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

P .Yanambaka[1], S. P. Mohanty[2], E. Kougianos[3] , D. Puthal[4] and L. Rachakonda[5]

Central Michigan University, USA[1], University of North Texas, Denton, TX 76203, USA.[2,3,5] and Newcastle University, UK[4].

Email: yanam1v@cmich.edu[1], saraju.mohanty@unt.edu[2] , elias.kougianos@unt.edu[3] , Deepak.Puthal@newcastle.ac.uk[4] and rachakondalaavanya@my.unt.edu[5]

Outline of Talk

- IoMT Security
- Wearable Medical Devices-Security
- Healthcare – Cyber Physical systems (HCPS) Security
- Hardware Security
- PUF – design, varieties, validation
- PMsec – Approach, implementation and Validation
- Conclusion and Future Research

IoMT Security Issue is Real & 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/

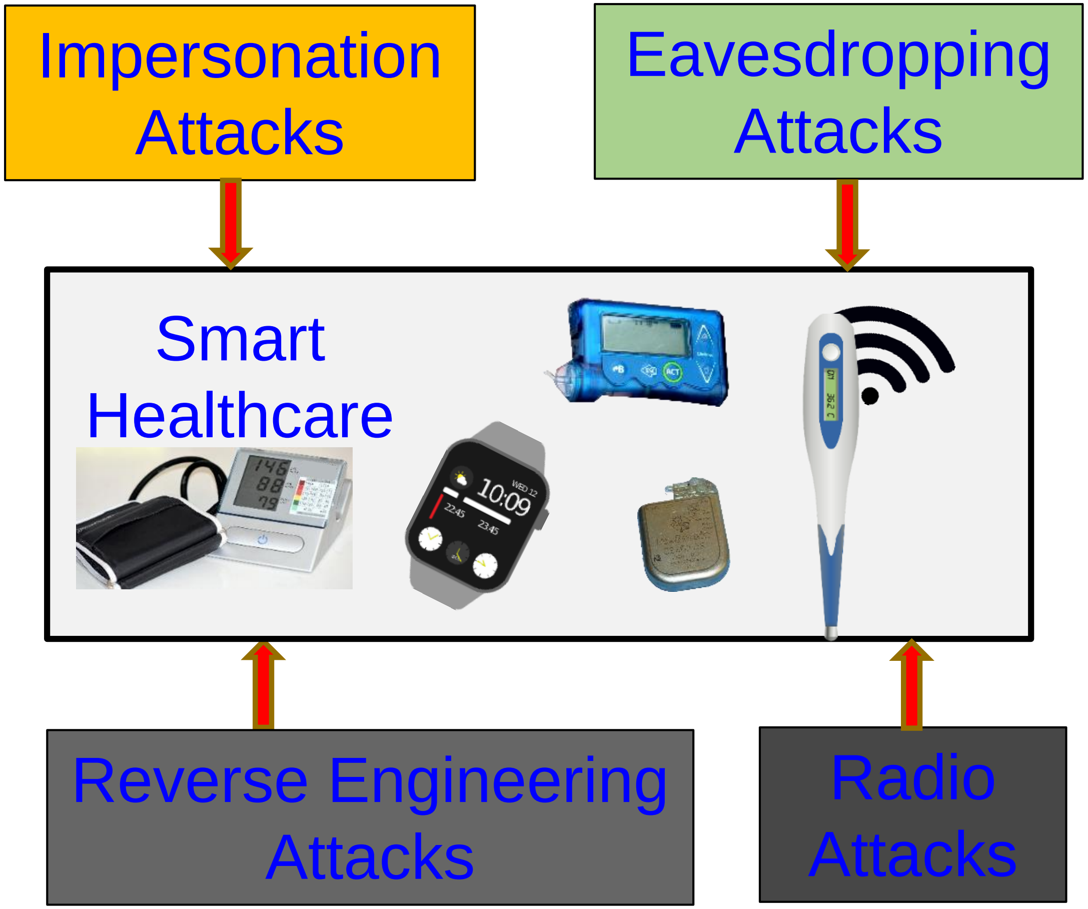
- Software vulnerabilities in some medical devices could leave them susceptible to hackers, FDA warns:

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

IoMT Security – Selected Attacks



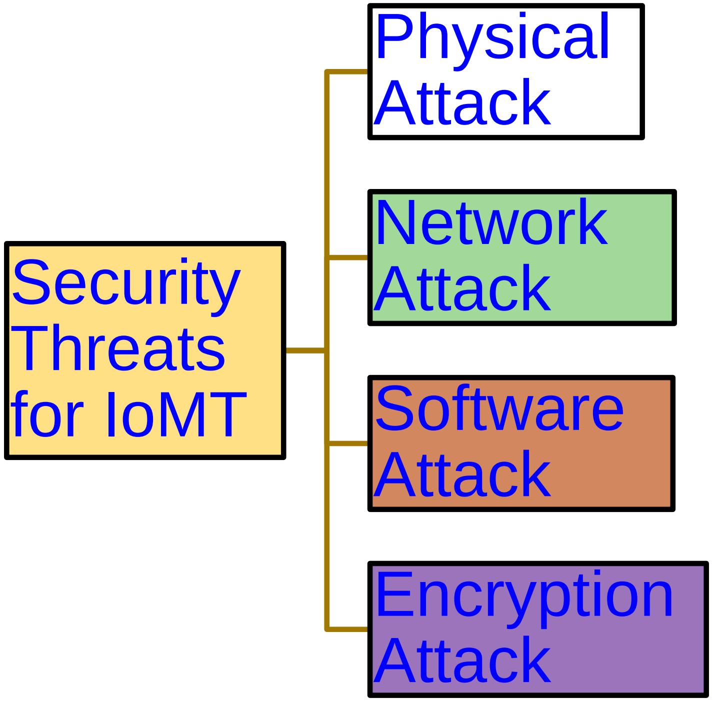
Impersonation Attacks

Eavesdropping Attacks

Smart Healthcare

Reverse Engineering Attacks

Radio Attacks



Security Threats for IoMT

- Physical Attack
- Network Attack
- Software Attack
- Encryption Attack

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.

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.

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

IT Security

- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

IoT Security

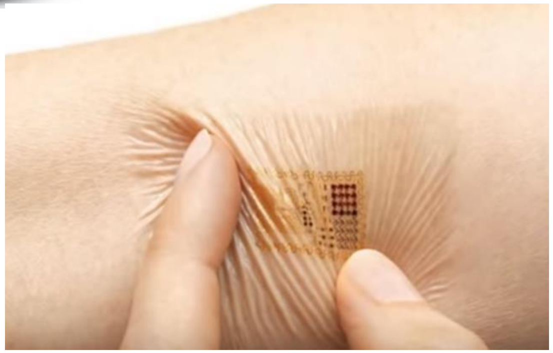
- IoT may be deployed in open hostile environments
- Significantly large variety of IoT devices
- Billions of IoT devices
- May not have computational power to run security solutions
- IoT security breach (e.g. in a IoMT device like pacemaker, insulin pump) can be life threatening

Maintaining of Security of Consumer Electronics, Electronic Systems, IoT, CPS, etc. needs Energy and affects performance.

