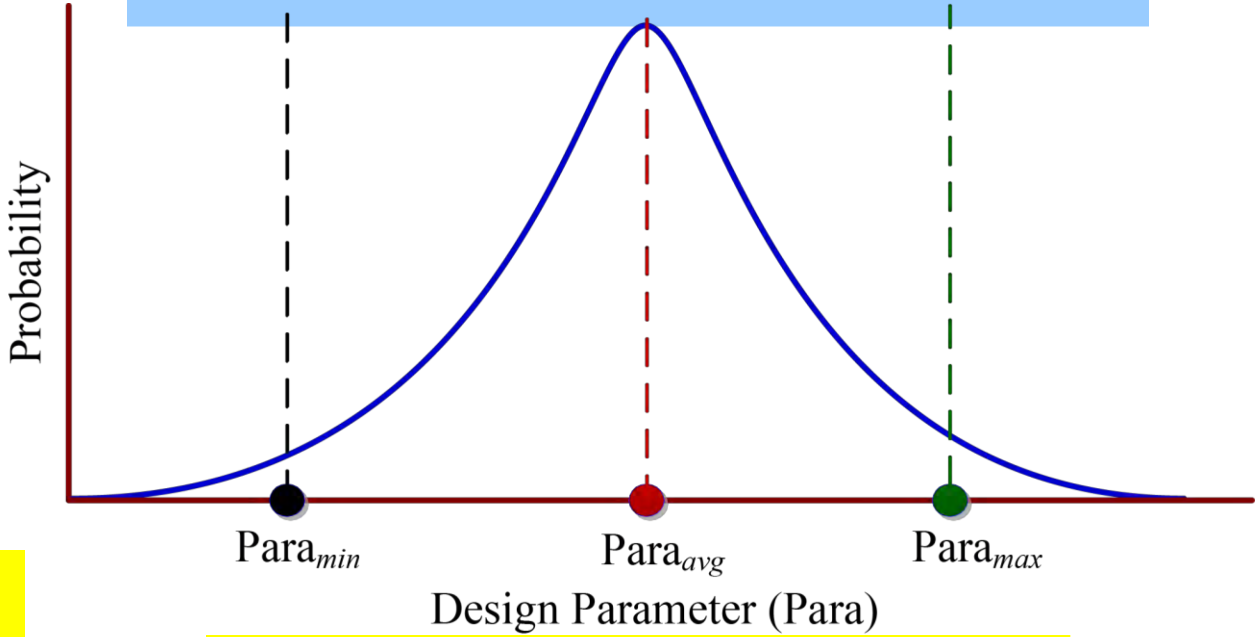
IC for PUF – Variability versus Variability-Aware Design

Variability → Randomness for PUF

Manufacturing Variations (e.g. Oxide Growth, Ion Implantation, Lithography)



Variability-Aware Design → Robust Hardware

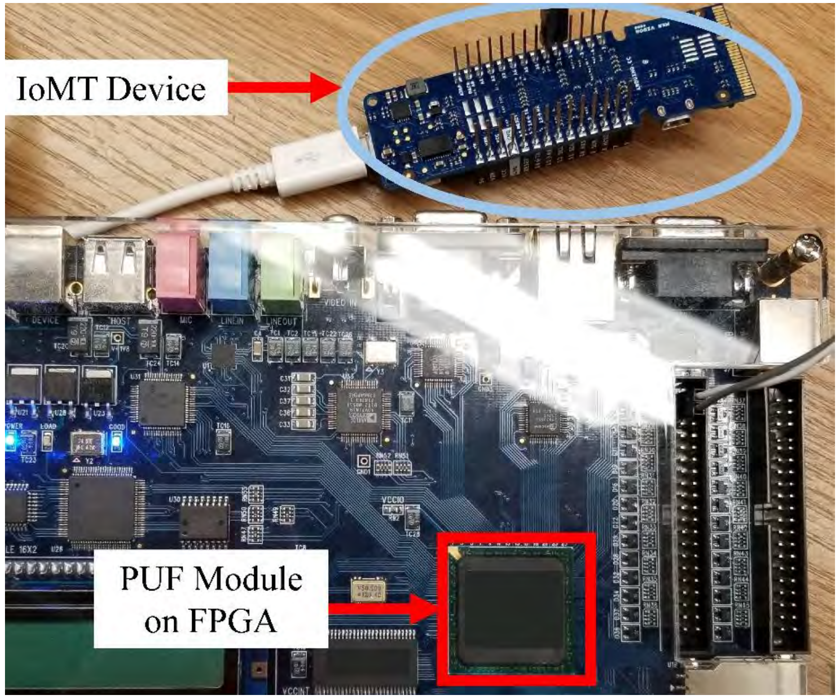


Variability Features → Randomness → PUF

Is it not case of Conflicting Objectives?
How to have a Robust-IC design that functions as a PUF?

