A Physical Unclonable Function Using Time-to-Digital Converter

K. Katoh, S. Yamamoto, Z. Zhao, Y. Zhao, S. Katayama, A. Kuwana,
K. Sato, T. Ishida, T. Okamoto, T. Ichikawa,
T. Nakatani, K. Hatayama, H. Kobayashi

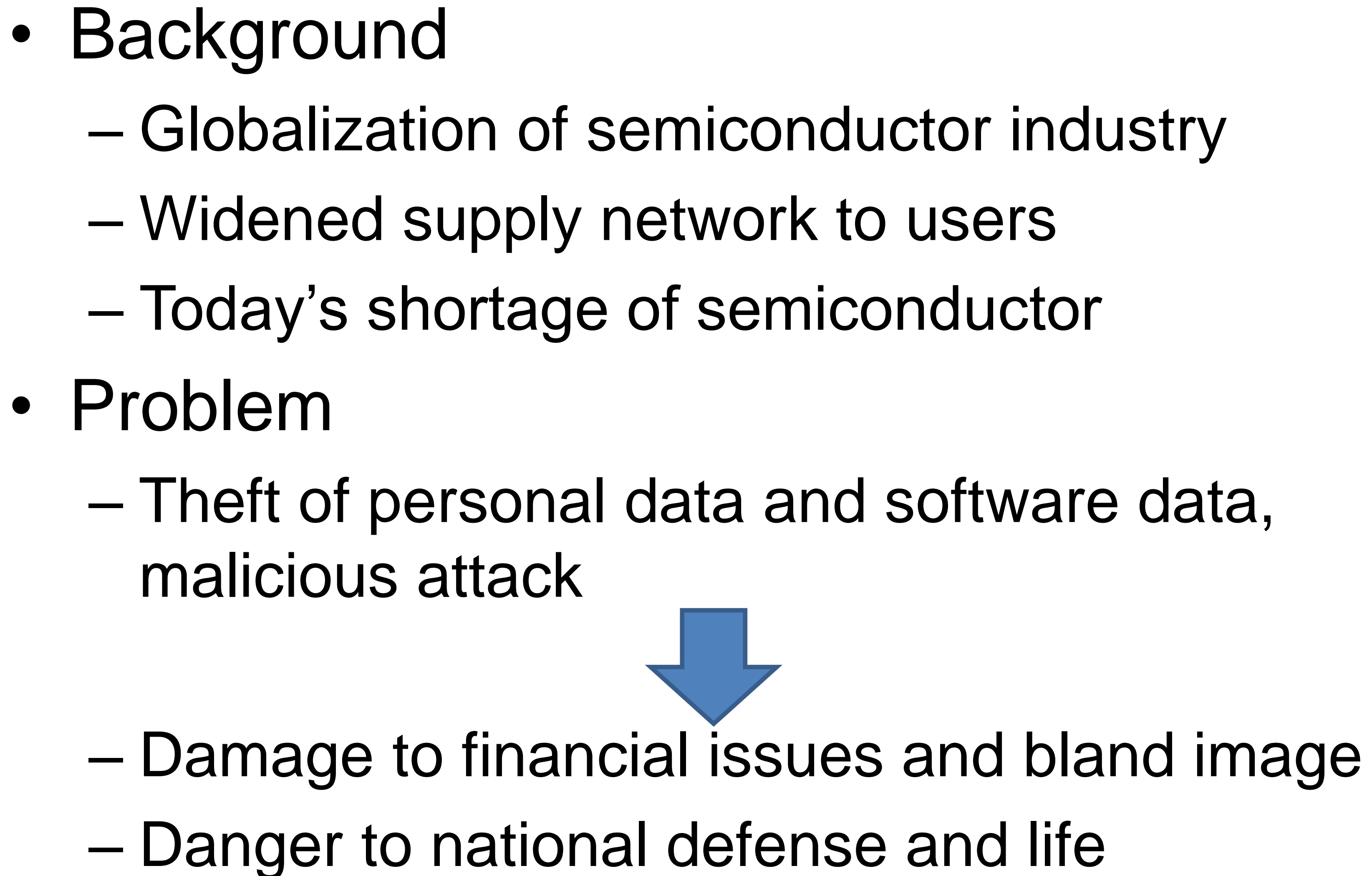
Gunma University
ROHM Semiconductor

Outline

- Background and objective
- Proposed physical unclonable function using time-to-digital converter (TDC PUF)
- Evaluation
- Conclusion

Spread of Counterfeit ICs

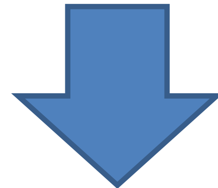
- Background
  - Globalization of semiconductor industry
  - Widened supply network to users
  - Today’s shortage of semiconductor
- Problem
  - Theft of personal data and software data, malicious attack



  - Damage to financial issues and bland image
  - Danger to national defense and life

