PUF and TRNG in FPGA

R.RAJA ADHITHAN

Project Associate,SETS-Chennai

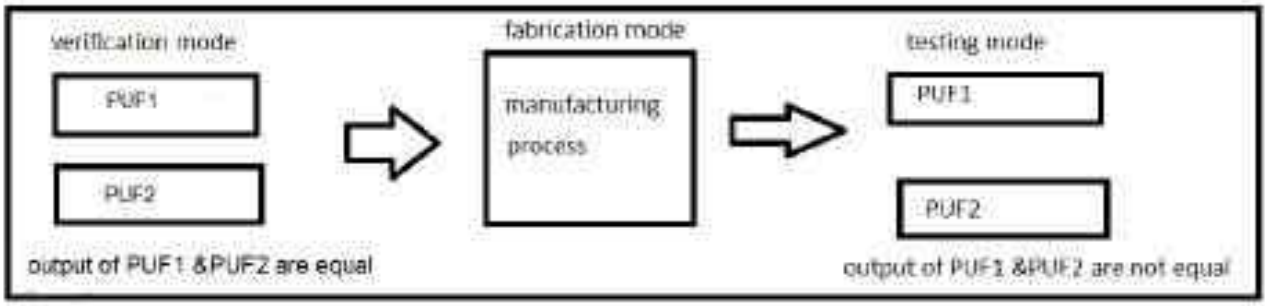
October 22,2020

OBJECTIVES

- PUF Concept.
- Classification OF PUF
- Application OF PUF
- Security analysis of PUF
- TRNG

PUF Concept

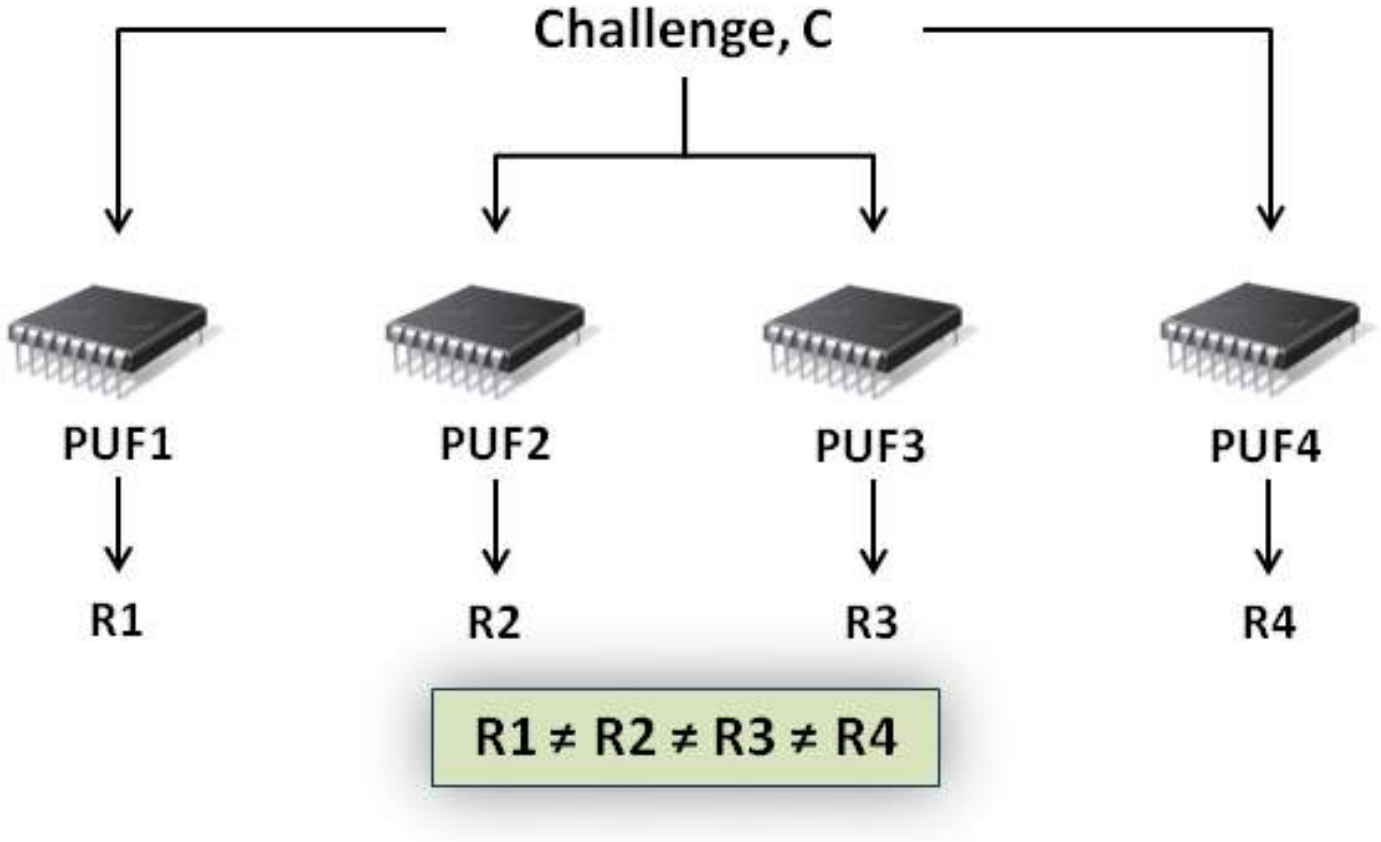
- The Circuits which have same functionality that use the manufacturing process variation to generate the unique nature of ICs. The circuit is termed as PUF.(unique nature of ICs is used as digital fingerprint for ICs, like biometric for human)



- PUF1 and PUF2 are same, but PUF1 and PUF2 are slightly different due to manufacturing process variation.