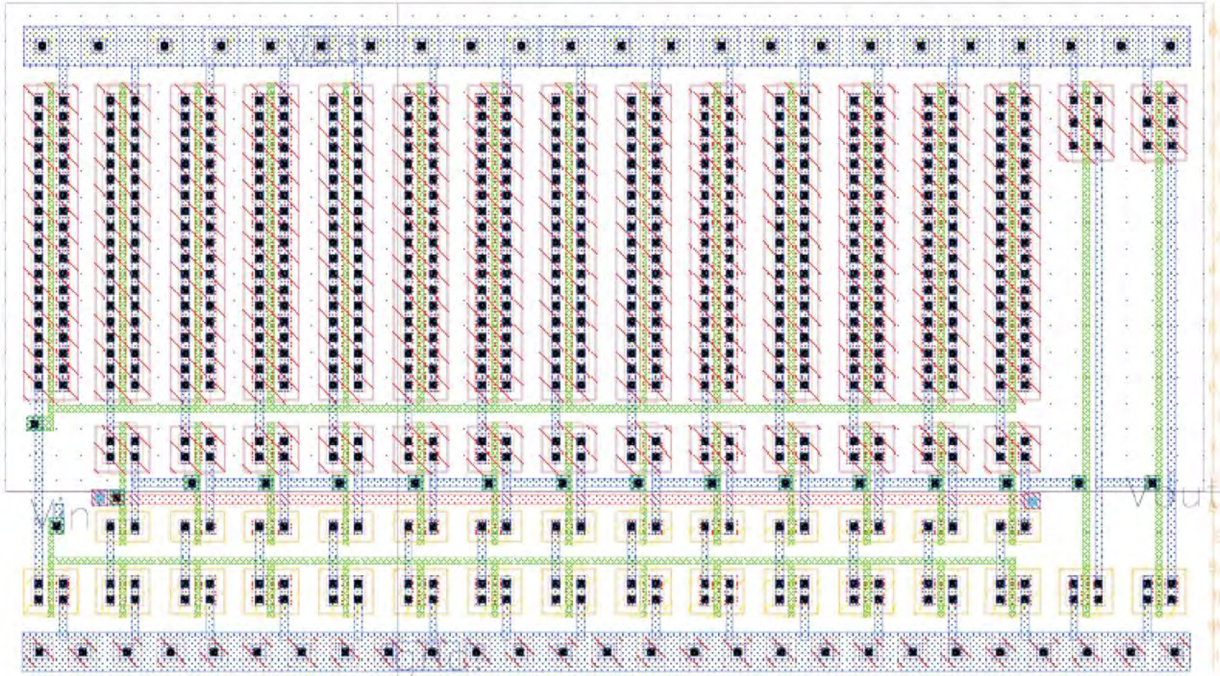
Optimize $(\mu+n\sigma)$ to reduce variability for Robust Design

PUF – FPGA versus IC



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

- Faster prototyping
- Lesser design effort
- Minimal skills
- Cheap
- Rely on already existing post fabrication variability



Source: **S. P. Mohanty** and E. Kougianos, "Incorporating Manufacturing Process Variation Awareness in Fast Design Optimization of Nanoscale CMOS VCOs", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 27, Issue 1, February 2014, pp. 22--31.

- Takes time to get it from fab
- More design effort
- Needs analog design skills
- Can be expensive
- Choice to send to fab as per the need

