2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

Cause Analysis Method of Entropy Loss in Physically Unclonable Functions

Mitsuru Shiozaki*, Yohei Hori†, Tatsuya Oyama*,
Masayoshi Shirahata*, Takeshi Fujino*

* Ritsumeikan university
† National Institute of Advanced Industrial Science and Technology

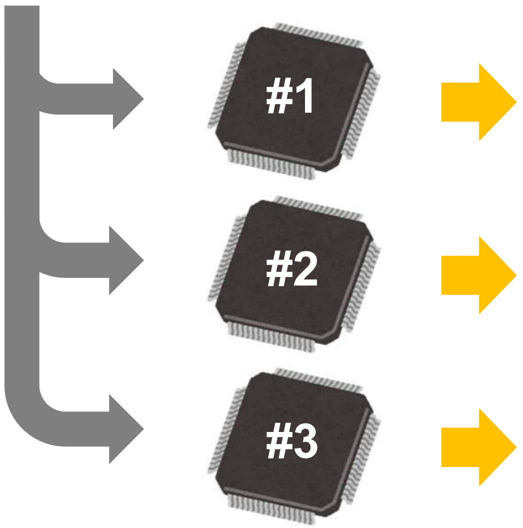
2020 IEEE International Symposium on Circuits and Systems
Virtual, October 10-21, 2020

This work is based on results obtained from a project commissioned
by the New Energy and Industrial Technology Development Organization (NEDO).

Physically unclonable functions

- ✓ Physically unclonable functions (PUFs) extract inherent physical properties from variations in manufacturing
- ✓ A PUF provides security to low-cost applications such as IoT
- ✓ Challenge-and-response authentication and key generation are well-known applications using PUFs

Identically designed chips



Challenge

	#1	#2	#3	#4		#N
#1	0	1	1	0	···	0
#2	1	0	1	1	···	1
#3	1	0	0	0	···	1

Device-unique responses (Unique ID)

Our Contribution

- Organization of the causes of entropy loss during implementation
- Proposal of a method for analyzing the causes
- Demonstration of the validity of our proposed method using our PUFs

✓ The following methods are used to show the performance of a PUF
  - Inter-/Intra-HD
  - Statistical Test (NIST SP 800-22)
  - **Min-entropy estimation** (NIST SP 800-90B)

✓ In some cases, a PUF designer should understand the causes of entropy loss before estimating the min-entropy

[Example] Ring-oscillator PUF (RO PUF)
The number of ROs: N_{RO} → The number of PUF-response bits: $N_{RO} \times (N_{RO} - 1) / 2$
However, the number of IDs depends on the oscillation-frequency ordering.
(The number of output IDs: $N_{RO}!$)
Therefore, When estimating the min-entropy, a designer should encode the frequency ordering to a bit vector.

*Roel Maes, et. al., "PUFKY: A Fully Functional PUF-based Cryptographic Key generator," Cryptographic Hardware and Embedded Systems (CHES), pp.302-319, 2012.

Inter-HD

- ✓ Inter-HD is the comparison characteristic of PUF responses from two different PUF chips
- ✓ The calculated value means how unique output IDs of a specified length (i.e., 128 bits) are

$$\boldsymbol{D}^{inter} = \left[\boldsymbol{HD}\left(y_{i_1}^{j}(x_k);\, y_{i_2}^{j}(x_k)\right)\right] \quad \forall 1 \le i_1 \ne i_2 \le N_{puf};\ \forall 1 \le k \le N_{res};\ \forall 1 \le j \le N_{meas}$$

$$\mu^{inter} = \frac{2}{N_{puf} \cdot \left(N_{puf} - 1\right) \cdot N_{res} \cdot N_{meas}} \sum \boldsymbol{D}^{inter}$$

$$\sigma^{inter} = \sqrt{\frac{2}{N_{puf} \cdot \left(N_{puf} - 1\right) \cdot N_{res} \cdot N_{meas} - 2} \sum \left(\boldsymbol{D}^{inter} - \boldsymbol{\mu}^{inter}\right)^2}$$

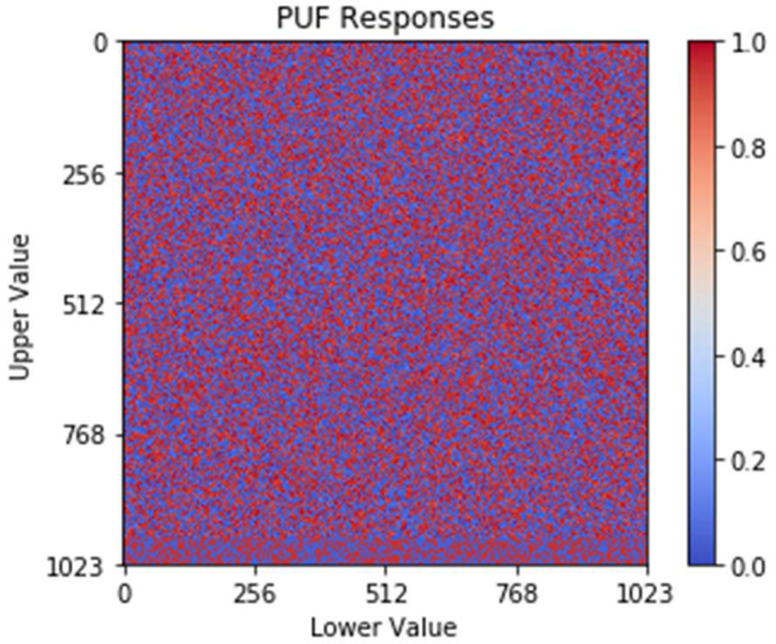
N_{puf}	: Number of devices
N_{res}	: Number of PUF-response bits
N_{meas}	: Number of repeated measurements on each device

