
# A Framework for the Evaluation of Physical Unclonable Functions

**Abhranil Maiti, Vikash Gunreddy, and Patrick Schaumont**

**Electrical and Computer Engineering Department**

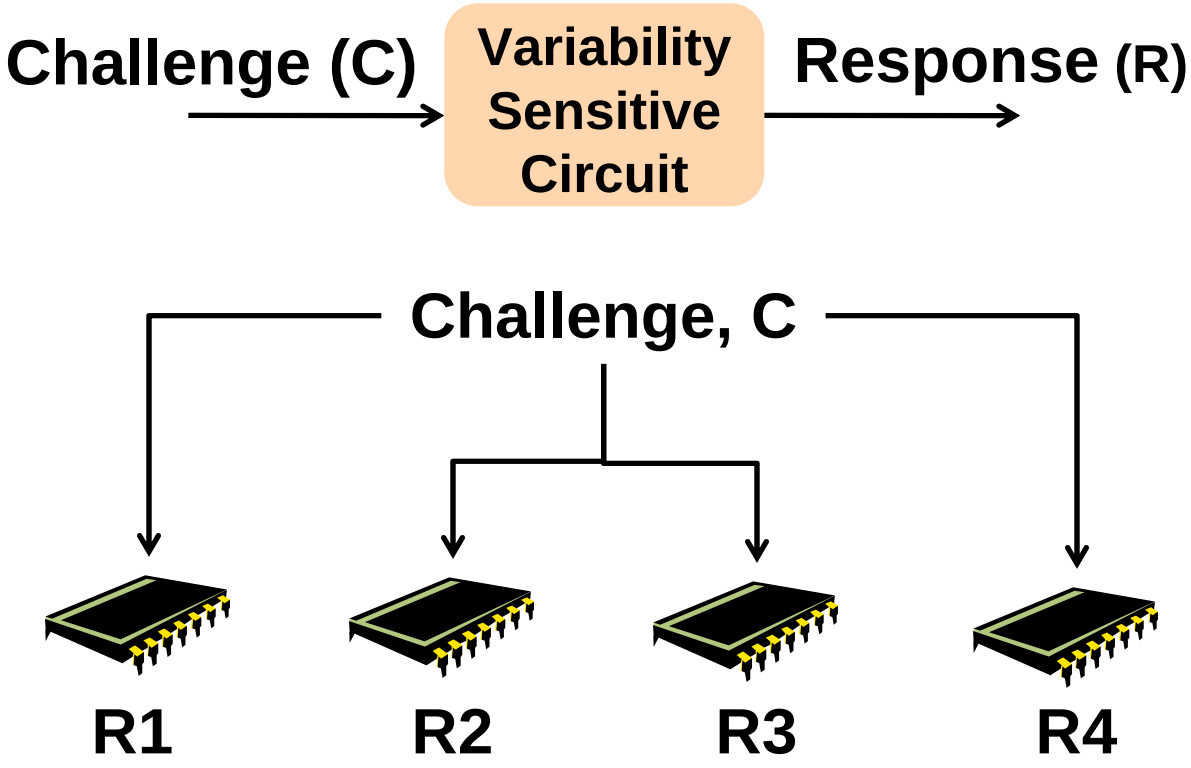
**Virginia Tech**

**NIST Workshop on Cryptography for Emerging Technologies and Applications**

11/07/2011

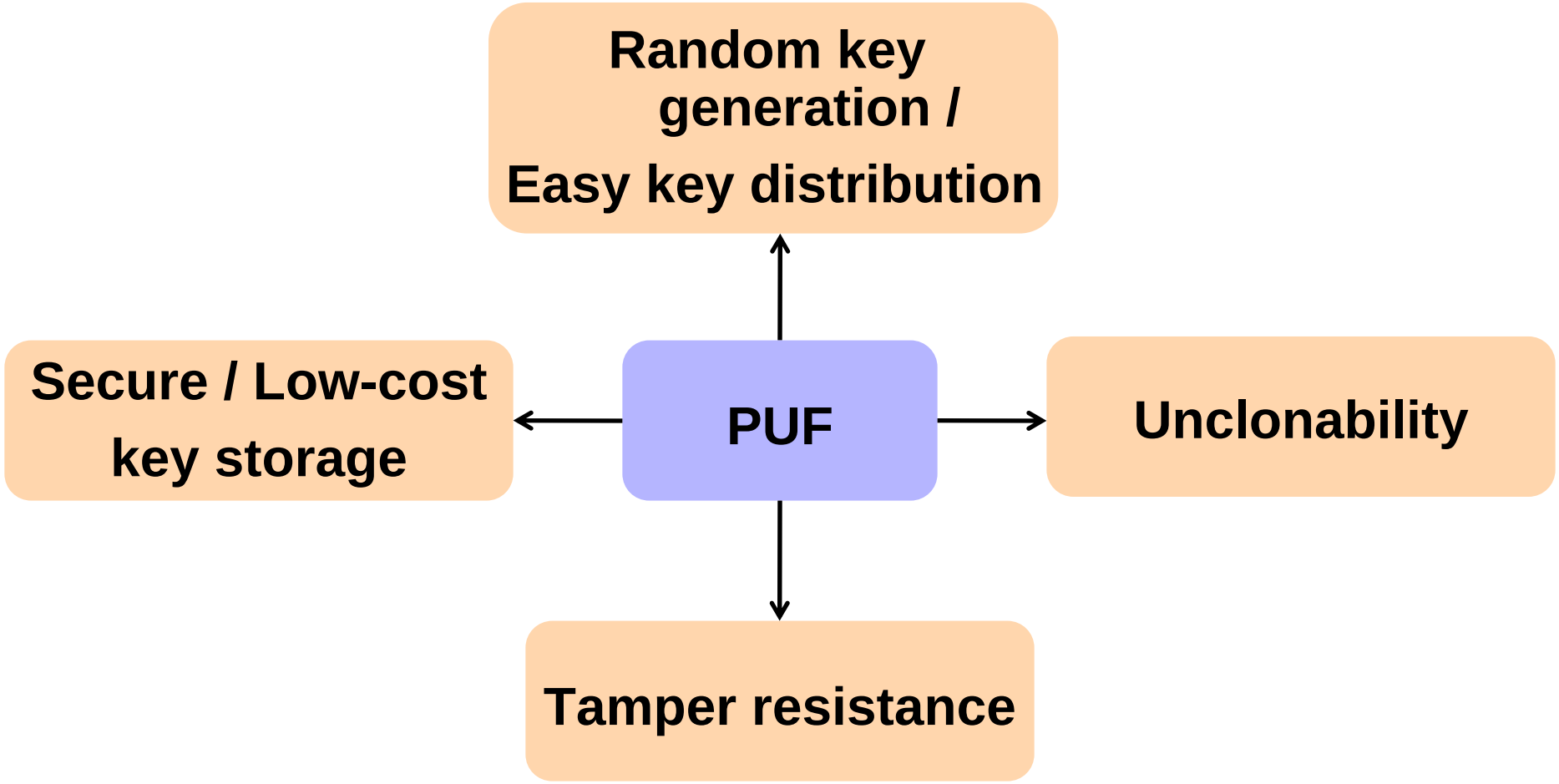
# On-chip PUF

A **P**hysical **U**nclonable **F**unction is a chip-unique challenge-response mechanism




$$R_1 \neq R_2 \neq R_3 \neq R_4$$

# Why is PUF useful as a security solution?



# Applications of PUF

- **Mobile Devices**
  - **authentication, piracy prevention - distribution and updating software in legitimate devices using PUFs**
- **Smart objects / internet of things**
  - **PUF-based RFID tags : anti-counterfeiting of products, secure identification/ authentication (credit cards, passport)**
- **Cyber physical system**
  - **aerospace, energy, healthcare : PUF is a low-cost solution to provide privacy/confidentiality**

**Secure financial transaction**


**Secure identification**


**Anti-counterfeiting**

# Types of PUF

- **Several PUFs proposed in past few years**