Strong PUF

- It has large number of challenge response pair
- It is used for Device Authentication and Identification



Weak PUF

- It has small challenge-response set (some time no or one fixed challenge)
- This is used for key generation,seed for PRNG
- Eg:Memory based PUFs

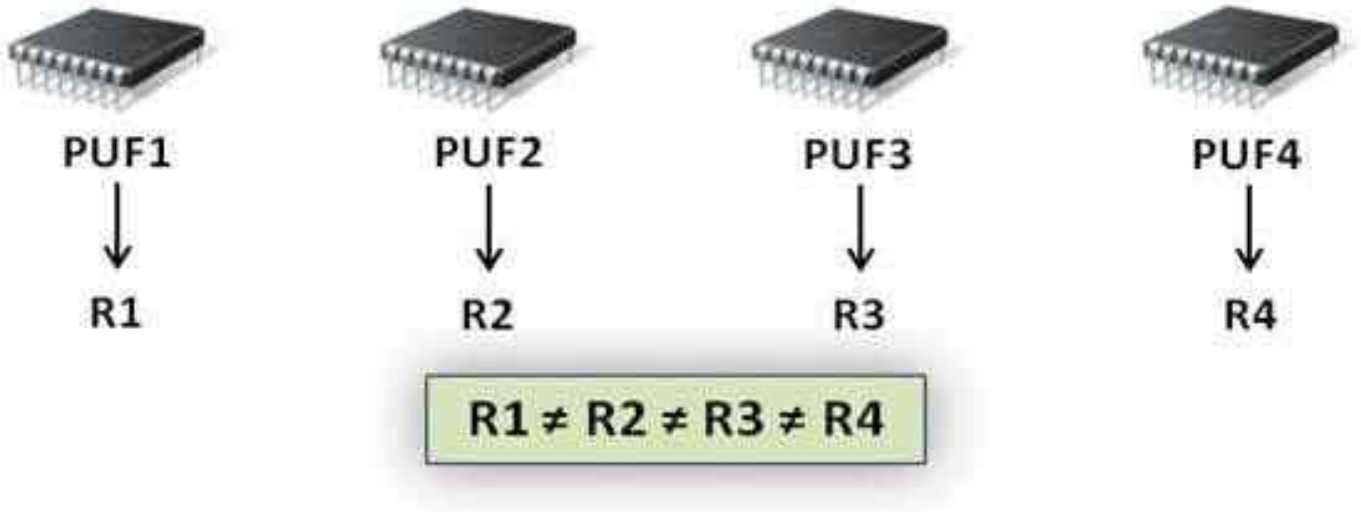
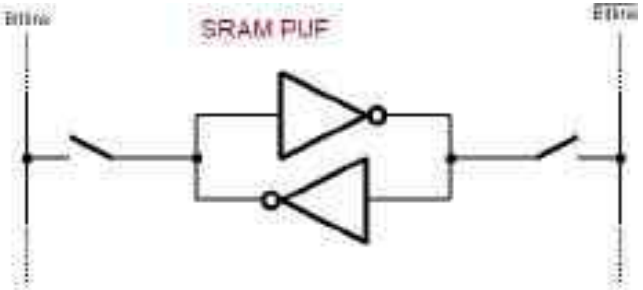


Figure 1: Weak PUF

Memory Based PUFs

Commercially Available PUF

OTP PUF,SRAM PUF are two memory based PUFs are commercially available PUF in the market



Research Proposed PUF

There are also different type of PUFs are under research such as ReRAMPUF,MRAM,PUF,DRAM,Flash PUF.

a) ReRAM PUF: Y.Yoshimoto et.al,2016.
b)MRAM PUF: Jayita Das et.al,2015.
c)DRAM PUF :F.Tehranipoor et.al,2017
d)Flash PUF :Moon-seok Kim et al,2015.

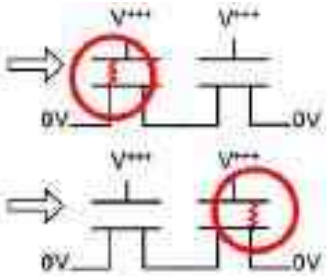
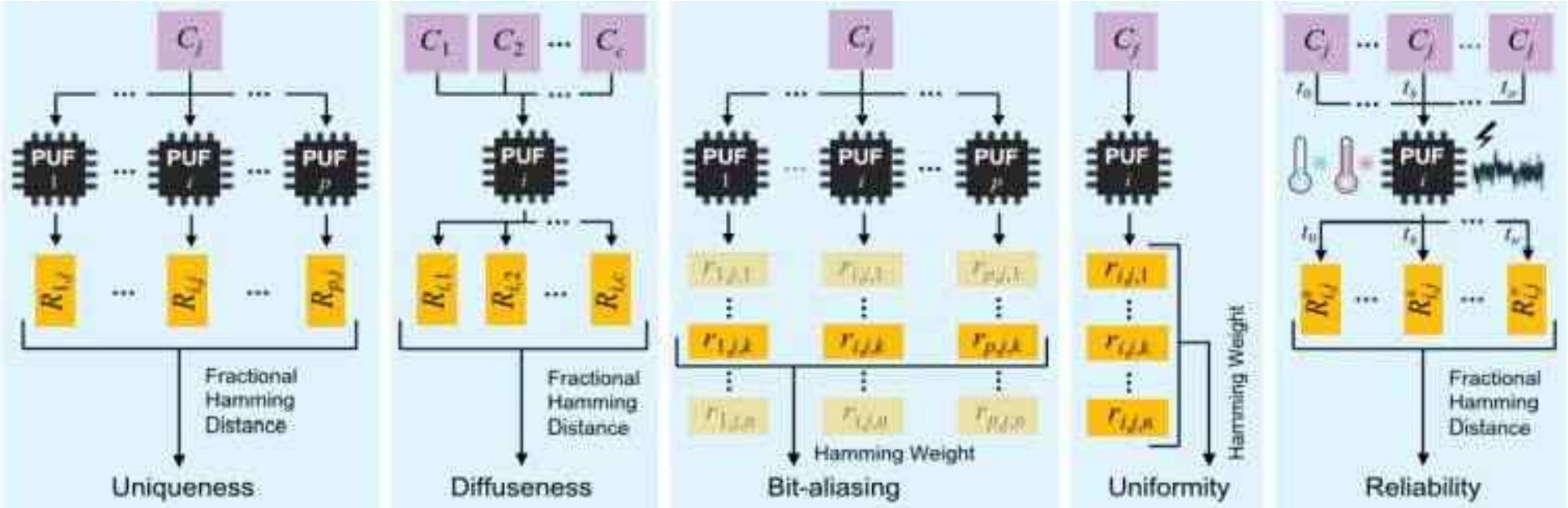