Conventional Solution

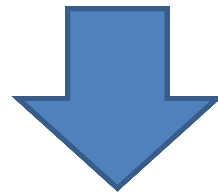
- Unique chip ID
  - Used to check genuine/counterfeit IC
  - Stored in non-volatile memory (EEPROM, Flash memory) of devices



- Vulnerable to side-channel attack
- Easily clonable
- Active tamper detection/prevention circuity → costly

Physical Unclonable Function (PUF)

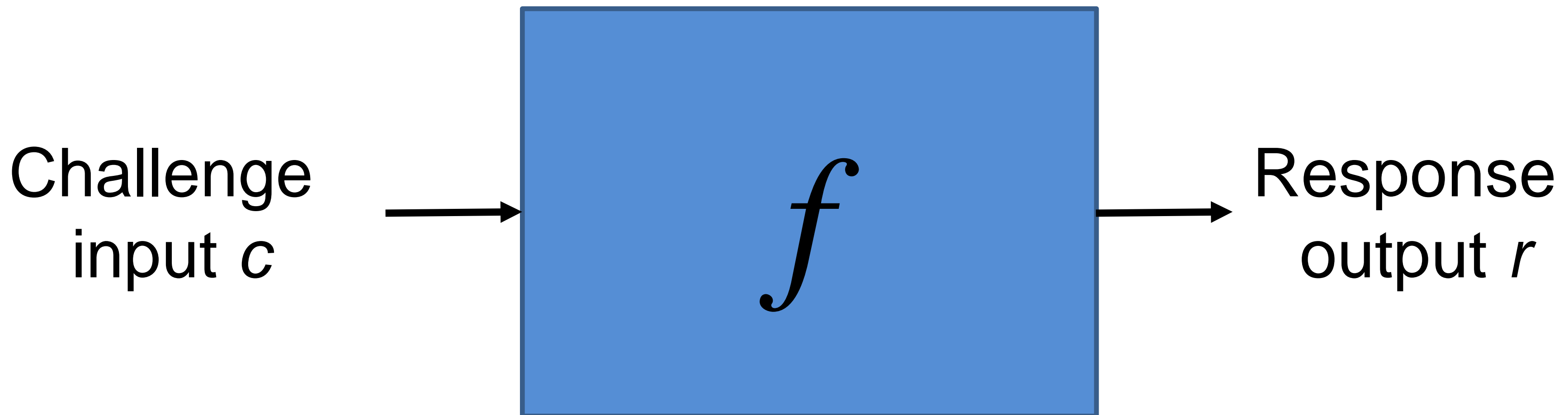
- Generate unique bitstring
  - utilizing physically unclonable device parameters derived from manufacturing variation such as
    - Delay, leakage current, initial state of memory
  - for device authentication and secure communication