Wearable Medical Devices (WMDs)

Fitness Trackers

Headband with Embedded Neurosensors



Embedded Skin Patch

Source: http://www.sciencetimes.com/articles/8087/20160107/ces-loreals-smart-skin-patch-reveals-long-exposed-sun.htm

Source: https://www.empatica.com/embrace2/

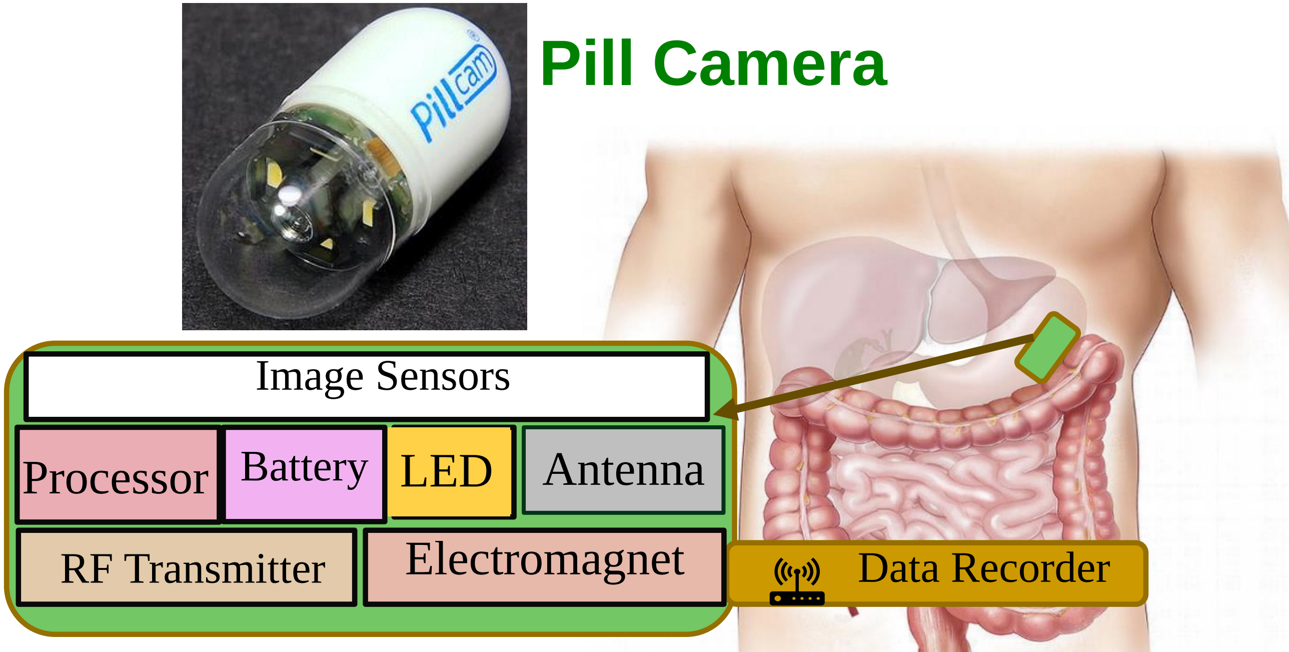
Smart watch to detect seizure

Wearable Medical Devices (WMDs)
→ Battery Constrained

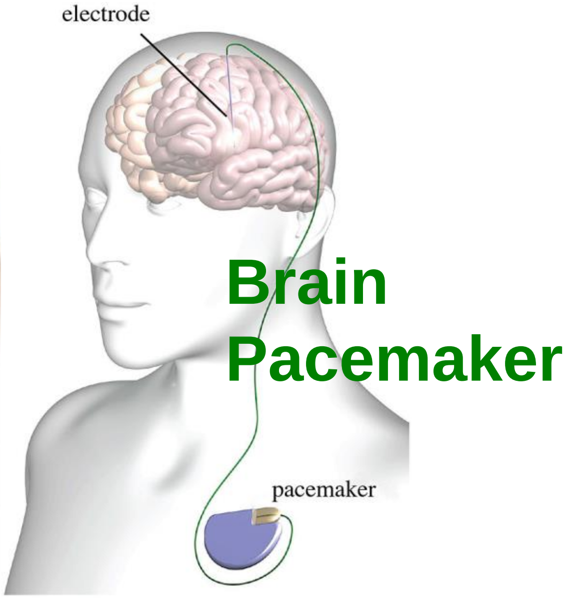
Insulin Pump

Source: https://www.webmd.com

Implantable Medical Devices (IMDs)



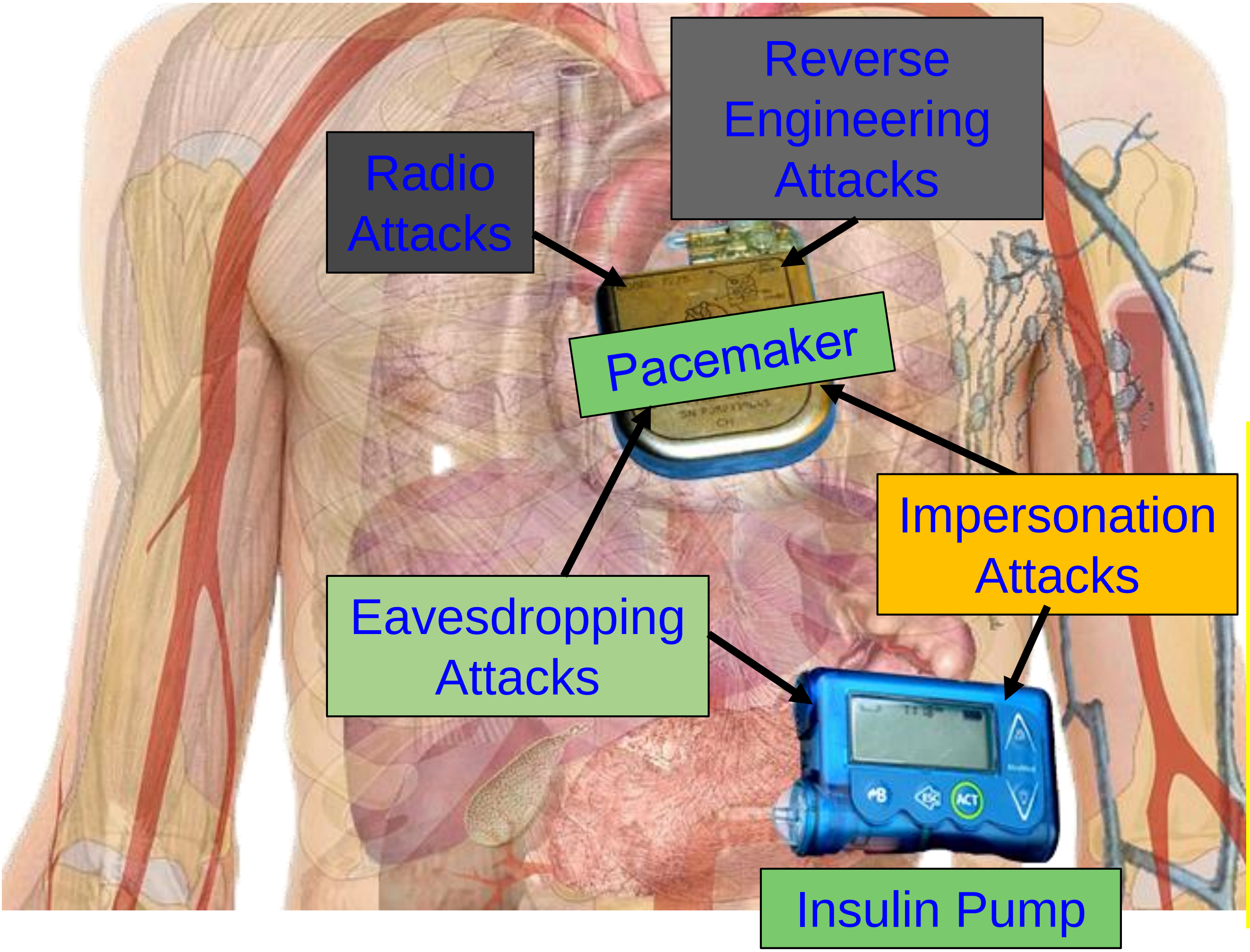
Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Health Care”, *IEEE Consumer Electronics Magazine (CEM)*, Vol. 7, No. 1, January 2018, pp. 18-28.



