POSTER #14

Delay Characterization for FPGA PUFs Using Fully Synchronous On-Chip PLL Techniques

K. Katoh, T. Nakura
Fukuoka University

H. Kobayashi
Gunma University

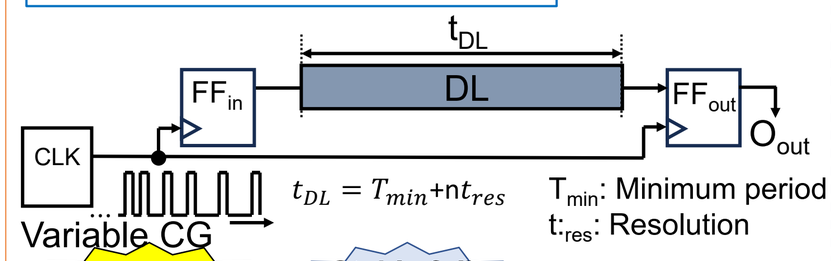
Introduction

- **Objective:**
  - To develop a high-resolution, reliable delay characterization method for FPGA-based Physical Unclonable Functions (PUFs) using fully synchronous on-chip Phase-Locked Loop (PLL) techniques.
- **Key Techniques:**
  - Utilizes two synchronous clock signals from an on-chip PLL-based Clock Generator (CG).
  - Adds minimal extra circuitry: only two Flip-Flops and two logic gates per characterization point.
  - Employs stochastic delay measurement with ps-level resolution (25.2ps without SSCG, 9.8ps with SSCG).
- **Advantages:**
  - Fully synchronous design ensures high reliability.
  - High-resolution delay characterization enables precise PUF evaluation.
  - Parallelization reduces total measurement time.
  - Applicable to broader domains like:·Built-Out-Self-Test (BOST) for memory
  - ATE timing skew adjustment
  - Timing calibration for test quality improvement
- **Conclusion:**
  - The proposed technique offers a compact, high-resolution, and reliable method for delay characterization in FPGA PUFs, with potential application domains.