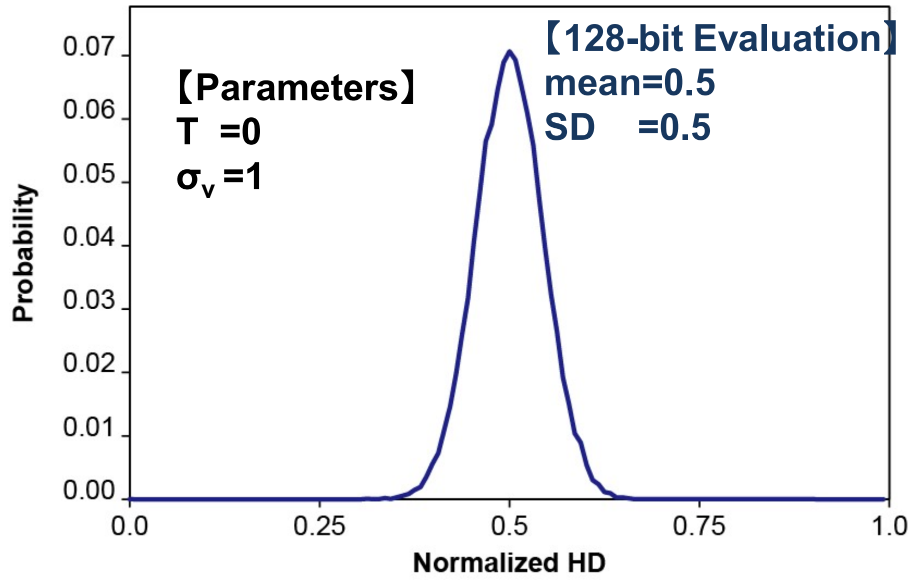
Result of Ideal PUF Model

- ✓ Inter-HD of an ideal PUF model is calculated
  - ➢ The total number of PUF-Response bits : 1M (=2^{20})
  - ➢ Entropy : 1M bits per device

【Ideal PUF model】

$$R_{p,r} = \begin{cases} 0 & (v_{p,r} \leq T) \\ 1 & (v_{p,r} > T) \end{cases} \qquad v_{p,r} \sim N(T, \sigma_v) \qquad \begin{array}{l} \forall 1 \leq p \leq 250\ (= N_{puf}) \\ \forall 1 \leq r \leq 2^{20}\ (= N_{res}) \end{array}$$





Really good PUF?

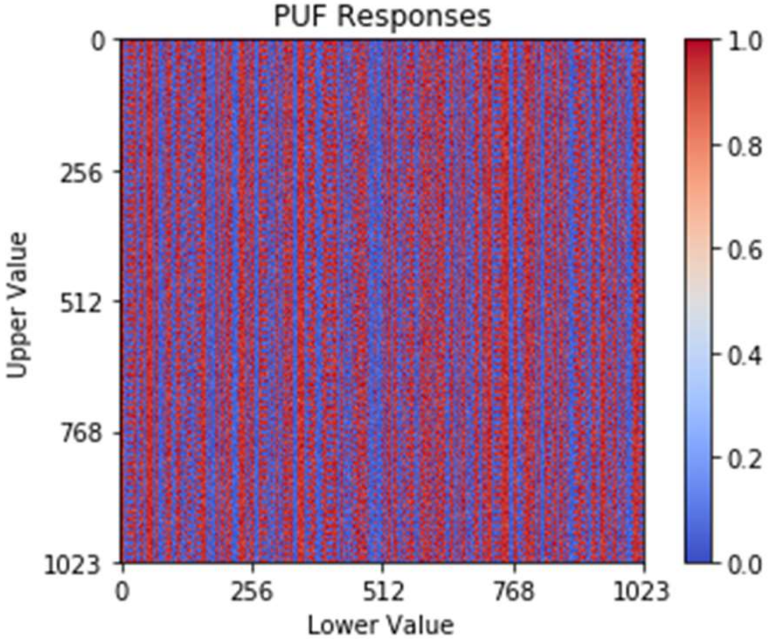
✓ Inter-HD of the bad PUF model is calculated