Collectively:
Implantable and Wearable Medical Devices (IWMDs)

Source: http://web.mit.edu/cprl/www/research.shtml

Security Measures in Healthcare Cyber-Physical Systems is Hard



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

Implantable and Wearable Medical Devices (IWMDs) -- Battery Characteristics:

→ Longer life

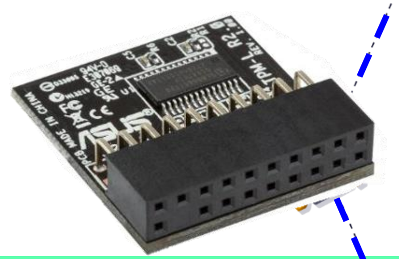
→ Safer

→ Smaller size

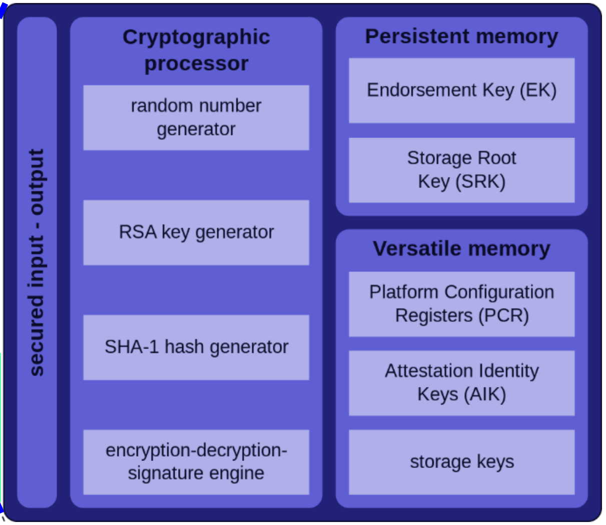
→ Smaller weight

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

Hardware Security Module (HSM)



Trusted Platform Module (TPM)



secured input - output

Cryptographic processor

random number generator

RSA key generator

SHA-1 hash generator

encryption-decryption-signature engine

Persistent memory

Endorsement Key (EK)

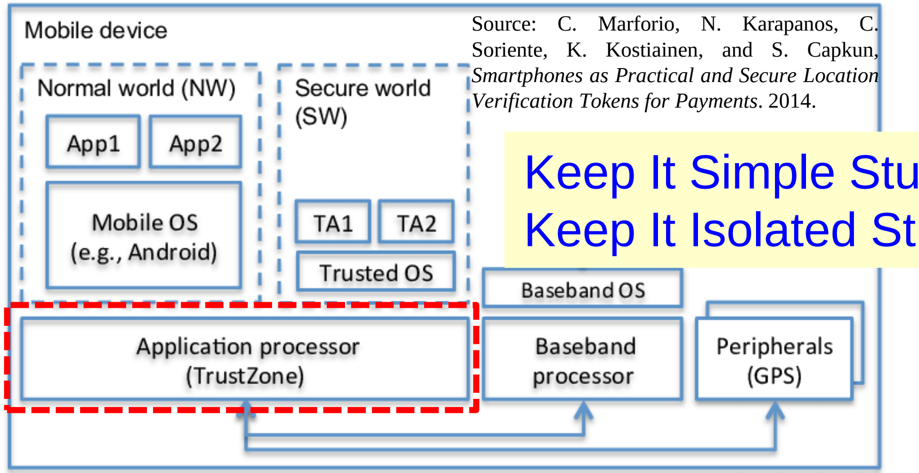
Storage Root Key (SRK)

Versatile memory

Platform Configuration Registers (PCR)

Attestation Identity Keys (AIK)

storage keys



Mobile device

Normal world (NW)

App1

App2

Mobile OS (e.g., Android)

Secure world (SW)

TA1

TA2

Trusted OS

Baseband OS

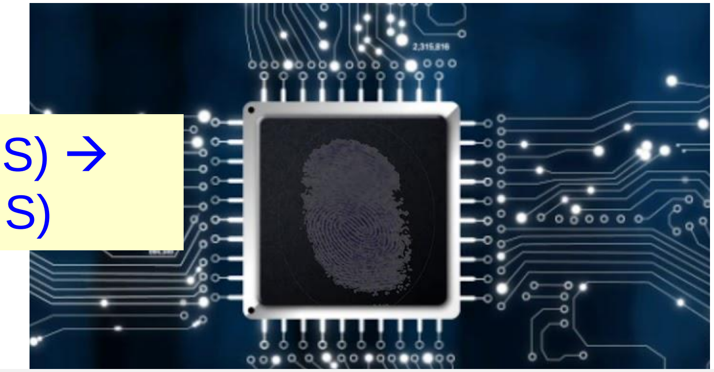
Application processor (TrustZone)

Baseband processor

Peripherals (GPS)

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)

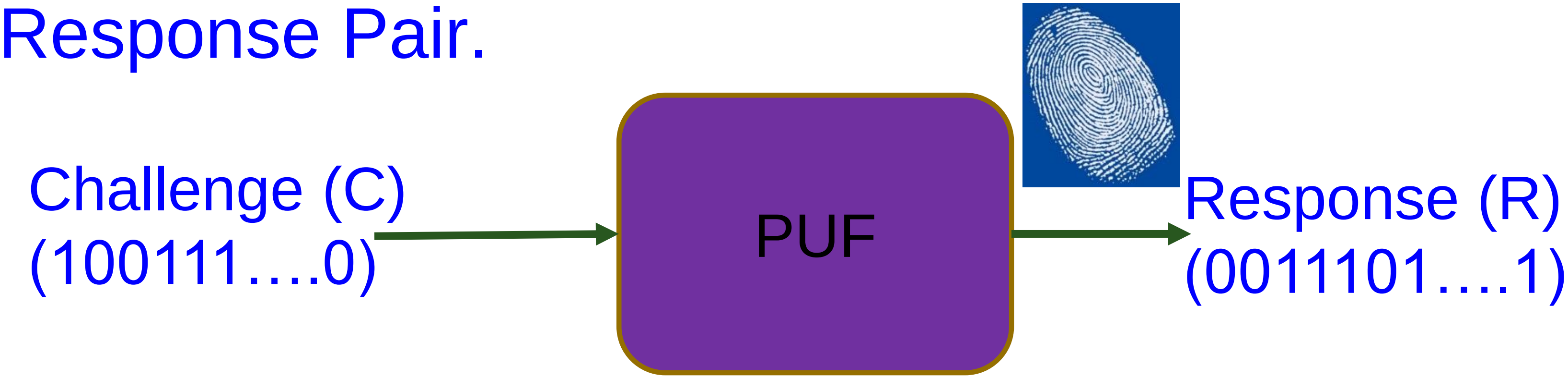


Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

Physical Unclonable Functions (PUFs)

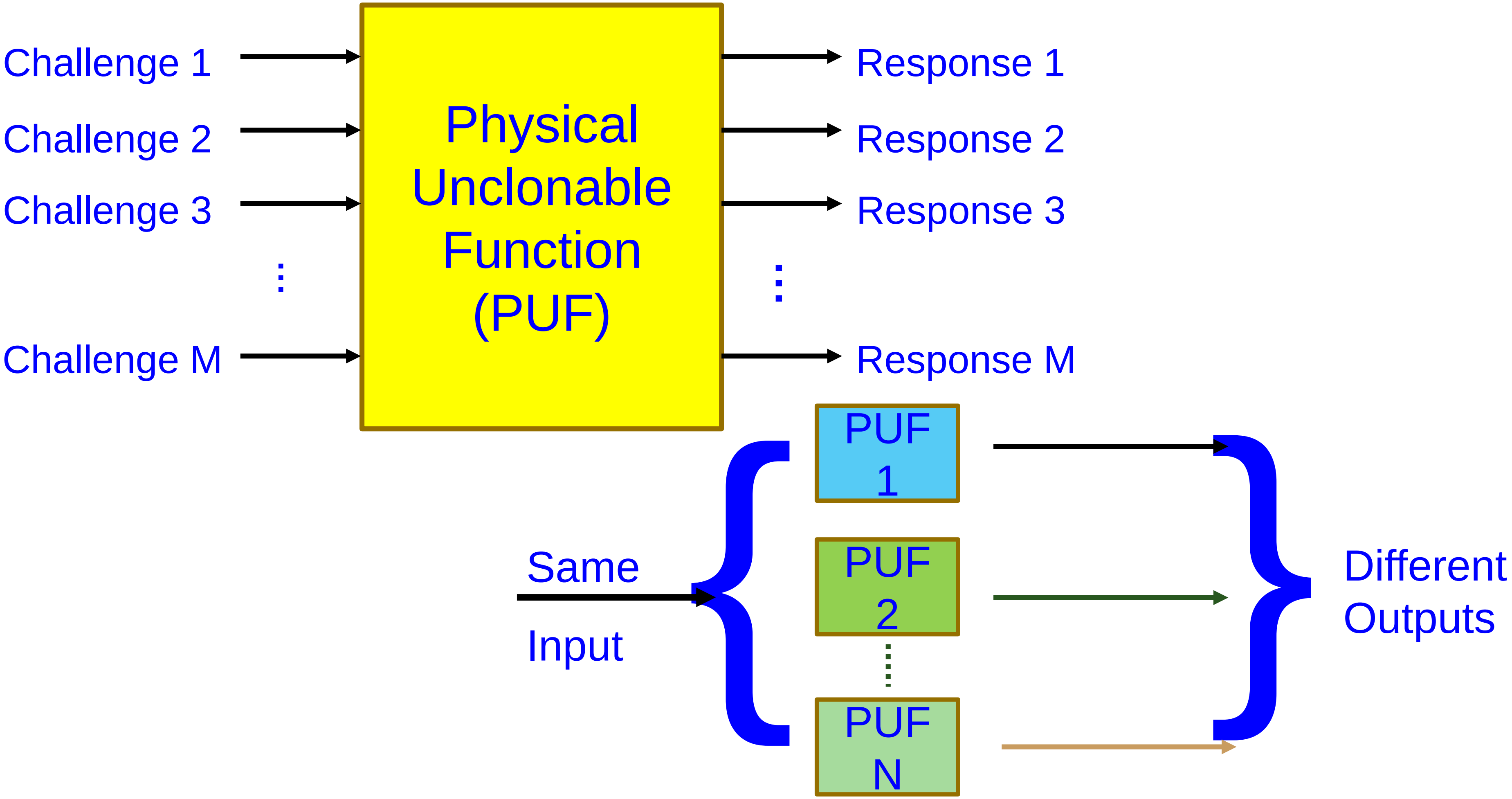
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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.