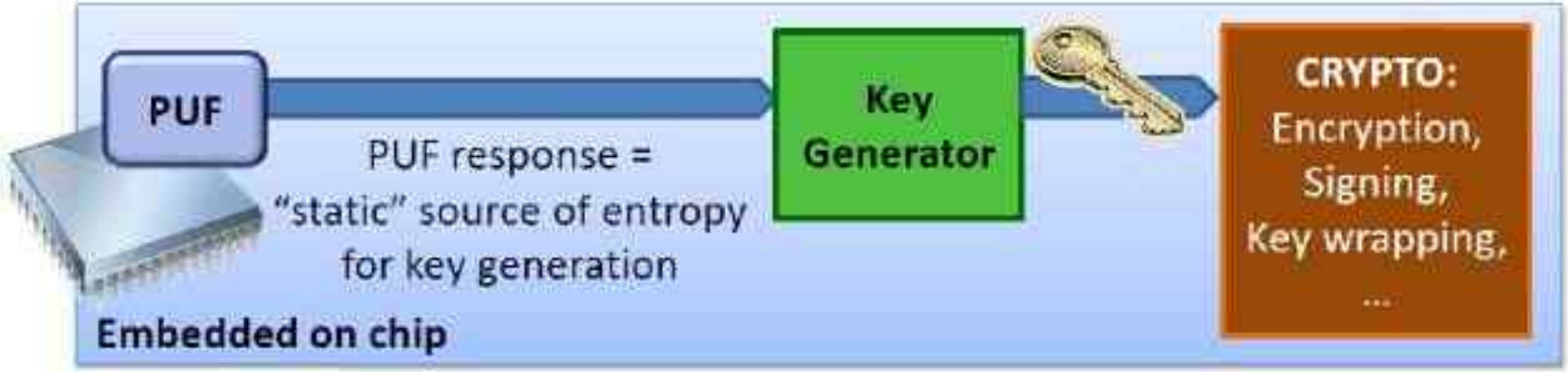
Figure 2: OTP PUF(based on oxide breakdown)

PERFORMANCE ANALYSIS OF PUF



- Uniqueness: each device has its own signature
- Diffuseness: Not the same response for two challenges
- Bit-aliasing: happens when different chips may produce nearly identical PUF responses, which is an undesirable effect
- Uniformity: determines how uniform the proportion of 0's and 1's are in the PUF response
- Reliability: the PUF response is always the same, whatever the noise and environment