- Strong to tamper attack
- Unclonable
- Cheap

System-level Modeling of PUF

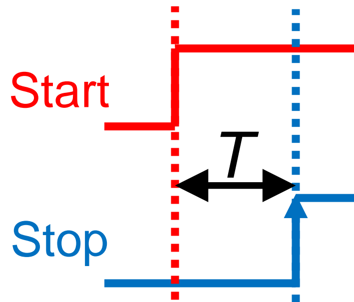
- PUF: Challenge-Response system



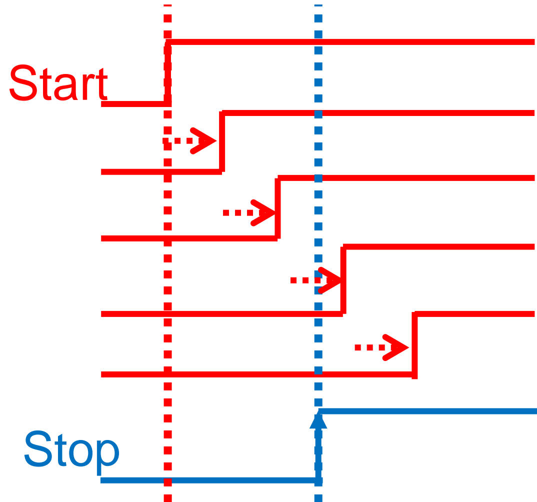
$$r = f(c)$$

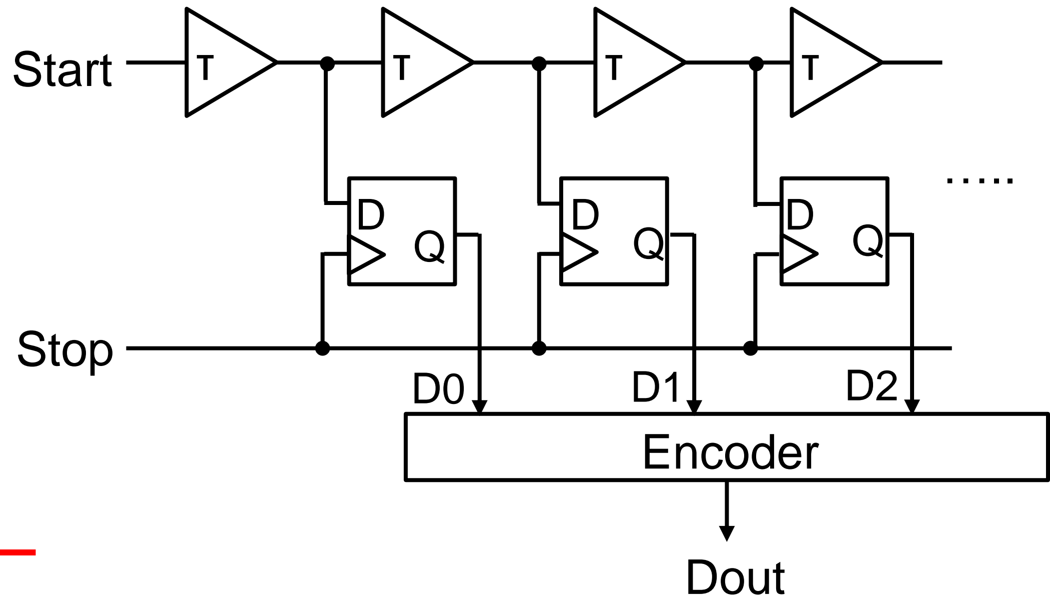
- r: not only function of input c,
  but also function of internal unique and unclonable device parameter
  $\rightarrow r$: unique in each device

Flash Time-to-Digital Converter (TDC)