Principle of Generating Multiple Random Response using PUF



Challenge 1

Challenge 2

Challenge 3

⋮

Challenge M

Physical Unclonable Function (PUF)

Response 1

Response 2

Response 3

⋮

Response M

Same Input

PUF 1

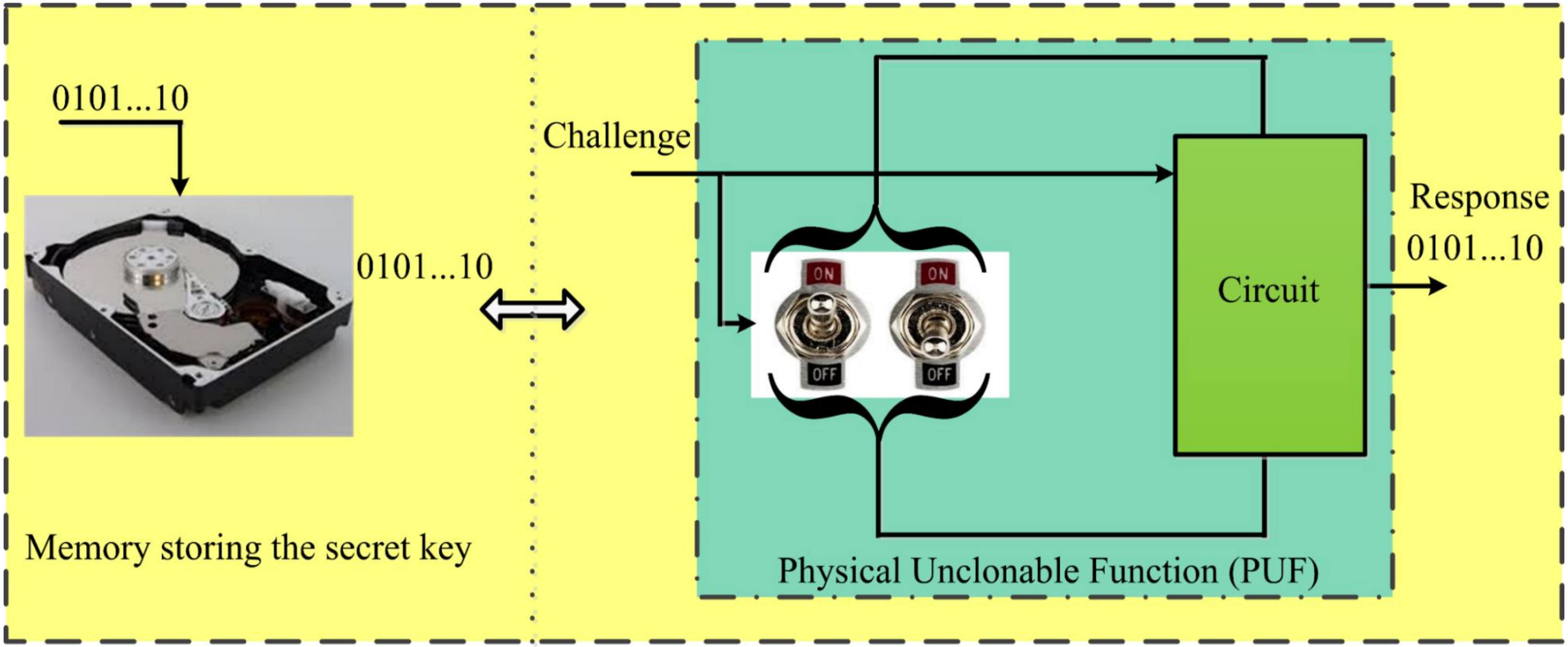
PUF 2

⋮

PUF N

Different Outputs

PUFs Don’t Store Keys

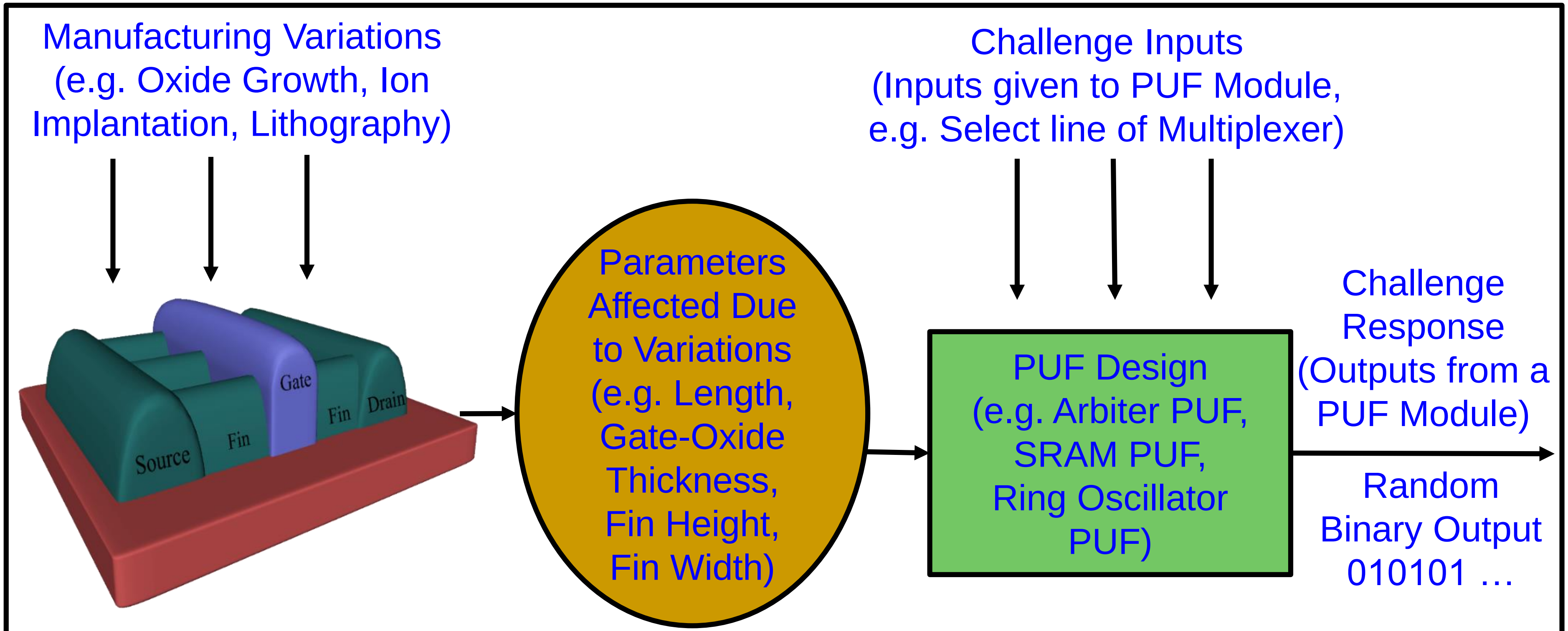


0101...10
0101...10
Memory storing the secret key
Challenge
ON
ON
OFF
OFF
Circuit
Response
0101...10
Physical Unclonable Function (PUF)