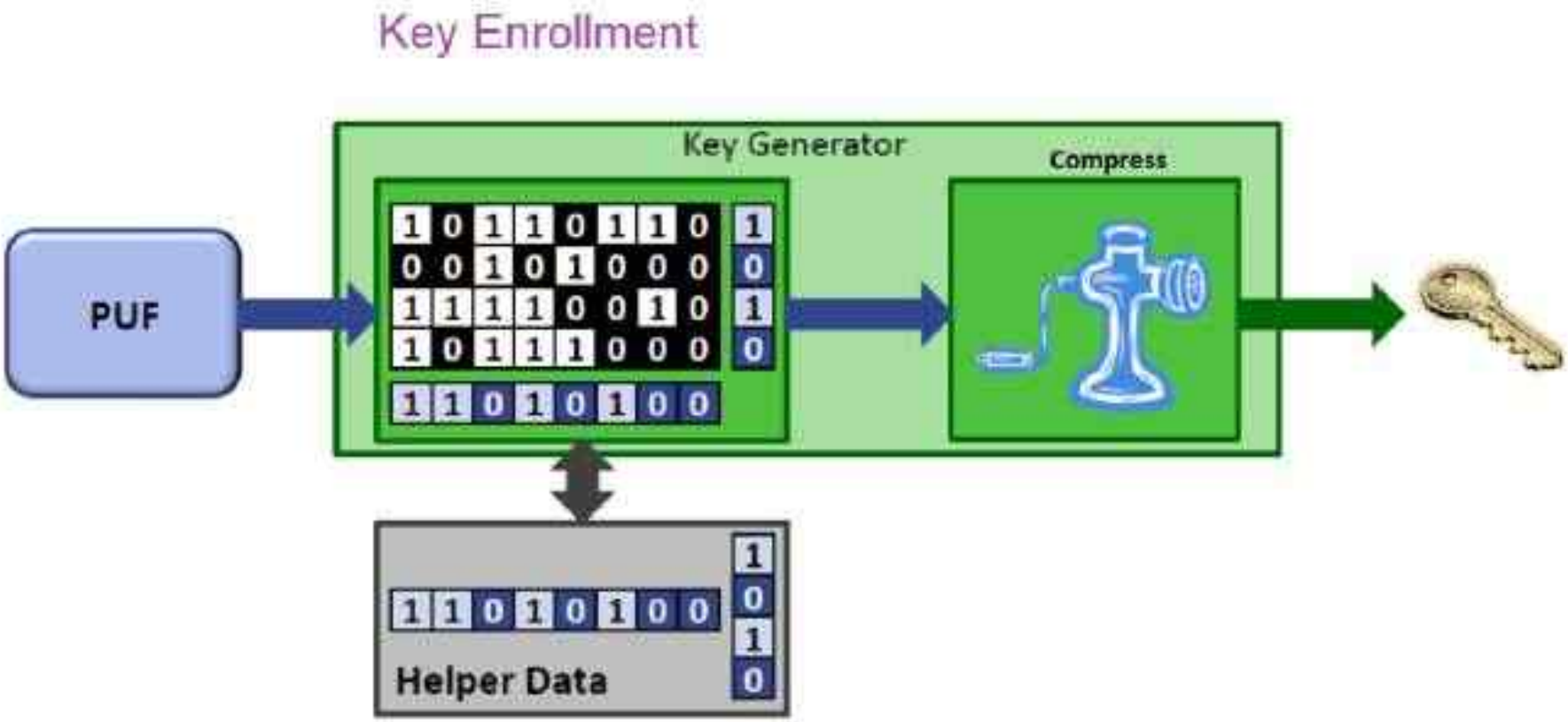
PUF Applications - Key Generation



- In general weak PUF is used as intrinsic key generator
- No key present when device is powered down.
- Key depends on device intrinsic randomness
- Example:SRAM PUF,OTP PUF,Via PUF etc.

Key Generation

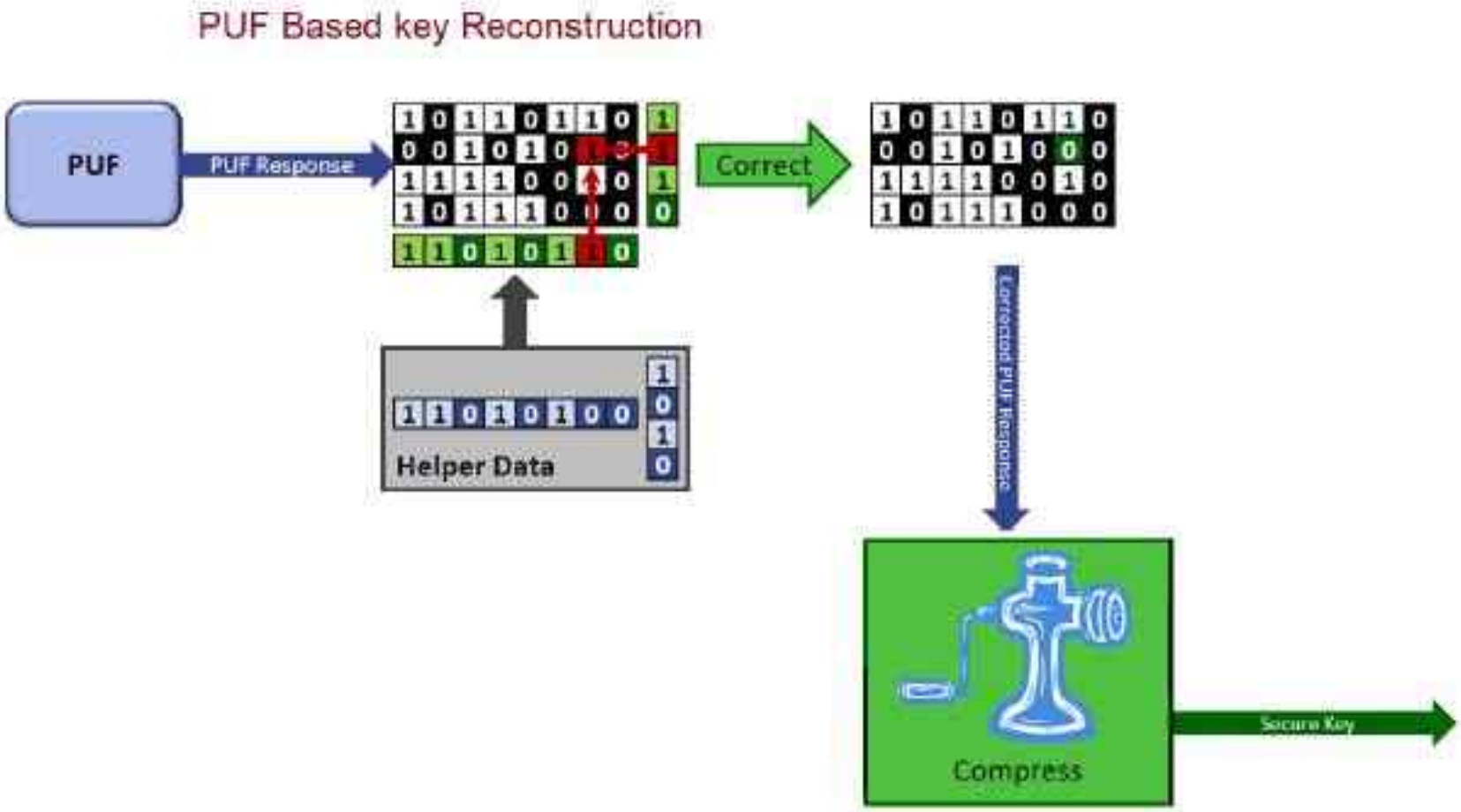
Key Enrolment



- Key Enrollment is nothing but stable key generation
- In conventional crypto algorithms helper data is used as public key and compressed key is used as private key