Timing chart



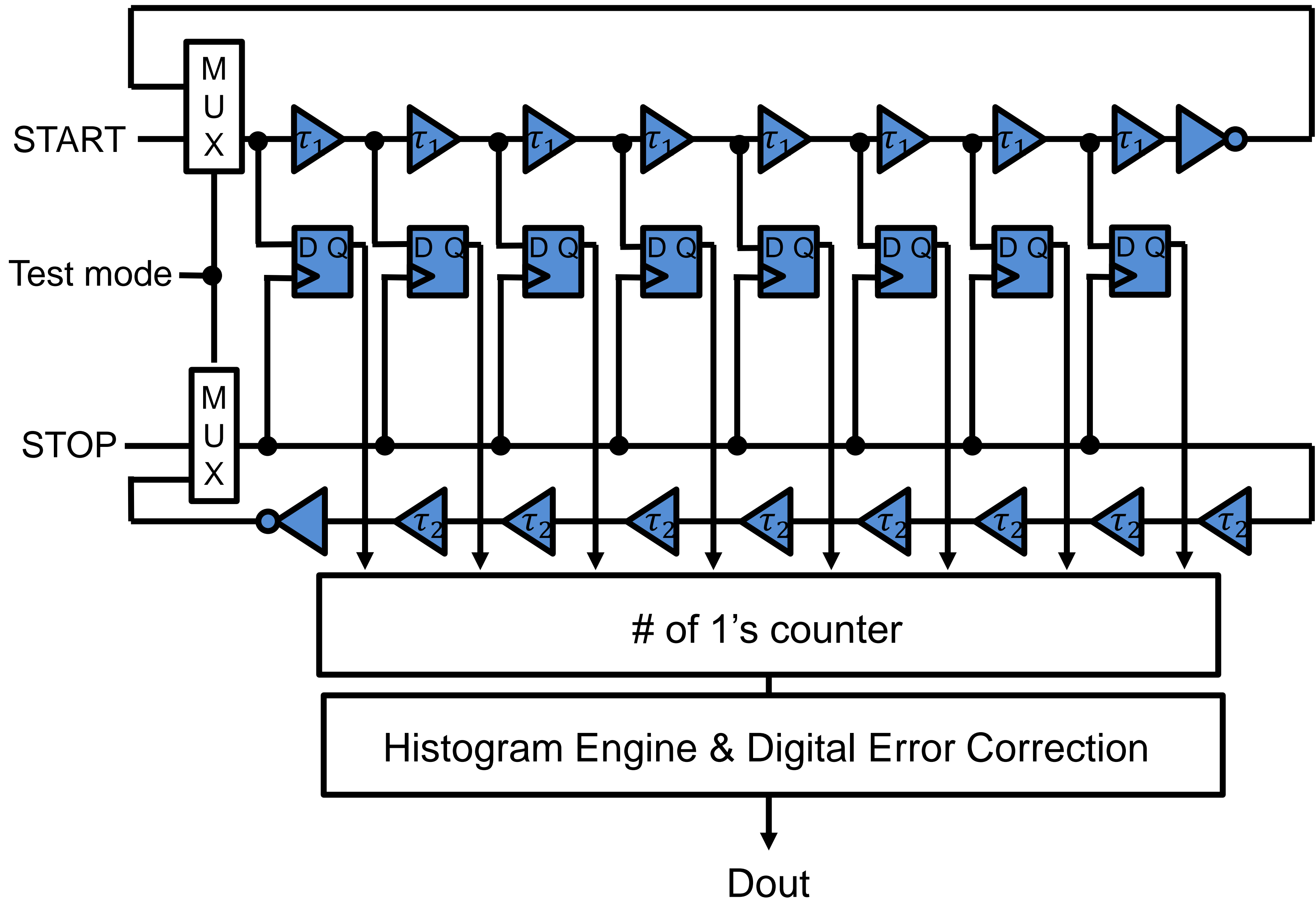


Encoder

Thermometer code

binary code

TDC with Linearity Self-Calibration

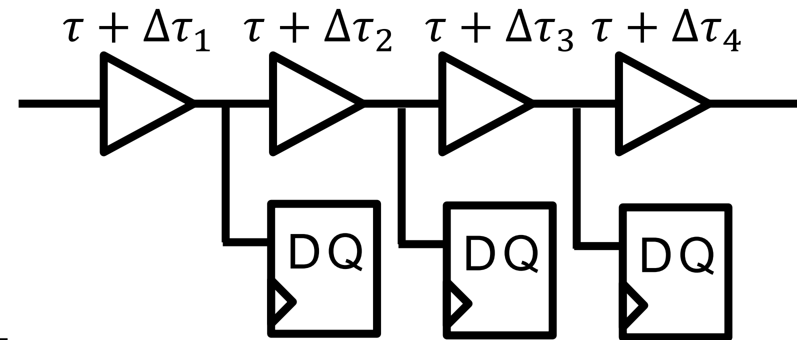


Histogram and Buffer Delay

In case TDC has nonlinearity

Histogram

Buffer delay



$\Delta\tau_2$ $\Delta\tau_3$ $\Delta\tau_5$

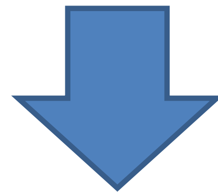
τ

$\Delta\tau_4$

1 2 3 4 5 6 Digital output

Research Objective

- Non-linearity of TDC
  - derived from process variation
  - unique to each device
  - caused by variation of buffer delay of TDC
  - calculated from histogram obtained with linearity self-calibration