Conclusions

Conclusions

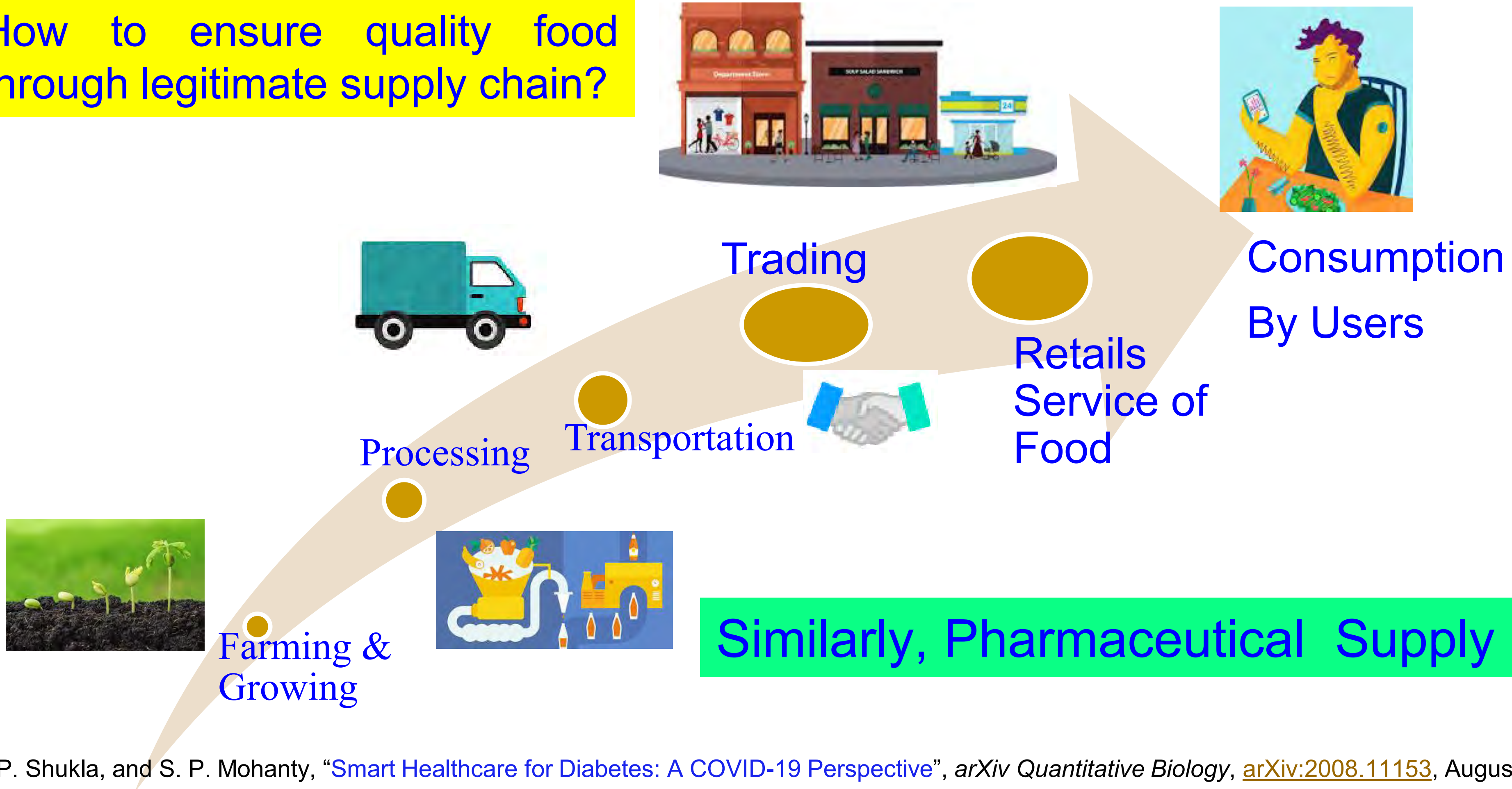
- Cybersecurity and Privacy are important problems in IoT-driven Cyber-Physical Systems (CPS).
- Various elements and components of IoT/CPS including Data, Devices, System Components, AI need security.
- Both software and hardware-based attacks and solutions are possible for cybersecurity in IoT/CPS.
- Cybersecurity in IoT-based H-CPS, A-CPS, E-CPS, and T-CPS, etc. can have serious consequences.
- Existing cybersecurity solutions have serious overheads and may not even run in the end-devices (e.g. a medical device) of CPS/IoT.
- Security-by-Design (SbD) advocate features at early design phases, no-retrofitting.
- Hardware-Assisted Security (HAS): Security provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system.
- Research on topologies and protocols for PUF based cybersecurity is ongoing.

Future Directions

- Privacy and/or Security by Design (PbD or SbD) needs research.
- Cybersecurity, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS) need more research.
- Cybersecurity of IoT-based systems (e.g. Smart Healthcare device/data, Smart Agriculture, Smart Grid, UAV, Smart Cars) needs research.
- Sustainable Smart City and Smart Villages: need sustainable IoT/CPS.
- More research is needed for low-overhead PUF design and protocols that can be integrated in any IoT-enabled systems.