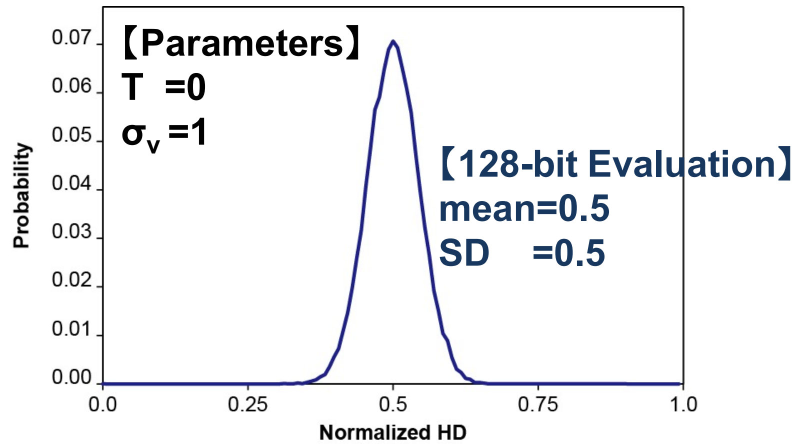
- ➢ The total number of PUF-Response bits : 1M (=2^{20}) bits
- ➢ Entropy : 2,048 bits per device

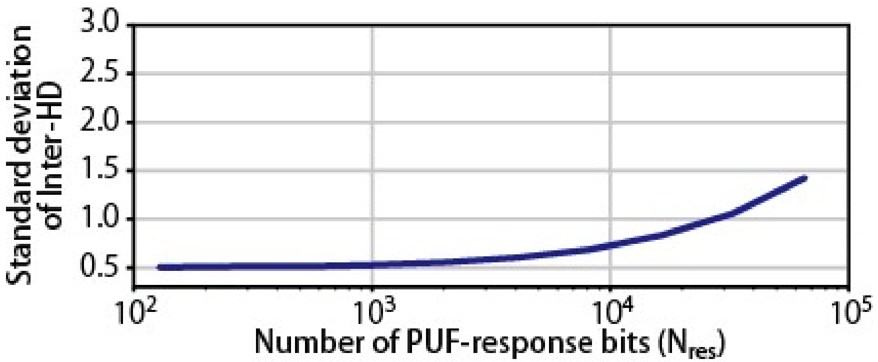
【Bad PUF model】

$$R_{p,r} = \begin{cases} 0 & (v_{p,r'} \leq T) \\ 1 & (v_{p,r'} > T) \end{cases} \quad \begin{array}{l} \forall 1 \leq p \leq 250 \quad (= N_{puf}) \\ \forall 1 \leq \boldsymbol{r'} \leq 2048\ (= N_{res}) \\ \boldsymbol{r' = r \bmod 2048} \end{array}$$

$$v_{p,r'} \sim N(T, \sigma_v)$$







Classification of Causes

✓ We classify causes of entropy loss into the following three types

- Source bias
- Generation scheme
- Multiple sources

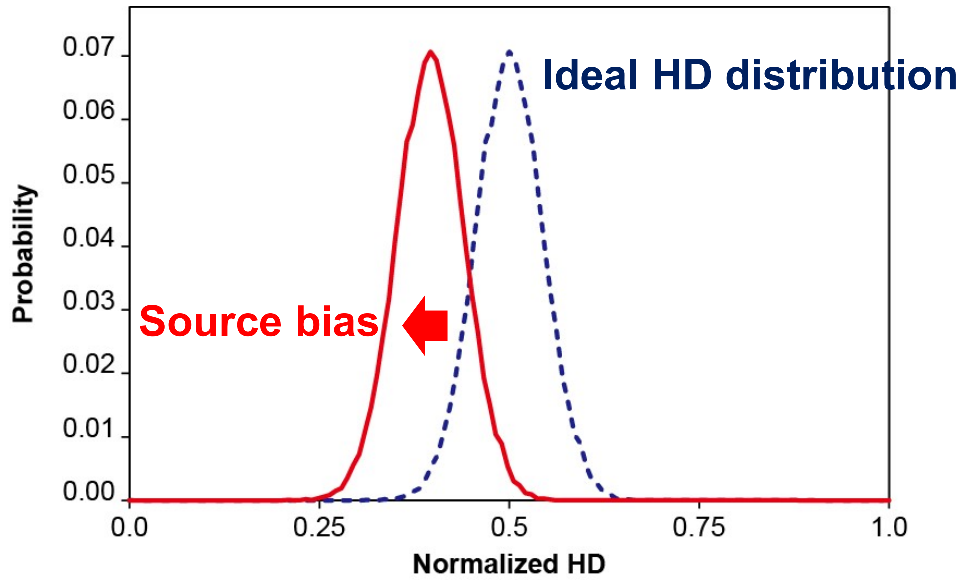
Source bias

- ✓ Basic cause
- ✓ Example: unbalanced layout in an LSI chip
- ✓ PUF-response bits are biased to '1' or '0'
- ✓ The mean of Inter-HD becomes lower than 0.5 of the ideal value