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



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

Parameters Affected Due to Variations (e.g. Length, Gate-Oxide Thickness, Fin Height, Fin Width)

Challenge Inputs (Inputs given to PUF Module, e.g. Select line of Multiplexer)

PUF Design (e.g. Arbiter PUF, SRAM PUF, Ring Oscillator PUF)

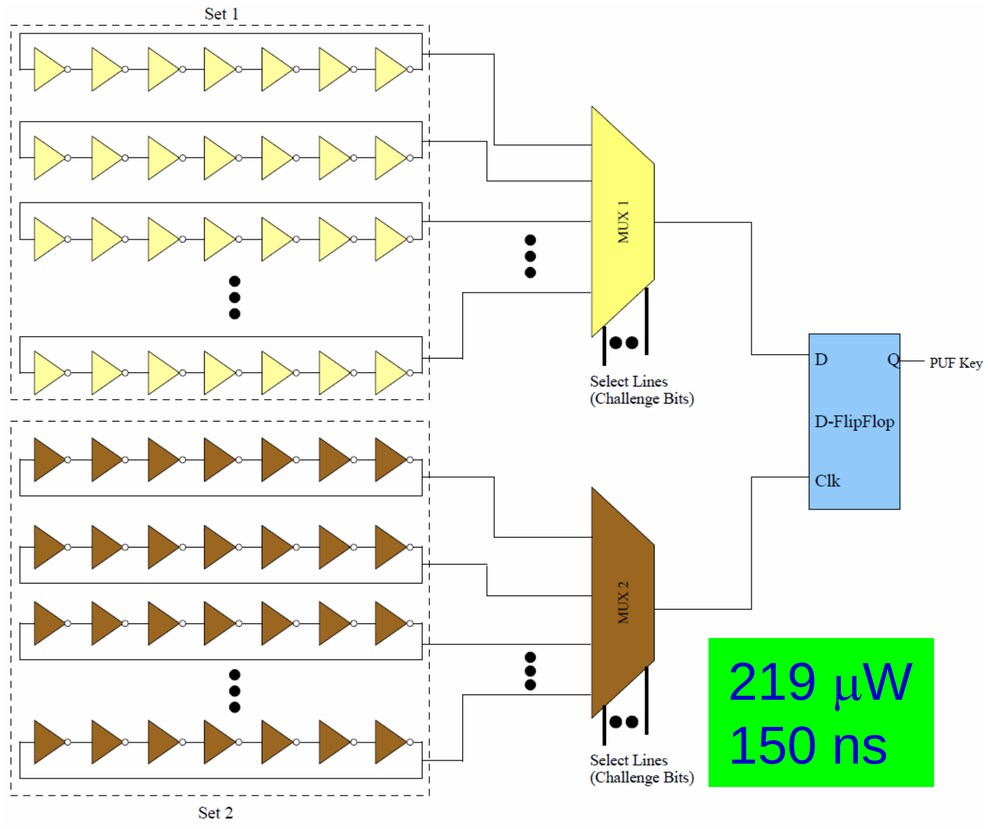
Challenge Response (Outputs from a PUF Module)

Random Binary Output 010101 …

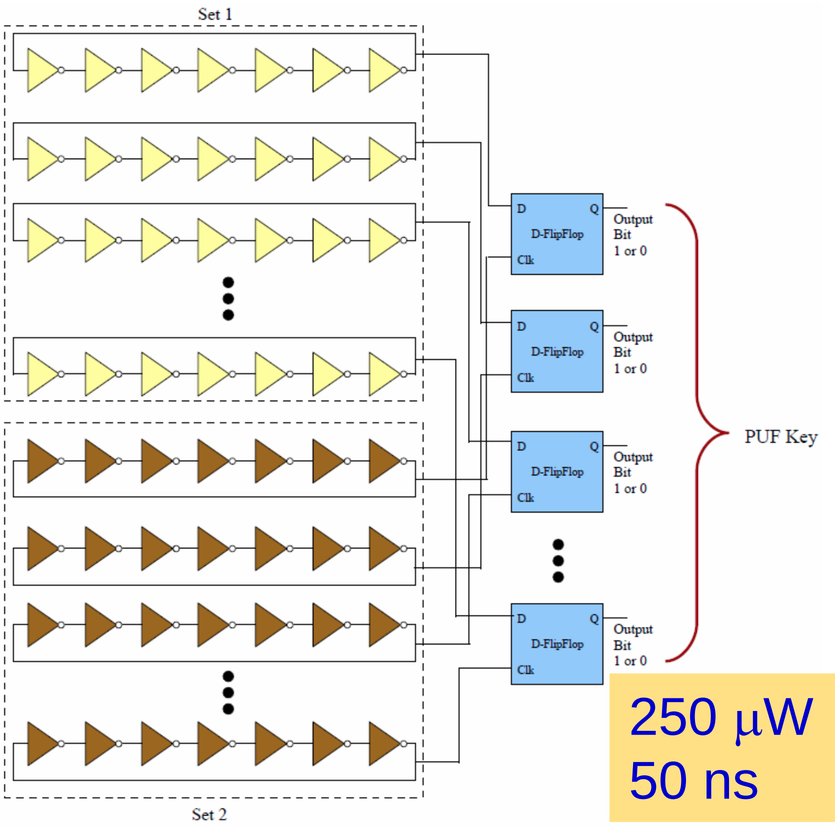
Silicon manufacturing process variations are turned into a feature rather than a problem.

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.

PUFs- Varieties and their Designs



219 µW
150 ns



250 µW
50 ns

Power Optimized Hybrid Oscillator Arbiter PUF

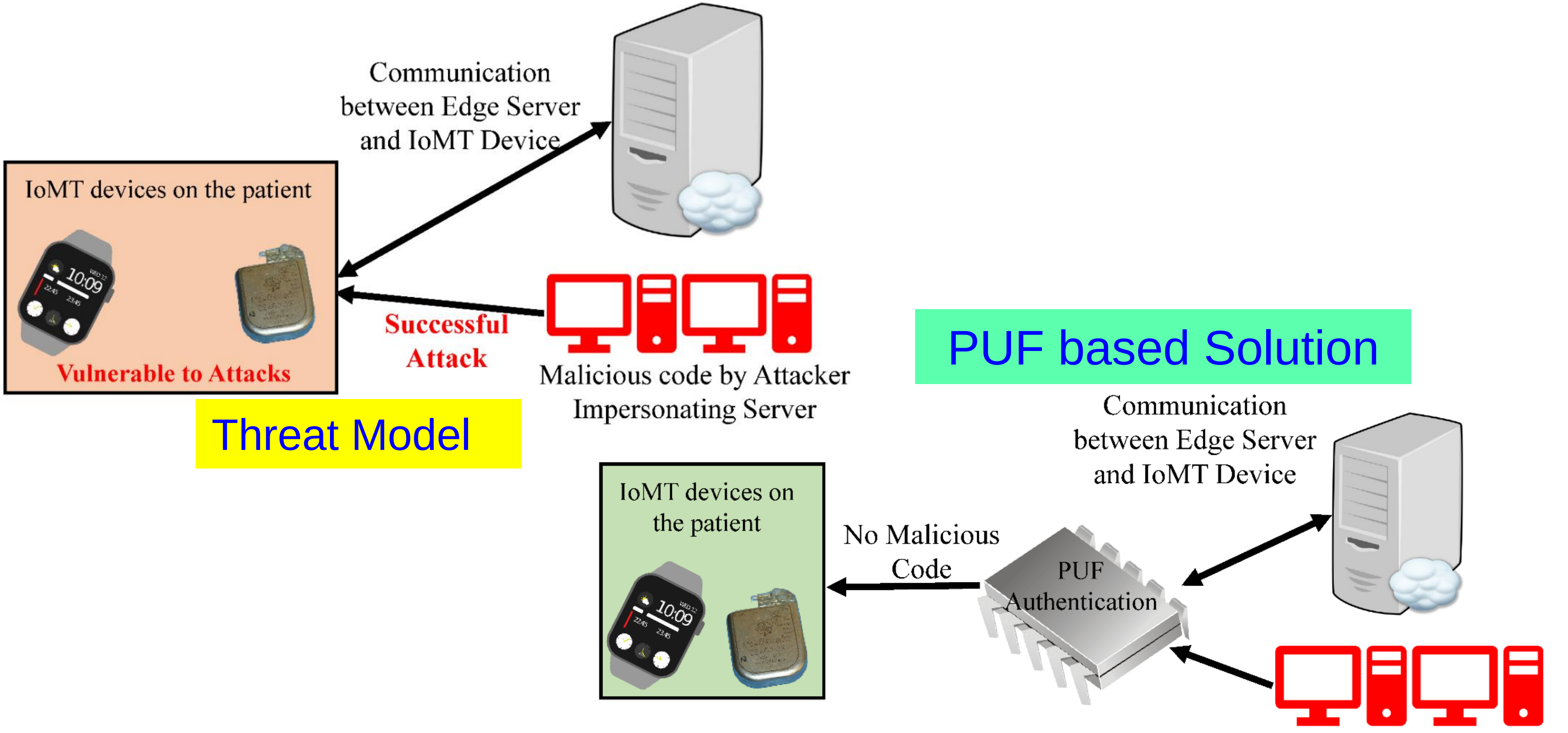
Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS

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.

Secure Design Approach for Robust Security in Healthcare CPS



Communication between Edge Server and IoMT Device

IoMT devices on the patient

Vulnerable to Attacks

Successful Attack

Malicious code by Attacker Impersonating Server

Threat Model

PUF based Solution

Communication between Edge Server and IoMT Device

IoMT devices on the patient

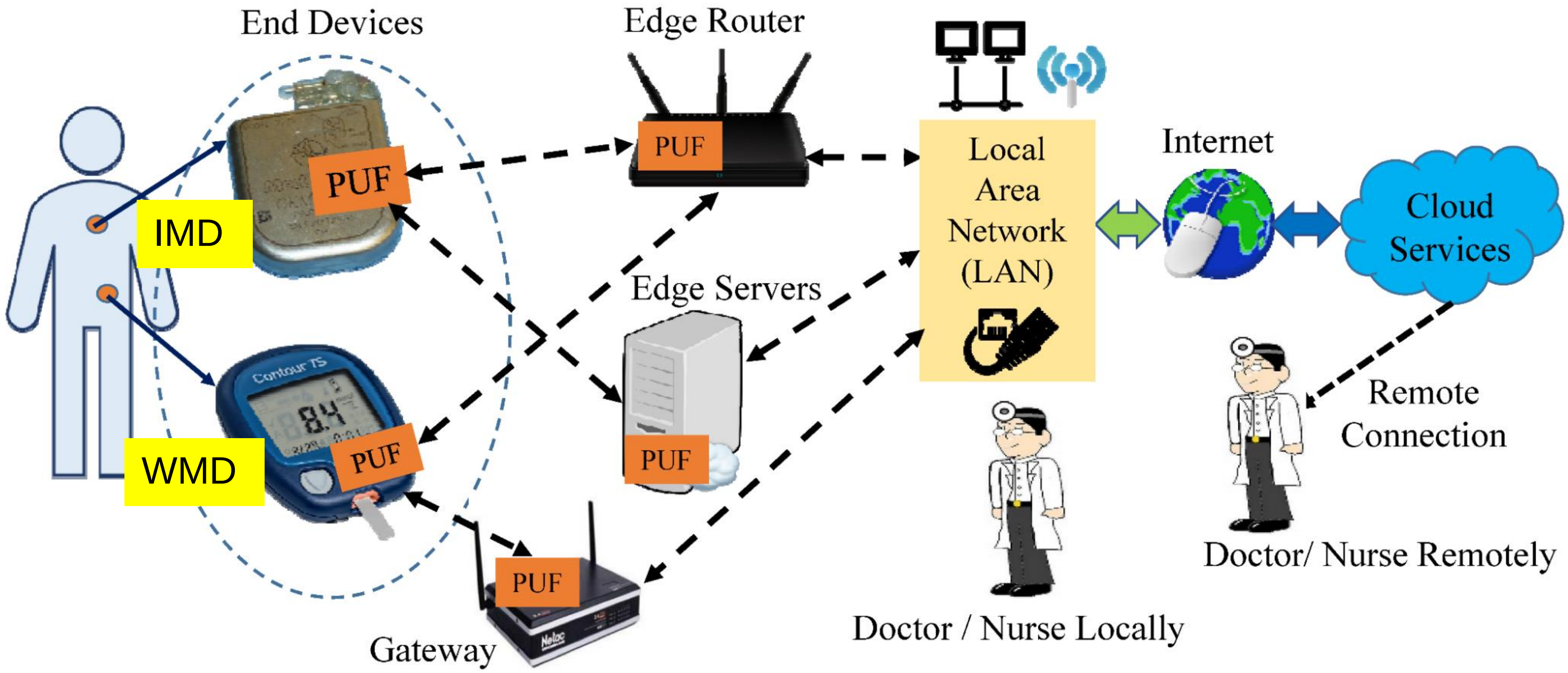
No Malicious Code

PUF Authentication

Malicious code by Attacker Impersonating Server

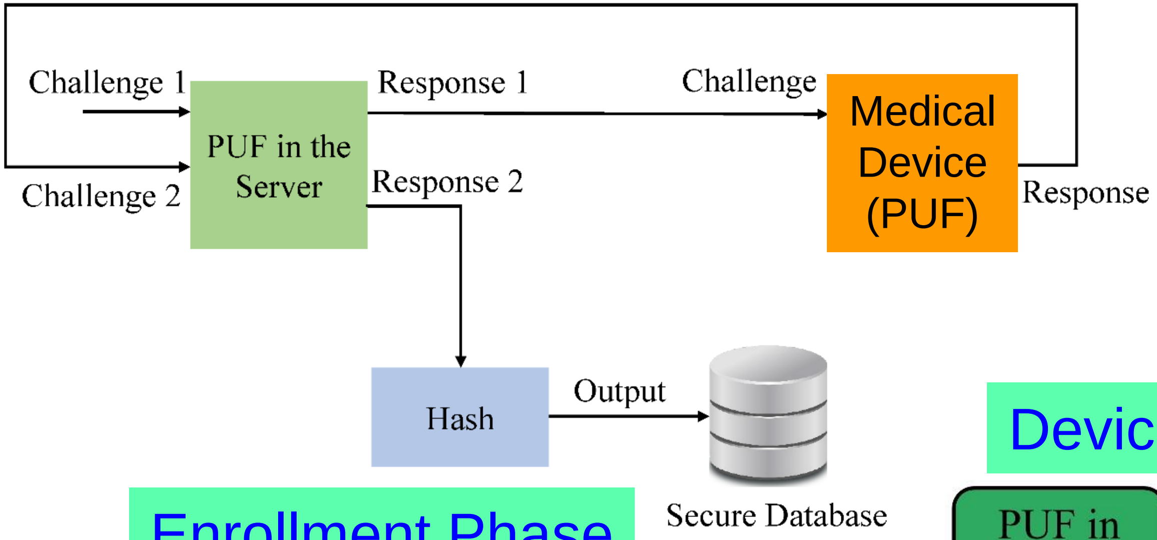
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Secure Design Approach for Robust Security in Healthcare CPS



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.