Delay Characterization Using Fully Synchronous On-Chip PLL

Difference of Conventional and Proposed Delay Characterizations

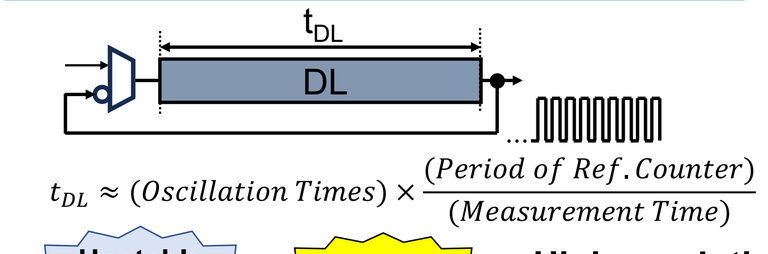
Conventional PLL-based



High-driving power PLL clock signals — Stable fully synchronous circuit

- High reliability
- Low (100ps-order)resolution

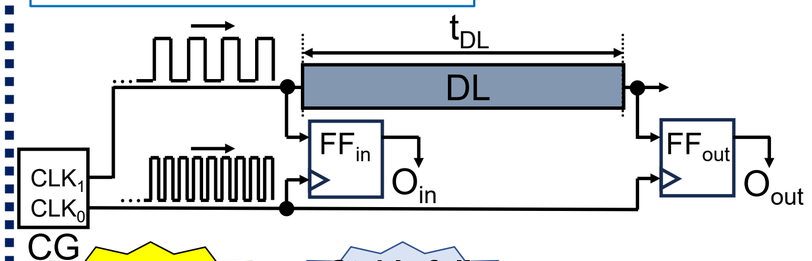
Conventional Ring Oscillator-based



Unstable asynchronous circuit — Vulnerable to Noise

- High resolution
- Low reliability

Proposed PLL-based

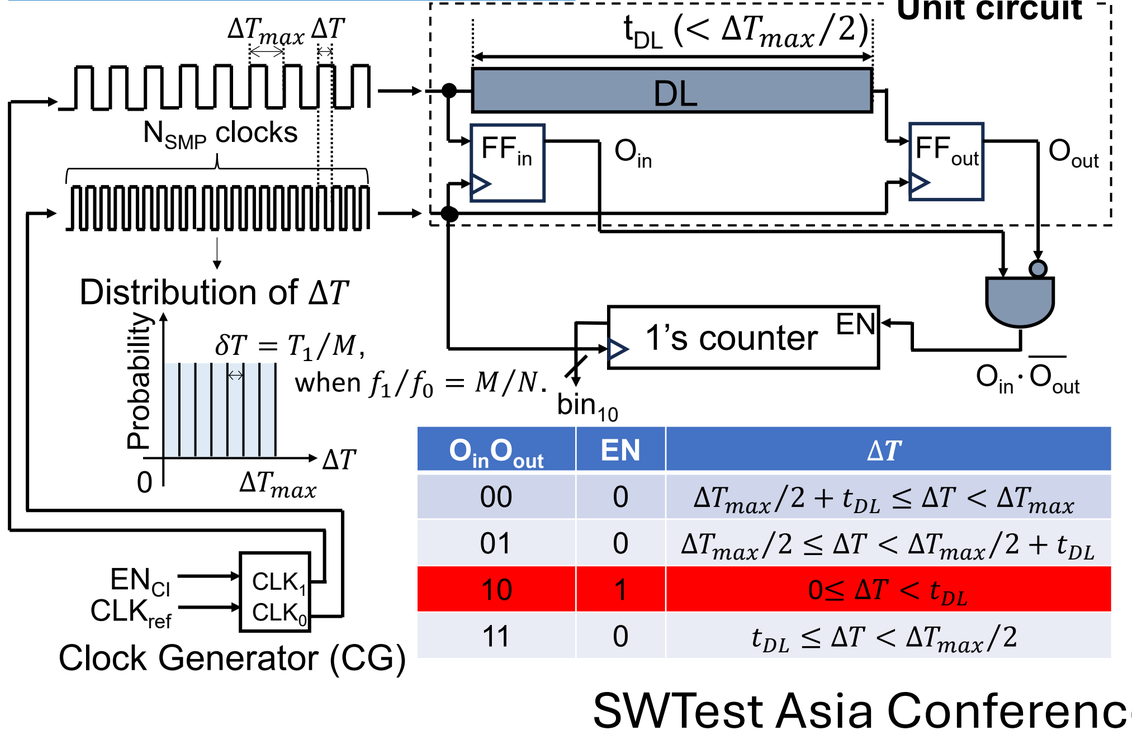


High-driving power PLL clock signals — Stable fully synchronous circuit

- High reliability
- High (10-25ps-order) resolution

Proposed Delay Characterization

Measurement Architecture

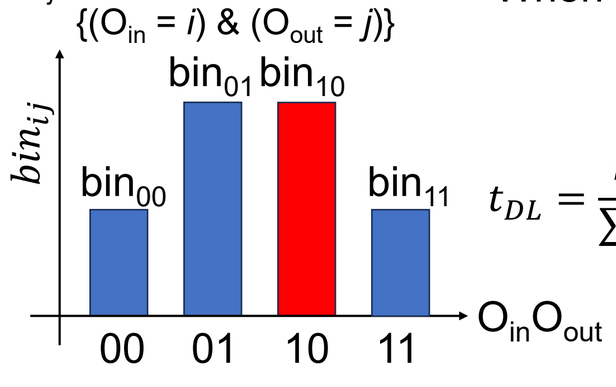


$O_{in}O_{out}$	EN	ΔT
00	0	$\Delta T_{max}/2 + t_{DL} \le \Delta T < \Delta T_{max}$
01	0	$\Delta T_{max}/2 \le \Delta T < \Delta T_{max}/2 + t_{DL}$
10	1	$0 \le \Delta T < t_{DL}$
11	0	$t_{DL} \le \Delta T < \Delta T_{max}/2$

