ROBUSTNESS OF THE LOOP PUF

EXPERIMENTAL EVALUATION UNDER ISO/IEC 20897

Authors:

Lukas Vlasak, Khaled Karray, François Forlot,

Idris Rais-Ali, Oualid Trabelsi, Sylvain Guilley

Version 1.0

SECURE-iC THE SECURITY SCIENCE COMPANY

MOTIVATION

- PUF systems generate unique and random keys, that can be used for authentication
- Lightweight and unclonable hardware-based security without necessity to store the key
- For all security devices it is important to evaluate the PUF using a robust methodology
- PUFs can be employed under different environmental conditions and for a long period of time
- Existing methods (ISO/IEC 20897) provide a rather vague incomplete method

SECURE-iC
THE SECURITY SCIENCE COMPANY

CONTRIBUTION

- We have conducted an evaluation of the Loop-PUF [1] design on FPGA
- Variety of environmental conditions: Internal parameter, Voltage, Temperature, aging
- Adress some shortcomings of the ISO/IEC 20897 and definition of precise and statistically grounded pass/fail criteria

[1] Cherif, Z., Danger, J. L., Guilley, S., & Bossuet, L. (2012, September). An easy-to-design PUF based on a single oscillator: The loop PUF. In 2012 15th Euromicro Conference on Digital System Design (pp. 156-162). IEEE.

LOOP PUF DESIGN

- Oscillation Loop with configurable delay elements
  - 8 entropy sources per device
  - 63 possible challanges

- For an entropy source *i*, a challenge *c* and its complement, we measure thenumber of oscillations under this configuration 2 times:

$$\Delta_c = \big(S_{i,0}(c) - S_{i,1}(c)\big) - \big(S_{i,0}(\bar{c}) - S_{i,1}(\bar{c})\big)$$

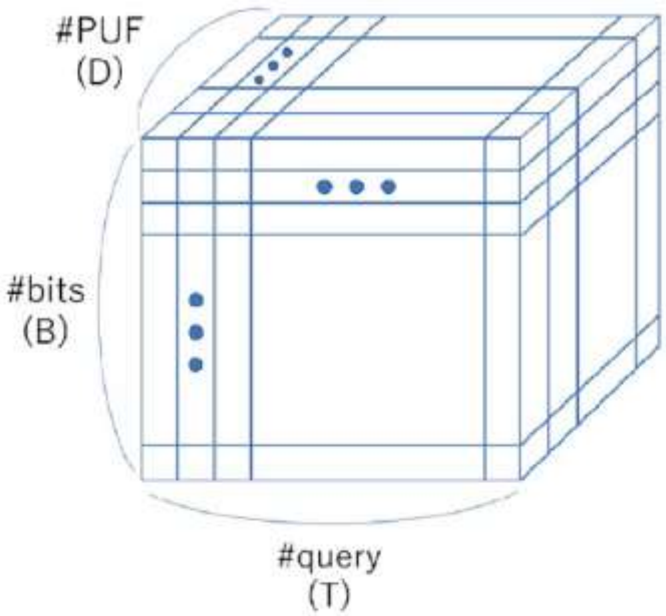
- The PUF is called in two contexts:
  - **Enrollment:** process of selecting challenges for reference key
  - **Rebuild:** reconstructing the key

- Post-processing Error correction with Hamming-Code (8,4) on 4-bit segments
  - Correction capacity: 1 bit
  - Detection capacity: 2 bits

