Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT

Venkata P. Yanambaka[1], Saraju P. Mohanty[2], Elias Kougianos[3], Babu K. Baniya[4], Bibhudutta Rout[5]

Central Michigan University, Mt. Pleasant, MI, USA[1]

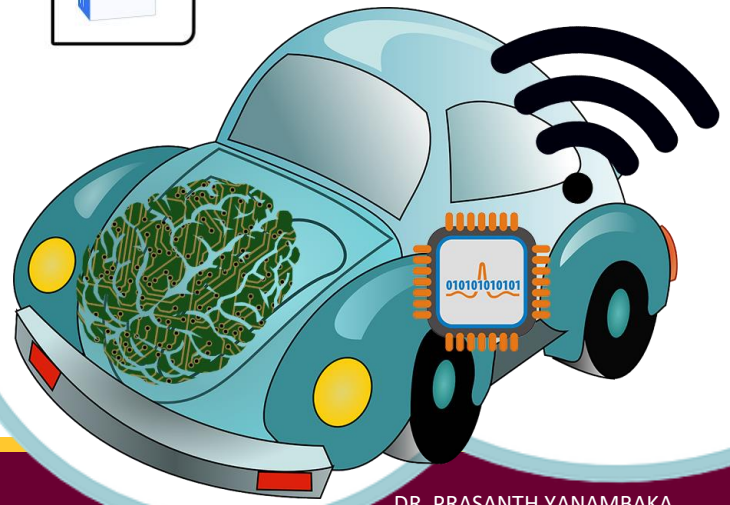
University of North Texas, Denton, TX, USA[2,3,5]

Grambling State University, LA, USA[4]

Outline of the talk

- Attacks on IoT
- Hardware Assisted Security (HAS) using Physical Unclonable Functions (PUF)
- Proposed Veda - PUF Architecture
- Experimental Results
- Conclusion and Future Research

Internet of Things (IoT)



Cyber Attacks

- 1.51 Billion IoT device breaches in 2021.
- Pandemic increased the attacks with a high home environmental usage.
- Smart home lighting and Smart Thermostat were hacked recently.

https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/
https://latesthackingnews.com/2019/02/01/lifx-iot-smart-light-bulb-hacked-in-under-an-hour

Attacks on IoT Devices

Impersonation Attack

Reverse Engineering Attack

Denial of Service Attack

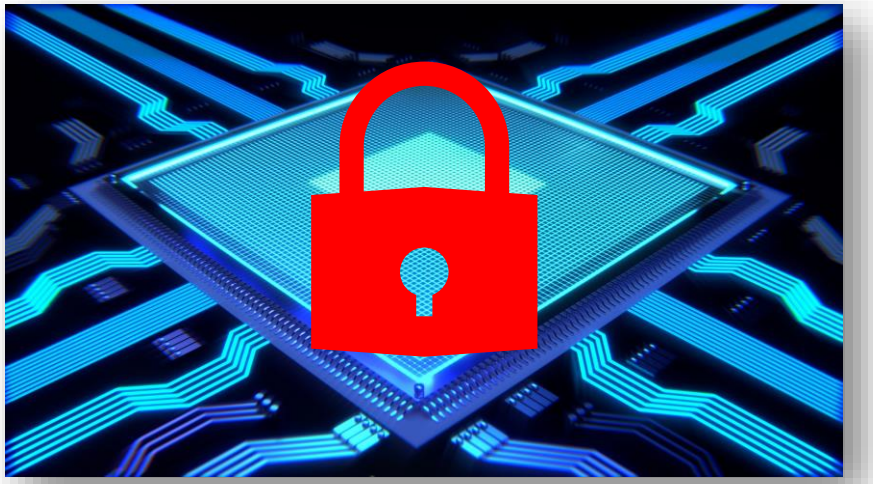
Dictionary and Brute Force Attack

Eavesdropping Attack

Hardware Assisted Security (HAS)