【PUF model with source bias】

$$R_{p,r} = \begin{cases} 0 & (v_{p,r} \leq T + \boldsymbol{\alpha}) \\ 1 & (v_{p,r} > T + \boldsymbol{\alpha}) \end{cases}$$

$$v_{p,r} \sim N(T, \sigma_v)$$

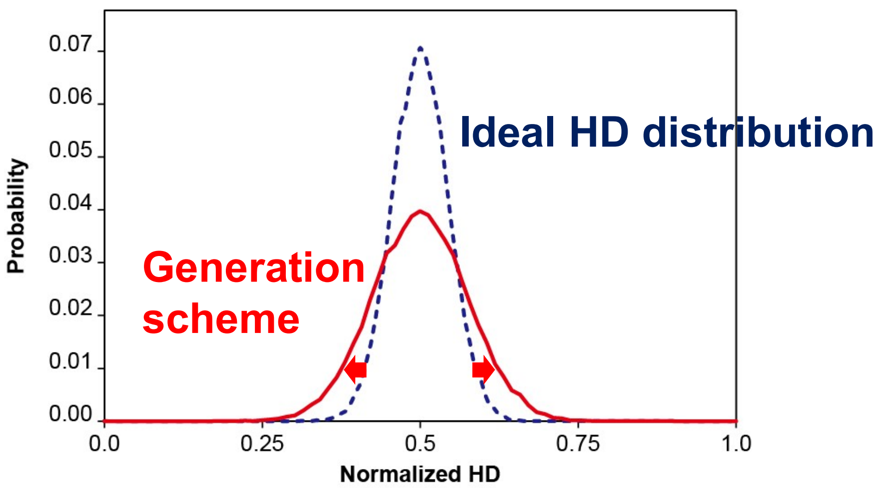


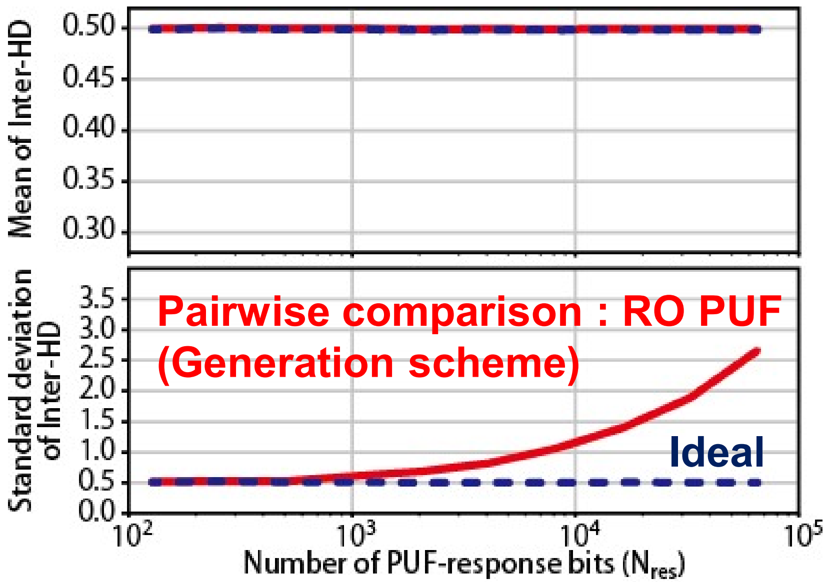
Generation scheme

- ✓ Algorithmic cause
- ✓ Examples: pairwise comparison, *k*-sum scheme
- ✓ The number of PUF responses becomes much higher than that of PUF sources
- ✓ The standard deviation of Inter-HD becomes larger

【PUF model with generation scheme】

$$R_{p,r} = \begin{cases} 0 & (f(v_{p,}, r) \leq T) \\ 1 & (f(v_{p}, r) > T) \end{cases}$$