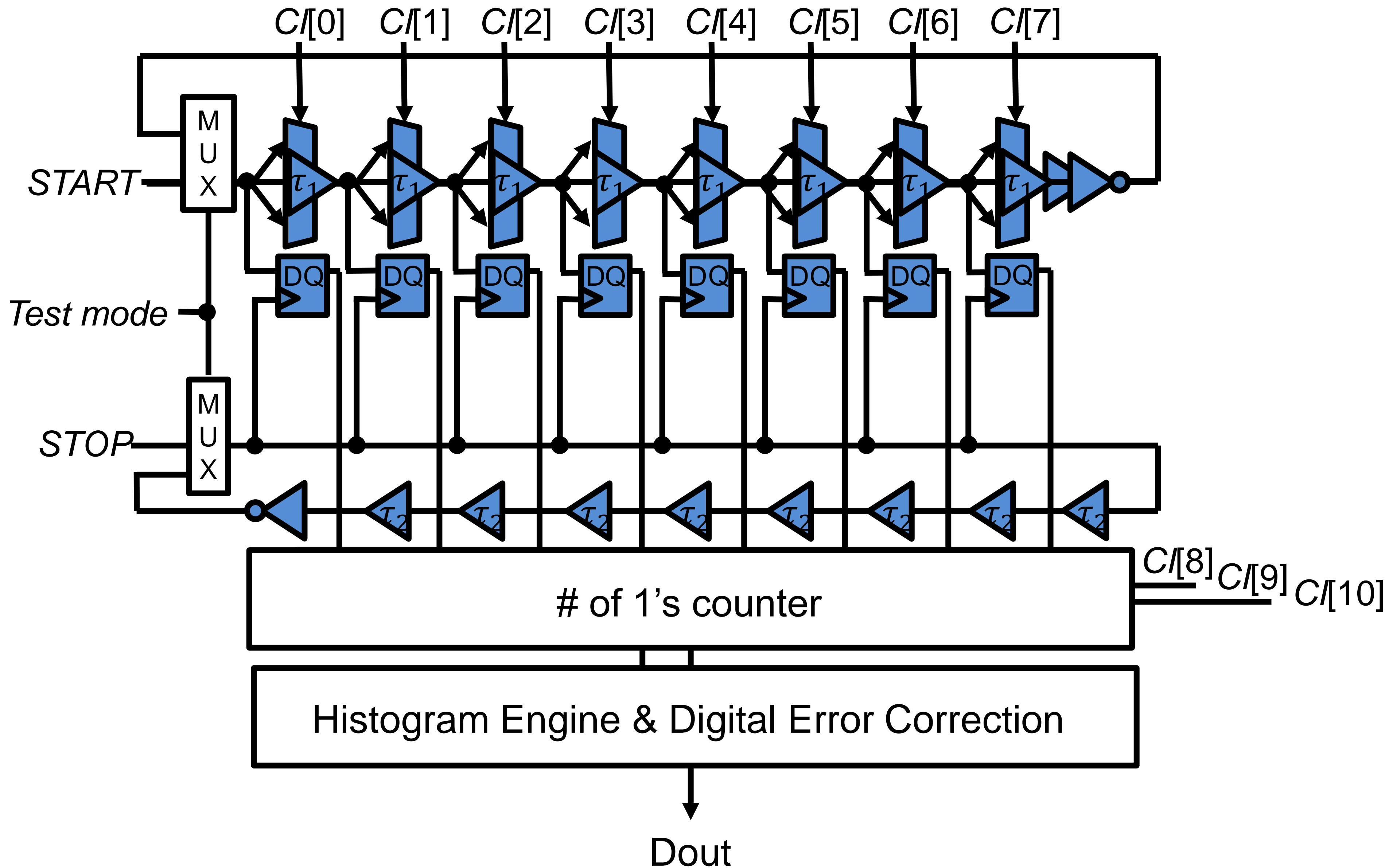


Development of PUF using TDC with linearity self-calibration

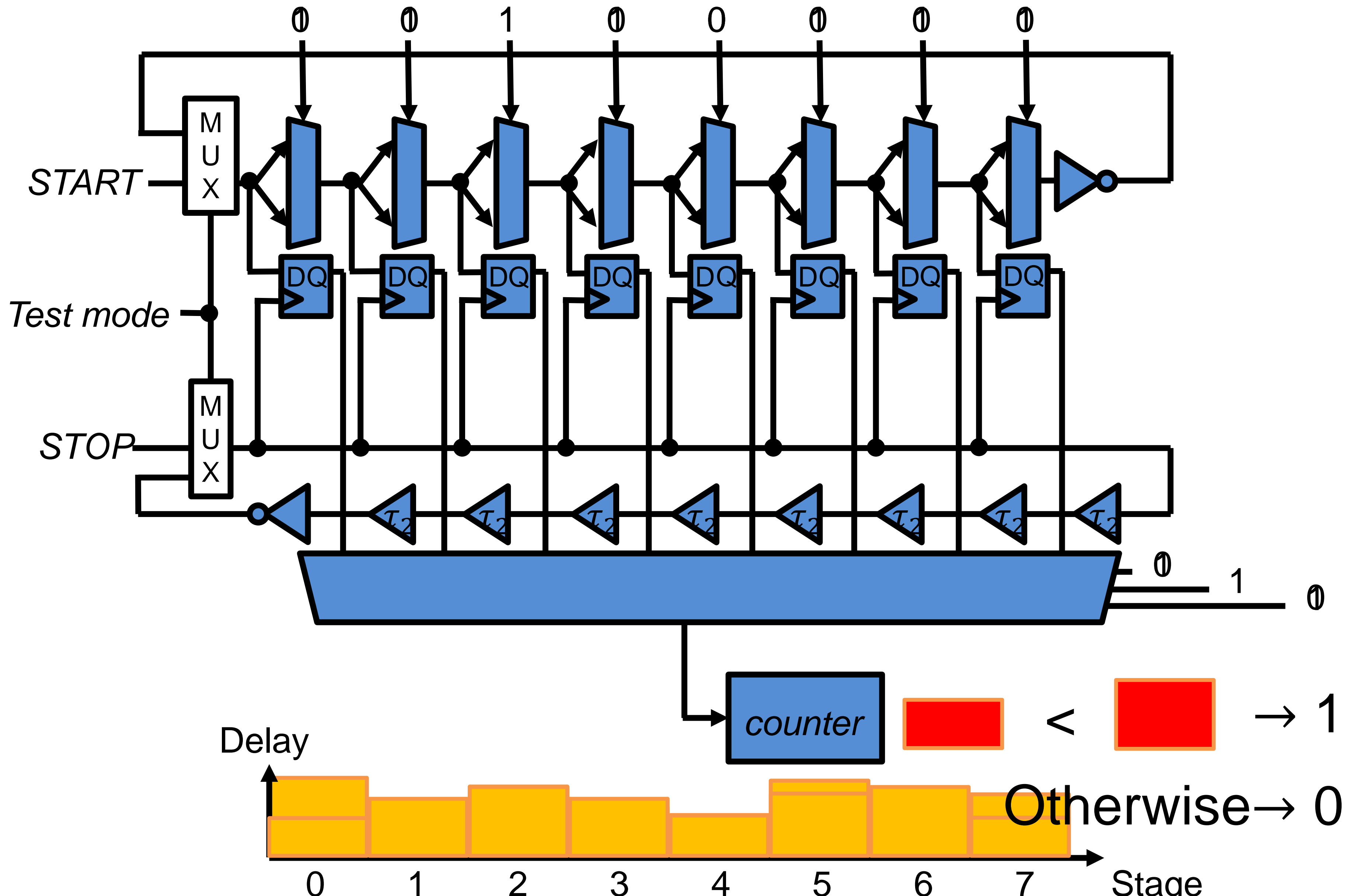
Contents

- Background and objective
- <u>Proposed physical unclonable function using time-to-digital converter (TDC PUF)</u>
- Evaluation
- Conclusion