- **IC identification using device mismatch (2000)**
- **Physical one-way function (2001)**
- **Silicon Physical Random Function (2002)**
- **Arbiter PUF (2004)**
- **Coating PUF (2006)**
- **SRAM PUF (2007)**
- **Ring Oscillator PUF (2007)**
- **Butterfly PUF (2009)**
- **PUF using power distribution system (2009)**
- **Glitch PUF (2010)**
- **Mecca PUF (2011)**

**And many more…**

# Questions to answer

- **How do we know if a PUF is efficient?**
- **How do we compare one PUF with another?**
- **Need to evaluate PUF Quality factors:**
  - **Randomness / entropy**
  - **Reliability**
  - **Attack resiliency**
- **This is not straight-forward: different PUFs have different challenge-response mechanisms, number of response bits produced are not same.**

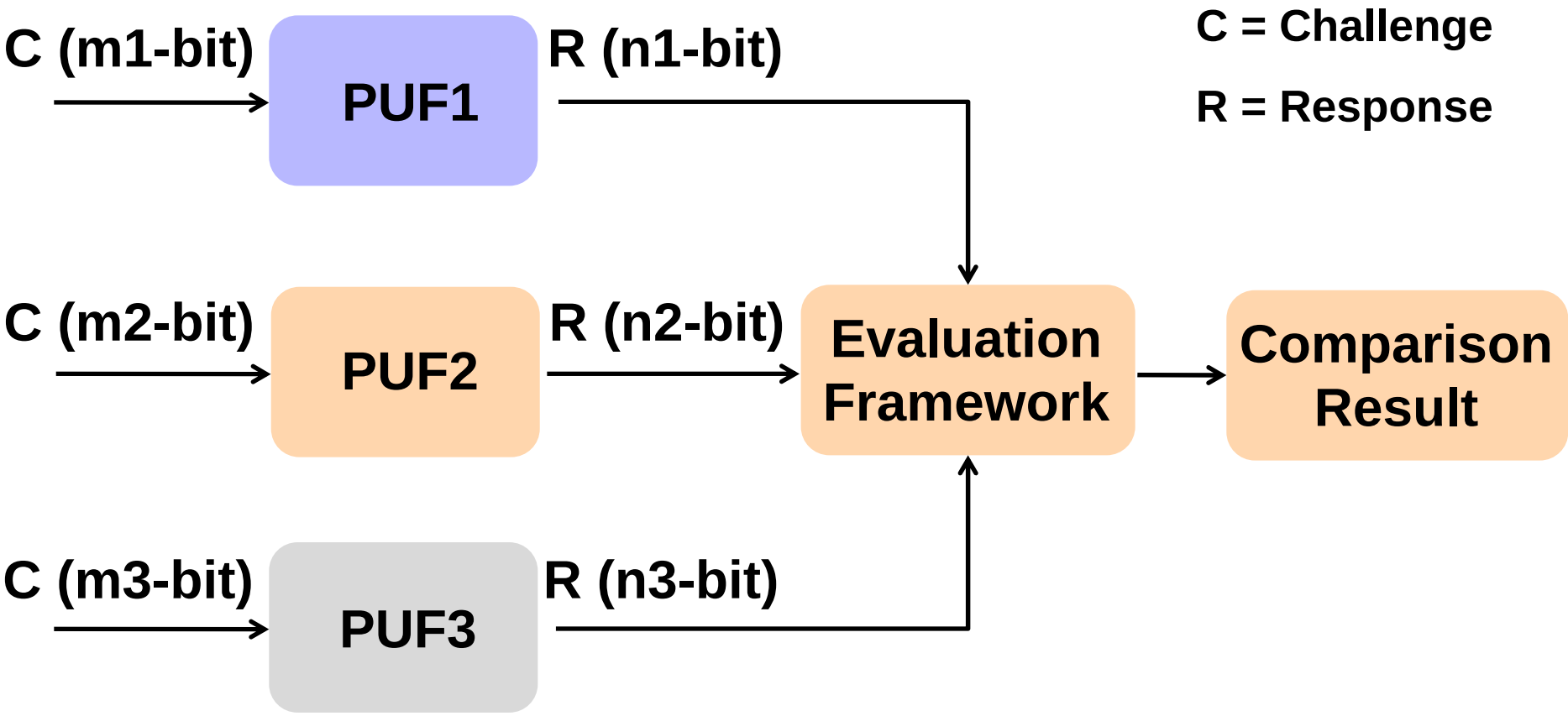
# Framework for PUF evaluation

- **Main goal – standardization of PUF performance evaluation**

- **To quantify several quality factors of a PUF and to define performance criteria**
  - **defining parameters / analyzing existing ones by other researchers**