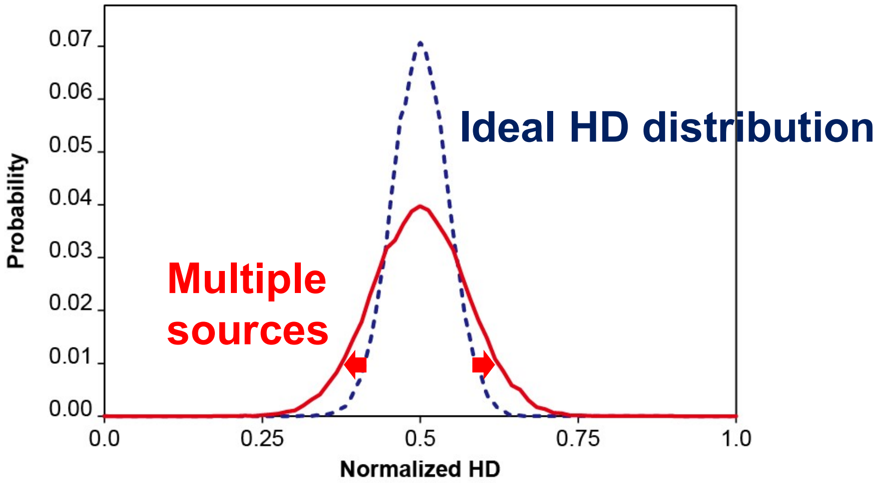


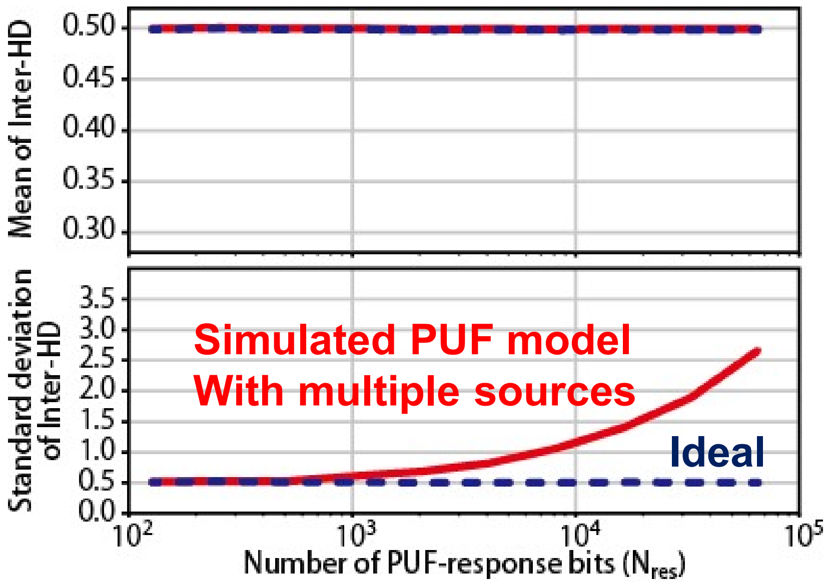
Multiple sources

- ✓ Physical cause
- ✓ Example: variation of digitizing circuits (i.e., sense amplifier, arbiter)
- ✓ PUF-response bits are biased to ‘1’ or ‘0’
- ✓ The standard deviation of Inter-HD becomes larger

【PUF model with multiple sources】

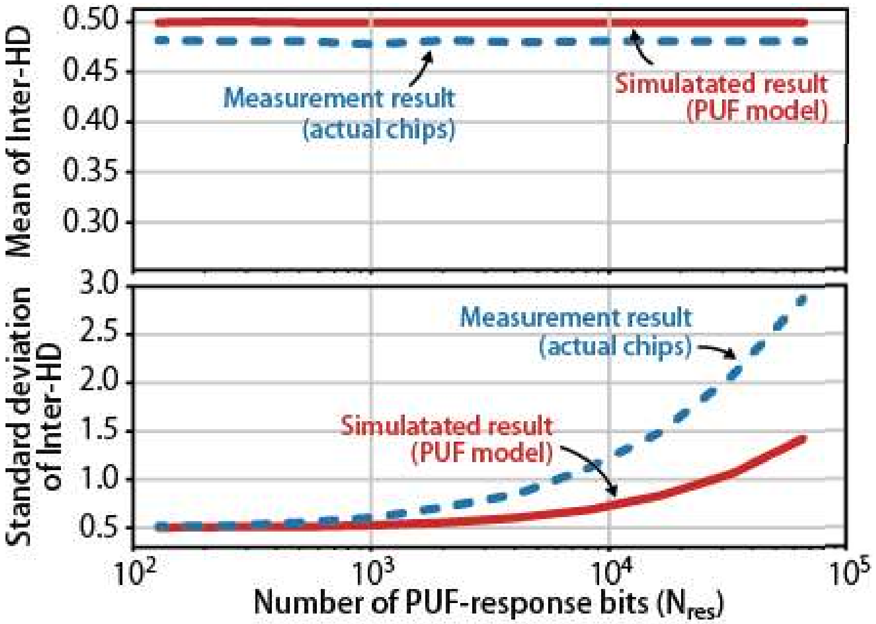
$$R_{p,r} = \begin{cases} 0 & (v_{p,r} + \boldsymbol{v'_p} \le T) \\ 1 & (v_{p,r} + \boldsymbol{v'_p} > T) \end{cases} \quad \begin{array}{l} v_{p,r} \sim N(T, \sigma_v) \\ v'_p \sim N(T, \sigma_{v'}) \end{array}$$





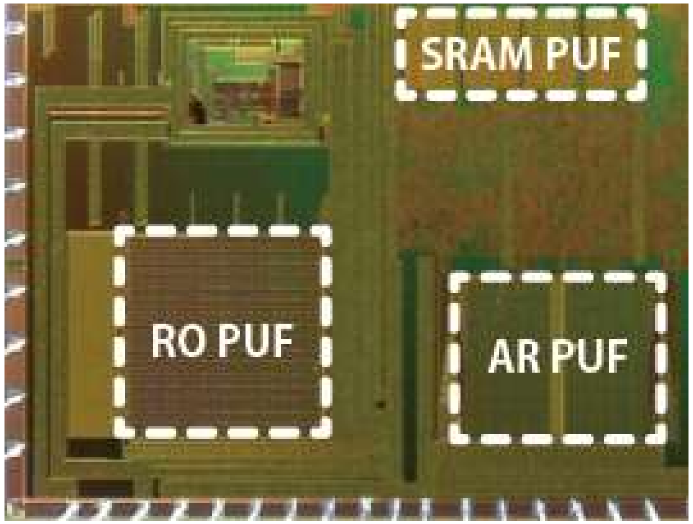
Our Proposal

- ✓ Our cause analysis method focuses on the trend toward a fluctuation in Inter-HD according to the PUF-response bits
- ✓ The trend of an actual PUF is compared to that of the PUF model with expected causes