How to Measure

- **Step 1: Sample O_{in} and O_{out} N_{SMP} times counting occurrence times of {(O_{in} = 1) & (O_{out} = 0)} with 1's counter, which is bin_{10}**
- **Step 2: Calculate t_{DL} with bin_{10}**

bin_{ij}: occurrence times of {(O_{in} = i) & (O_{out} = j)}



When N_{SMP} is sufficiently large,

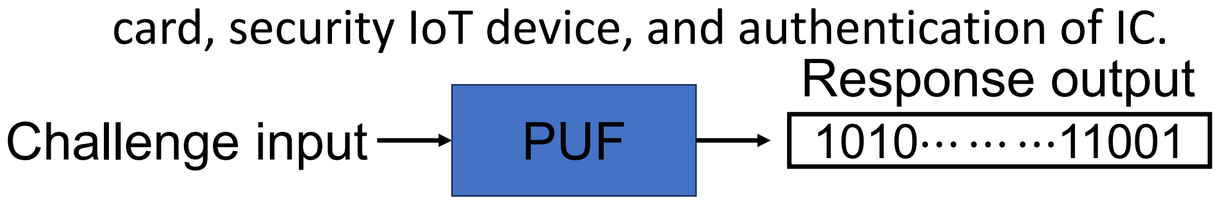
$$\frac{bin_{10}}{\sum bin_{ij}} \approx \frac{t_{DL}}{\Delta T_{max}}. \quad (1)$$

$$t_{DL} = \frac{bin_{10}}{\sum bin_{ij}} \Delta T_{max} = \frac{bin_{10}}{N_{SMP}} \Delta T_{max}. \quad (2)$$

Application of Proposed Delay Characterization for FPGA PUF

What is FPGA PUF?

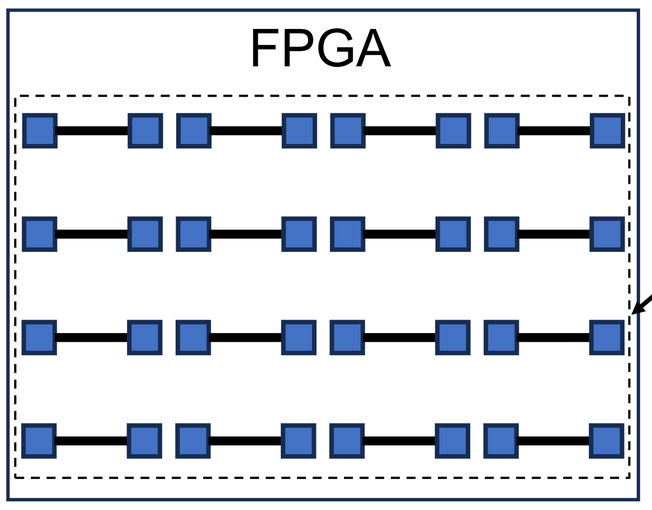
- **Physical Unclonable Function (PUF):**
  - An important security primitive.
  - Generates reproducible random values utilizing variation from manufacturing variation.
  - Random values: generated from set of challenge-response pairs (CRPs).
  - Application: authentication of smartphone and IC card, security IoT device, and authentication of IC.



- **FPGA PUF:** PUF for FPGA.
  - Random values: generated with delay variation.

Basics of Applied FPGA PUF

- **Basic idea:**
  - Generates random values using delays of variated identical delay-lines measured with proposed delay characterization technique.