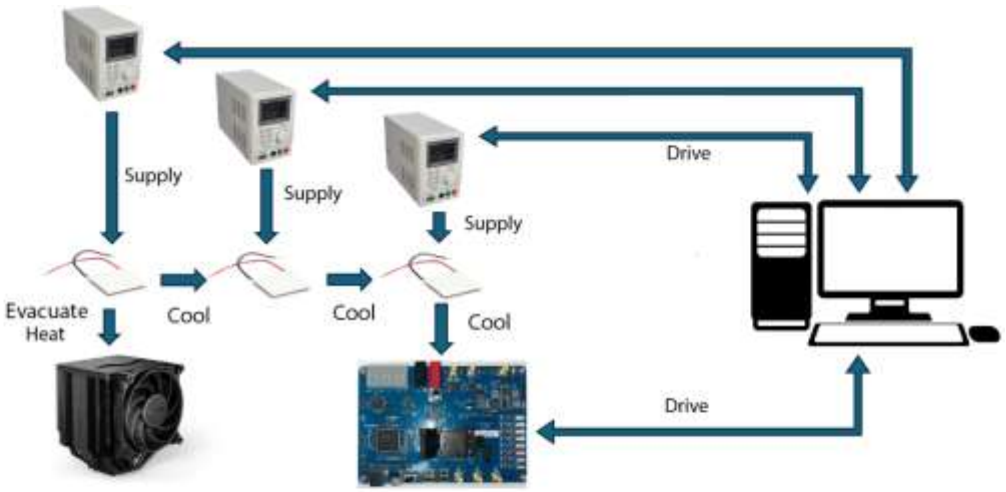
EVALUATION UNDER ISO/IEC 20897

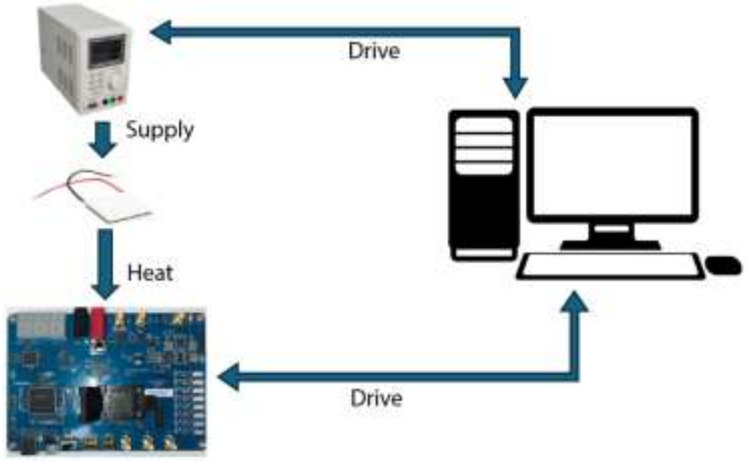
- Requirements for PUFs are defined in the ISO/IEC 20897:
  - **Entropy:** unpredictable
  - **Stability:** always the same
  - **Unicity:** always different (on two devices)

- The functionality is tested under different cicumstances:
  - **Latency**: 10, 30, 50, 70, 90 k-cycles
  - **Voltage**: 0.95V, 1.0V, 1.05V
  - **Temperature**: 0°C, room temperature (25-35 °C), 85°C
  - **Aging**



EXPERIMENTAL SETUP





Type	Name	Purpose
FPGA	Xilinx Artix-7 XC7A100T	Target of Evaluation
Evaluation Board	FlexEval Board rev 1.1	Evaluation platform
Power Supply	Vellman LABPS3005DN	Peltier power source
Peltier Modules	Tark Thermal Solution 13x13, MOUSER 15x15, MULTICOMP PRO 30x30	Thermal control system
Heatsink	Cooler Master Hyper 212 EVO	Heat dissipation

ACCELERATED AGING

- Accelerated aging based on experiments by Li *et al.* [2]

- Combination of temperature, voltage, and logic activity accelerates degradation mechanisms

- Accelerated Aging Scenario
  - **Temperature stress**: 85°C or 75°C (night and holydays for safety related reasons)
  - **Voltage stress**: 1.05V
  - **Functional stress**: continuously use more than 99% of the FPGA LookUp Tables (LUTs)
  - Stress is applied for 10 successive days

- We used 100 FPGAs
  - 50 devices before and after aging
  - 50 only before aging

[2] Zeyu Li, Zhao Huang, Quan Wang, Junjie Wang, and Nan Luo. Implementation of aging mechanism analysis and prediction for xilinx 7-series fpgas with a 28-nm process. Sensors, 22(12), 2022.

