iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics

Presenter: Venkata K. V. V. Bathalapalli

Venkata K. V. V. Bathalapalli[1], S. P. Mohanty[2], E. Kougianos[3]
Vasanth Iyer[4], and Bibhudutta Rout[5]

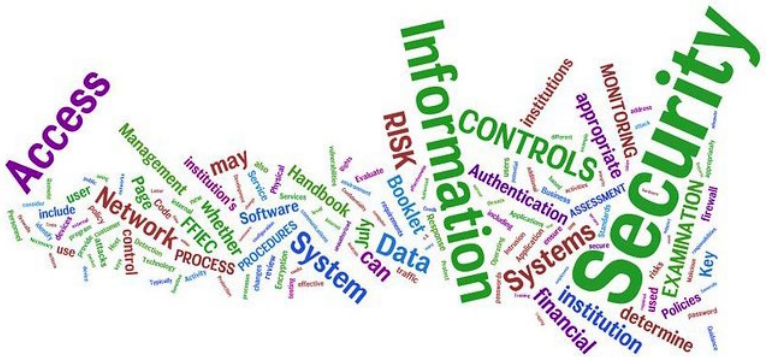
University of North Texas, Denton, TX, USA.[1,2,3,5] and Grambling State University[4].

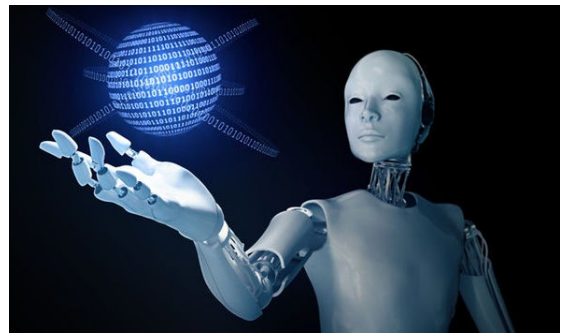
Email: **vb0194@unt.edu, saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3], iyerv@gram.edu[4], bibhudutta.rout@unt.edu[5]**

Outline

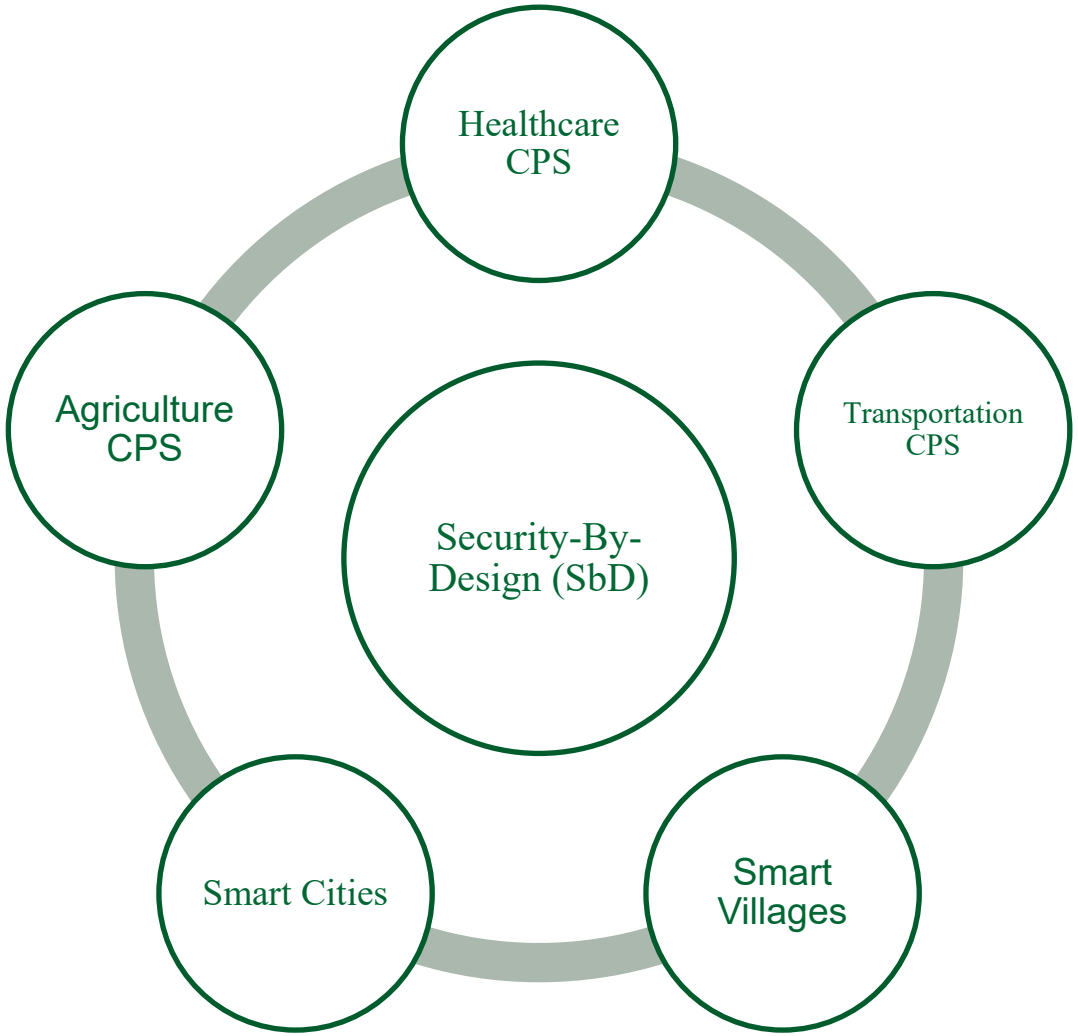
- Security-by-Design (SbD) Principles
- Novelty of Proposed PUF-based-TPM Security-by-Design primitive
- Related Research
- Working Flow of Proposed iTPM
- Experimental implementation Overview
- Conclusion & Future Research Directions

Security-by-Design (SbD) – The Principle





Applications of Security-by-Design (SbD)



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

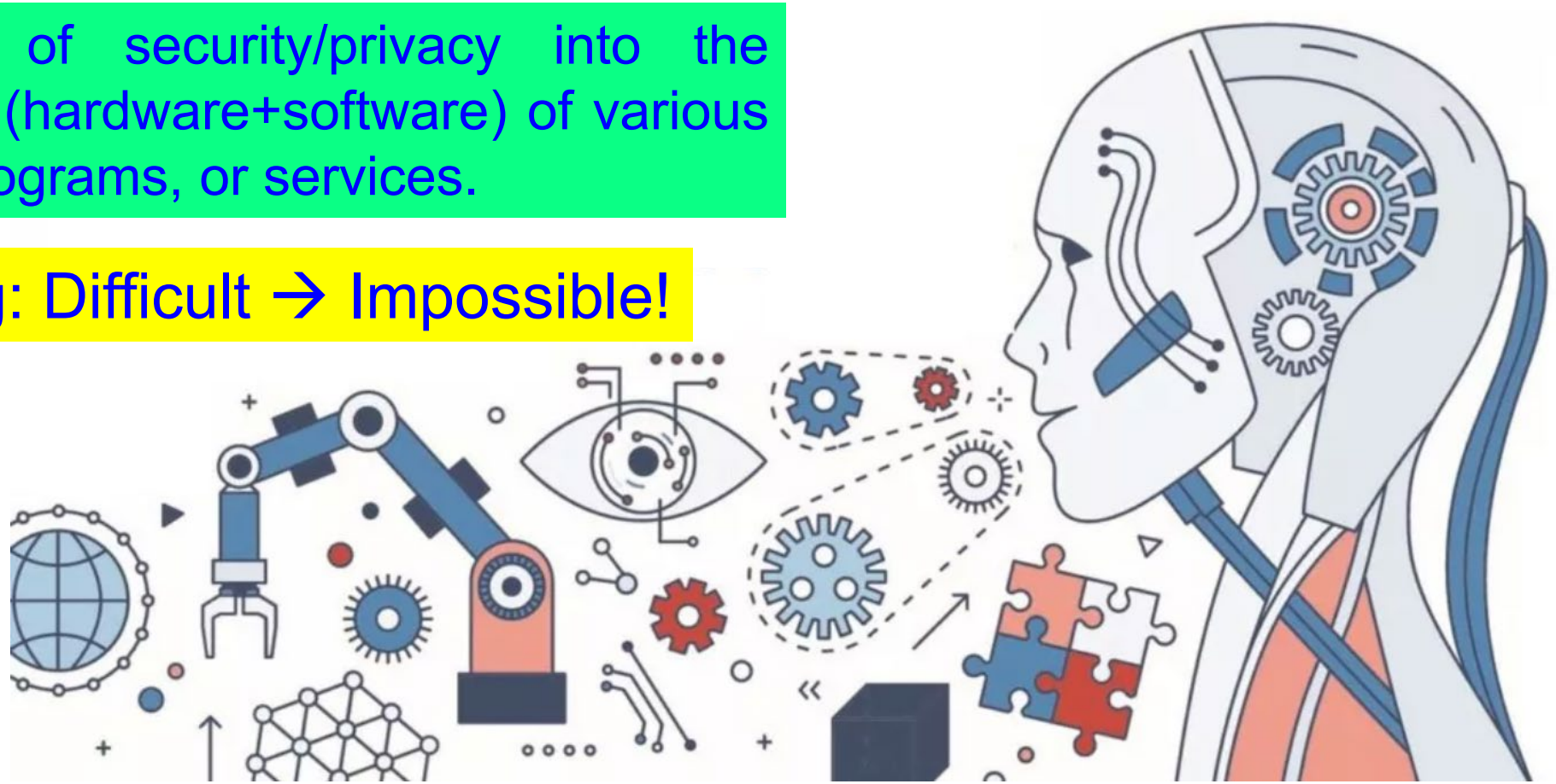
- Security by Design (SbD) is a system design paradigm that ensures security and privacy are considered right from the beginning of the design phase so that retrofitting at the later stage is not needed.
- Privacy by Design (PbD) Treat privacy concerns as design requirements when developing technology, rather than trying to retrofit privacy controls after it is built.

Source: S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," in *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4-5, 1 March 2020, doi: 10.1109/MCE.2019.2954959.