TDC PUF



Calculation of Response Output



Calculation of Response Output

- Calculation of response output R over challenge input C
  - $C = \{C_0, C_1\}$ $|C_i|$=number of input of TDCPUF
  - Step 1: Perform calibration and calculate COEF[n]
  - Step 2: Former sub input C_0 to TDCPUF
  - Step 3: Perform calibration
  - Step 4: Get $COUNT_0$ and $COEF_0$
  - Step 5: Latter sub input C_1 to TDCPUF
  - Step 6: Perform calibration
  - Step 7: Get $COUNT_1$ and $COEF_1$
  - Step 8: If $COEF_1 * COUNT_1 > COEF_0 * COUNT_0$ R=1 otherwise R=0

Contents

- Background and objective
- Proposed physical unclonable function using time-to-digital converter (TDC PUF)
- Evaluation
- Conclusion

Experimental Setup

- Evaluate proposed TDC PUF implemented with FPGA board
- FPGA board
  - Digilent BASYS3
    - FPGA: Xilinx Arix7 (XC7A35T-1CPG236C)
    - External clock: 100MHz
- TDC PUF
  - Number of stages: 8
  - CI: 11 bits
  - Challenge input C: 22 bits
  - Response output R: 1 bit/C

Experimental Setup (Cont.)

- TDC PUF (Cont.)
  - Upper oscillation frequency: 41.4MHz
  - Lower oscillation frequency: 100MHz
  - Number of sampling for a calibration: 2^{17}
- Bit string: 128 bits
- Implementation
  - 15 proposed TDC PUFs and one embedded processor MicroBlaze are implemented on a chip
  - MicroBlaze (embedded processor)
    - Send challenge inputs to TDC PUFs
    - Receive counter values from TDC PUFs

Evaluation Metrics

- Intra-chip variation:
  - Average ratio of different bits among bit string when it is re-generated from same PUF→Metric of reproducibility
- Inter-chip variation:
  - Average ratio of different bits when two bit strings generated by two different PUFs→Metric of uniqueness
- Misclassification rate:
  - Probability that a PUF is mistook as other PUFs and other PUFs are mistook as the PUF

Calculation of Evaluation Metrics

- Intra-chip variation v_{intra}

$$v_{intra} = \frac{1}{N_q}\frac{1}{N_{PUF}}\sum_{i=1}^{N_{PUF}}\sum_{j=1}^{N_q}\frac{HD(B_i,B_{i,j})}{N_B}\times 100.\ (\%)$$

- Inter-chip variation v_{inter}

$$v_{inter} = \frac{2}{N_{PUF}\cdot(N_{PUF}-1)}\sum_{i=1}^{N_{PUF}-1}\sum_{j=i+1}^{N_{PUF}}\left(\frac{HD(B_i,B_j)}{N_B}\right)\times 100.\ (\%)$$

  - N_q: number of query, N_{PUF}: number of PUFs, B_i:bit string of ith PUF, $B_{i,j}$: bit string generated by the jth query of the ith PUF, N_B: length of generated bit strings, $HD(B_i, B_j)$: hamming distance between B_i and B_j