Proposed PMsec

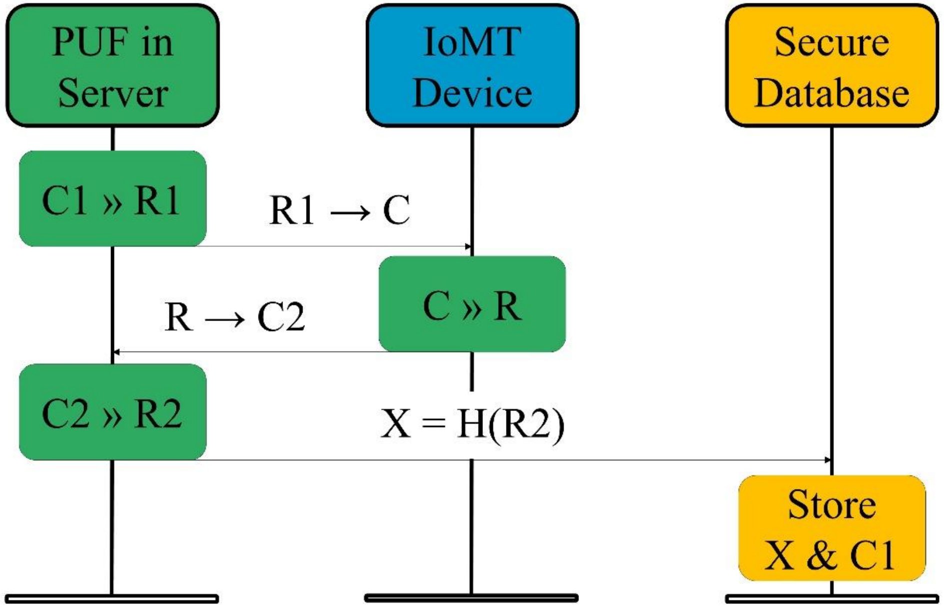


Enrollment Phase

At the Doctor

- as a new Device comes for an User

Device Registration Procedure

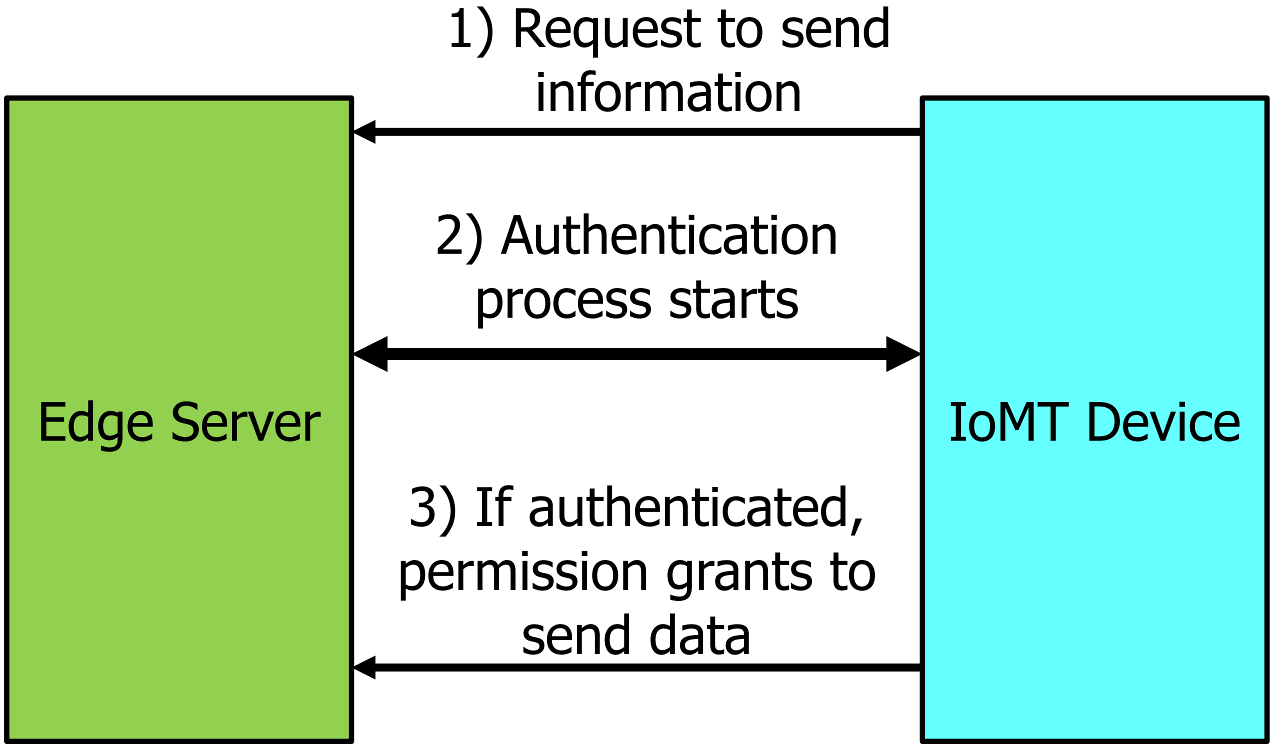


PUF Security Full Proof:

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

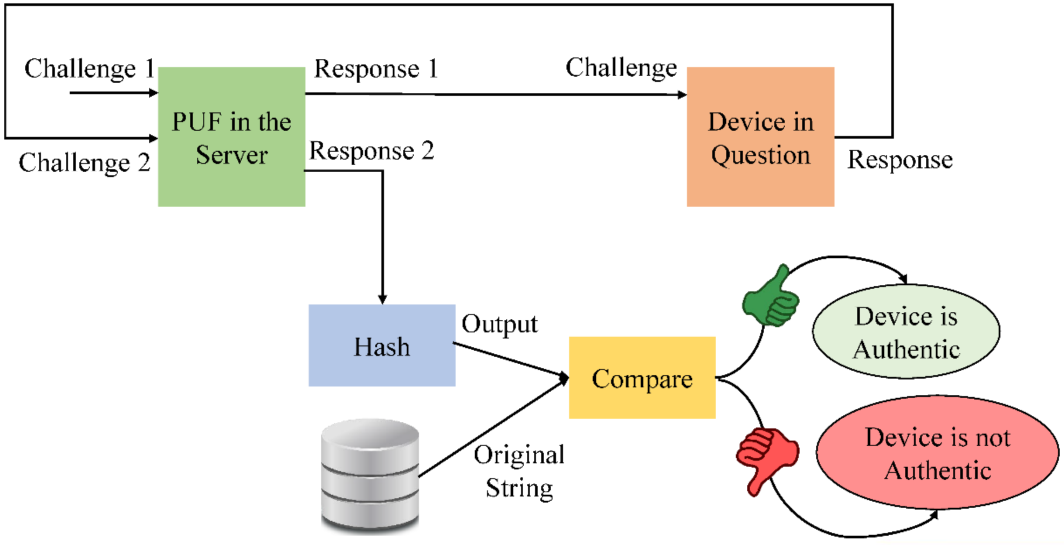
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Proposed PMsec


1) Request to send information
2) Authentication process starts
Edge Server
IoMT Device
3) If authenticated, permission grants to send data

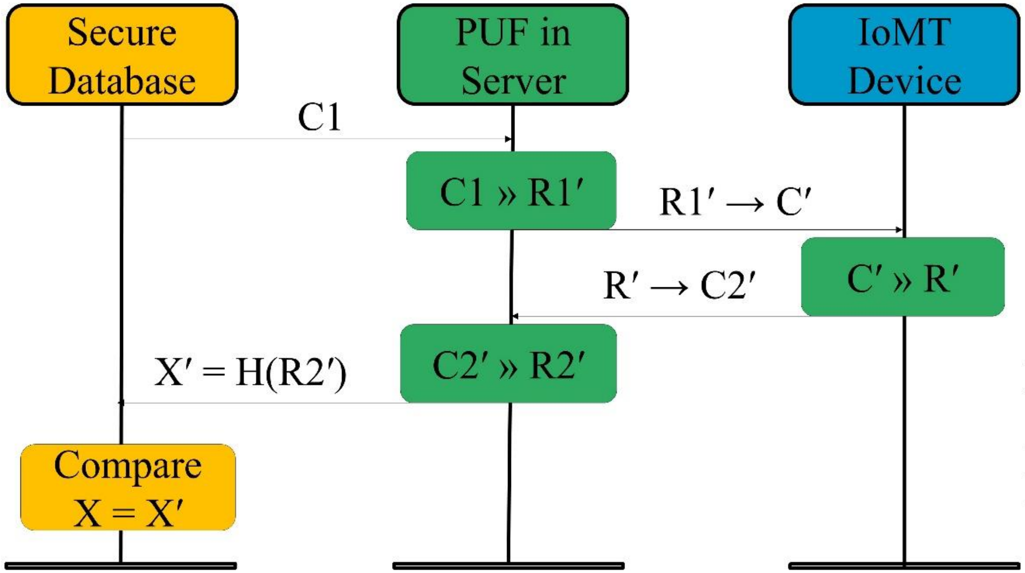
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Proposed PMsec