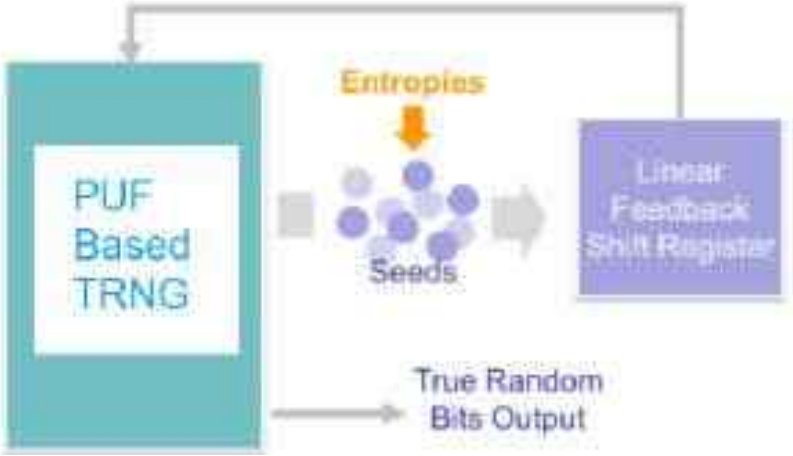
Key Generation

Key Reconstruction



- Key Reconstruction is nothing but retrieving the original key by using helper data

True Random Number Generator



- PUF based TRNG randomness pass all NIST tests
- PUF TRNG provides high quality random seeds
- Post processing or Hardware tuning is unnecessary because of completely true random bits
- Unique TRNG sampling space for chip to chip

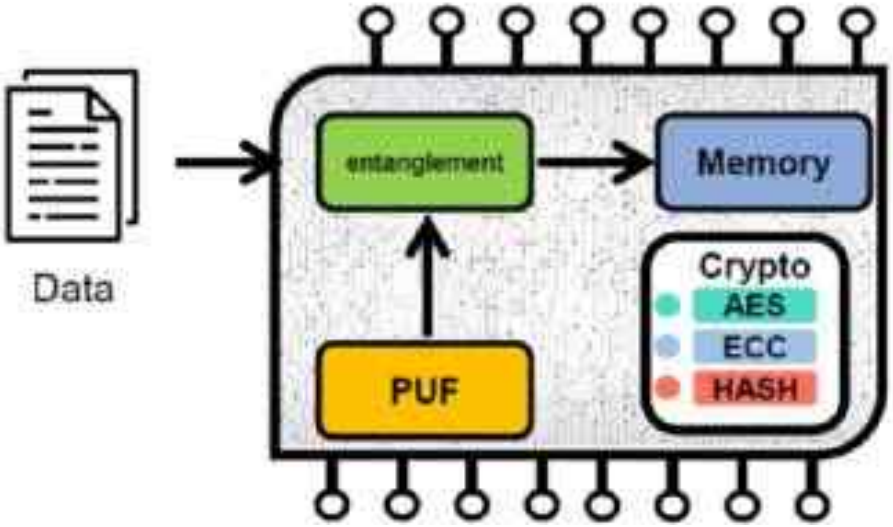
Authentication

Using Strong PUF

Figure 3: Strong PUF based Authentication

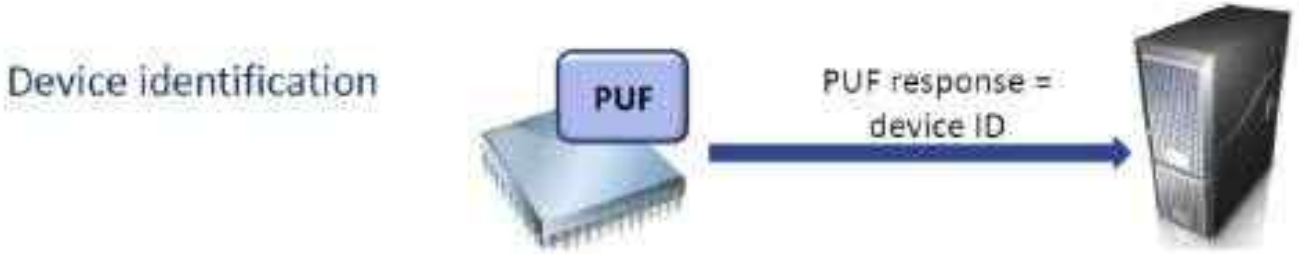
- The Authentication is done by Challenge Response Pairs(CRPs)
- Obtained CRPs compared with the CRPs which are stored in the database

Secure Storage



- Secure storage is essential for IoT devices.
- PUF can be the intrinsic root of trust for secure storage
- Data can be protected by entangling with the PUF secret
- Because it doesn't involve complex cryptographic algorithms, which require higher power consumption
- Secure storage can prevent the data from being stolen, tampered, and accessed while unauthorized.

Onchip Unique ID



- Direct ID: use PUF itself as unique ID
  Eg:OTP PUF,Via PUF
- Indirect ID: Inject ID store by"Secure Memory" concept
- No risk of cloning
- Eg:ID Cards,passport,Driving license,Drone ID etc.