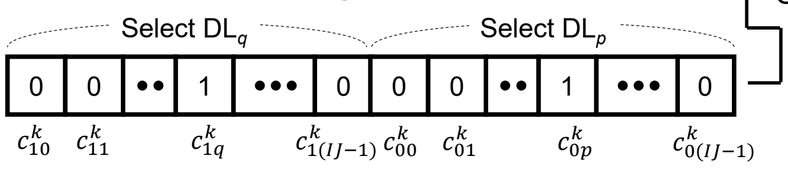


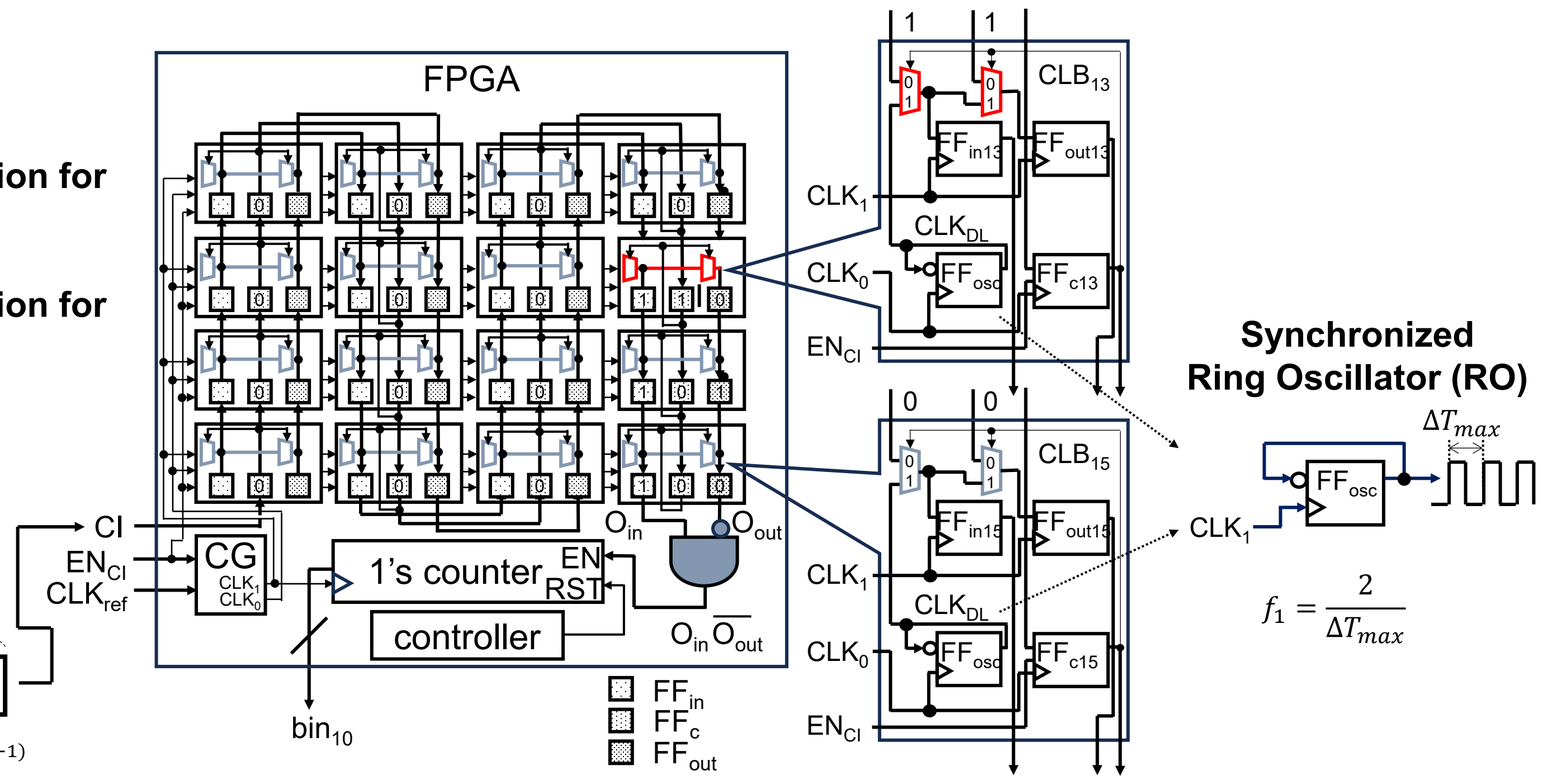
Applied FPGA PUF with 4×4 Delay-Line Array

1-Bit Response Output Generation Scheme

Step 1: Select the 1st delay-line (DL_p)
Step 2: Perform proposed delay characterization for DL_p measurement(bin_{10p})
Step 3: Select the 2nd delay-line (DL_q)
Step 4: Perform proposed delay characterization for DL_p measurement(bin_{10p})
Step 5: If $bin_{10p} > bin_{10q}$ response output is 1, otherwise 0

A Challenge Input Data

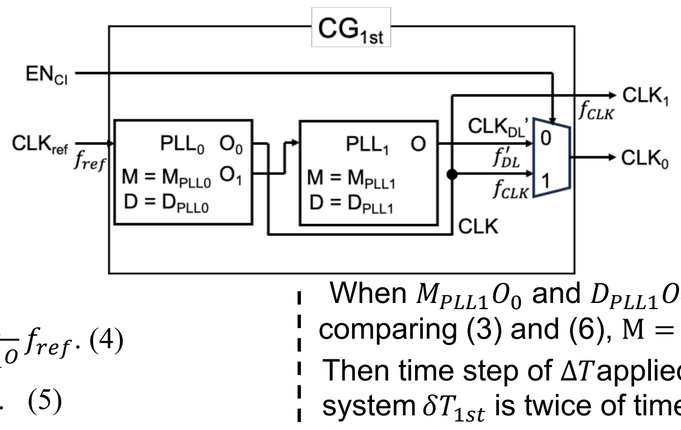




Clock Generators (CGs)