- **To build a framework independent of the underlying PUFs for fair comparison using evaluation parameters**
  - **For example: we should be able to compare a memory-based PUF such as SRAM PUF with a delay-based PUF such as RO-PUF**

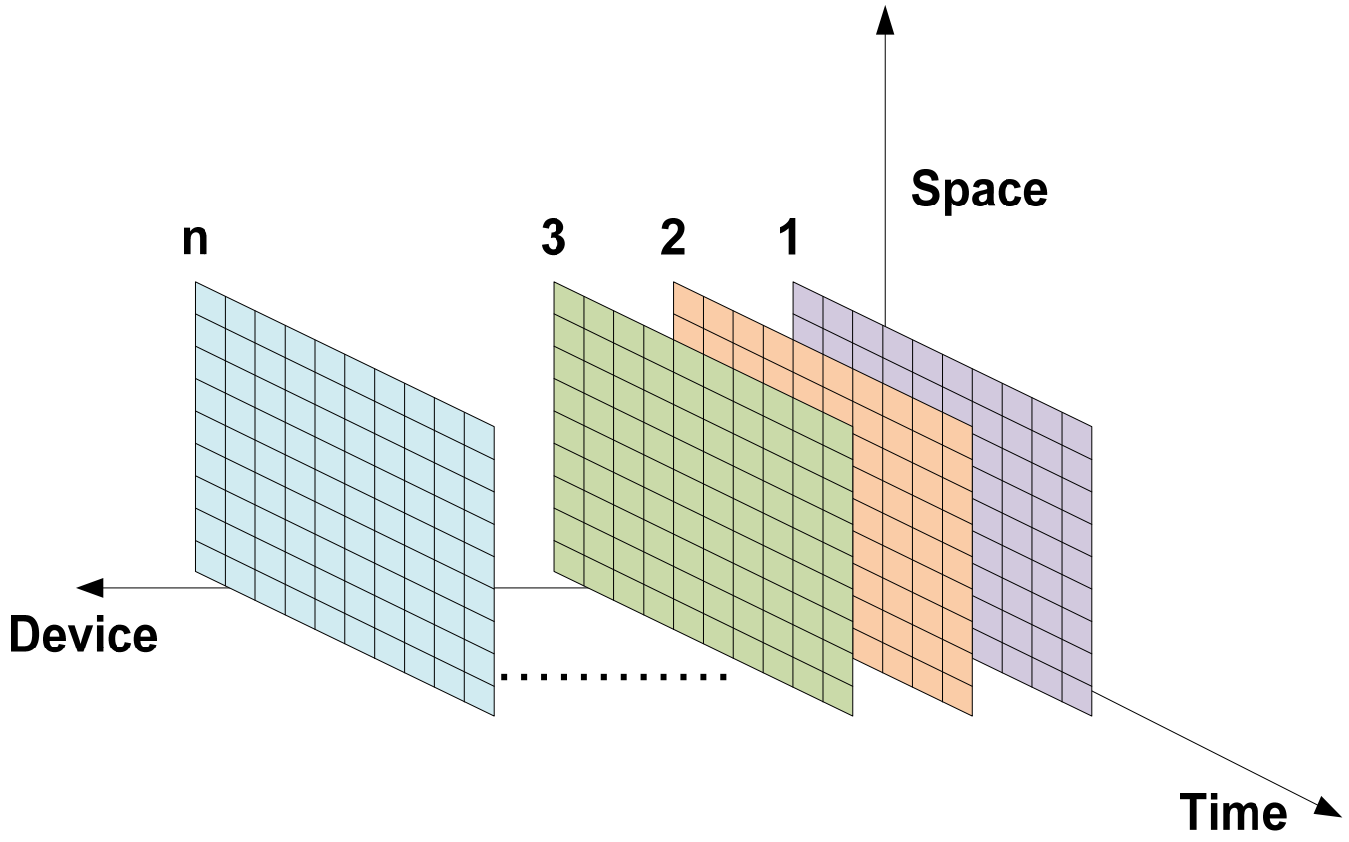
# Main idea

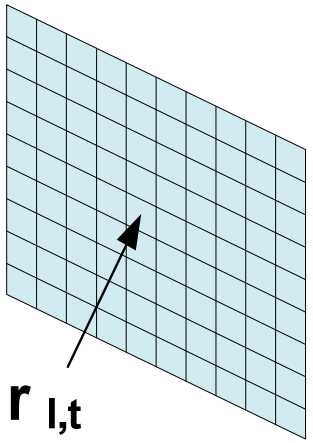



- The framework relies on the response bits of the PUFs irrespective of the underlying PUFs