Fast

Reliable



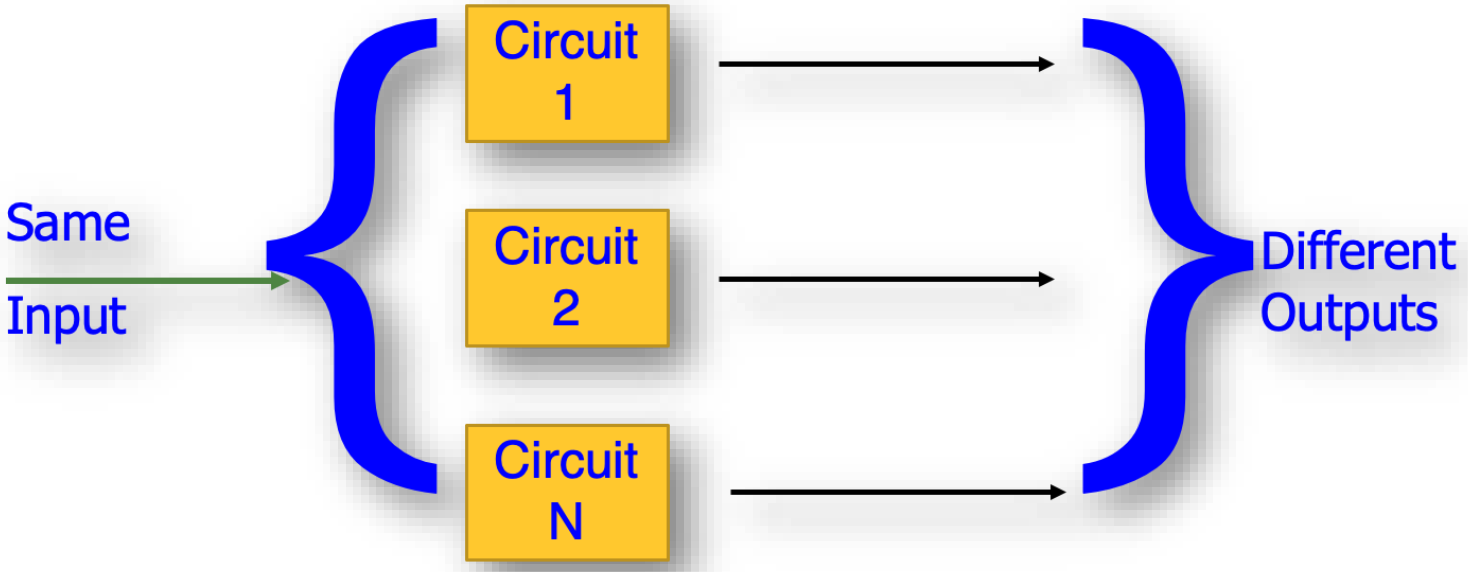
Robust

Low – Cost

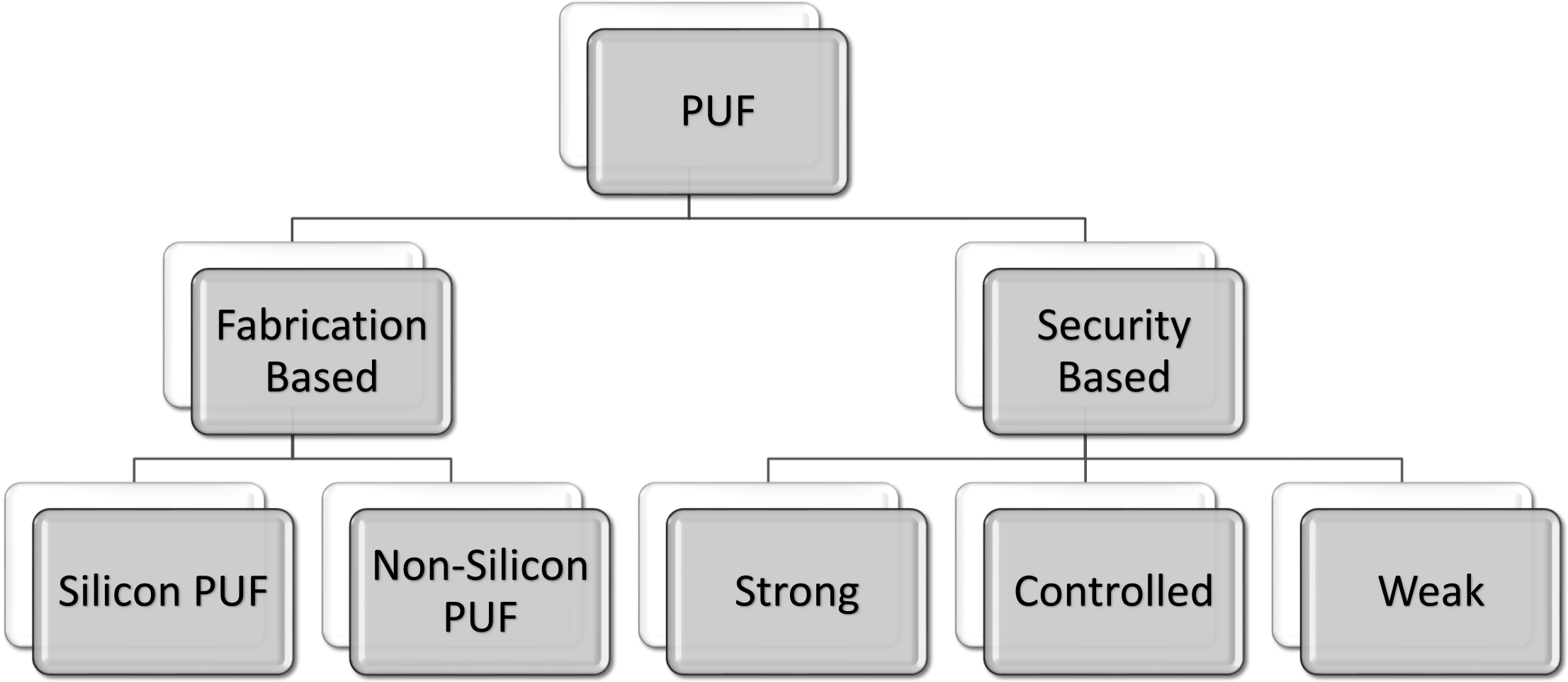
Energy Efficient

Physical Unclonable Functions (PUF)

- PUF are one of the HAS solutions for IoT
- Uses manufacturing variations for generating unique set of keys for cryptographic applications.
- Input of PUF is a challenge and output from PUF is response.