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/

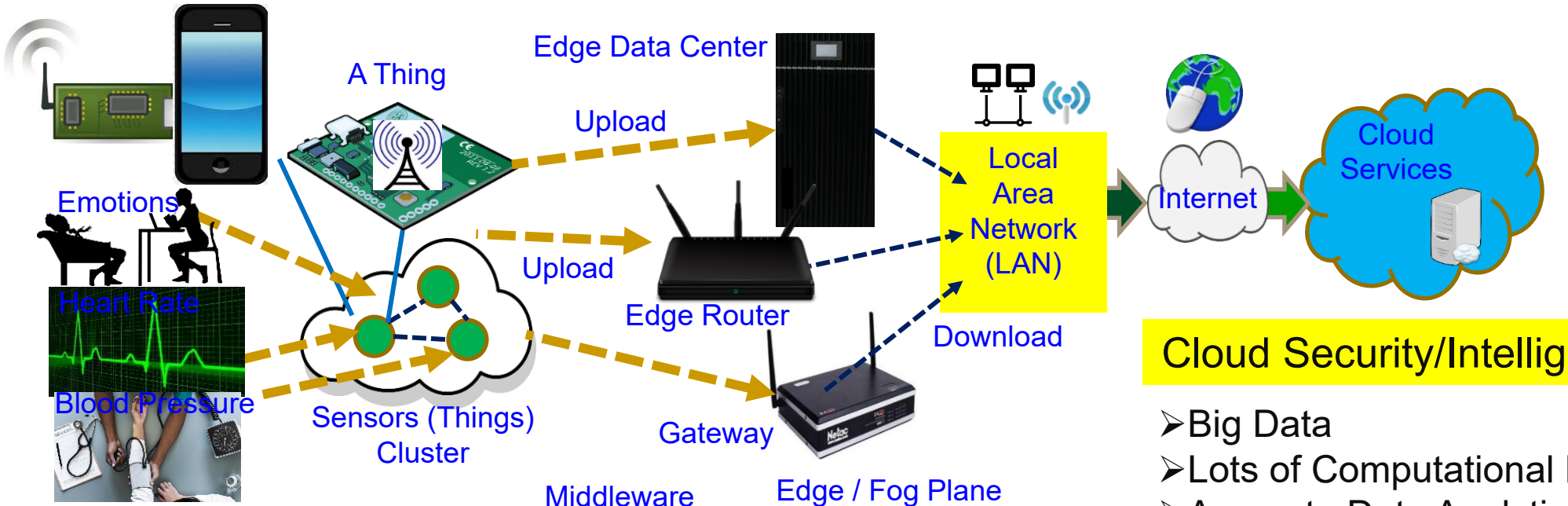
Source: S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4-5, 1 March 2020, doi: 10.1109/MCE.2019.2954959.

Security by Design (SbD)-Principles

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

CPS – IoT-Edge Vs IoT-Cloud



End Security/Intelligence

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

Edge Security/Intelligence

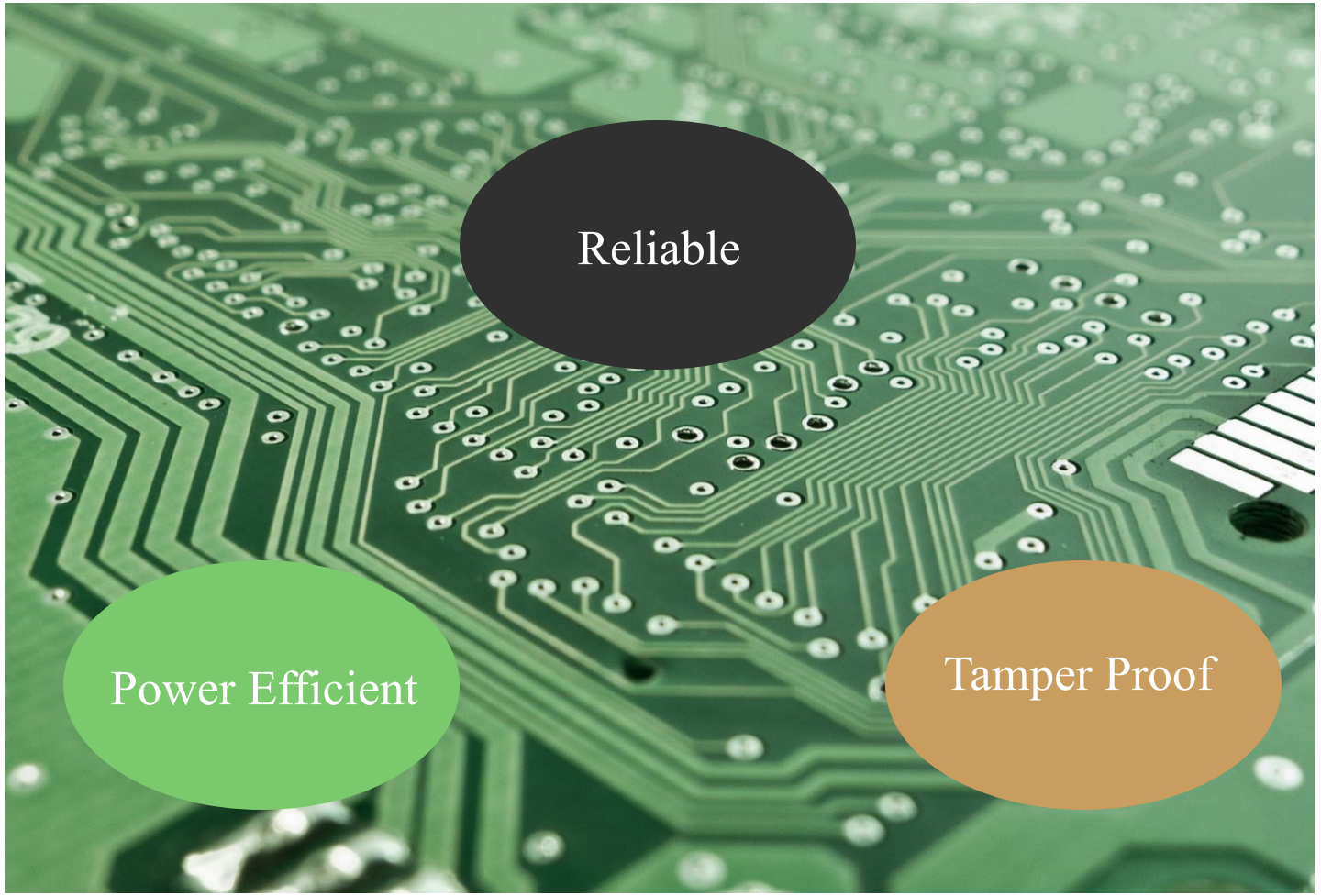
- Less Data
- Less Computational Resource
- Less Accurate Data Analytics
- Rapid Response

Cloud Security/Intelligence

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

Physical Unclonable Function (PUF)

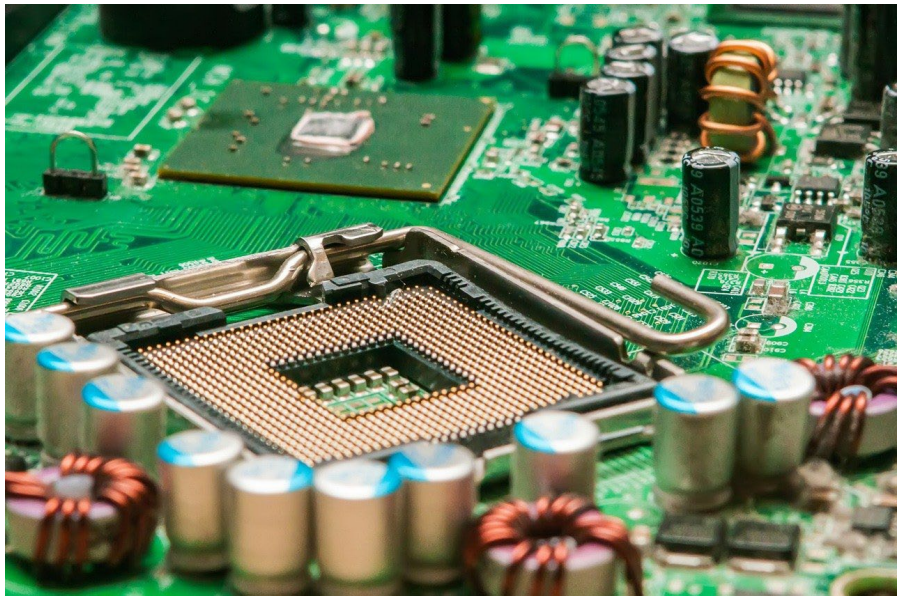
PUF: A Hardware-Assisted Security Primitive



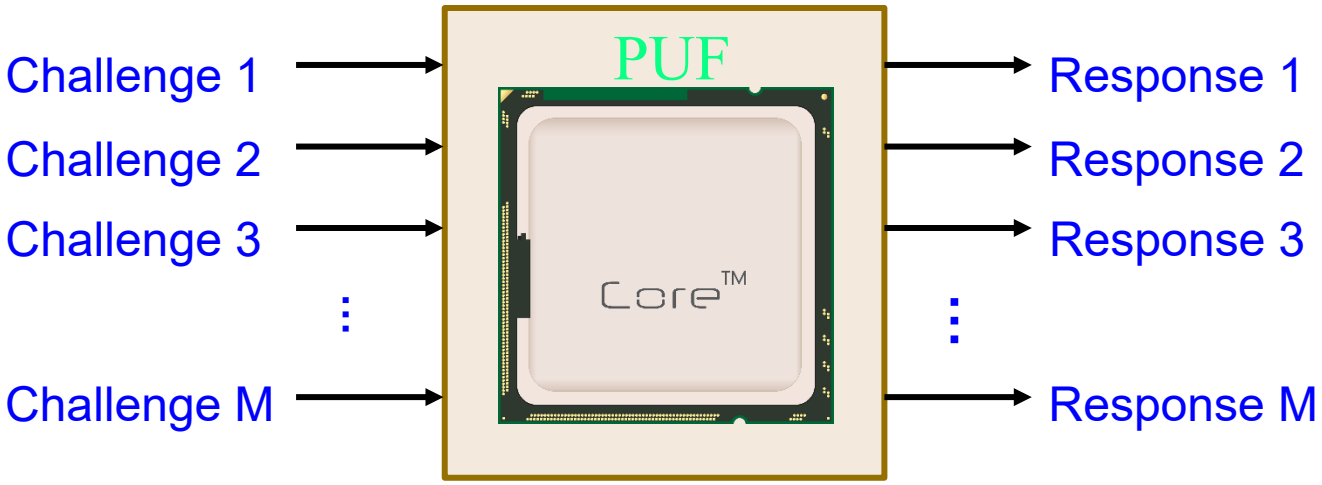
- A secure fingerprint generation scheme based on process variations in an Integrated Circuit
- PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.
- A simple design that generates cryptographically secure keys for the device authentication

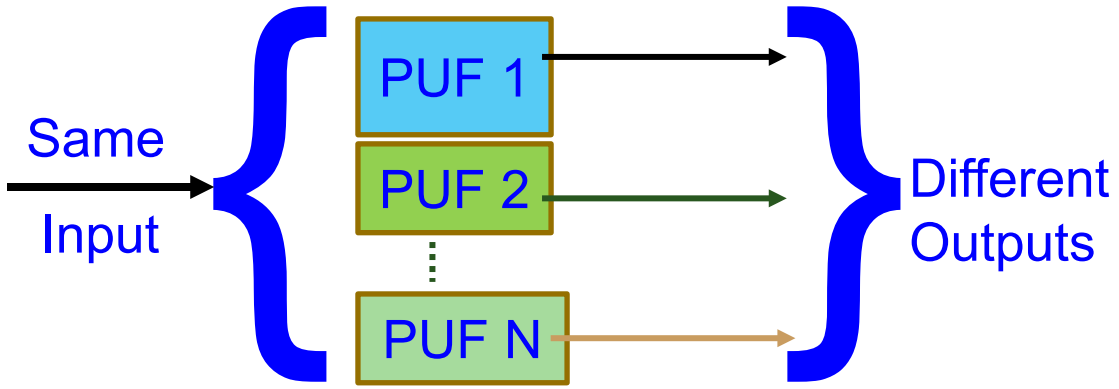
PUF: A Hardware-Assisted Security Primitive