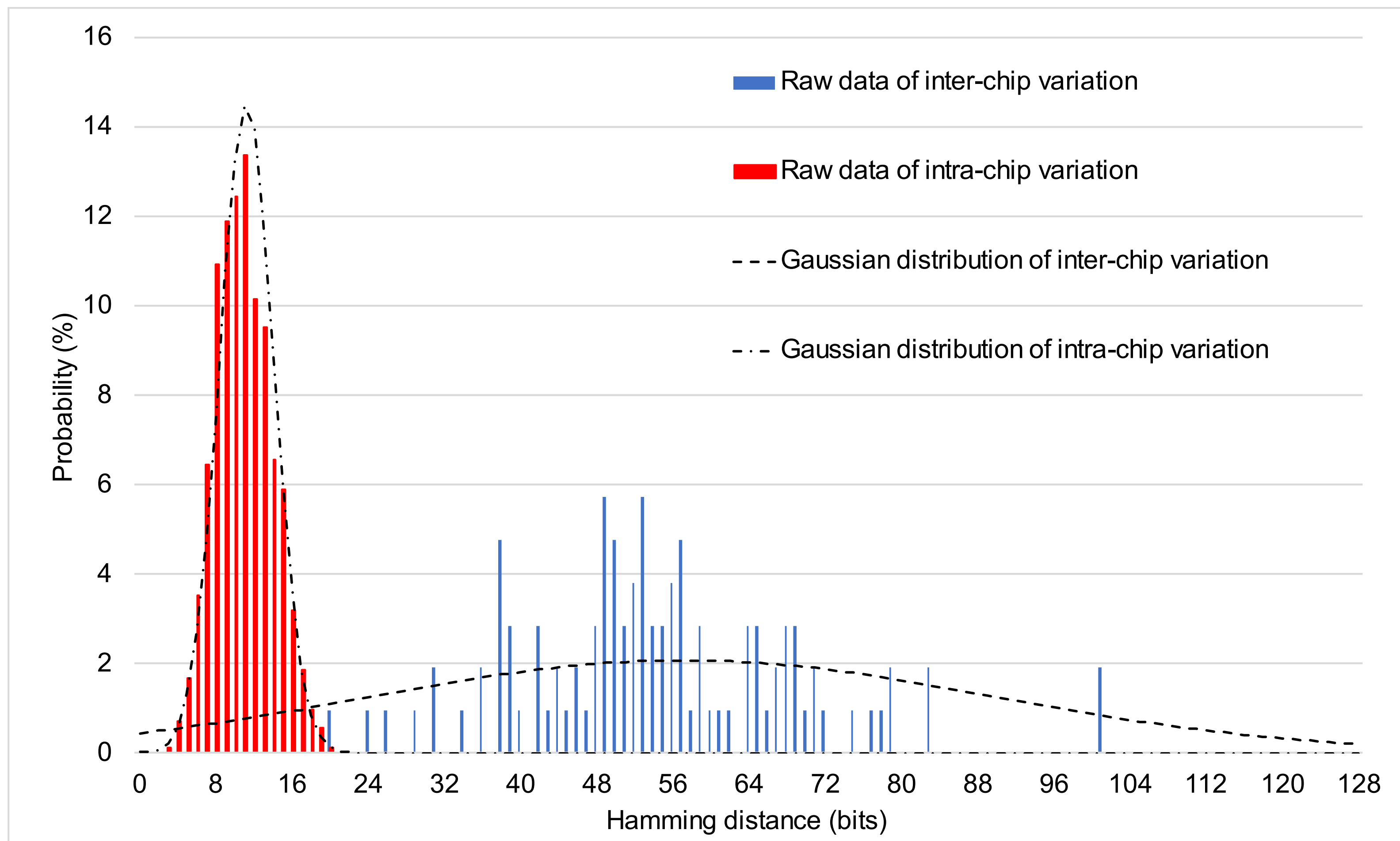
- Misclassification rate P_{mis}

$$P_{mis} = \sum_{i=0}^{N_B} A_{intra}\, A_{inter}\exp\left(-\frac{1}{2\sigma_{intra}^2}(i-u_{intra})^2-\frac{1}{2\sigma_{inter}^2}(i-u_{inter})^2\right)\times 100.\ (\%)$$

  - $A_{intra/inter}$, $u_{intra/inter}$, $\sigma_{intra/inter}$: parameters of Gaussian fitting of probability distribution of hamming distance of intra/inter-chip variation

Evaluation Results

	v_{intra} (%)	v_{inter} (%)	P_{mis} (%)
ideal	0	50	0
result	8.5	42.5	0.8



Conclusion

- Proposed PUF using flash TDC with linearity self-calibration using histogram method
- Utilizes uniqueness of nonlinearity of TDC
- Simple digital circuits: easy to implement on SoC and FPGA
- Evaluation with FPGA board
  - Intra-chip variation: 8.5 %
  - Inter-chip variation: 42.5 %
  - Misclassification rate: 0.8 %
  - meets the need for strong PUF

Appendix

- Calculation

$$P_{mis} = \sum_{i=0}^{N_B} A_{intra} A_{inter} \exp(-\frac{1}{2\sigma_{intra}^2}(i - u_{intra})^2 - \frac{1}{2\sigma_{inter}^2}(i - u_{inter})^2) \times 100. \ (\%)$$

  - A_{intra}, u_{intra}, σ_{intra}: parameters of Gaussian fitting of probability distribution of hamming distance of intra-chip variation
  - A_{inter}, u_{inter}, σ_{inter}: parameters of Gaussian fitting of probability distribution of hamming distance of inter-chip variation