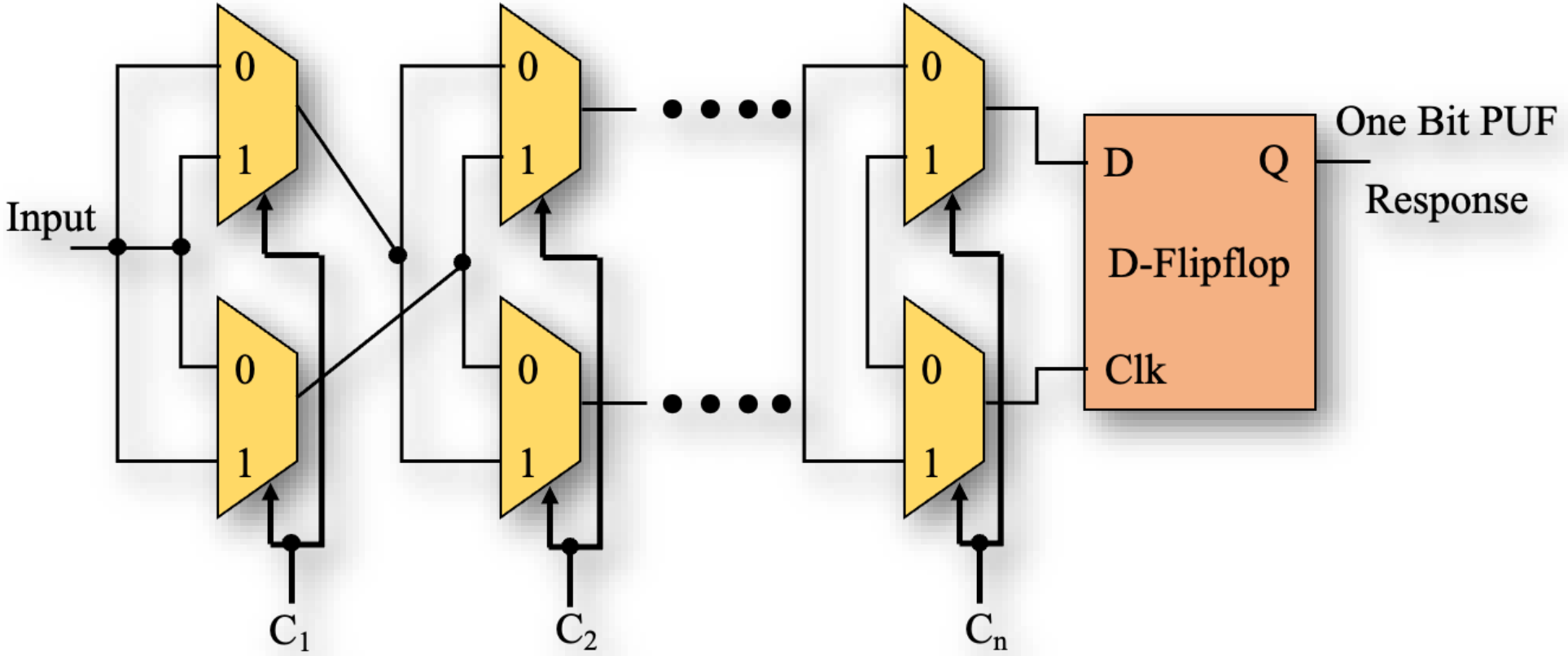


Types of PUF


PUF
Fabrication Based
Security Based
Silicon PUF
Non-Silicon PUF
Strong
Controlled
Weak