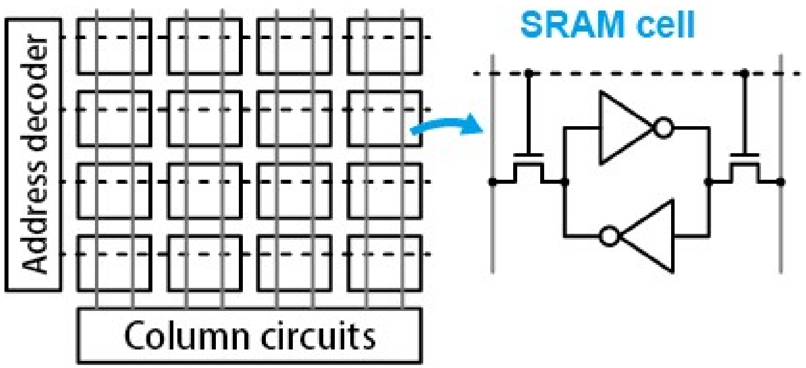
Experimental Environment

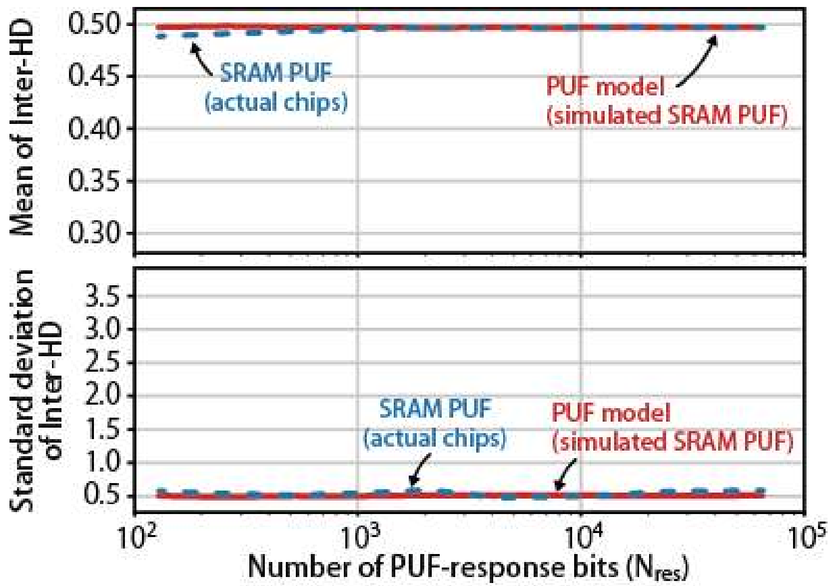
- ✓ Three types of PUFs were designed with a 180-nm CMOS process
  - ➢ SRAM PUF
  - ➢ Ring-Oscillator PUF (RO PUF)
  - ➢ Arbiter PUF (APUF)
- ✓ Measurement conditions
  - ➢ Number of PUF-response bits (N_{res}) : 65,536 bits (SRAM PUF), 20,480 bits (RO PUF, APUF)
  - ➢ Number of chips (N_{puf}) : 8
  - ➢ Number of repeated measurements (N_{meas}) : 100



SRAM PUF

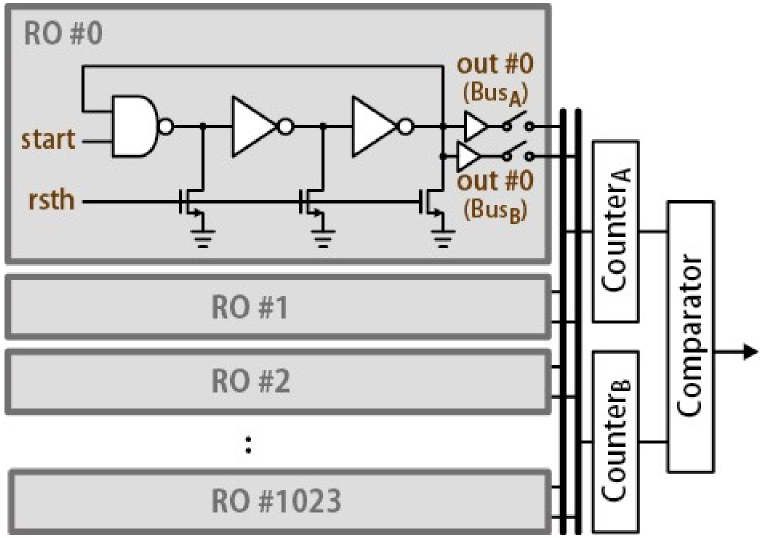
- ✓ An SRAM PUF uses initial start-up values of SRAM cells
- ✓ Our chip has 4 SRAM (1K word X 16 bit) standard cells
- ✓ The mean and standard deviation of Inter-HD were ideal values regardless of the number of PUF-response bits
- ✓ The PUF responses of our SRAM PUF are likely to be independent and identically distributed (IID)