# Defining PUF parameters

- **Dimensions of PUF measurements**



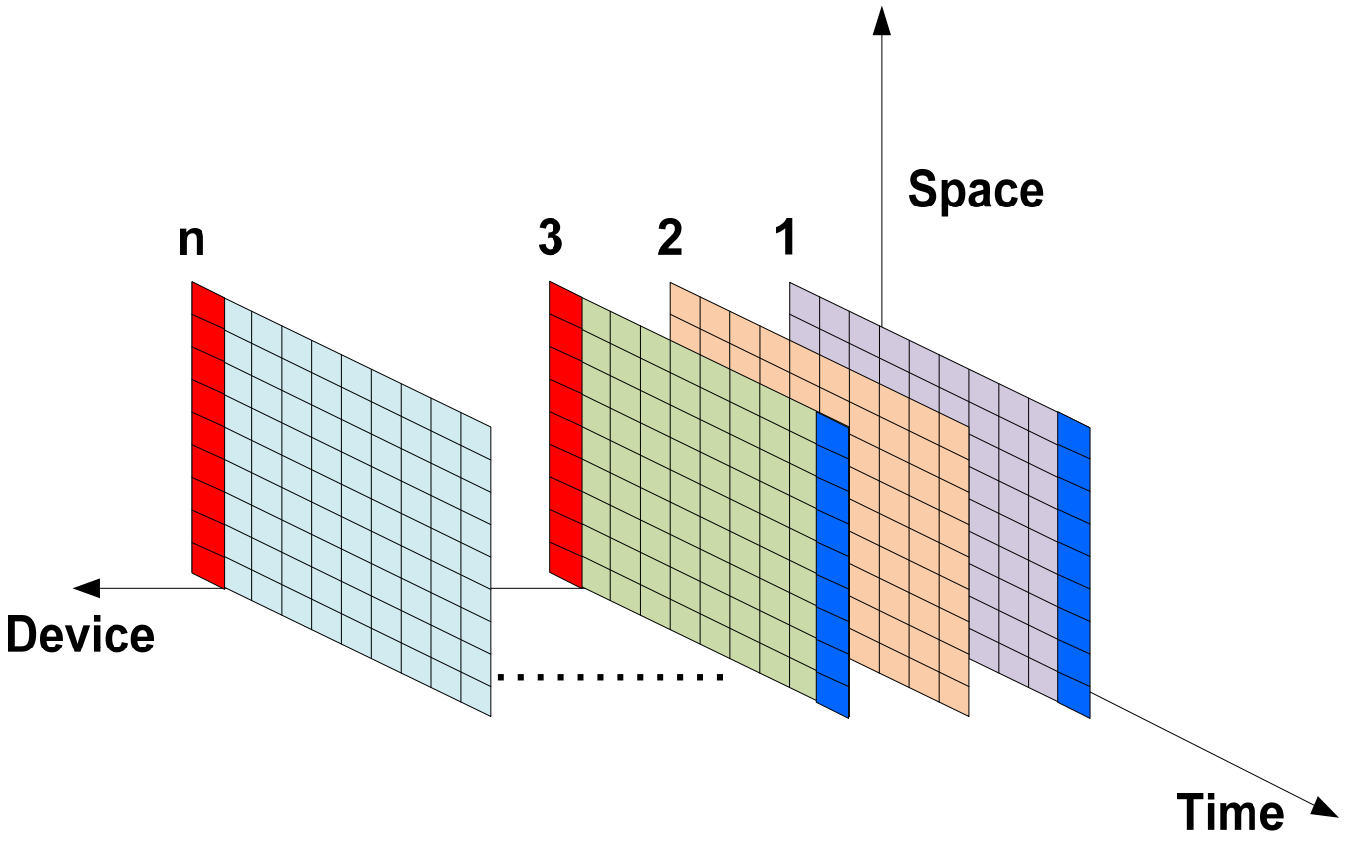



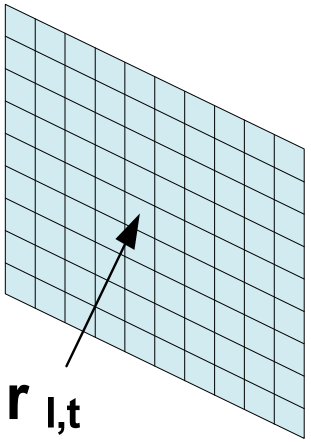

$r_{l,t}$ = t-th sample of the l-th response bit

- **Device axis – population of chips**
- **Time axis – samples of response bits**
- **Space axis – different response bits**