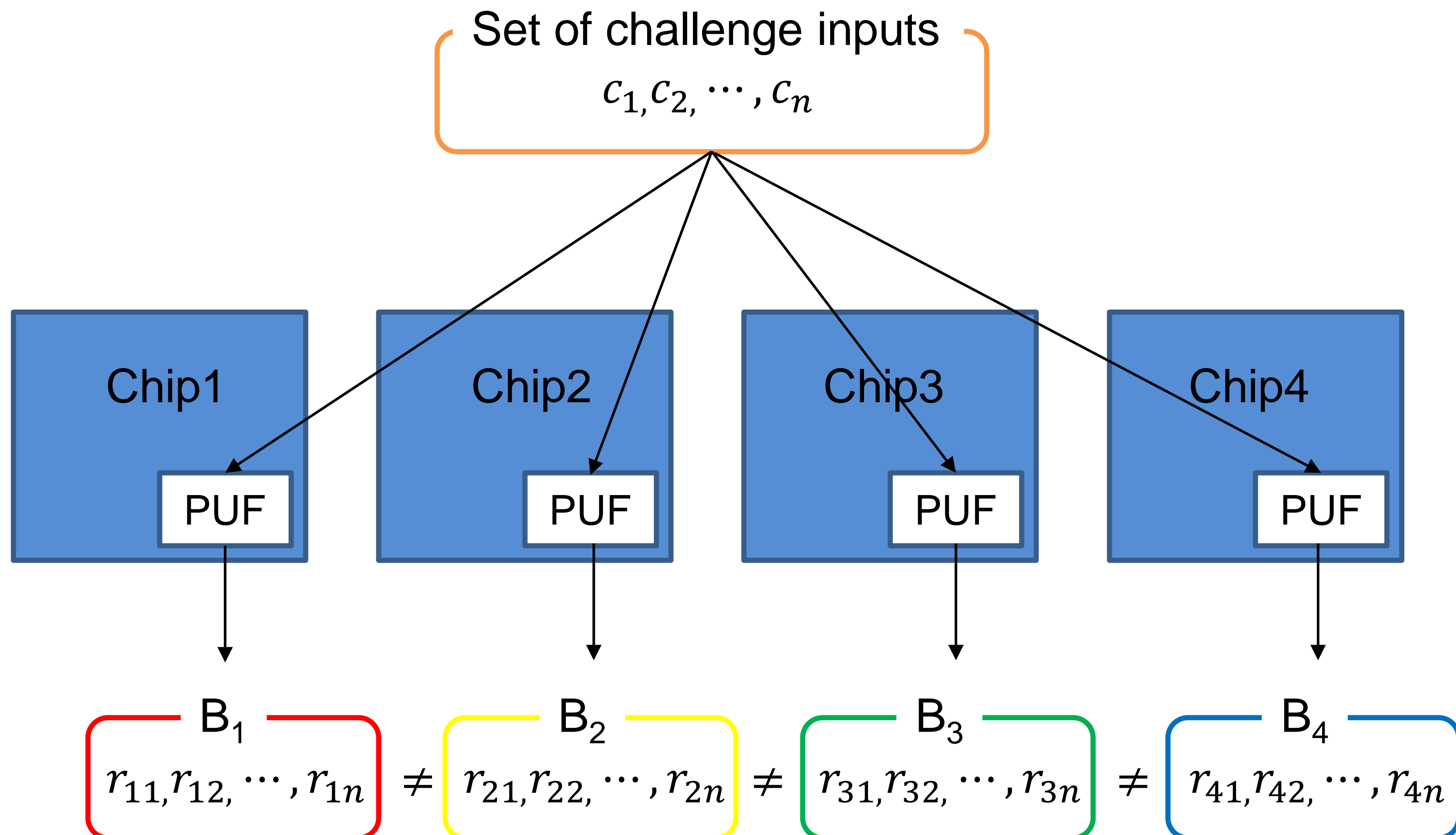
Misclassification rate (%)
0.8

Appendix

- Reproducibility and uniqueness
  - Reproducibility： ideally, a PUF generate identical bit string independent to external environment and time
  - Uniqueness: different PUF must generate different bit string
- Misclassification rate
  - Probability that a PUF is mistook as other PUFs and other PUFs are mistook as the PUF

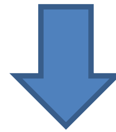
Appendix

- Bit string: set of response outputs of set of common challenge inputs



Appendix

- Variation among stages of TDC: give bad effects to function of TDC PUF



- Compensate variation among stages by multiplying COEF[n] to obtained bin[n]

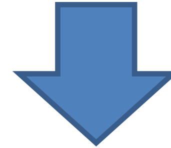
$$COEF[n] = \frac{1}{4} \times \sum_{ci=\{h00,h55,hAA,hFF\}} COEF_{ci}[n]$$

$$COEF_{ci}[n] = \frac{1}{b_{ci}[n]} \times \frac{\sum_{i=0}^{N} b_{ci}[i]}{N} \times 2^q$$

ci: value of CI[0:7]
$b_{ci}[n]$: bin length of nth stage
N: number of stages of TDC
q: required number of digits after decimal point

Appendix

- Longer wire length → Larger variation



Good for implementation of PUF

Appendix

- Use 4 CLB per 1 stage to compensate asymmetry of wire length
  - C[n] = 0:path → $l'_i - l_{i+1}$ C[n] = 1:path → $l_i - l'_{i+1}$