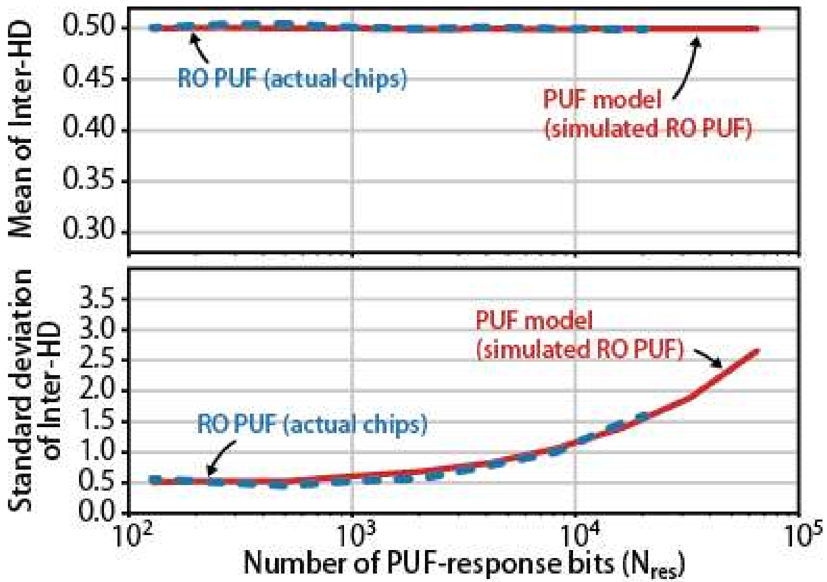




RO PUF

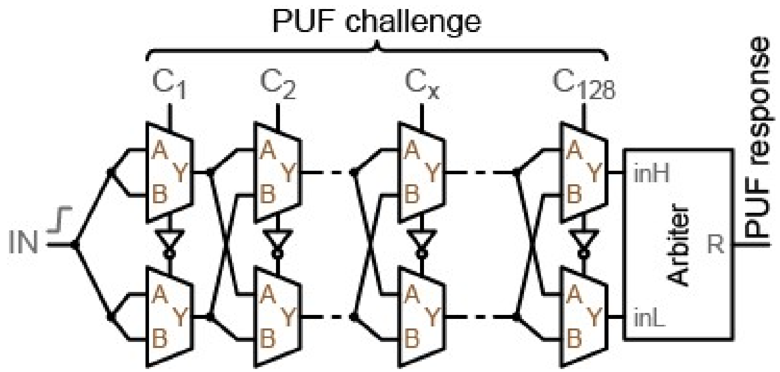
- ✓ An RO PUF extracts PUF responses from frequency variations of ROs
- ✓ Our RO PUF has 1,024 identically designed 3-stage-inverter ROs
  - ➢ Designed oscillation frequency: mean=33.3 MHz, SD=3.03 MHz
- ✓ Expected causes:
  - ➢ Pairwise comparison - Generation scheme
- ✓ Both the results using the actual chips and the PUF model corresponded approximately





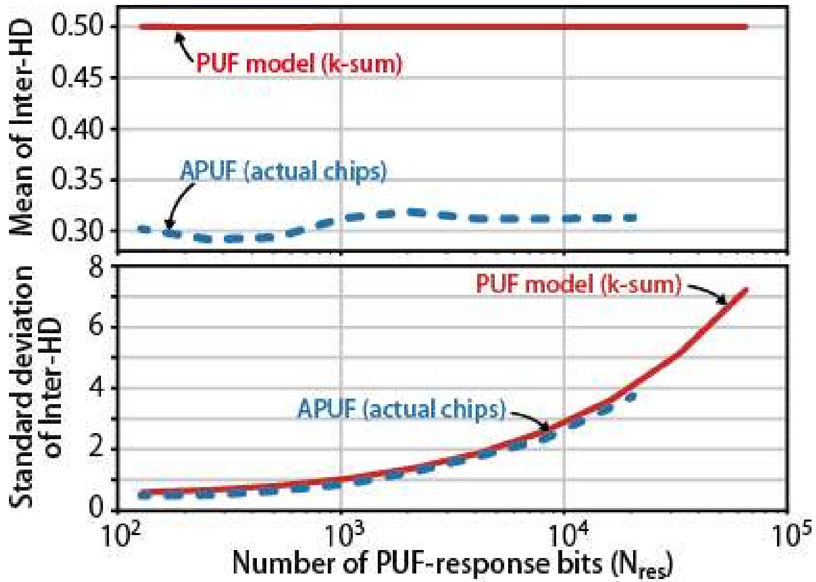
APUF

- ✓ An APUF converts a delay-time difference between two equivalent paths into a PUF response
- ✓ Our APUF consists of a 128-stage serpentine selector chain and a sense-amplifier-based arbiter circuit
  - ➢ Delay-time-difference variations: mean = 0 ps, SD = 8 ps per selector
- ✓ Expected causes:
  - ➢ <u>*k*-sum scheme - Generation scheme</u>
  - ➢ <u>Unbalanced layout - Source bias</u>
    (The offset delay time of the upper path: 9ps)
  - ➢ <u>Variation of arbiter circuits - Multiple sources</u>
    (The variation of arbiter circuits: mean = 0 ps, SD = 28 ps)