- ✓ PUF has a Challenge as an Input and Response as an Output
- ✓ Response output from the PUF design will be unique for the challenge input on that PUF design
- ✓ Arbiter and Ring Oscillator PUFs are the most widely used PUF designs for IoT applications
- ✓ Delay-based PUF designs support the higher number of Challenge-Response pairs (CRP)



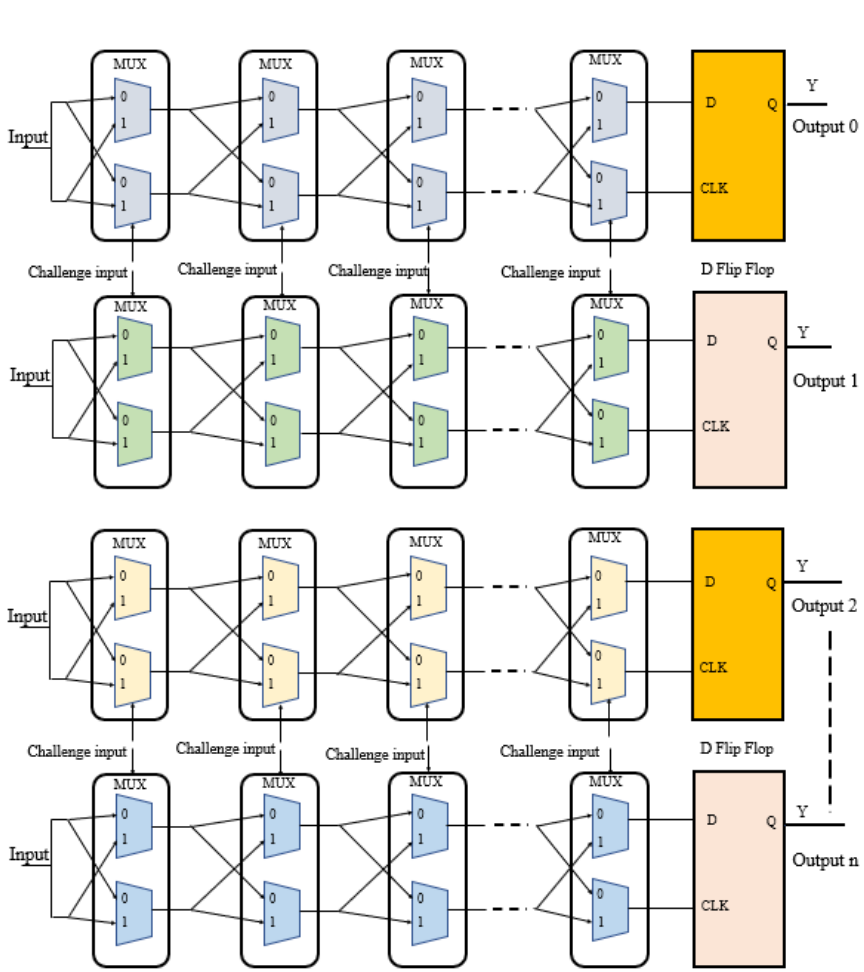
PUF Key Generation and Working

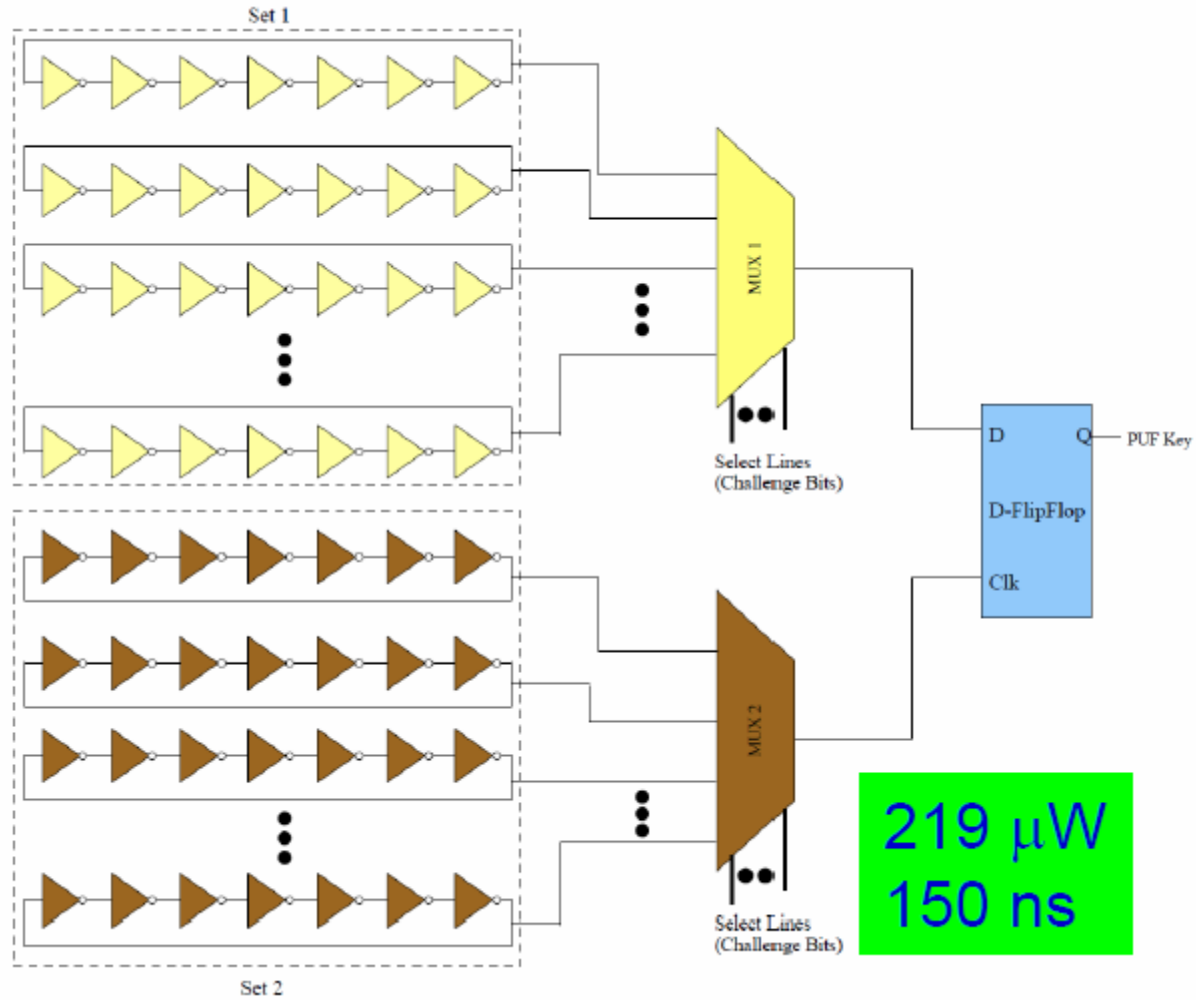




Source: International Symposium on Smart Electronics Systems (iSES) 2019 Demo (PUFchain: Hardware-Integrated Scalable Blockchain)

PUF Designs



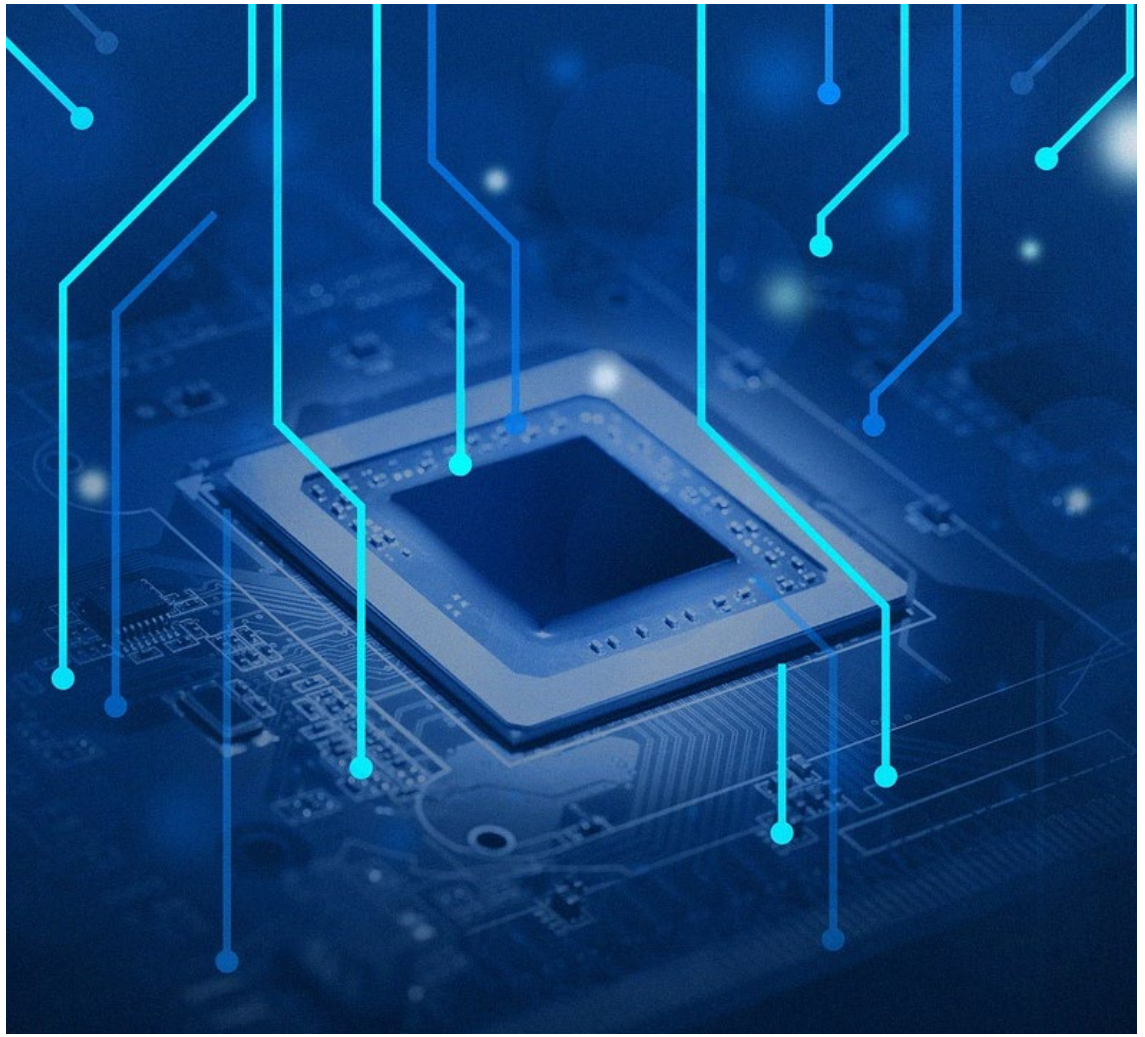


Source: iSES 2019 Demo (PMsec: PUF-Based Energy-Efficient Authentication of Devices in the Internet of Medical Things (IoMT))

Trusted Platform Module (TPM)

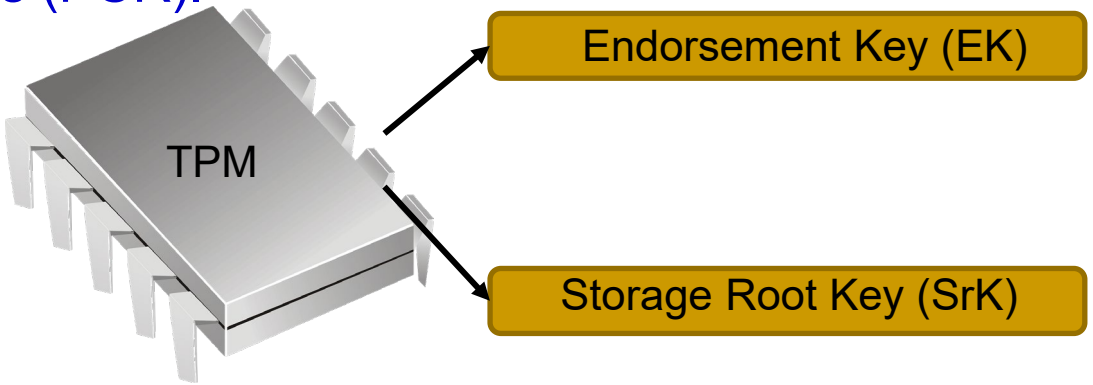
Trusted Platform Module-Overview

- A Trusted Platform Module (TPM) is a hardware security primitive introduced by the Trust Computing Group (TCG), which provides the root of trust for the computing platform as a simple System-On-Chip (Soc).
- A TPM is a secure cryptoprocessor being used in all advanced computing systems
- TPM Non-Volatile Memory (NVRAM) can seal and unseal the secret keys generated inside or outside TPM.