IP Protection

Secure IP using PUF

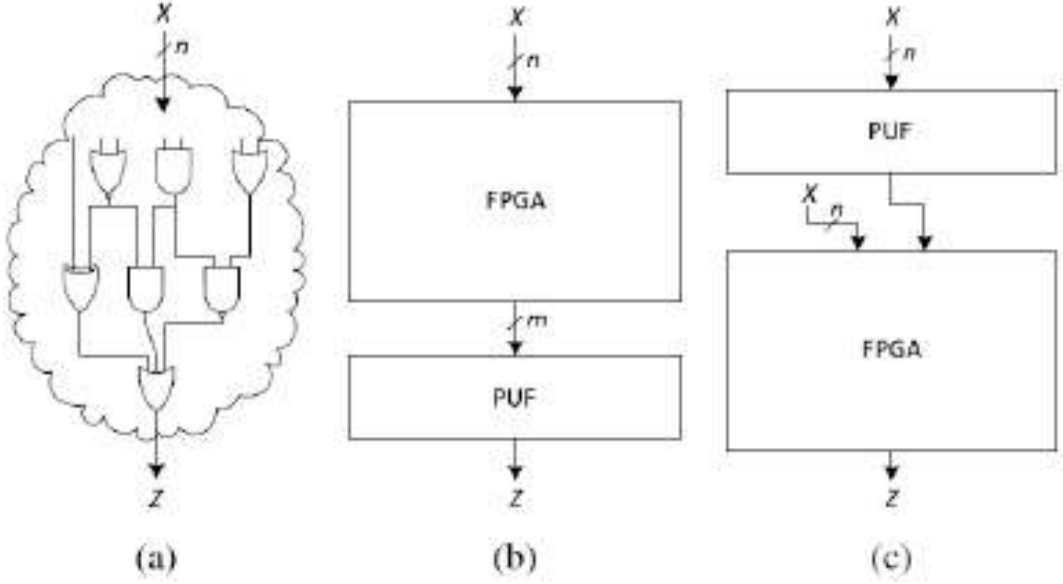


Figure 4: Three architectures implementing the same functionality. (a) Arbitrary circuitry. (b) PUF-based logic using a preceding FPGA. (c) PUF-based logic using a preceding PUF

- In the above Fig(a) is a example of a hardware IP which can be protected by either Fig(b) or Fig(c) configuration

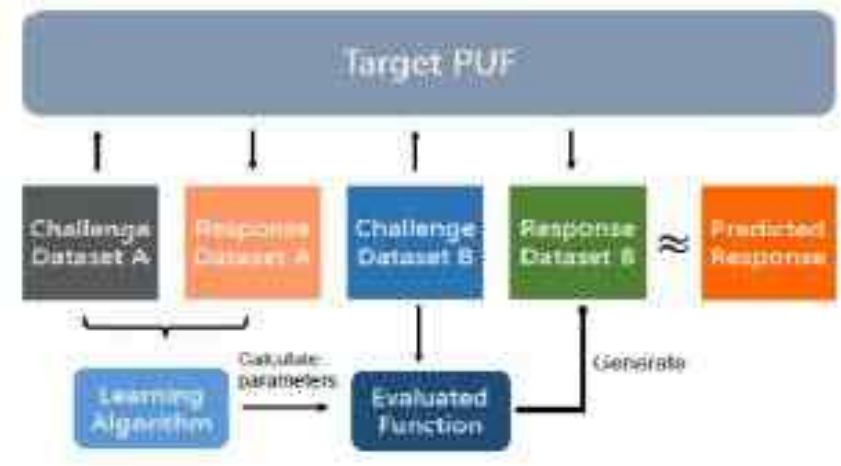
Attacks possible in PUF,when implementing in crypto applications

- PUF does not have good reliability every time, So there should be a need of error correction block for key generation , that can be vulnerable to side channel attack.
- PUF is used for authentication without a crypto module . but its CRPs kept public that leads to modelling attacks.

PUF Security Analysis

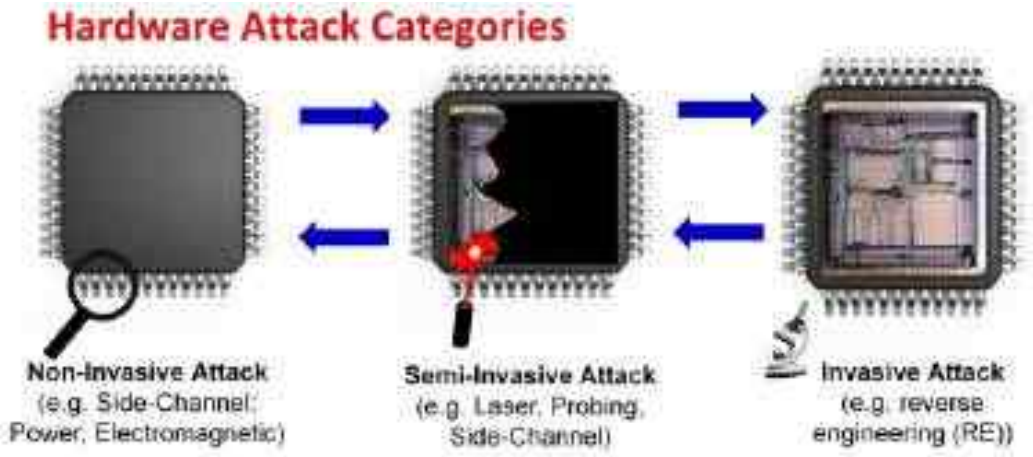
PUF could be attacked by the following methods:

1. Modelling Attacks
   - Step 1:Collecting adequate CRPs
   - Step 2:Choosing an appropriate model or algorithm (usually machine learning algorithms)
   - Step 3:Calculating the parameters with the provided CRPs
   - Step 4:With the trained model and a new challenge, one can predict the response without the PUF circuit

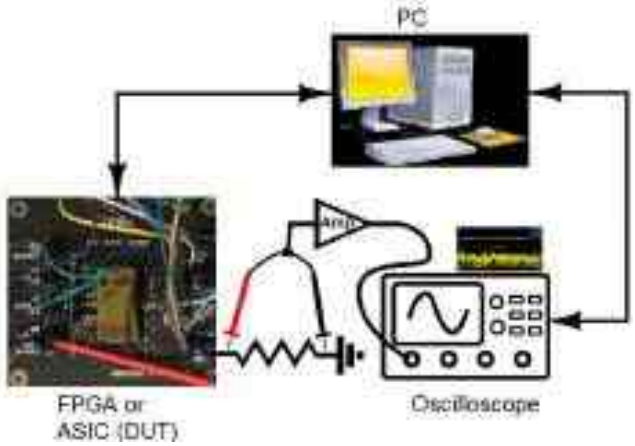


Modeling Attacks: More suitable for Strong PUFs (i.e., delay based PUFs)