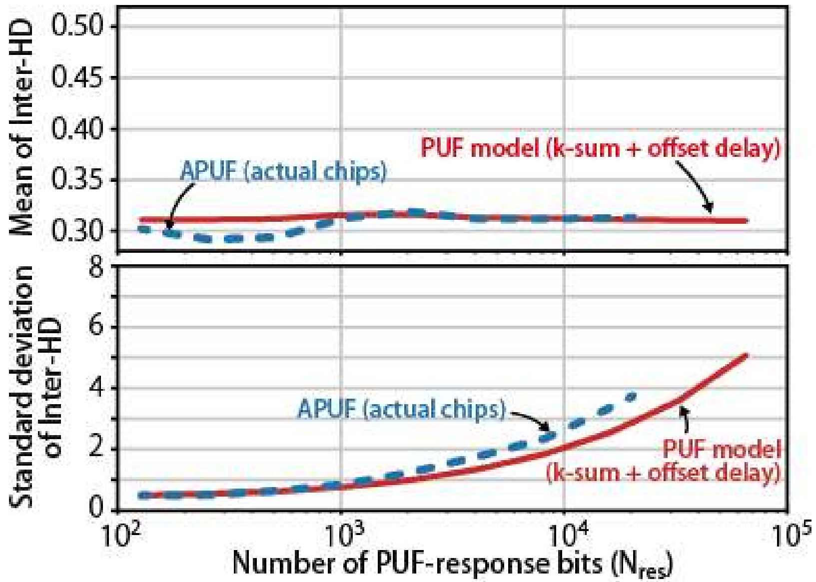
APUF vs. PUF Model

- ✓ The result using the actual chips is compared with that using the PUF model
- ✓ Expected causes:
  - ➢ ***k*-sum scheme - Generation scheme**
  - ➢ Unbalanced layout - Source bias
  - ➢ Variation of arbiter circuits - Multiple sources
- ✓ The means of Inter-HD are clearly different



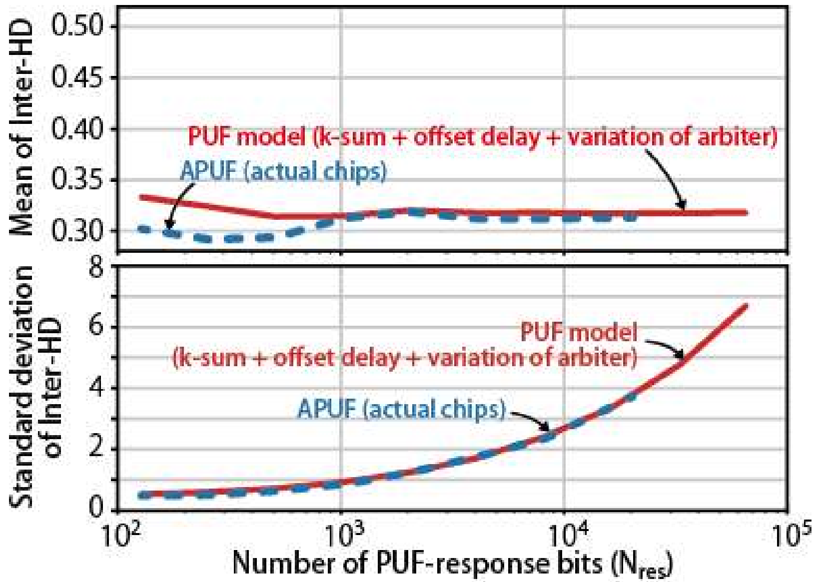
APUF vs. PUF Model

- ✓ The result using the actual chips is compared with that using the PUF model
- ✓ Expected causes:
  - ➢ ***k*-sum scheme (generation scheme)**
  - ➢ **Unbalanced layout (source bias)**
  - ➢ Variation of arbiter circuits (multiple sources)
- ✓ The means look the same, but the SDs are different



APUF vs. PUF Model

- ✓ The result using the actual chips is compared with that using the PUF model
- ✓ Expected causes:
  - ➢ ***k*-sum scheme (generation scheme)**
  - ➢ **Unbalanced layout (source bias)**
  - ➢ **Variation of arbiter circuits (multiple sources)**
- ✓ Our proposed scheme detected all the expected causes



Conclusion

- ✓ We organized causes of entropy loss during implementation into three types (source bias, multiple sources, generation scheme)
- ✓ We proposed a cause analysis method using Inter-HD
- ✓ We prototyped SRAM PUF, RO PUF, and APUF with a 180-nm CMOS process
- ✓ We demonstrated the validity of our proposed method by using our PUFs

Thank you!