# Uniqueness of PUF

- **Inter-chip variation using Hamming distance**



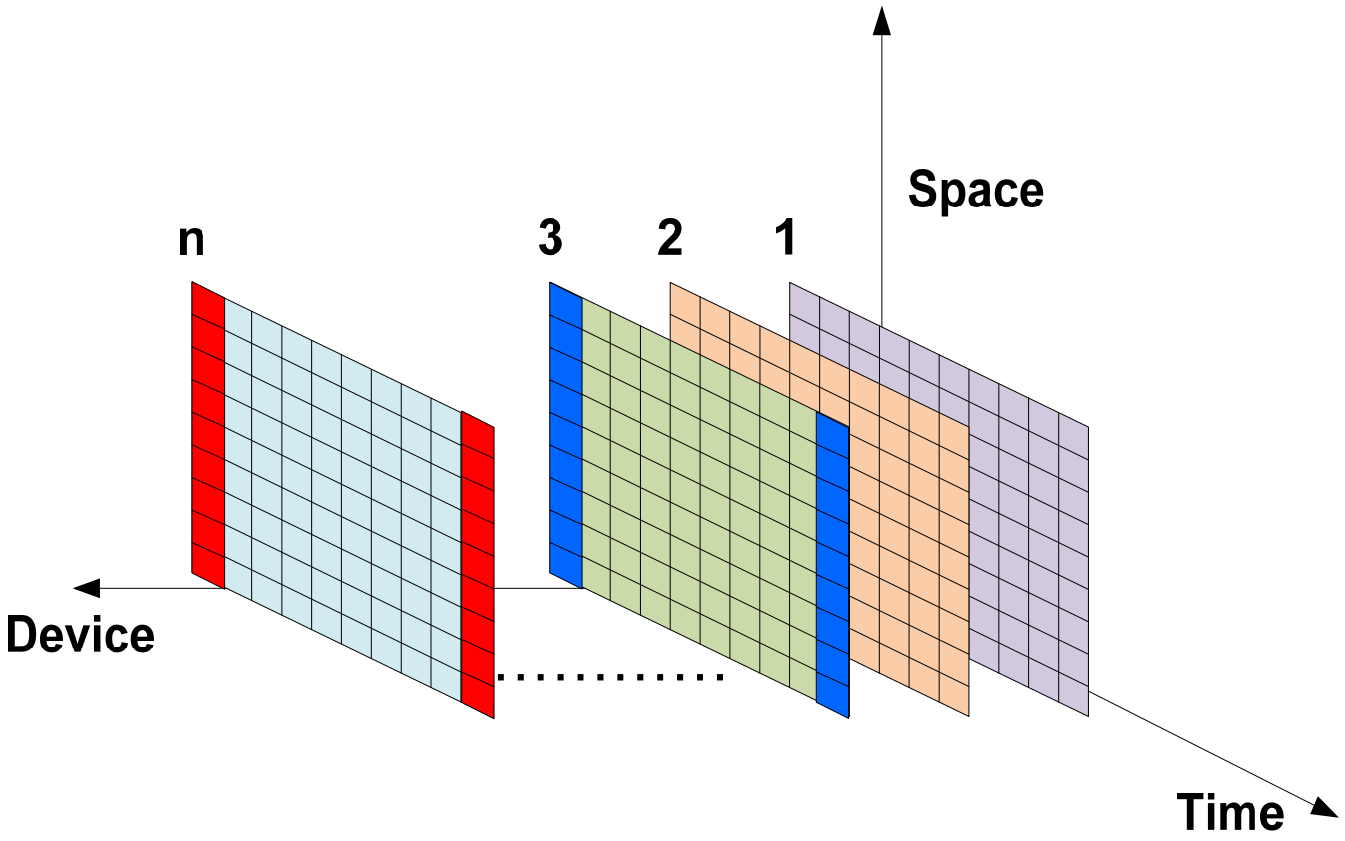



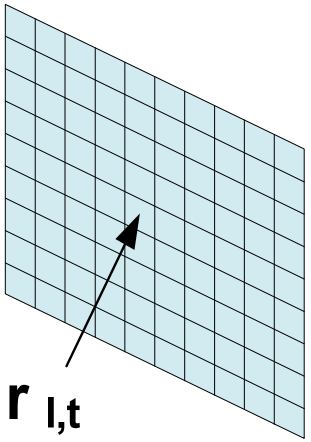

$r_{l,t}$ = t-th sample of the l-th response bit

- **Dependent on the device axis**

# Reliability of PUF

- **Intra-chip variation using Hamming distance**



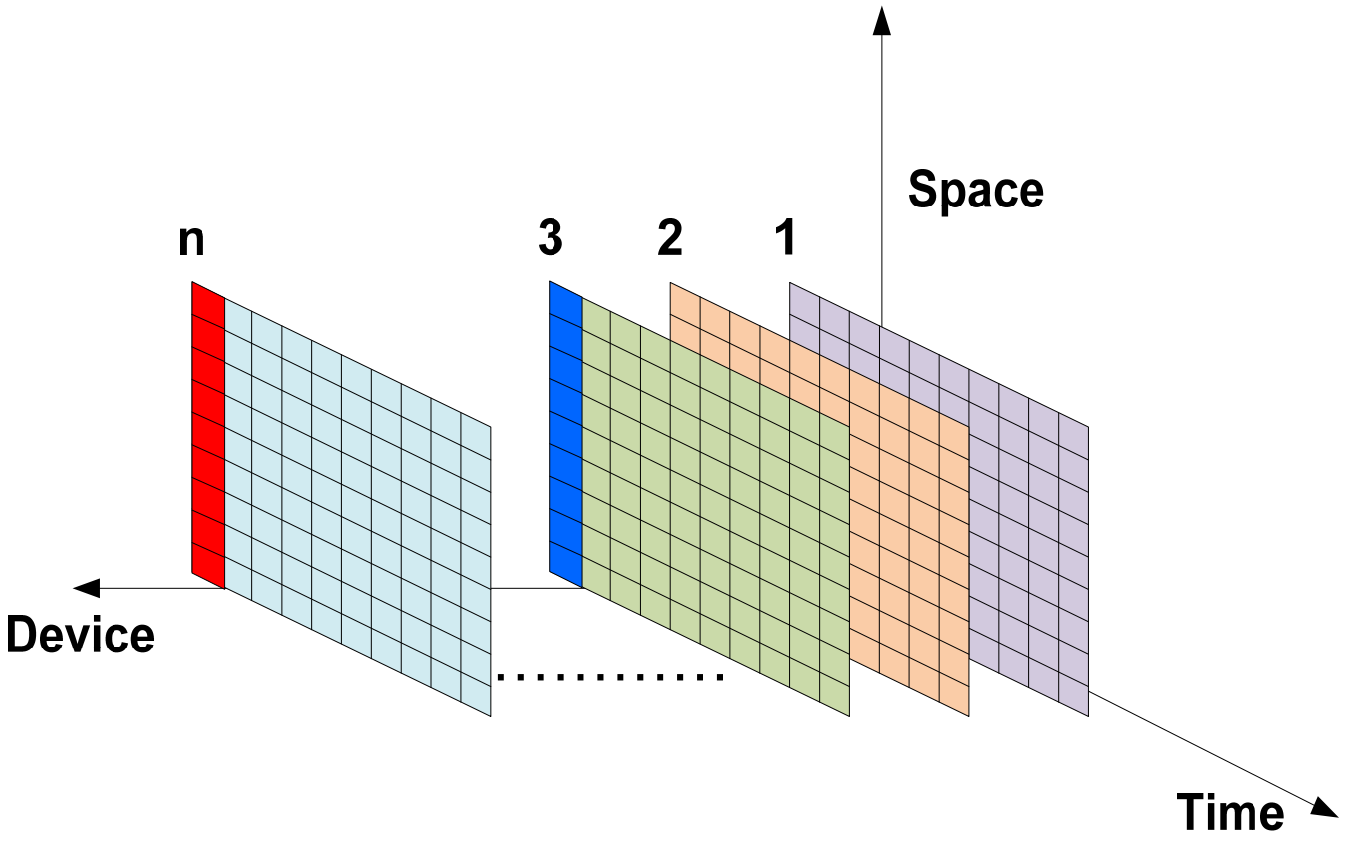



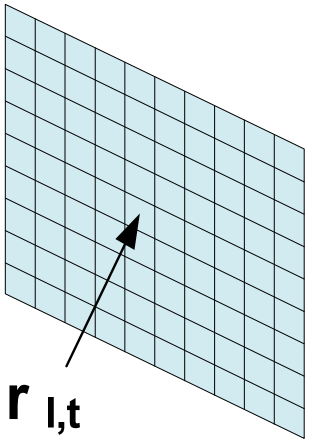

**r l,t = t-th sample of the l-th response bit**

- **Dependent on the time axis**

# Uniformity of PUF

- **Intra-chip variation using Hamming weight (HW)**



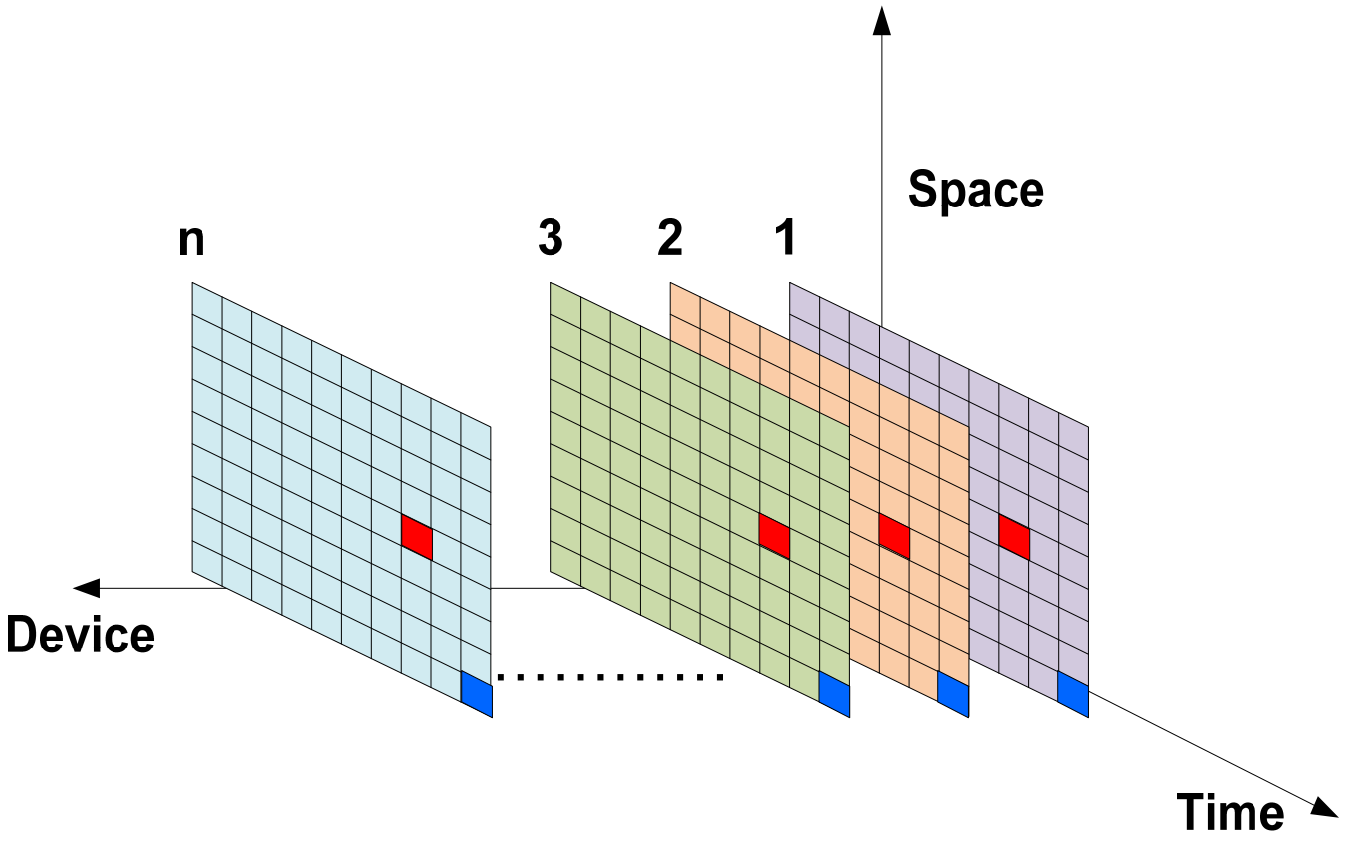



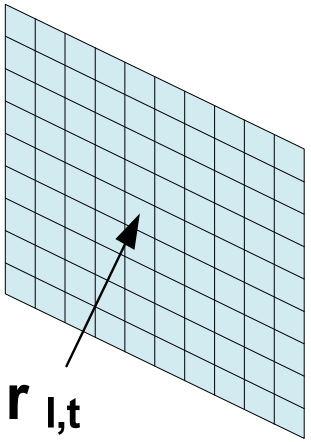

$r_{l,t}$ = t-th sample of the l-th response bit

- **Dependent on the space axis**

# Bit-aliasing of PUF

- **Inter-chip variation using bit-wise Hamming weight**




$r_{l,t}$ = t-th sample of the l-th response bit

- **Dependent on the device axis**

# Existing PUF parameters

- **Analysis of several PUF parameters proposed by other researchers to build the framework**

| AIST, Japan | Virginia Tech | University of Washington | Rice University | Fujitsu Lab |
|---|---|---|---|---|
| Randomness | Average Inter-chip Hamming Distance | Collision Probability | Single bit probability | Variety |
| Steadiness | Uniformity | | Conditional Probability | |
| Correctness | Bit-aliasing | | | |
| Diffuseness | Reliability | | | |
| Uniqueness | | | | |