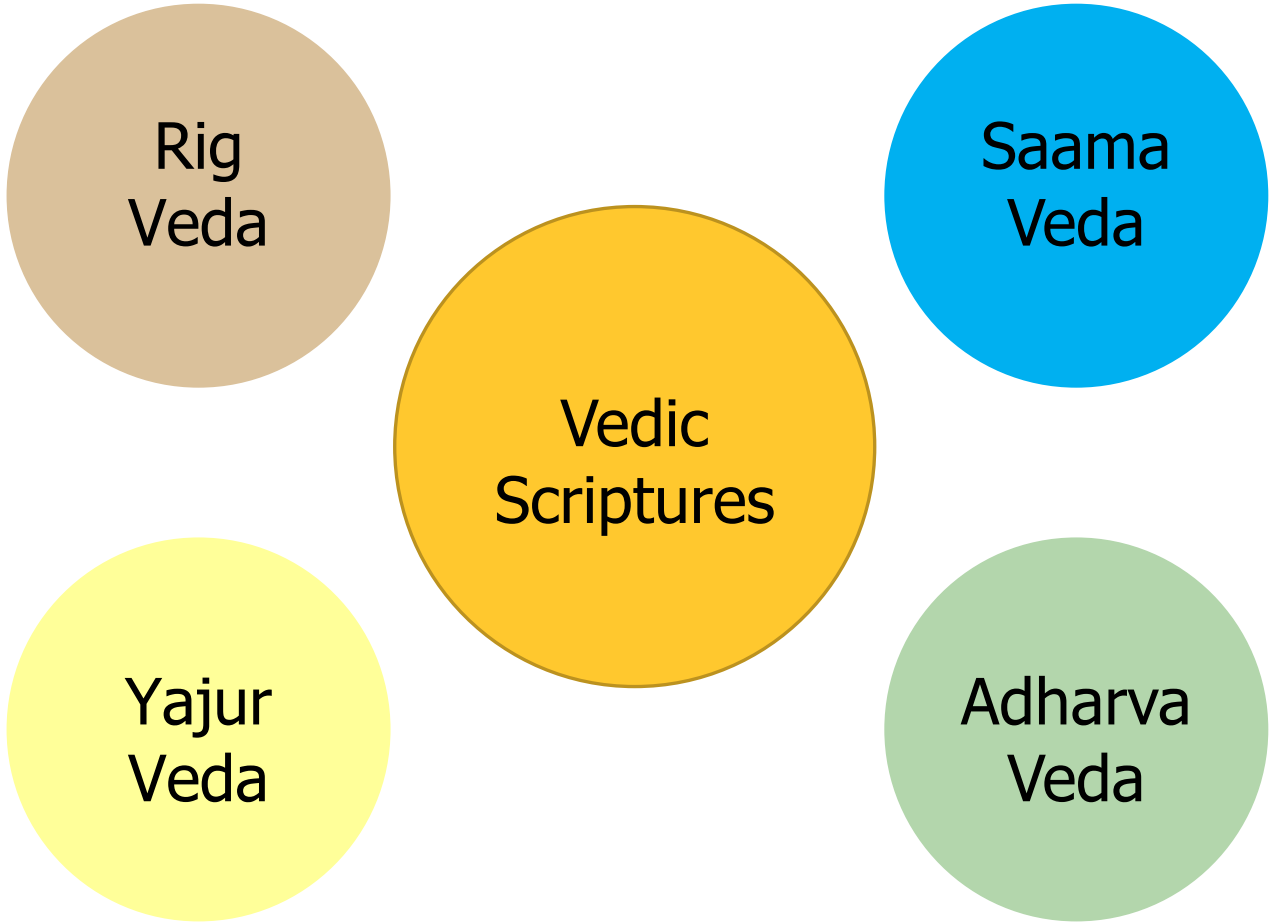
PUF Limitations

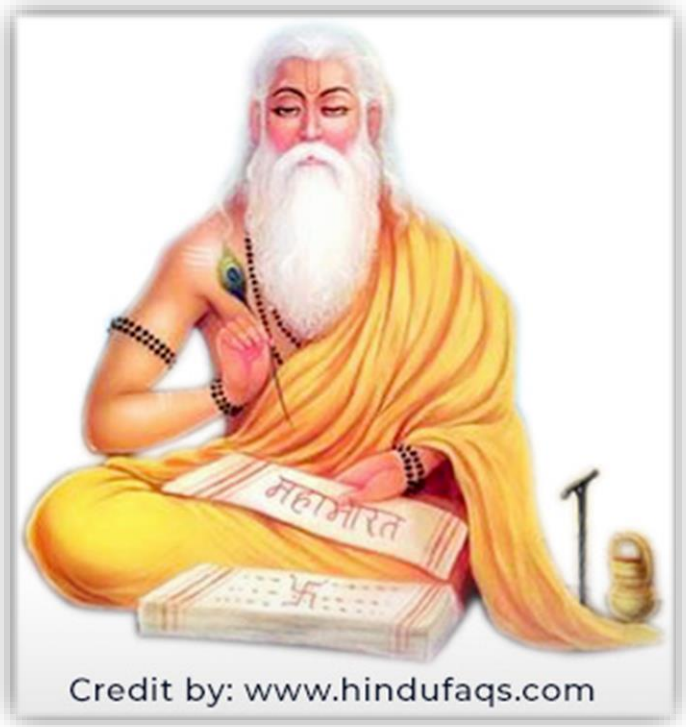
Larger key requires larger chip circuit.



1 – Bit Arbiter PUF Architecture

Vedas – Ancient Indian Scriptures





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.,

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.

Jata and Ghana Patham

- Consider three words – b_1, b_2, and b_3.
- Following is the formula to recite the words in the Jata patham:
  - $\{b_1, b_2\}, \{b_2, b_1\}, \{b_1, b_2\}$
- Following is the formula to recite the words in the Ghana patham:
  - $\{b_1, b_2\}, \{b_2, b_1\}, \{b_1, b_2,b_3\}, \{b_3, b_2,b_1\}, \{b_1, b_2,b_3\}$
- Using the formula above, a 128-bit key is transformed into a 2.5Kbit key in the processing algorithm.

Ghana Paatham

Original Verse:

gaṇānāṁ tvā gaṇapátigm havāmahē

Ghana Paatham (considering first 3 words):

gaṇānāṁ tvā tvā gaṇānāṁ gaṇānāṁ tvā gaṇapátiṃ gaṇapátiṃ tvā gaṇānāṁ gaṇānāṁ tvā gaṇapátim ॥

Ghana Paatham

Original Verse:

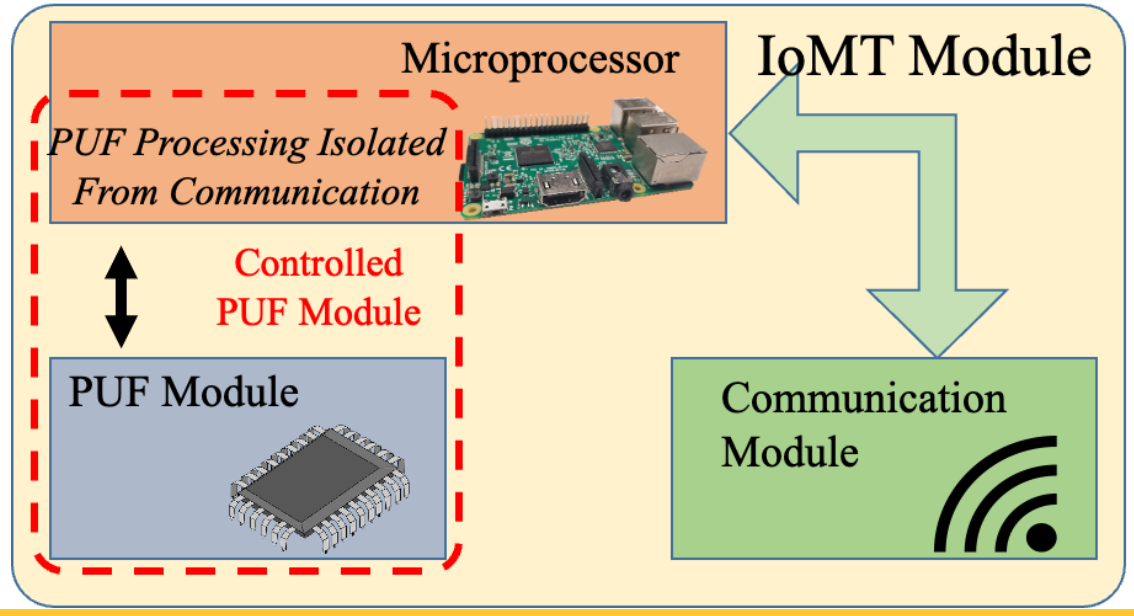
gaṇānāṁ tvā gaṇapátigm havāmahē

Ghana Paatham (considering words 2, 3, and 4):

tvā gaṇapátim gaṇapátim tvā tvā gaṇapátigm havāmahē havāmahē gaṇapátim tvā tvā gaṇapátigm havāmahē