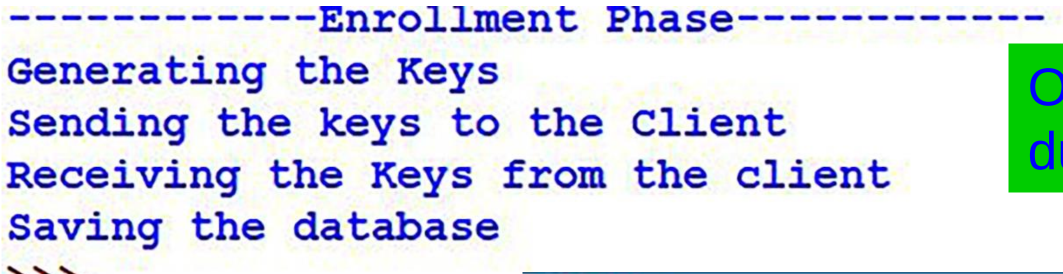
Authentication Phase

Device Authentication Procedure



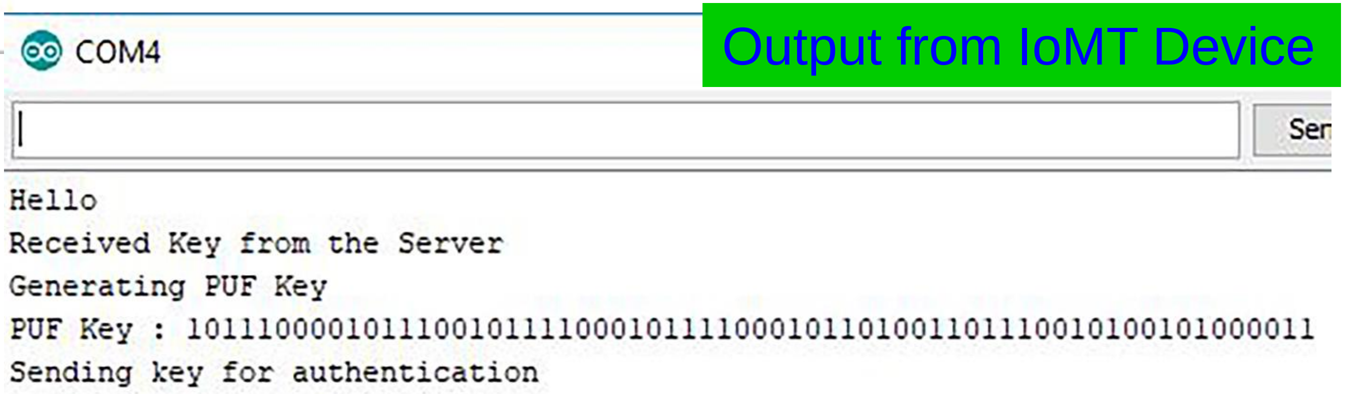
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

PMsec in Action



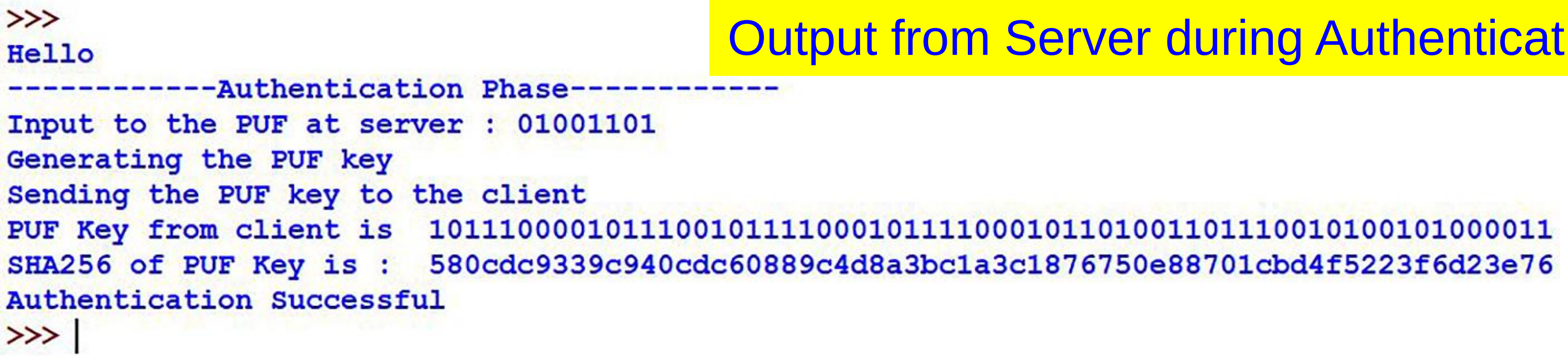
```
------------Enrollment Phase------------
Generating the Keys
Sending the keys to the Client
Receiving the Keys from the client
Saving the database
>>>
```

Output from Server during Enrollment



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

Output from IoMT Device

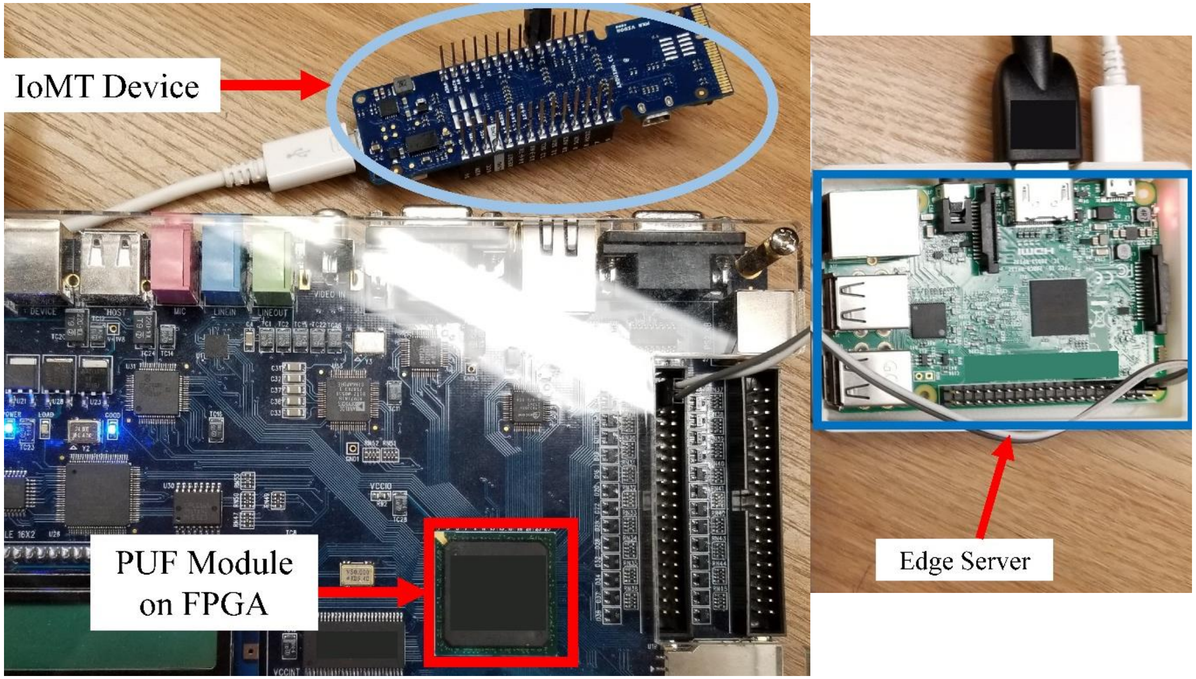


```
>>>
Hello
-----------Authentication Phase-----------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  1011100001011100101111000101111000101101001101110010100101000011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76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

Output from Server during Authentication

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 Module



Average Power Overhead – ~ 200 μW

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 (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Conclusions

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

Future Directions

Our future research interests include:

- Privacy and/or Security by Design (PbD or SbD).
- Security, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS).
- Security of systems (e.g. Smart Healthcare device/data, Smart Grid, UAV, Smart Cars).
- Sustainable Smart City: needs sustainable IoT/CPS
- Internet-of-Everything (IoE) is the domain in which humans are active parts.

Acknowledgment

This material is based upon work supported by the National Science Foundation (NSF) under Grant No. OAC-1924112.

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.