CG_{1st}: CG with Cascaded PLLs

f_1/T_1: frequency/ period of CLK_1
f_0/T_0: frequency/ period of CLK_0



$$\frac{f_1}{f_0} = \frac{M}{N}. \quad (3)$$

$$f_1 = \frac{M_{PLL0}M_{PLL1}}{D_{PLL0}D_{PLL1}O_1O} f_{ref}. \quad (4)$$

$$f_0 = \frac{M_{PLL0}}{D_{PLL0}O_0} f_{ref}. \quad (5)$$

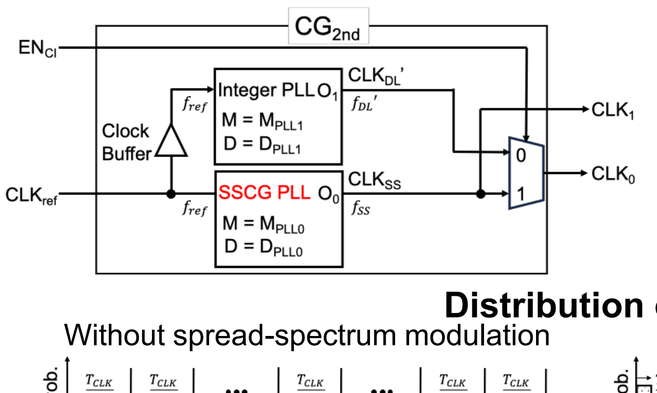
$$\frac{f_1}{f_0} = \frac{\frac{M_{PLL0}M_{PLL1}}{D_{PLL0}D_{PLL1}O_1O} f_{ref}}{\frac{M_{PLL0}}{D_{PLL0}O_0} f_{ref}} = \frac{M_{PLL1}O_0}{D_{PLL1}O_1O}. \quad (6)$$

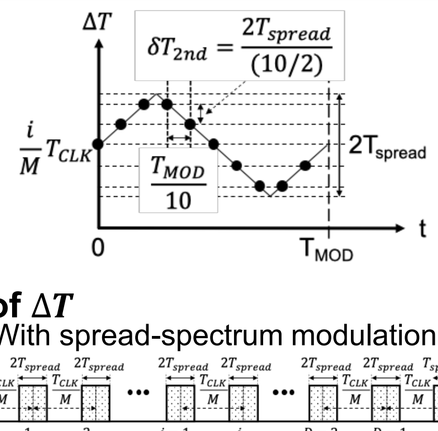
When $M_{PLL1}O_0$ and $D_{PLL1}O_1O$ are co-prime, comparing (3) and (6), $M = M_{PLL1}O_0$.

Then time step of ΔT applied to measurement system δT_{1st} is twice of time interval between CLK_0 & CLK_1.Accordingly,

$$\boldsymbol{\delta T_{1st} = \frac{2T_{CLK}}{M} = \frac{2T_{CLK}}{M_{PLL1O_0}}}. \quad (7)$$

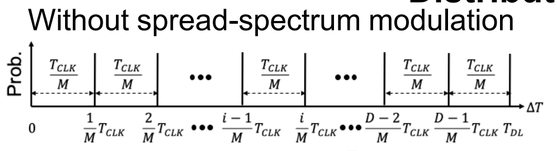
CG_{2nd}: CG with Spread-Spectrum CG PLL



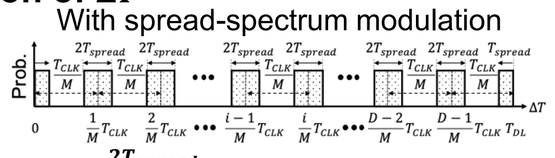


Distribution of ΔT

Without spread-spectrum modulation



With spread-spectrum modulation

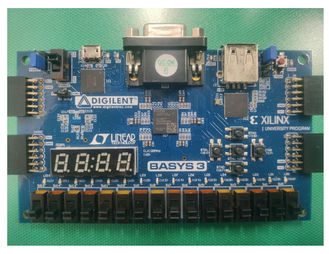


When $\frac{T_{CLK}}{M} = 2T_{spread}$, $\boldsymbol{\delta T_{2nd} = \frac{2T_{spread}}{(r/2)}}$. (8)