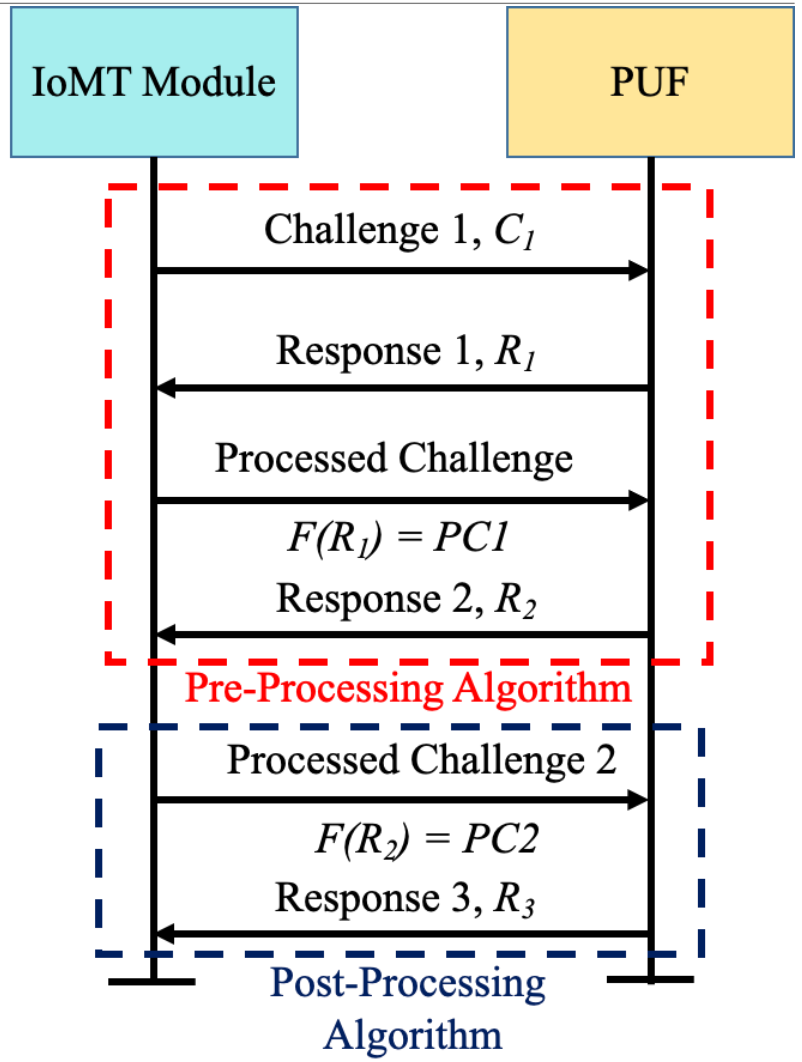
Proposed Veda – PUF Architecture

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



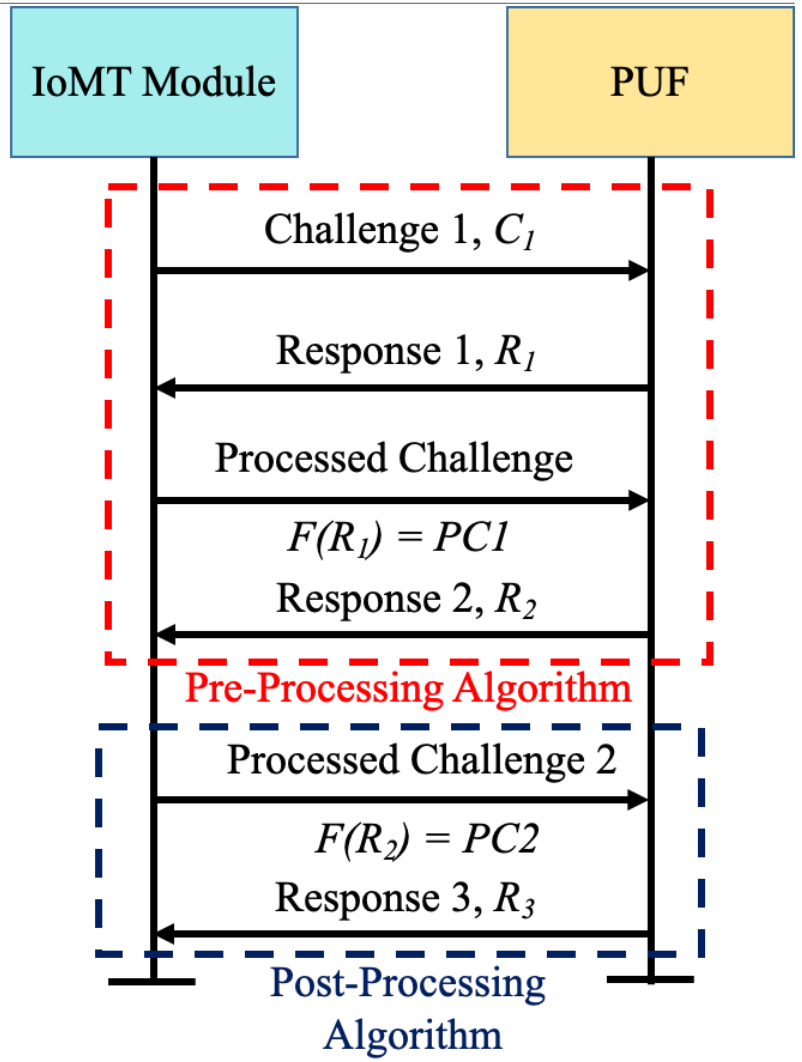
Proposed Controller Algorithm for Veda – PUF

- 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.