TESTING METRICS

- **Randomness** – NIST SP800-22 [3]
  - Monobit Test

  - Frequency within a block Test

  - Runs Test

Proportionality:

$$(1-\alpha)\pm 3\sqrt{\frac{\alpha(1-\alpha)}{D}}$$

Uniformity:

$$\chi^2 = \sum_{i=1}^{10} \frac{\left(F_i - \frac{T}{10}\right)^2}{\frac{T}{10}} \qquad \mathrm{igamc}\left(\frac{10-1}{2}, \frac{\chi^2}{2}\right) \geq 0.0001$$

- *[3] National Institute of Standards and Technology. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report 800-22 Rev 1a, U.S. Department of Commerce, Washing*

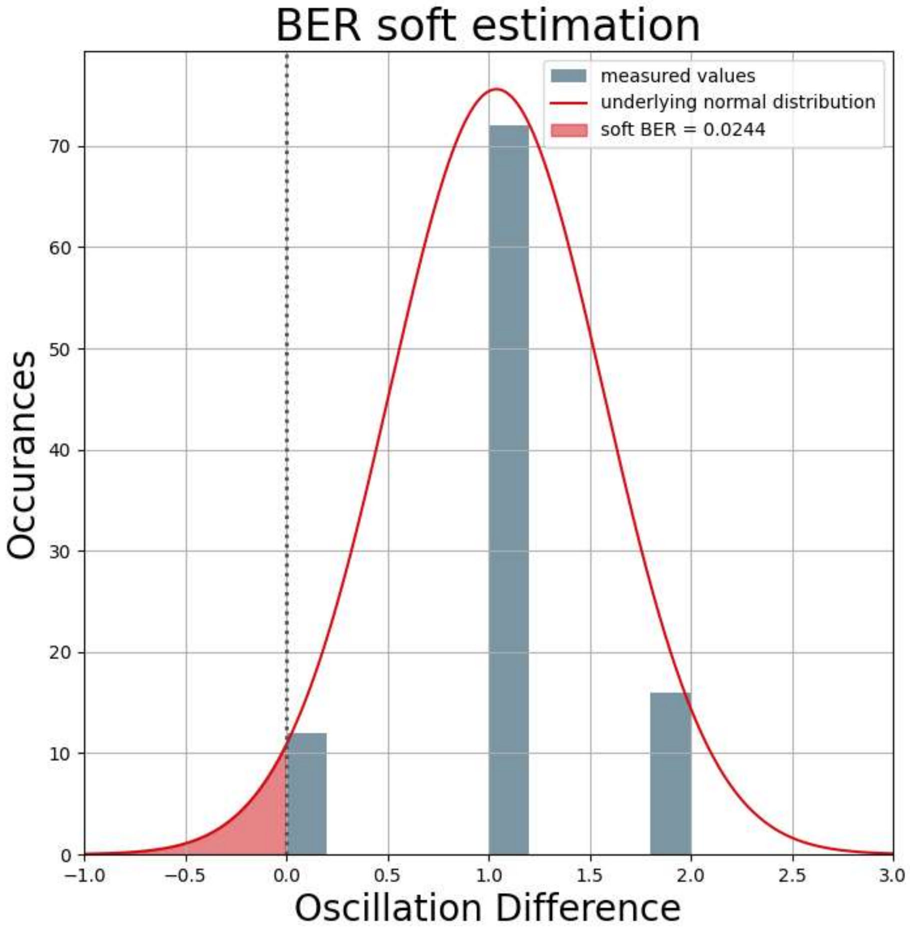
TESTING METRICS

- **Stability**
  - Success rate
    - Fail criterion: any fail after post processing
  - Intra HD [4] :

Stability parameter *S*

$$\frac{1}{T}\sum_{i=1}^{T}\frac{HD_{intra}(R,R_i)}{B} \in [0,1]$$

    - On **key** derived from raw data (before ECC)
    - Optimal value: 0
    - Fail criterion: based on ECC detection capacity
  - Bit-Error-Rate *(BER)* [5]
    - On **raw data**
    - Never 0
    - Probabilistic evidence
    - Fail criterion: $\#\{(p,c) \in PUF \times Chal \mid BER_p(c) < .001\} < 32$



- *[4] Tetsufumi Tanamoto, Satoshi Takaya, Nobuaki Sakamoto, Hirotsugu Kasho, Shinichi Yasuda, Takao Marukame, Shinobu Fujita, and Yuichiro Mitani. Physically unclonable function using initial waveform of ring oscillators on 65 nm cmos technology*
- *[5] Alexander Schaub, Jean-Luc Danger, Sylvain Guilley, and Olivier Rioul. An improved anal ysis of reliability and entropy for delay pufs.*