Security Attacks on PUFs

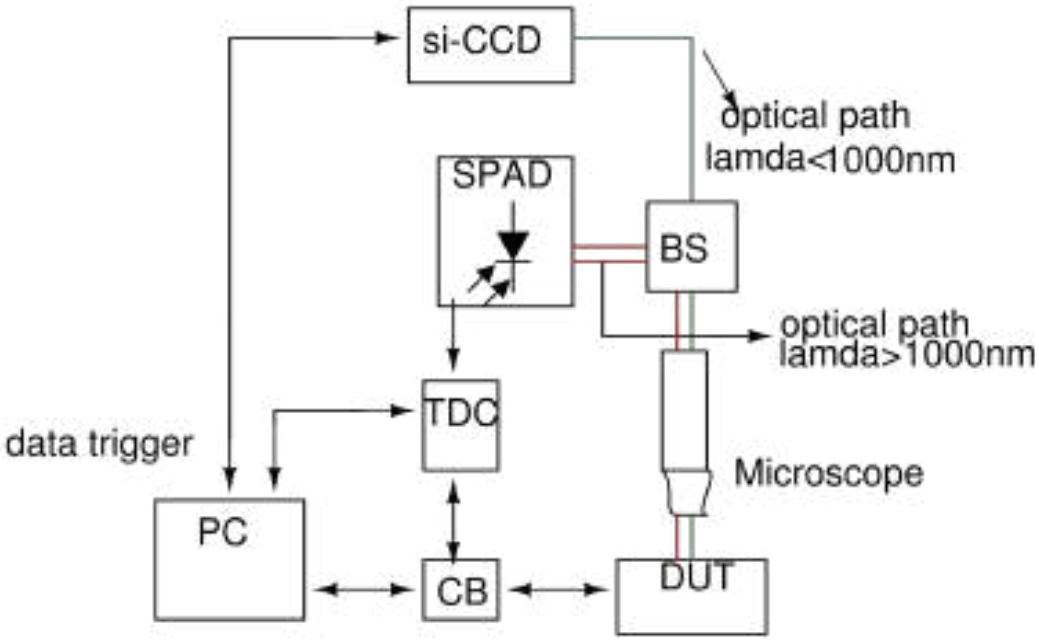


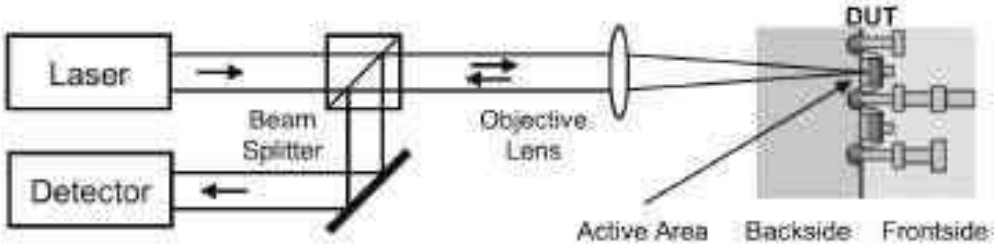
- Non-Invasive attacks
  - Power Analysis (PA) Attack[Arbiter PUF]
  - Electro-Magnetic (EM) Analysis Attack[RO,TERO PUF]
  - Data Remanence (DR) Attack [SRAM PUF]
  - Fault Injection Modeling (FIM) Attack[RO PUF]



Security Attacks on PUFs

- Semi-Invasive attacks
  - Photon Emission Analysis (PEA) Attack[RO PUF]
  - Semi-invasive EM Attack[RO PUF]
  - Laser Fault Injection (LFI) [RO PUF]
  - Optical Contactless Probing (OCP) [RO PUF]
- Invasive attacks[SRAM PUF]
- Cloning attacks[SRAM PUF]





Security Attacks on PUFs

Specifications	Attack Location	Attack Detection Chances	IC Damage Level	Attack Based on	Attack Cost (Relative)	Observed In
PA Attack [13,41]	External to the chip	Low	Low	Power Leakage	Low	Soft-BD PUF [13] Loop PUF [41]
EM [26,42,41] Attack	On the chip	Low	Low	EM Emission	Moderate	RO PUF [26], TERO PUF [42] Loop PUF [41]
PEA Attack [39]	On the chip	Low to Moderate	Low	Photon Emission	High	RO PUF [39]
OCP Attack [23]	Back side of the chip	Moderate	Low	Reflections of Photons	High	RO PUF [23]
DR Attack [46,2]	External to the chip	Moderate	Low	Remanance Decay	High	SRAM PUF [46,2]
FIM Attack [15]	External to the chip	High	Low	Injecting faults and modelling	Moderate	RO PUF [15]
LFI Attack [40]	On the chip	High	High	Injecting Laser	High	RO PUF [40]
SIEM Attack [27]	On the chip	Moderate	High	Injecting EM	High	RO PUF [27]
Cloning Attack [17]	On the chip	High	High	FIB	High	SRAM PUF [17]