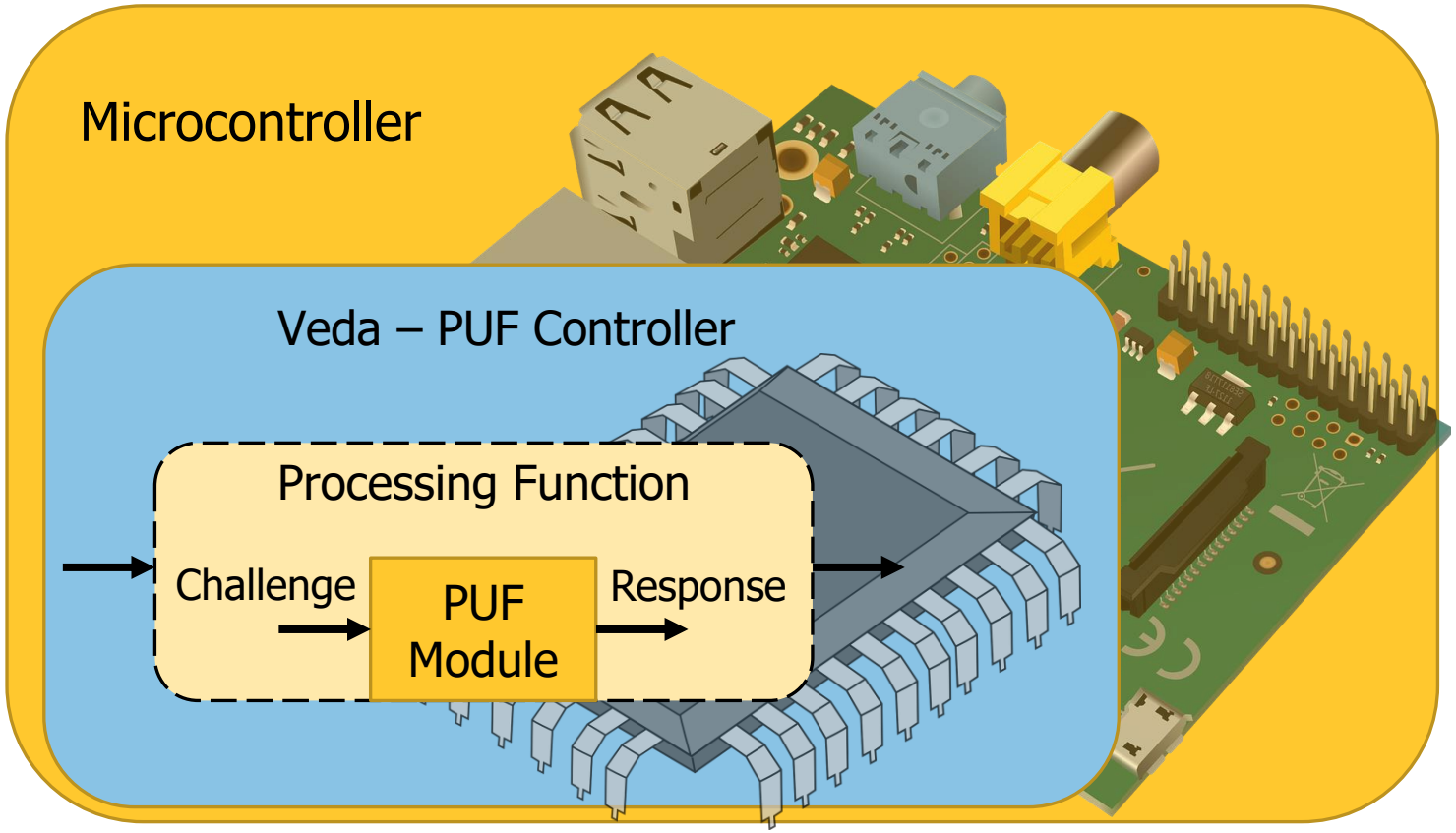


Key Processing Function Veda – PUF

- Considering the following binary key:
  - $b_1, b_2, \ldots b_n$
- Ghana Paatha formula is used for the bits b_1 -> b_{n-1}.
- Jata Paatha formula is used for the last two bits.