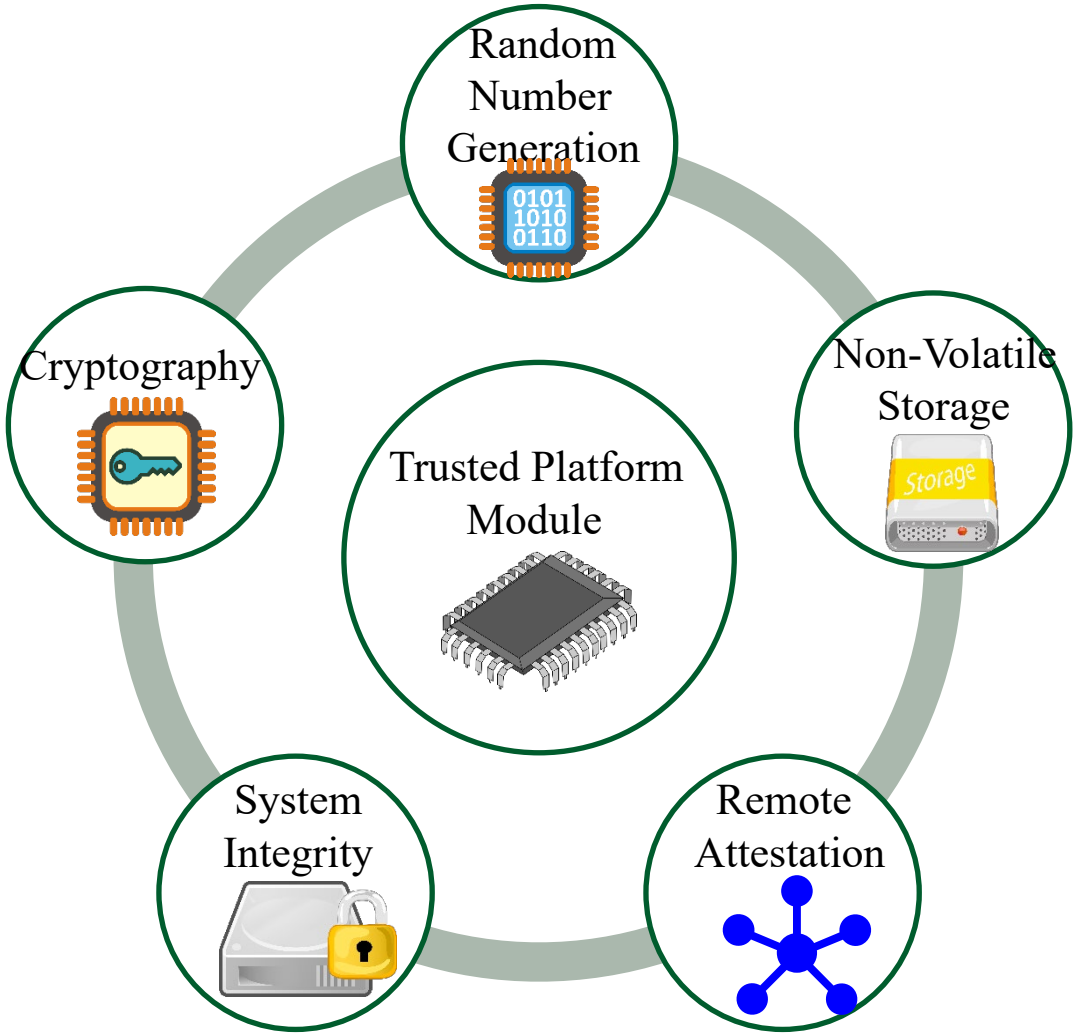
Functionality of TPM

- A TPM is composed of a cryptographic sub-system and two memories, one non-volatile and one volatile. The Endorsement Key (EK) is an RSA key with a 2048-bit length, stored at the non-volatile memory and created by the TPM manufacturer to be able to identify this unique chip.
- A specified NV-index is defined for secure storage and retrieval of private keys. Access to TPM NVRAM can be user-defined and password-protected, following TCG's procedures.
- The system configuration parameters during the boot process are stored in the TPM's Platform Configuration registers (PCR).

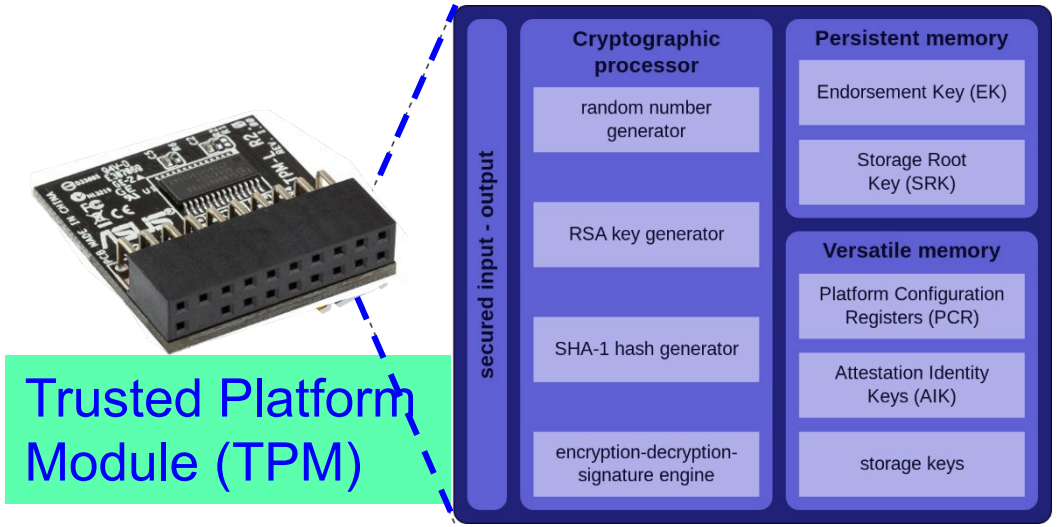


Source: M. Calvo and M. Beltrán, "Remote Attestation as a Service for Edge-Enabled IoT," *2021 IEEE International Conference on Services Computing (SCC)*, Chicago, IL, USA, 2021, pp. 329-339, doi: 10.1109/SCC53864.2021.00046.

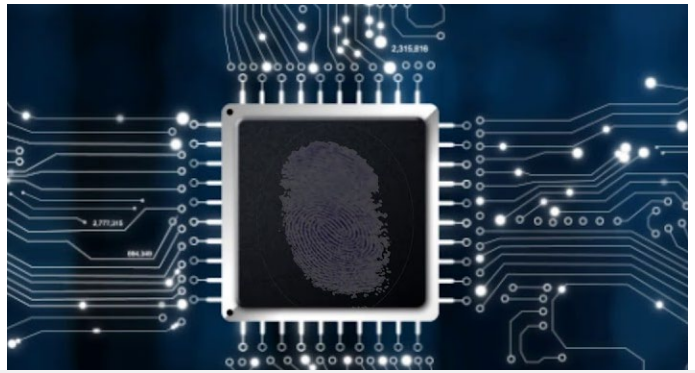
Applications of TPM



PUF versus TPM



Trusted Platform Module (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

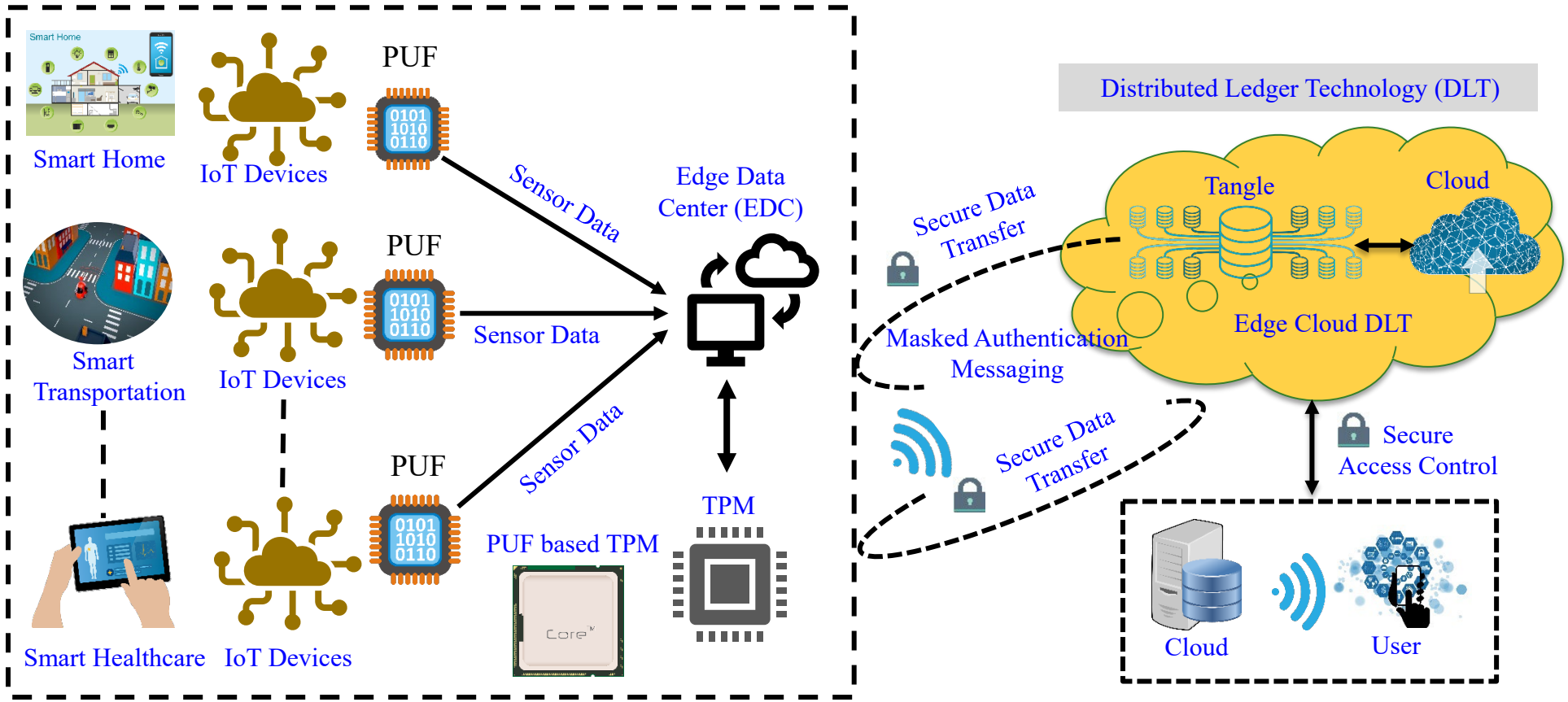
PUF:

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

Our First Novel Integration PUF with TPM in DLT
Security-by-Design of IoT

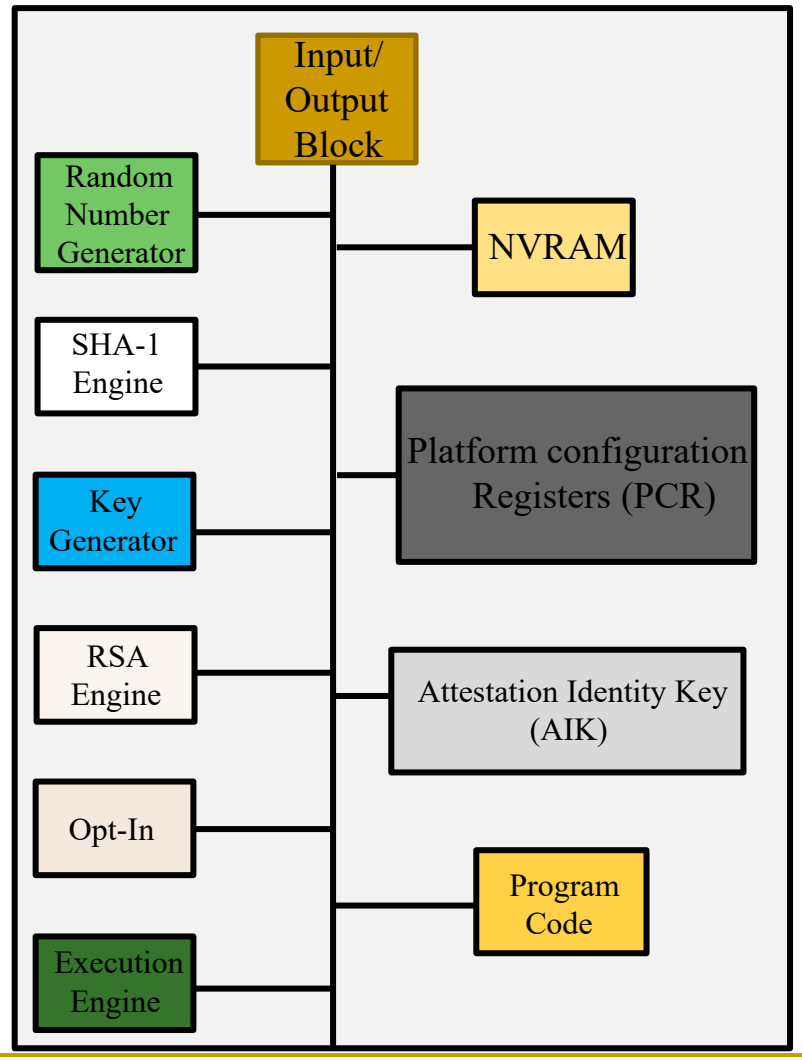
PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT

Architectural Overview of PUFchain 4.0

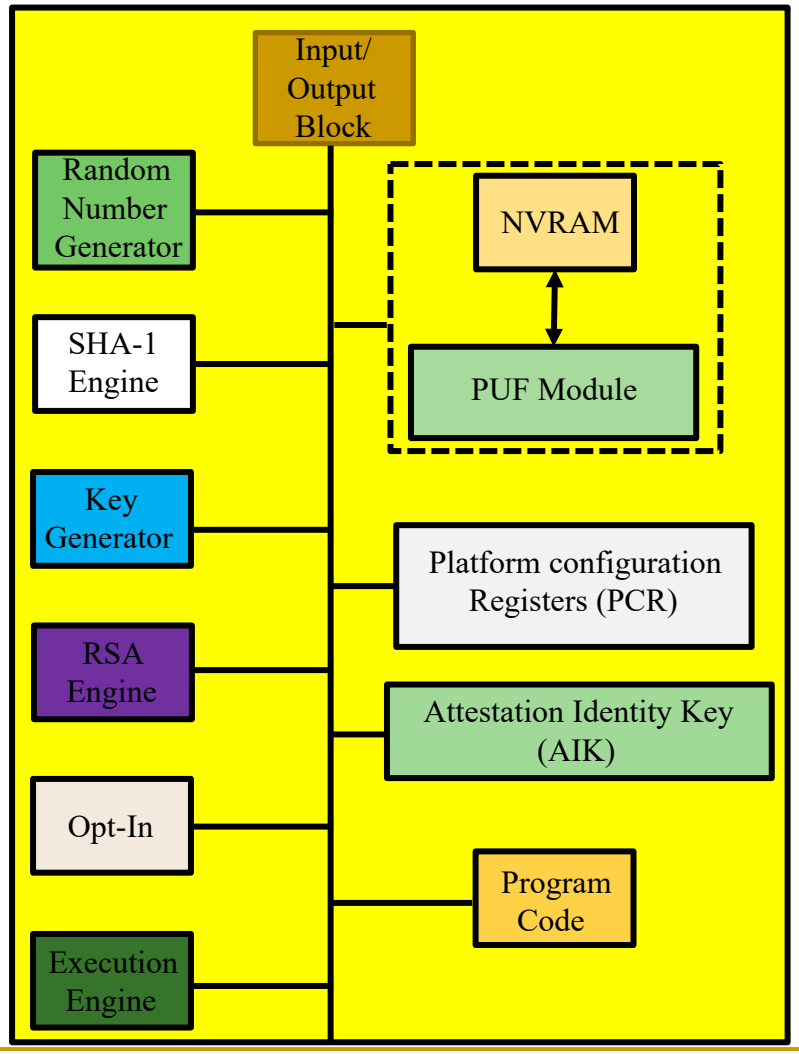


Architecture of Proposed PUF-based TPM

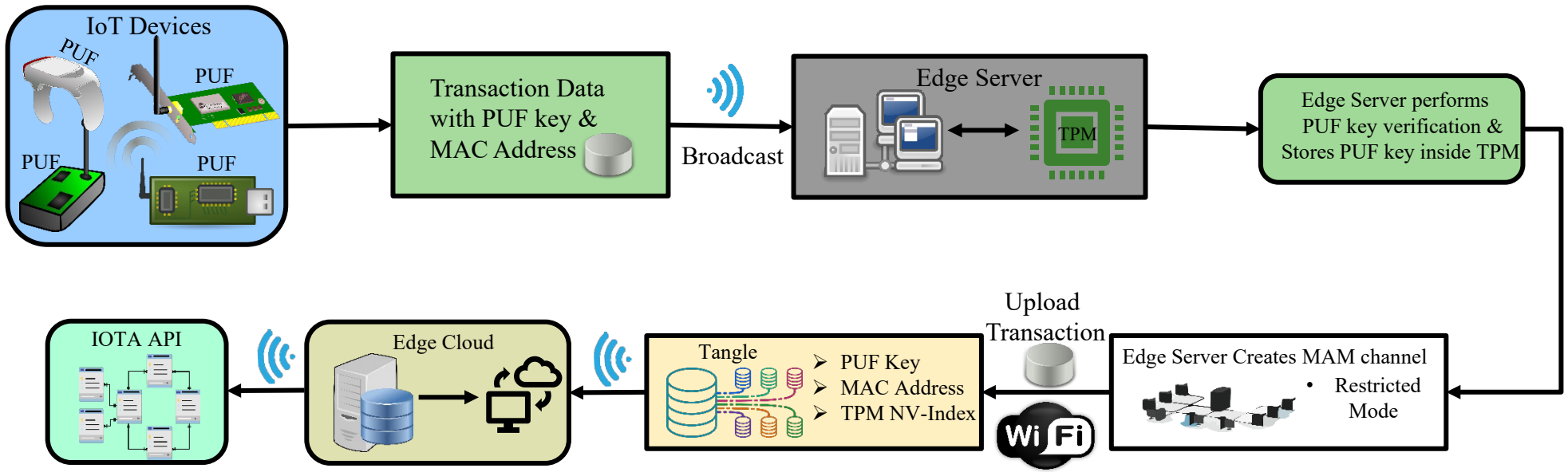
Conventional TPM Architecture



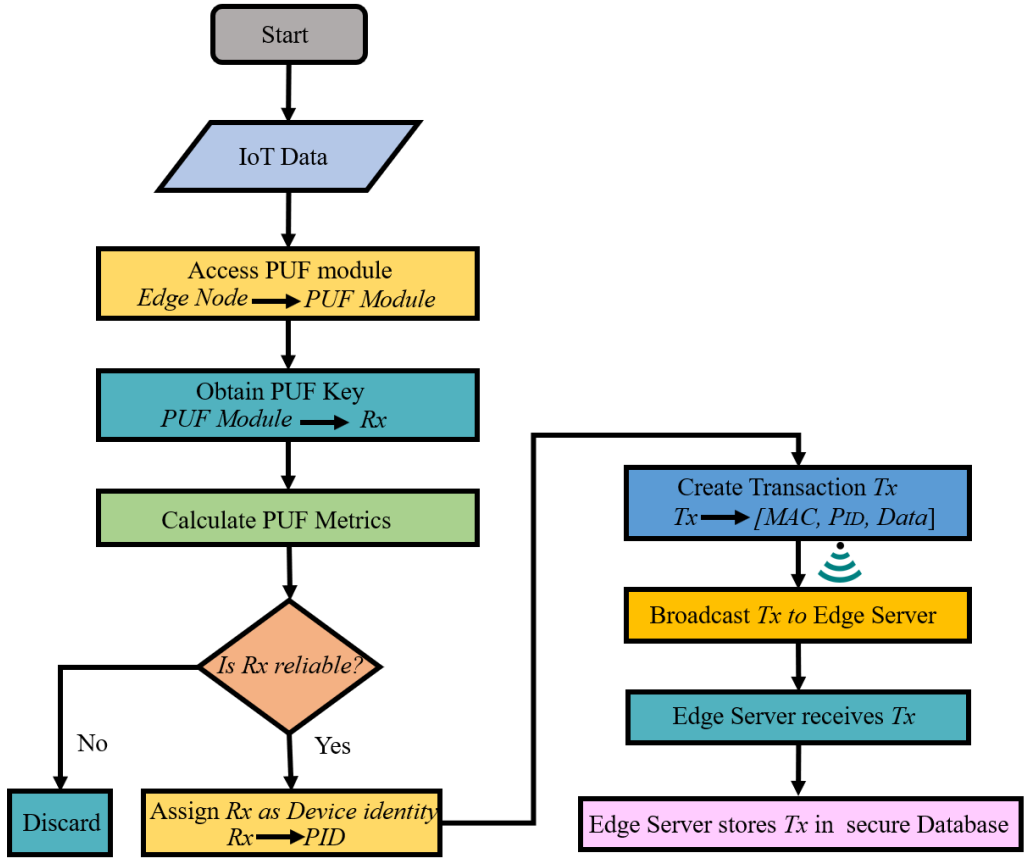
PUF-based TPM Architecture

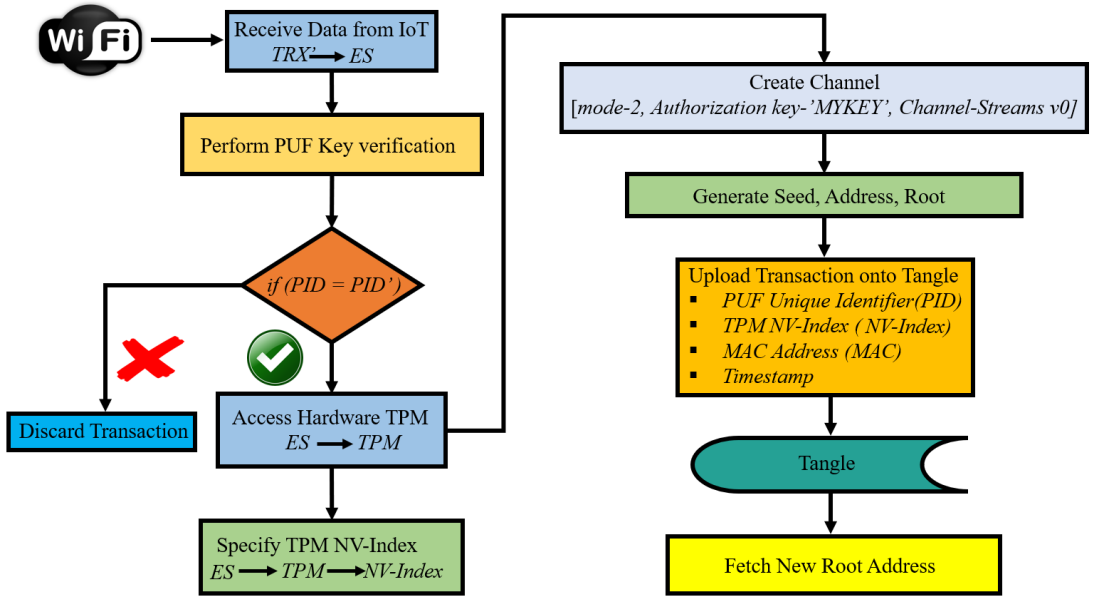


Working Overview of PUFchain 4.0



PUFchain 4.0:Enrollment and Authentication





Implementation and Validation

Sealing and unsealing PUF Key inside TPM by accessing NVRAM

```
pi@raspberrypi:~ $ echo "10100111101001111010011110100111101001111010011110100111101001111010011" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500020 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500020 -C o
10100111101001111010011110100111101001111010011110100111101001111010011
pi@raspberrypi:~ $ echo "11010010110100101101001011010010110100101101001011010010110100101101001" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500021 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500021 -C o          ---> 1st Edge Node PUF Key in TPM
11010010110100101101001011010010110100101101001011010010110100101101001

pi@raspberrypi:~ $ echo "10100111101001111010011110100111101001111010011110100111101001111010011" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500020 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500020 -C o
10100111101001111010011110100111101001111010011110100111101001111010011
pi@raspberrypi:~ $ echo "11010010110100101101001011010010110100101101001011010010110100101101001" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500021 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500021 -C o          ---> 2nd Edge Node PUF Key in TPM
11010010110100101101001011010010110100101101001011010010110100101101001

pi@raspberrypi:~ $ tpm2_nvread 0x1500020 -C o
10100111101001111010011110100111101001111010011110100111101001111010011
pi@raspberrypi:~ $
```

Authentication and Transaction verification outputs on IOTA Explorer

Streams v0 Channel

General

Root: JBLTQEGMBNEBWQPUNPYTTYJOWZJILVAVJGEYOAJ9BZFBOTXJMFXNYVFLSOSFCRGNESKGFKPGSRNFXWARP

Mode: Public | Private | Restricted

Side Key: MYKEY

Find Data | Stop

Root
JBLTQEGMBNEBWQPUNPYTTYJOWZJILVAVJGEYOAJ9BZFBOTXJMFXNYVFLSOSFCRGNESKGFKPGSRNFXWARP

Tag
MY9MAM

Message ascii

```
Node output: ['1676446728.9390807' '0x1500020' 'dc:a6:32:c0:77:88' '10100111101001111010011110100111101001111010011110100111101001111010011
1']
PUF Key
10100111101001111010011110100111101001111010011110100111101001111010011
Authentication is successful
TPM NV-Index for Node 1
0x1500020
```

→ 1st Edge Node Transaction o

Root
IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY

Tag
MY9MAM

Message ascii

```
Node output: ['1676447285.0460067' '0x1500021' 'dc:a6:32:c8:d7:50' '11010010110100101101001011010010110100101101001011010010110100101101001
1']
PUF Key
11010010110100101101001011010010110100101101001011010010110100101101001
Authentication is successful
TPM NV-Index for Node 2
0x1500021
```

→ 2nd Edge Node Transaction o

Performance Analysis of PUFchain 4.0

- Characterization

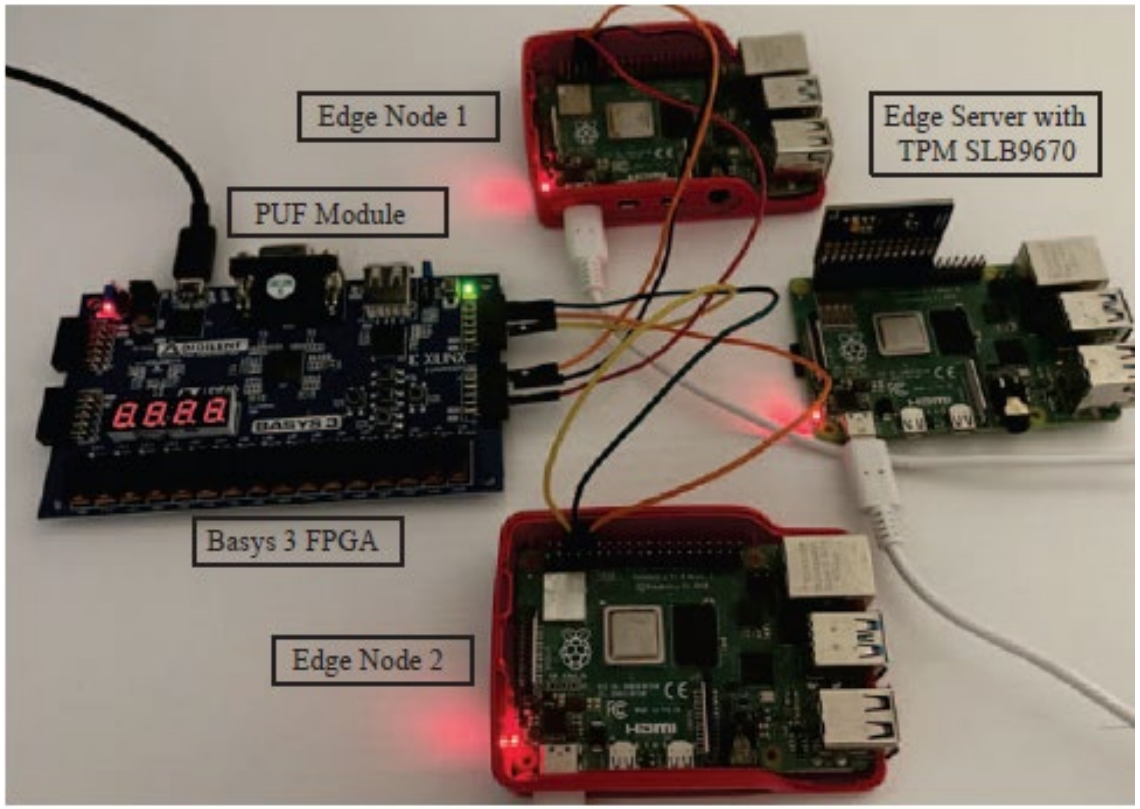
Parameters	Results
Application	IoT
Hardware Security Module	TPM, PUF
Hardware Security Mechanism	PUF-based Hardware TPM
TPM Board Specification	Infineon Optiga™ SLB 9670 TPM 2.0
TPM Storage	NVRAM
Free NV memory	6962 Bytes
Data Security System	Tangle
Communication Protocol	Masked Authentication Messaging
TPM module	Geek Pi TPM 2.0
PUF Module	Arbiter PUF
PUF Key	64 Bit

- Performance Analysis

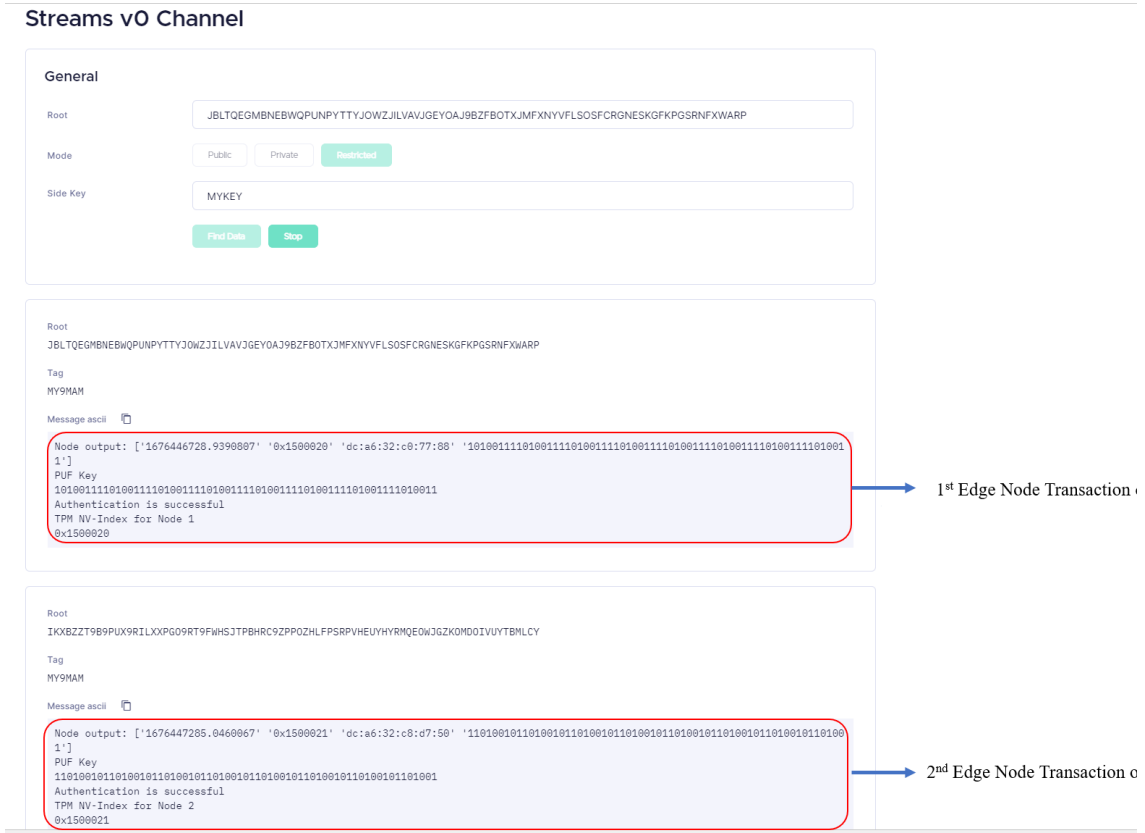
Parameters	Results
NV Storage capacity (Read/Write)	768 Bytes
Time to generate PUF key	87 ms
Power Consumption of pi with TPM	2.7-3.3 Watt
Time to perform device authentication	2000 ms
PUF Metrics	Reliability- 99%
Time to write PUF key to TPM	real-299 ms, user-12 ms, and sys-19 ms
Time to read PUF key from TPM	real-411 ms, user-22 ms, and sys-10 ms