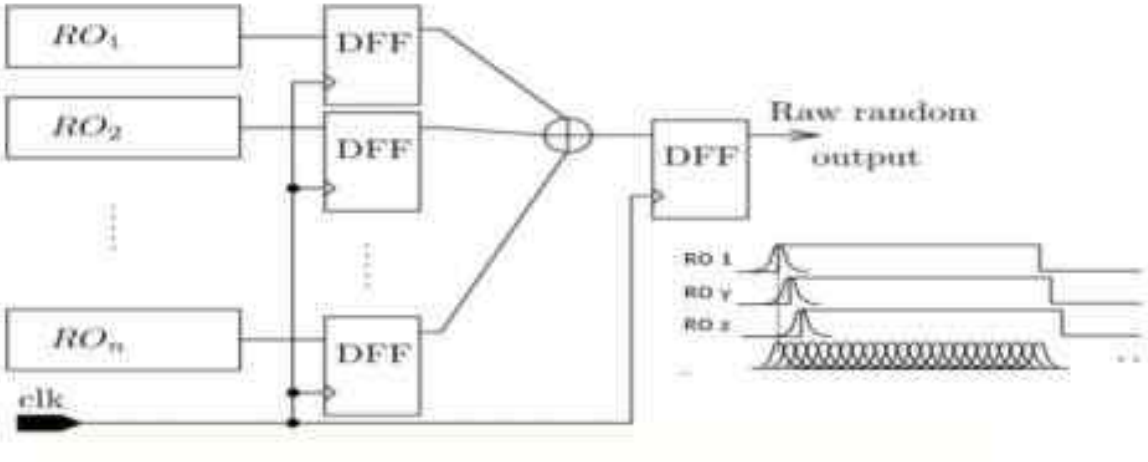
Figure 5: Comparative Analysis of Implementation Attacks on variants of PUFs

Countermeasures

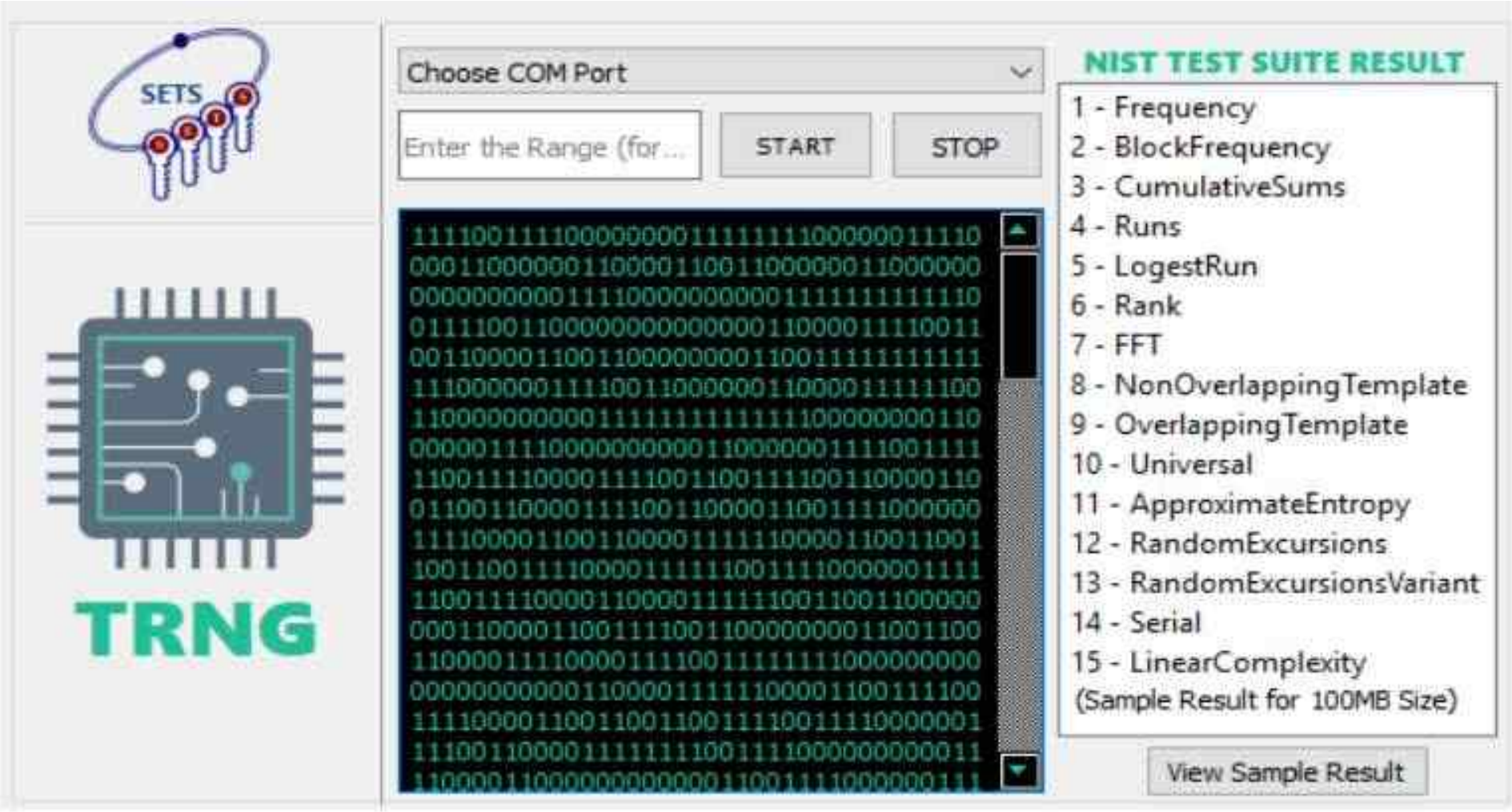
- Countermeasure for Modeling attack
  - challenge obfuscation
  - adding non linearity
- Countermeasure for Non-invasive attack
  - Temporal masking to protect the PUF from power and EM attacks
  - Randomization of RO ,interleaved placement and using Current starved inverters in the RO PUF design instead of normal inverters to prevent the EM attack
  - obfuscation of the memory and defining a specific minimum power-off time to SRAM to make data remanence attack harder
- Countermeasure for semi-invasive attack
  - obfuscated key registers by randomizing their order
  - randomized reset states of the registers
- Countermeasure for Invasive attack
  - serialized PUF implementation that exposure of the PUF response
  - implementing an asynchronous reset such way to destroy information inside the SRAM.

TRNG

- To generate unpredictable random number
- Source of Randomness : Clock jiter, Meta - stability



NIST TEST FOR TRNG



THANK YOU