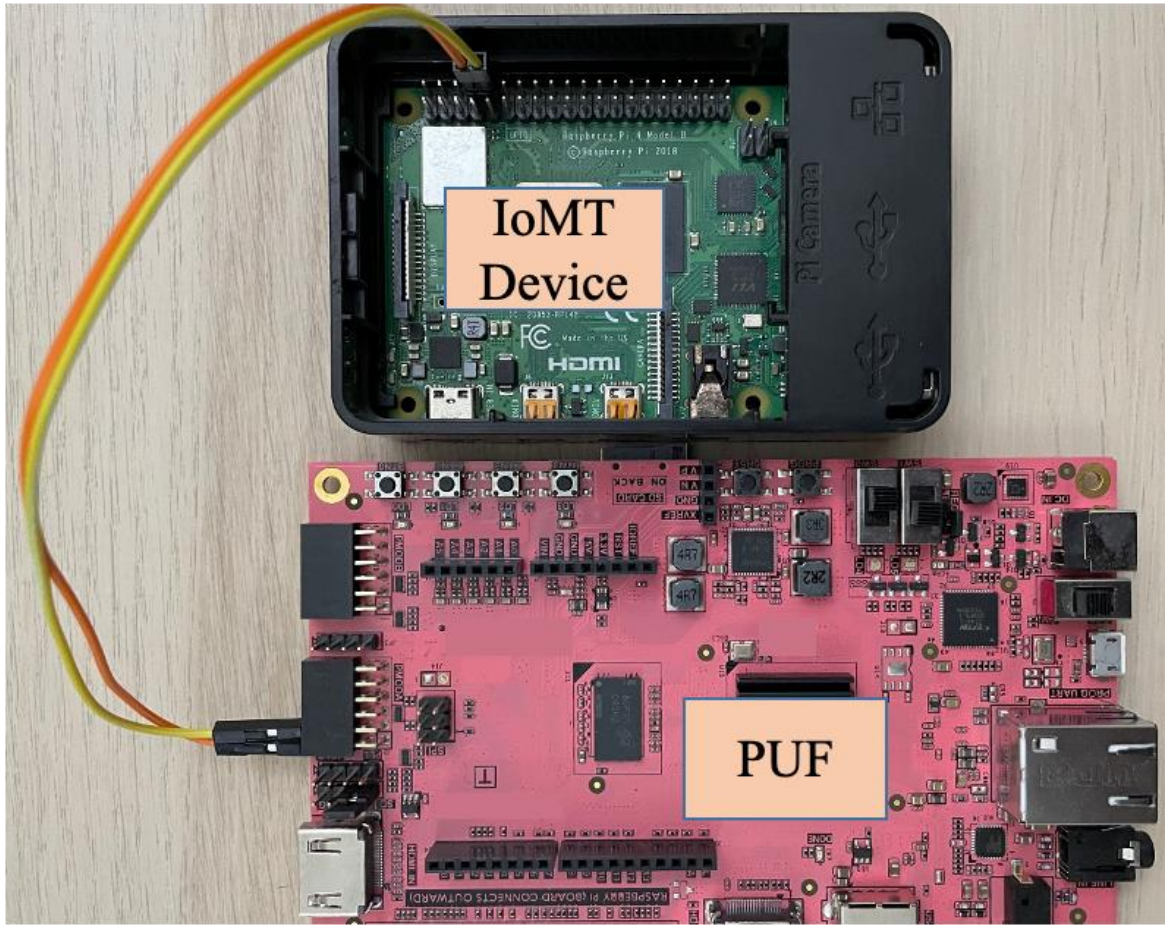


Veda-PUF Circuits



Experimental Setup

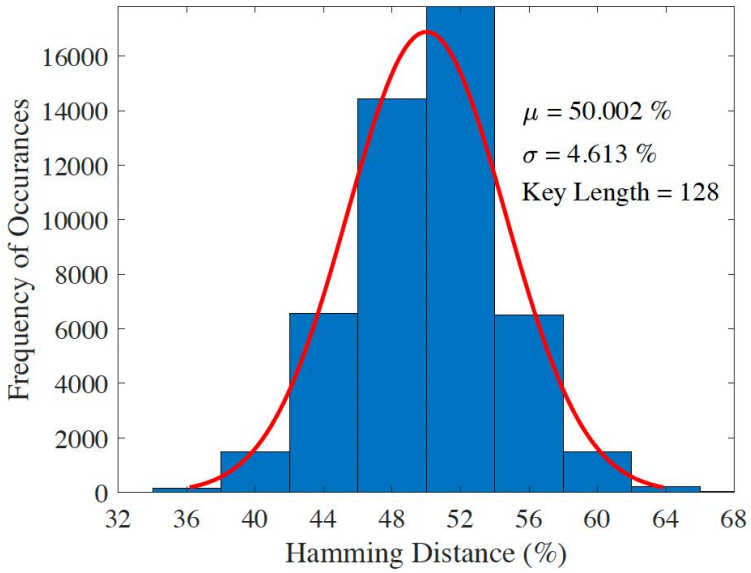
- Initial Considerations:
  - Initial challenge length is 128 – bits.
  - 1000 keys were generated.
  - Raspberry Pi– Key Generation IoMT device.
  - FPGA – PUF.



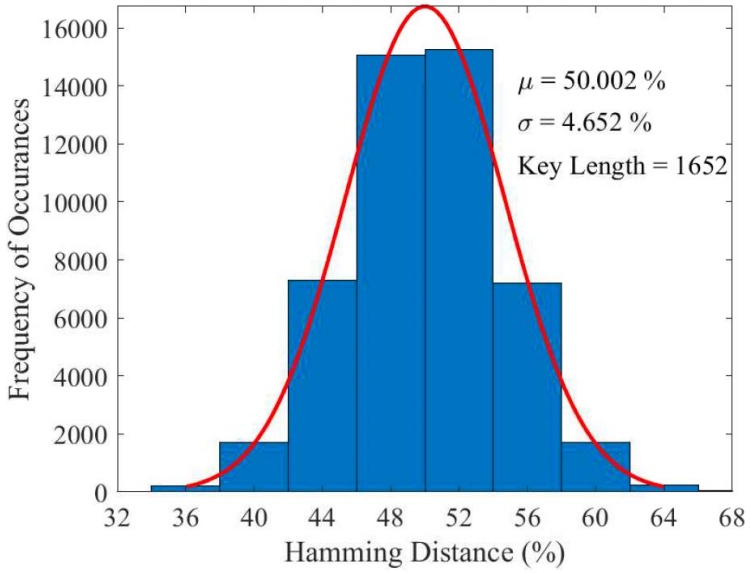
Figures of Merit (FOMs) of PUF

- Uniqueness
  - Property of PUF to generate unique keys for multiple challenges.
  - Unique keys generated across multiple PUF modules.
- Randomness
  - Equal distribution of 1 and 0 across the binary keys.
- Reliability
  - Generate the same Challenge Response pair under various circumstances.