Continued…

Working Prototype



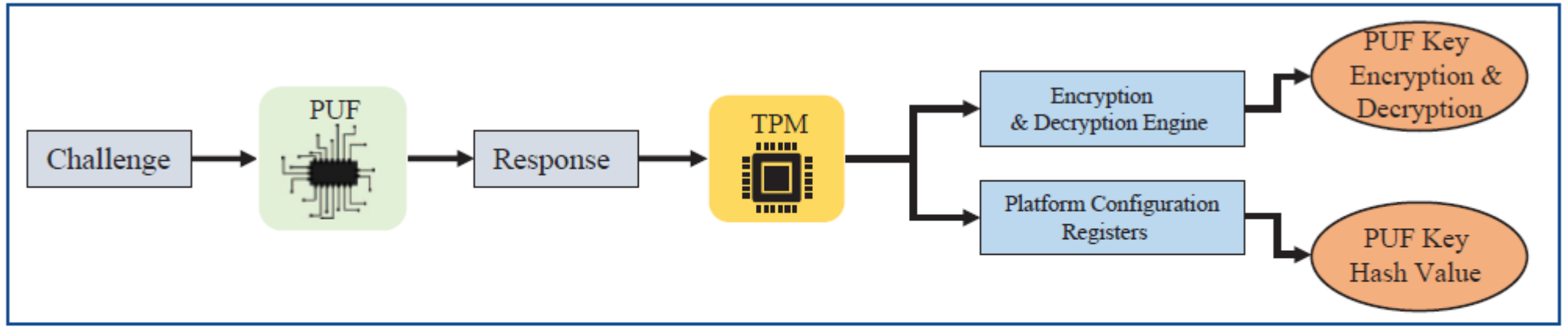
Transaction verification of outputs on IOTA Explorer



Our Novel Integration PUF with TPM using
PCR: Security-by-Design of IoT

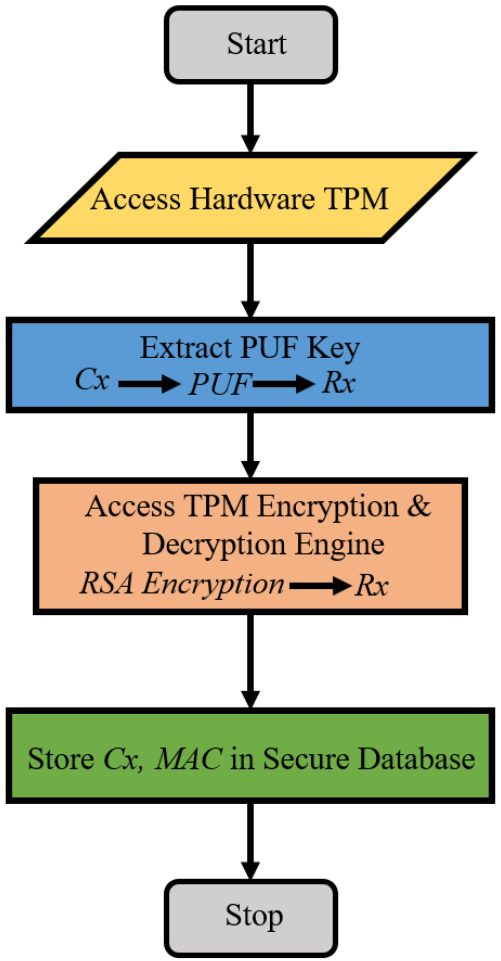
iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics

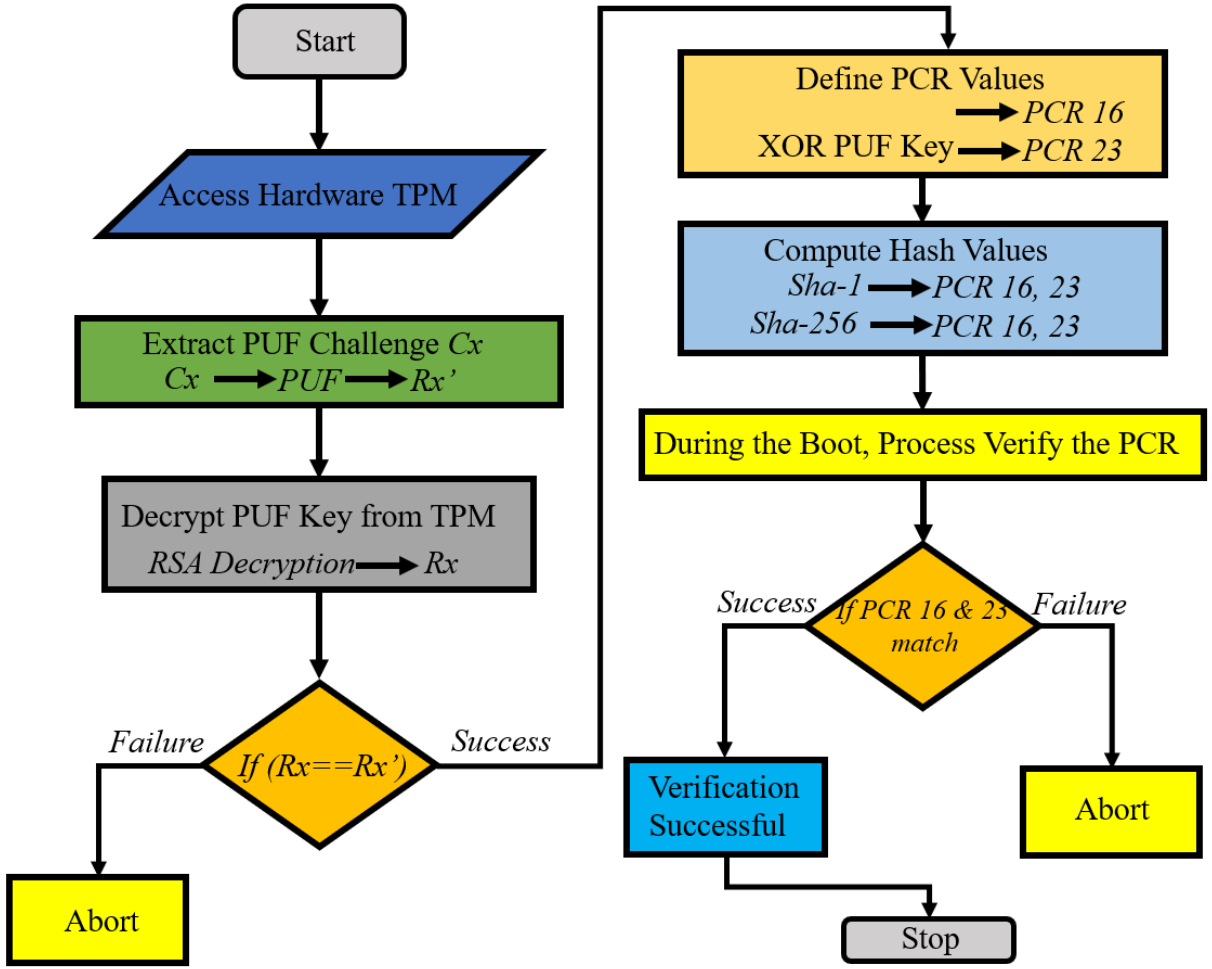
Overview of Proposed iTPM



- The proposed SbD primitive works by performing secure verification of the PUF key using TPM's Encryption and Decryption engine. The securely verified PUF Key is then bound to TPM using Platform Configuration Registers (PCR).
- By binding PUF with PCR in TPM, a novel PUF-based access control. The policy can be defined, as bringing in a new security ecosystem for the emerging Internet-of-Everything era.

Working Flow of Proposed iTPM





Novel Contributions

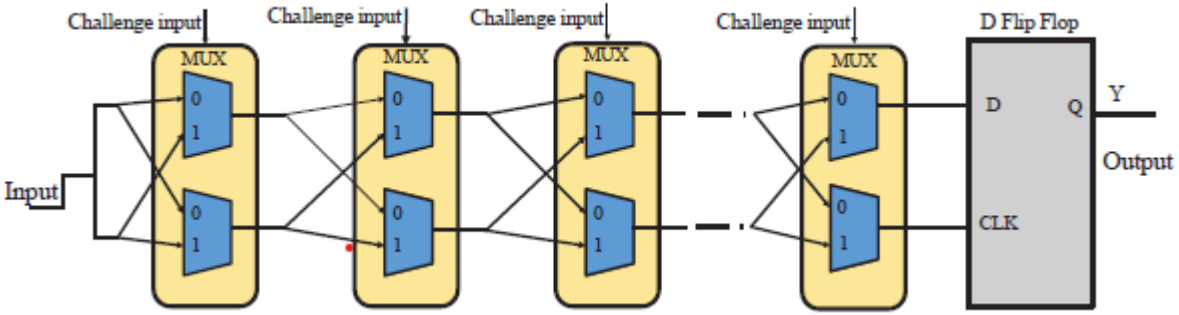
- A sustainable PUF-based TPM SbD approach that works by defining a PUF-based access control policy for TPM.
- A simple, lightweight, and robust approach for integrating two hardware security primitives PUF, and TPM to achieve the objective of sustainable and secure IoT
- A robust TPM-based PUF key verification scheme that utilizes TPM's encryption and decryption policy.
- A sustainable policy that can bind PUF with TPMs Platform Configuration Registers (PCR).
- A simple Edge computing drive PUF-based keyless TPM initiative that works by binding PUF with PCR that can facilitate a secure boot process, remote attestation, and NVRAM a
- A novel approach that explores the true potential of proposed SbD by integrating various PUF topologies with Hardware TPM.