- **Analyzing the effectiveness of the parameters**
- **Minimizing redundancy of parameters**

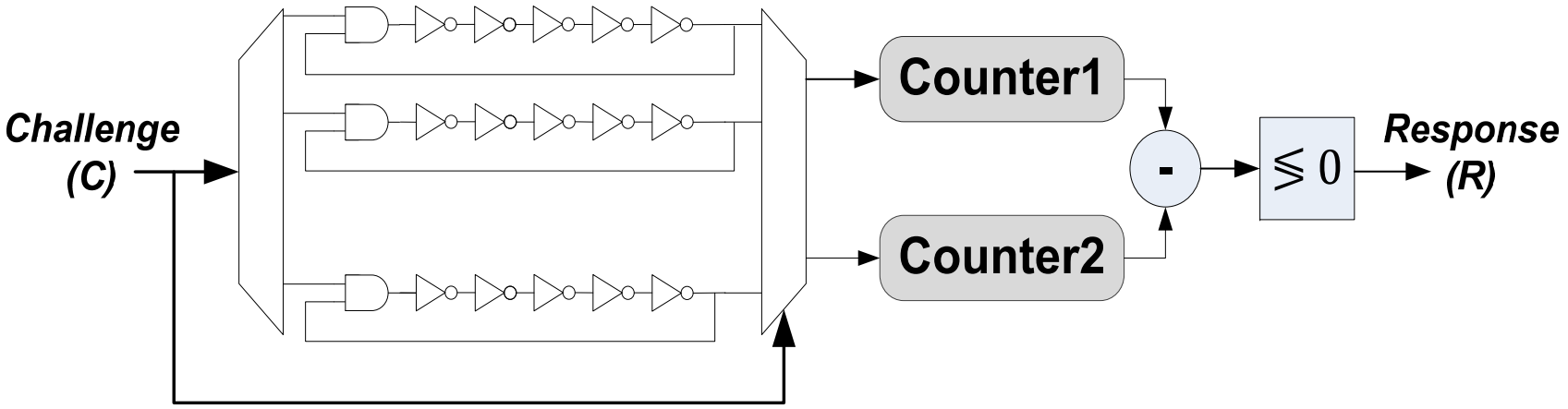
# Preliminary effort

- **Comparison of parameters: AIST, Japan vs Virginia Tech**

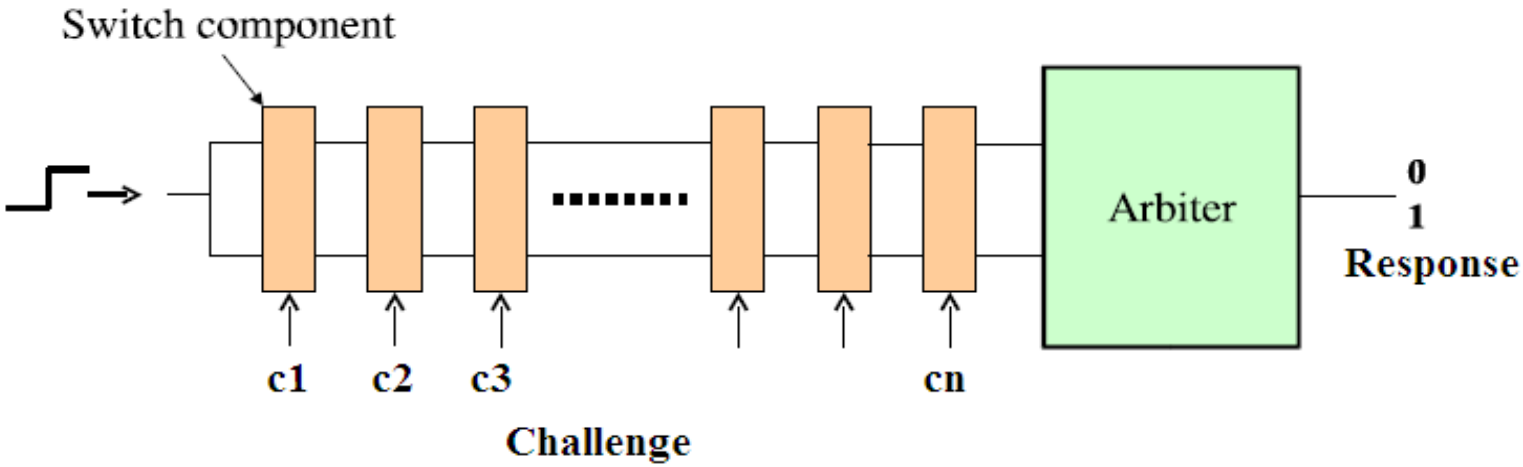
| AIST, Japan | Virginia Tech |
|---|---|
| Randomness | Uniformity |
| Steadiness (related to correctness) | |
| Correctness | Reliability |
| Diffuseness (related to uniqueness) | |
| Uniqueness | Average Inter-chip Hamming Distance |
| | Bit-aliasing |

- **Validation using existing dataset**
  - **Dataset from VT**
  - **Dataset from AIST, Japan**