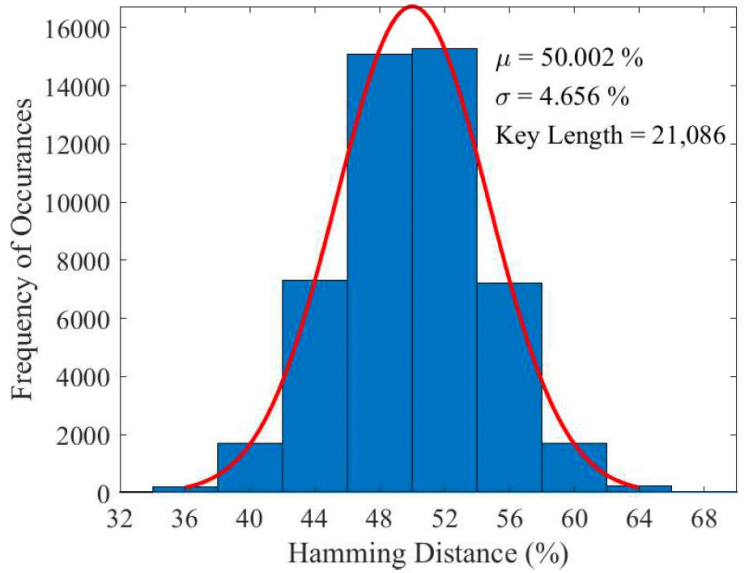
Uniqueness



(a) Uniqueness of Original Keys

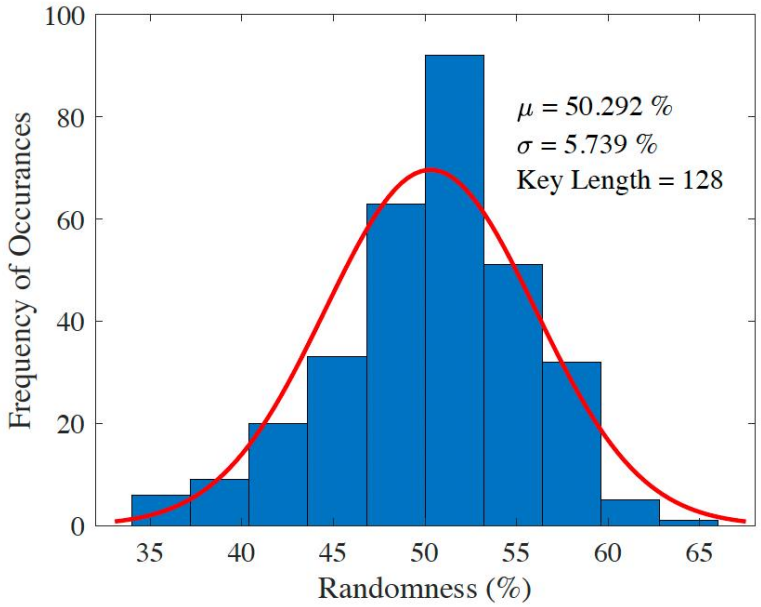


(b) Uniqueness of Processed Keys

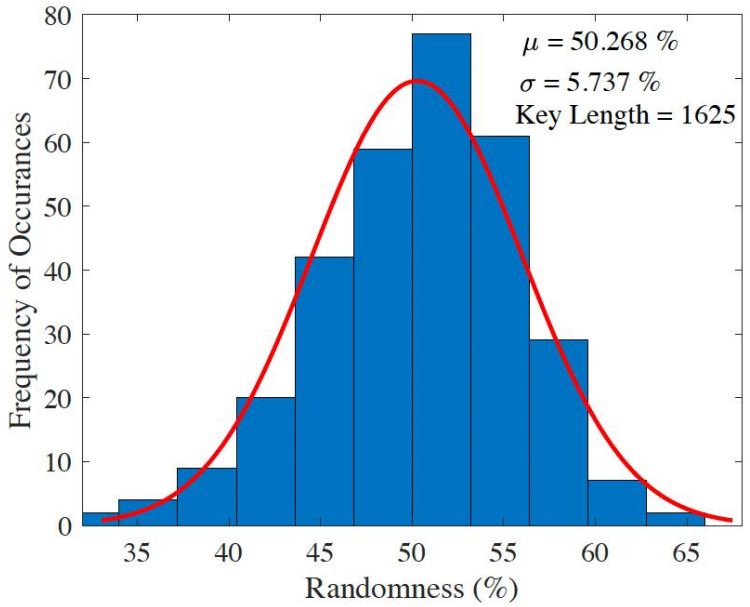


(c) Uniqueness of Keys Processed a Second Time

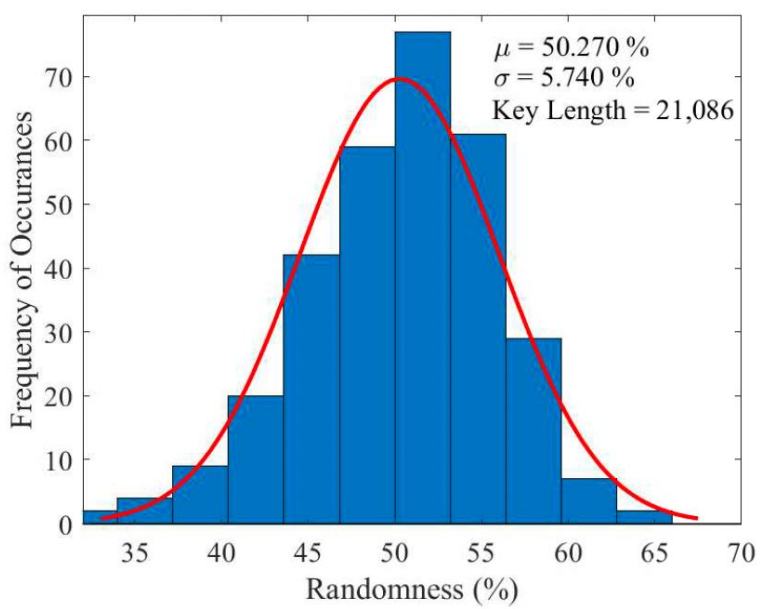
Randomness



(a) Randomness of Original Keys



(b) Randomness of Processed Keys



(c) Randomness of Keys Processed a Second Time

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.

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

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.

Acknowledgement

The authors would like to thank Mr. Dendukuri Swamynatha Sarma for his help on Vedic Literature and Ghana Patham.


THANK
YOU