Related Research Overview

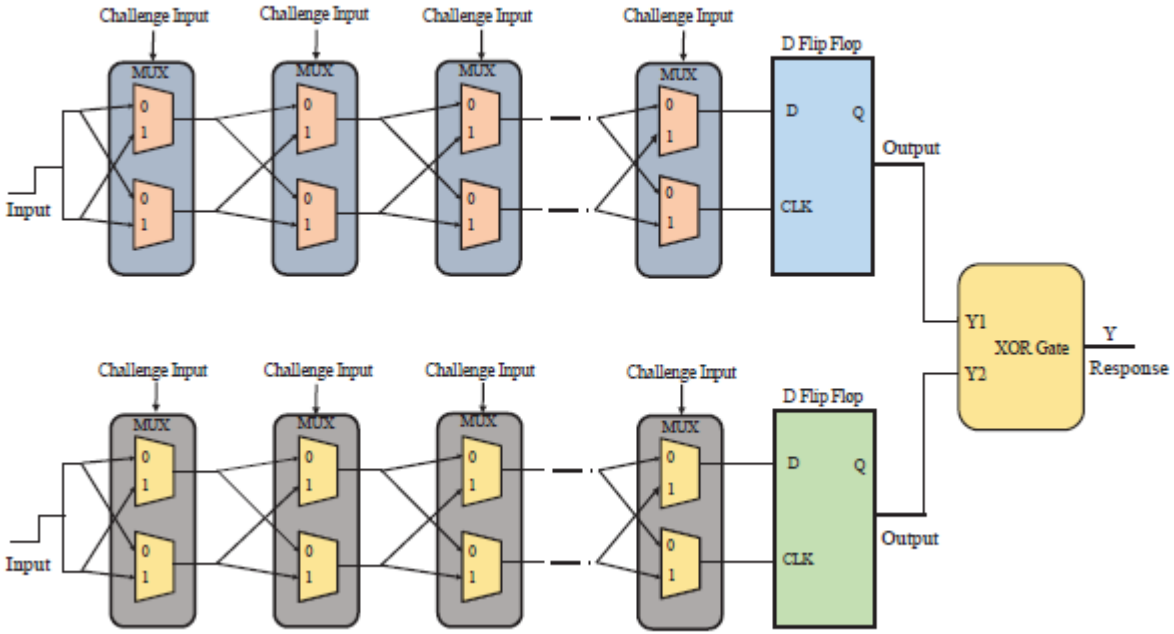
Research Works	Applications	Security Mechanism	Features	Approach
eTPM [18]	Cloud Computing	Software TPM	Virtual Machine(VM) Security	Cloud Computing
RADIS [19]	IoT	NA	Distributed Service Attestation	Distributed
xTSeH [4]	IoMT (Device)	Hardware TPM	TPM based Service Attestation	Decentralized
TPM-based Sensor Security [20]	Wireless Sensor Networks (WSN)	Hardware TPM	Secure WSN	NA
IoT Remote Attestation [14]	IoT	Raspberry pi based TPM, Blockchain	Malware Detection	NA
PUFchain 4.0 [12]	IoT (Device & Data)	PUF, Hardware TPM, Tangle	Sealing PUF key inside TPM (NVRAM)	Edge Computing
iTPM	**Smart Electronics**	**PUF, Hardware TPM**	**Securely Binding PUF with PCR**	**Edge Computing**

PUF Topologies

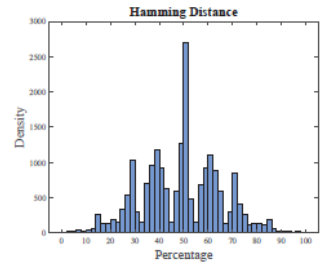
- Arbiter PUF



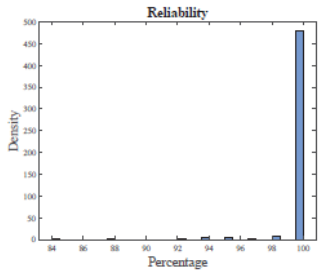
- XOR Arbiter PUF



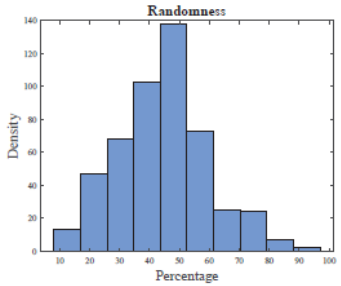
PUF Metrics



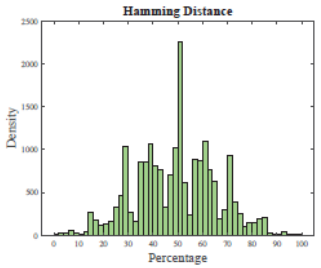
(a) Arbiter PUF Hamming Distance



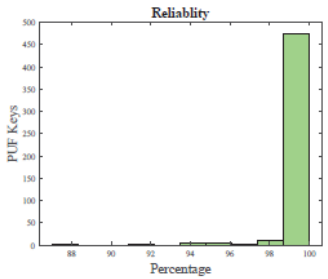
(b) Arbiter PUF Reliability



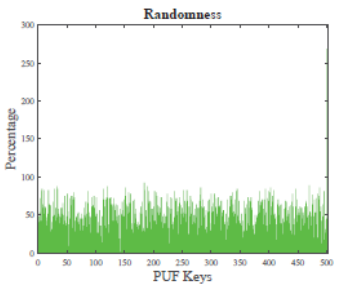
(c) Arbiter PUF Randomness



(d) XOR PUF Hamming Distance



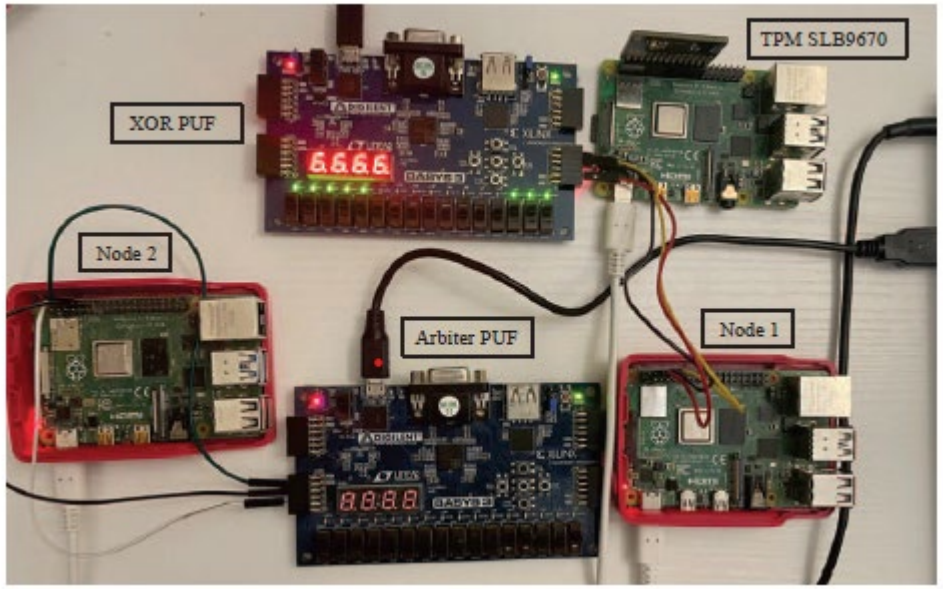
(e) XOR PUF Reliability



(f) XOR PUF Randomness

Prototype and Validation

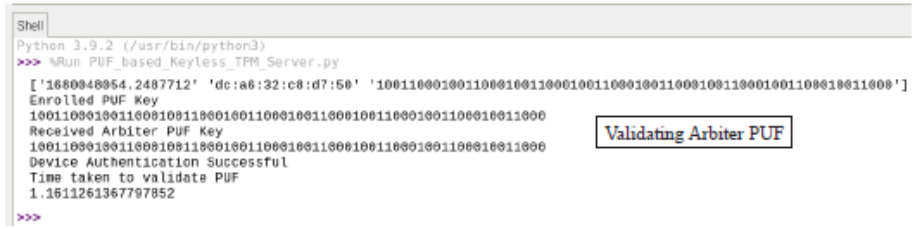
- Prototype



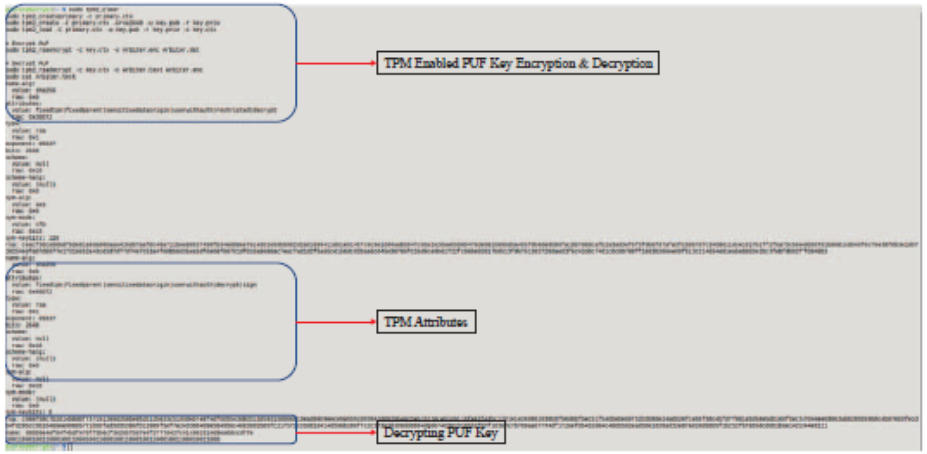
- Validation

Metrics	Results
Application	Smart Electronics
Hardware Security Mechanism	PUF-based Keyless TPM
Security Modules	TPM, PUF
PUF Modules	XOR Arbiter & Arbiter PUF
Approach	Integrating PUF with TPM's PCR
Platform Configuration Registers	16 & 23
TPM Integration	Encryption & Decryption Engine, and PCR
TPM	Hardware TPM
Hardware TPM Chip	Infineon SLB 9670
PUF	Xc7a35tcpg236-1
TPM Embedded Device	Single Board Computer
Interface	SPI, UART
Tools	tpm2-tools, tpm2-abrmd, VIVADO 2020.2
TPM Hash Algorithm	Sha-1 and Sha 256
Possible Applications	Remote Attestation, and Secure Boot Process

Experimental Results



(a) Arbiter & XOR PUF validation



(b) TPM Encryption and Decryption

(c) Binding PUF inside Platform Configuration Registers

Summary

- This paper presented and validated a novel SbD approach with a sustainable policy for integrating PUF and TPM by binding PUF with PCRs inside TPM.
- By successfully binding PUF in PCR, the PUF is made as a device integrity credential required for a secure boot process.
- Further, the experimental analysis revealed that integrating PUF inside PCR could bind PUF with TPM and facilitate security at the edge level in smart Electronics applications.
- The proposed approach also presents the possibility of PUF-enabled secure firmware and boot processes for computing systems
- By Integrating the PUF with TPM in this work, we validated the potential of PUF-based TPM security solutions for IoT.

Future Research

- Idea of implementing PUF-based TPM scheme for the Security-by-Design (SbD) in Smart Healthcare.
- Exploring the feasibility of a Trusted Platform Module (TPM) integrated scalable Blockchain-based cryptographic scheme to attain the Security by Design (SbD) objective in IoMT.
- Working on an integrated access control mechanism for resource-constrained electronic devices using TPM
- Developing scalable and sustainable TPM-enabled IoT device authentication scheme for Fog, Edge, and Cloud Computing Paradigms.
- Extending iTPM scheme for the resource-constrained IoMT and Internet of Agro-Things security.

Thank You !!