Reliable Supply Chain: Food Supply Chain: Farm → Dinning

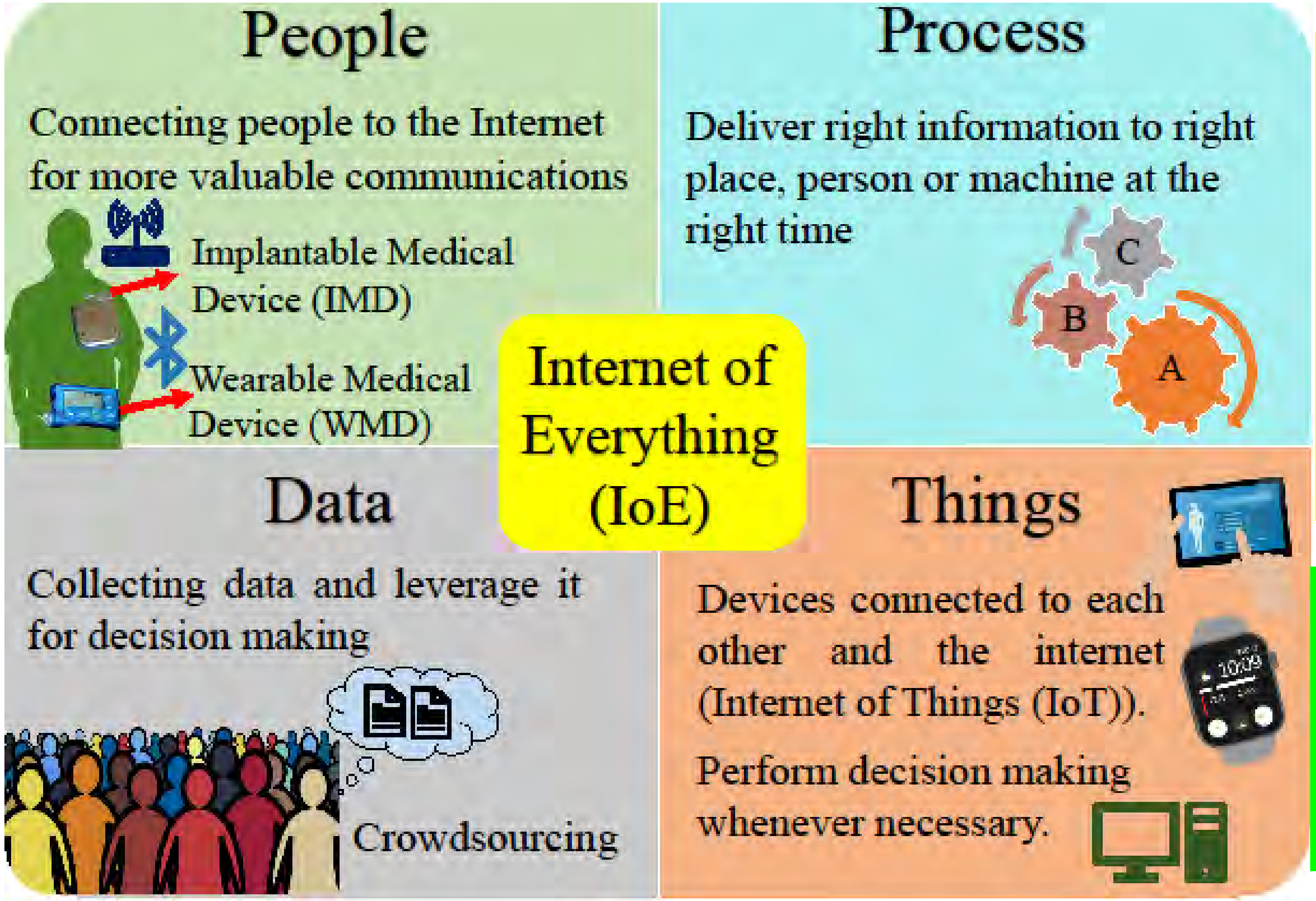
How to ensure quality food through legitimate supply chain?



Similarly, Pharmaceutical Supply Chain

Source: A. M. Joshi, U. P. Shukla, and S. P. Mohanty, "Smart Healthcare for Diabetes: A COVID-19 Perspective", *arXiv Quantitative Biology*, arXiv:2008.11153, August 2020, 18-pages.

Security of Internet of Every Things (IoE)



Requires:
- Data, Device, and System Security
- Data, Location, and System Privacy

Need of the Hour:
- Security/Secure by Design (SbD)
- Privacy by Design (PbD)

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)", *arXiv Computer Science*, arXiv:1909.06496, September 2019, 37-pages.

Acknowledgement(s)

This material is based upon work supported by the National Science Foundation under Grant Nos. OAC-1924112 and HBCU-EiR-2101181. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.