Evaluation of Applied FPGA PUF

Experimental Setup

- **# of PUFs: 20 PUFs (PUF_0-PUF_{19}) on 10 Artix-7 FPGA (XC7A35T) in Digilent Basys3 (2 PUFs/device) controlled by MicroBlaze**
- **Normal PLL: PLLE2, SSCG PLL: MMCME2**
- **Implementation tool: Vivado v2023.1**
- **f_{ref}: 100MHz, f_0: 50MHz**
- **f_1: CG_{1st} 52.87MHz, CG_{2nd} 105MHz (T_{spread}=487.805ps, f_{mod}=250kHz)**
- **Discrete time-step of time interval: δT_{1st}=25.2ps, δT_{2nd}=9.8ps**
- **N_{SMP}: 260096**
- **Response output: 128bits,used 1-out-of-8 masking scheme**



Basys3 FPGA board

Evaluation Metrics

- **Inter-Chip Hamming Distance (HD) HD_{INTER}: Uniqueness's**

$$HD_{INTER} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{N_{PUF}} \left(\frac{HD(R_i,R_j)}{n} \right) \times 100.0 \ (\%) \quad (9)$$

- **Intra-Chip HD HD_{INTRA}: Reliability's**

$$HD_{INTRA} = \frac{1}{N_q} \sum_{j=1}^{N_q} \frac{HD(R_i,R_{i,j})}{n} \times 100.0 \ (\%) \quad (10)$$

- **Uniformity $(Uniformity)_i$: Frequency of 1 in *i*-th PUF**

$$(Uniformity)_i = \frac{1}{n} \sum_{l=1}^{n} r_{i,l} \times 100.0 \ (\%) \quad (11)$$

- **Bit-aliasing $(Bit\text{-}aliasing)_l$: Frequency of 1 in *l*-th bit**

$$(Bit - aliasing)_l = \frac{1}{k} \sum_{i=1}^{k} r_{i,l} \times 100.0 \ (\%) \quad (12)$$

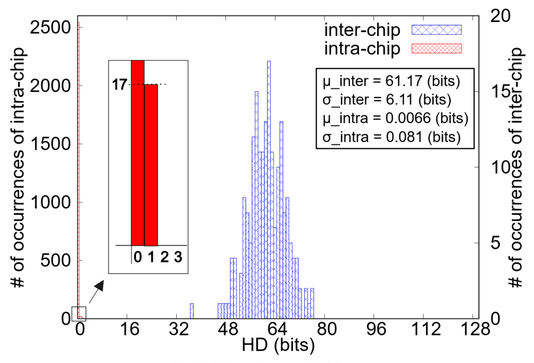
Evaluation of Applied FPGA PUF

Evaluation Results

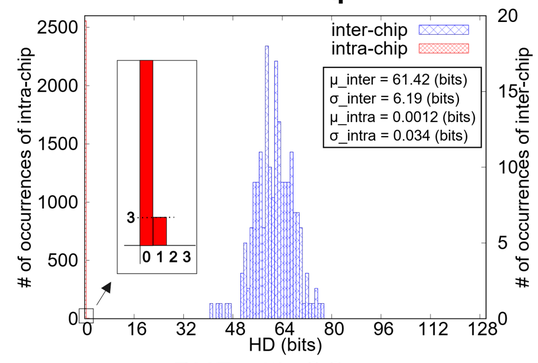
Average of inter-chip HD, intra-chip HD, & uniformity