# VT vs AIST Comparison




- **Ring Oscillator based PUF used by VT (Spartan 3E – 90nm)**



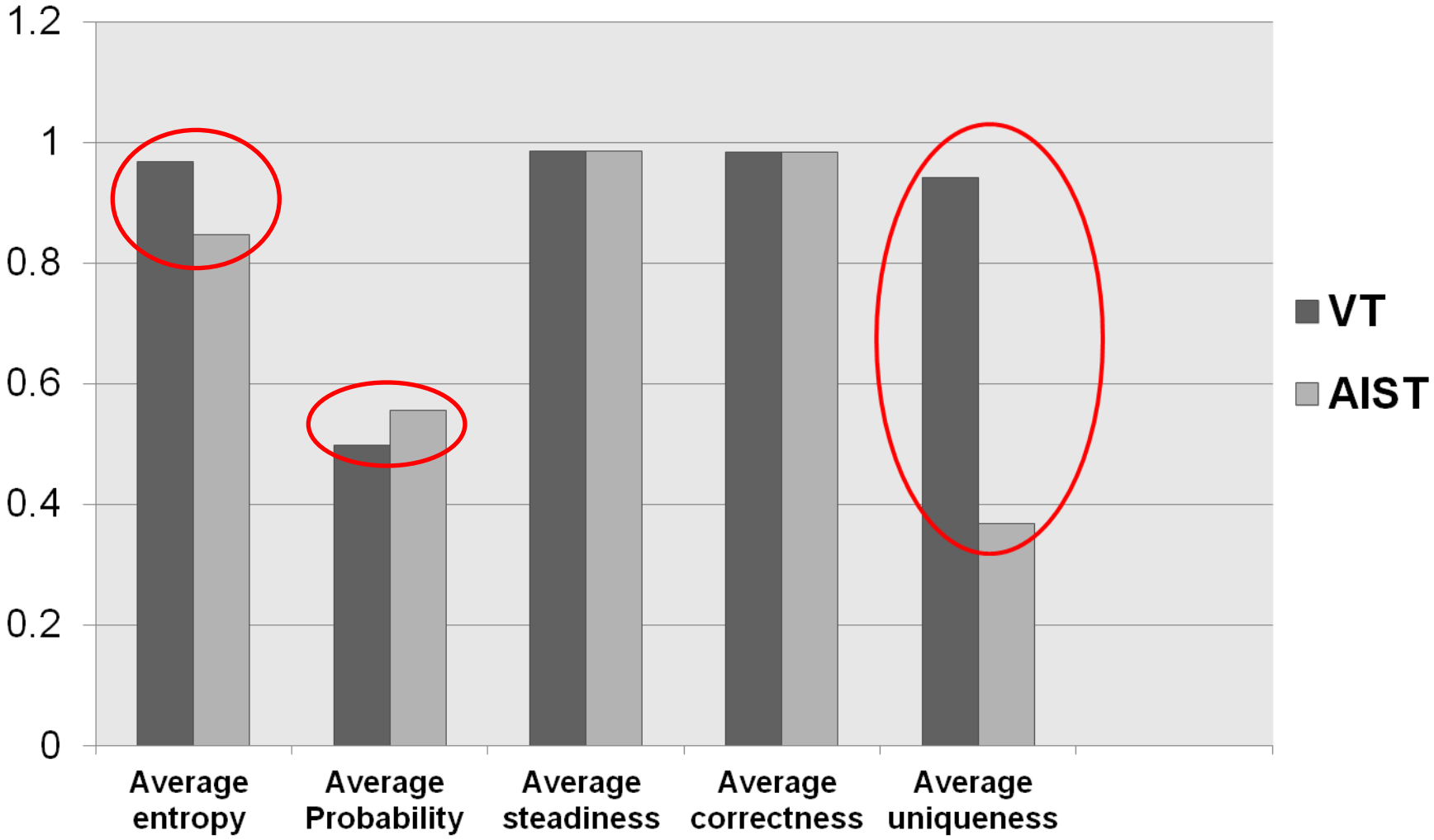

- **Arbiter PUF used by AIST (Virtex 5 – 65 nm)**

# Notations for the dataset

| | |
|---|---|
| $N$ = number of devices | $n$ = index of a device ($1 \le n \le N$) |
| $K$ = number of IDs generated per device | $k$ = index of an ID in a device ($1 \le k \le K$) |
| $T$ = number of samples measured per ID | $t$ = index of a sample of an ID ($1 \le t \le T$) |
| $L$ = length of an ID | $l$ = index of a bit in an ID ($1 \le l \le L$) |
| $M$ = number of ring oscillators | $m$ = index of a ring oscillator ($1 \le m \le M$) |

| | VT | AIST |
|---|---|---|
| N | 193 | 45 |
| T | 100 | 1024 |
| K | 1 | 1024 |
| L | 511 | 128 |
| M | 512 | - |

# Comparison Results



# Confidence Interval Comparison

| | VT | | AIST | |
|---|---|---|---|---|
| | **confidence interval** | **width** | **confidence interval** | **width** |
| Entropy | [0.9892, 0.9990] | 0.00986 | [ 0.8388, 0.8546 ] | .01586 |
| Bit Probability | [ 0.4962, 0.5003] | 0.00407 | [ 0.5530, 0.5591 ] | .006111 |
| Steadiness | [ 0.9846, 0.9857] | 0.00110 | [ 0.9626, 1.000 ] | .04134 |
| Correctness | [ 0.9822, 0.9834] | 0.00121 | [ 0.9579, 1.000 ] | .04206 |
| Uniqueness | [0.9334, 0.9481] | 0.02940 | [ 0.2127, 0.5222 ] | .3095 |

- **Better confidence interval in VT dataset**

# Discussion

- **Similarity in the definition of parameters found:**
  - **Randomness vs uniformity**
  - **Correctness vs reliability**
  - **Uniqueness vs  Inter-chip Hamming distance**

- **RO-PUF exhibited better performance compared to Arbiter PUF even if the former is implemented on a bigger device**

- **The size of the device population has significant impact on the confidence interval (CI) of the parameters**
  - **VT dataset with 193 chips shows much better CI compared to the AIST dataset with 45 chips**

## Online Variability Data


**http://rijndael.ece.vt.edu/variability/main.html**

# Thank you

# Questions ??

**This work was supported by the National Science Foundation by grant no. 0964680 and grant no. 0855095.**