Ref.	PUF Type	HD_{INTER}	HD_{INTRA}	Uniformity
[Suh07]	RO PUF	46.15	0.48	-
[Maiti11]	RO PUF	47.31	-	47-53
[Xin11]	RO PUF	41	0.71	-
[Pei18]	RO PUF	50.013	1.125	-
[Gupta24]	RO PUF	49.6	-	49.8
[Zheng16]	DScan PUF	49.9	-	-
[Anan22]	XOR PUF	48.69	0.59	50.73
[Rajput23]	APUF, XOR PUF	-	2	46.81
[G24]	Arbiter PUF	48.32	9.06	49.37
[Sala24]	NAND-PUF	49.50	1.38	50.20
[Sala24]	XOR PUF	49.47	1.06	50.29
[Sala24]	DD-PUF	49.38	1.67	51.22
[Sala24]	SS-RO-PUF	46.88	0.90	51.95
[Sala24]	PICO-PUF	48.32	2.33	50.24
[Sala24]	TERO-PUF	49.15	1.90	52.49
PUF with CG_{1st}		47.79	0.0052	50.9
PUF with CG_{2nd}		47.98	0.00092	51.13

Distribution of HD_{INTER} and HD_{INTRA} (k=20, N_q=128)

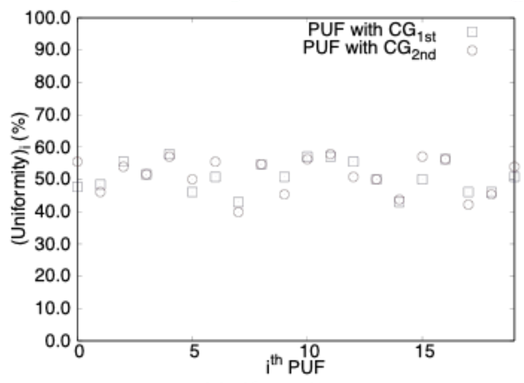


PUF with CG_{1st}

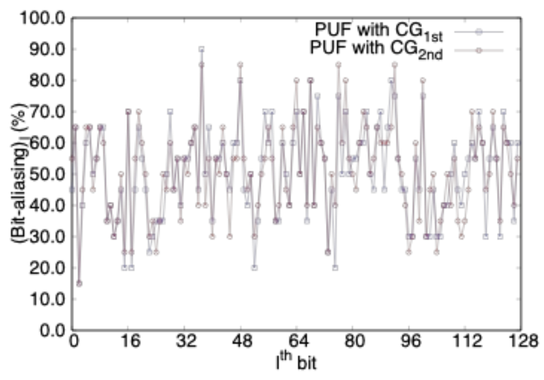


PUF with CG_{2nd}

Uniformity & Bit-aliasing

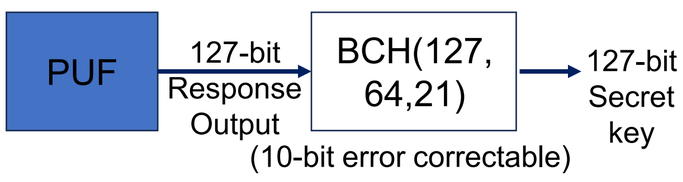


Uniformity



Bit-aliasing

Error probability of 127-bit secret-key generator



	Error probability
[Suh07]	4.53×10^{-11}
PUF with CG_{1st}	5.66×10^{-15}
PUF with CG_{2nd}	8.88×10^{-15}

Conclusion

- Applied proposed delay characterization technique for weak FPGA PUF
- Confirmed that resolution of delay characterization is 10-25ps.
- Performance of applied FPGA PUF
  - Inter-chip HD: 47.9%, Intra-chip HD: 0.003%
  - Error probability of an application: 1/10000 of high-reliability RO PUF

Possible Other Applications

- **Built-Out-Self-Test (BOST) for memory**
  - Timing test of inputs and outputs of high-speed memory.
- **ATE timing skew adjustment**
  - Delay adjustment of input and output pins of ATE instead of TDCs.
- **Timing calibration for test quality improvement**
  - Timing calibration of instruments for delay measurement such as time-to-digital converters.
- **Delay characterization and test of 3D IC and Chiplet**
  - Delay characterization, online, and offline test of TSVs of 3D IC and critical wires between dies of Chiplet.

Questions ?

If you have any questions, please contact

Fukuoka University	Gunma University
Kentaroh Katoh	Haruo Kobayashi
+81-92-871-6631	+81-277-30-1700
kentarohkatoh@fukuoka-u.ac.jp	koba@gunma-u.ac.jp

Related Links

Some related links for authors' information

- https://researchmap.jp/read859
- https://www.linkedin.com/in/kentaroh-katoh-ba1358175/
- https://orcid.org/0009-0003-5140-2413