TESTING METRICS

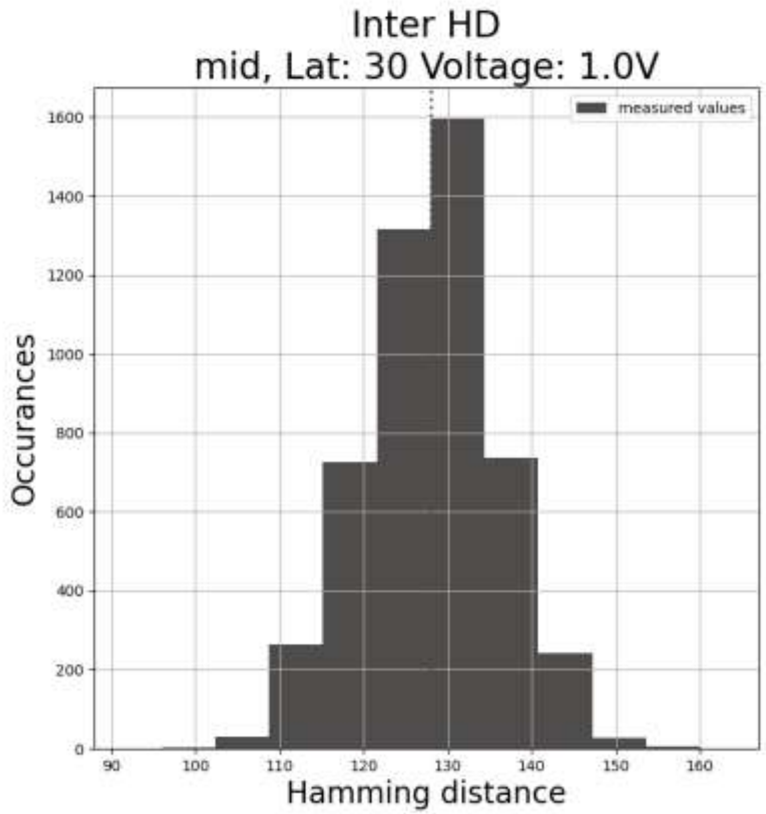
Uniqueness

- Inter HD [4]:

Uniqueness parameter *U*

$$\frac{2}{D(D-1)} \sum_{i=1}^{D-1} \sum_{j=i+1}^{D} \frac{HD_{inter}(R_t^i, R_t^j)}{B} \in [0,1]$$

- Normal distribution with
  - $\mu = 0.5\,B$
  - $\sigma = \sqrt{(B)}/2$
  - Fail criterion:
    - $|\,\mu - U\,| > 2\sigma$
    - any x with $3.7\sigma < |\,\mu - x\,|$



- *[4] Tetsufumi Tanamoto, Satoshi Takaya, Nobuaki Sakamoto, Hirotsugu Kasho, Shinichi Yasuda, Takao Marukame, Shinobu Fujita, and Yuichiro Mitani. Physically unclonable function using initial waveform of ring oscillators on 65 nm cmos technology*

RESULTS - STABILITY

- BER
  - Number of challenges with:

$$BER_{soft}(c) < 10^{-4}$$

- Observed errors
  - detection capacity of ECC

- **Voltage**: no effect
- **Temperature**: cold<mid<hot
- **Aging**: slightly worse results

Temp.	Lat.	Before Aging Max	Before Aging Mean	Before Aging Min	After Aging Max	After Aging Mean	After Aging Min	#errors Max
0°C	10	31	18	6	29	17	9	17
	30	55	45	32	54	45	33	2
	50	60	51	38	59	51	41	
	70	62	54	42	62	54	45	
	90	62	55	45	62	55	46	
25°C	10	28	16	5	28	16	9	17
	30	54	43	31	54	43	33	2
	50	60	50	39	59	50	41	
	70	60	53	43	60	53	45	
	90	61	54	44	61	55	46	
85°C	10	26	13	4	24	13	4	21
	30	53	42	30	51	42	31	2
	50	59	49	39	58	49	40	
	70	61	52	41	60	52	42	
	90	61	54	44	60	54	43	

RESULTS - STABILITY

- Stability parameter *S*

- Worst cases:
  - *Cold + low voltage*
  - *Hot + high voltage*
  - *Visible aging effect*

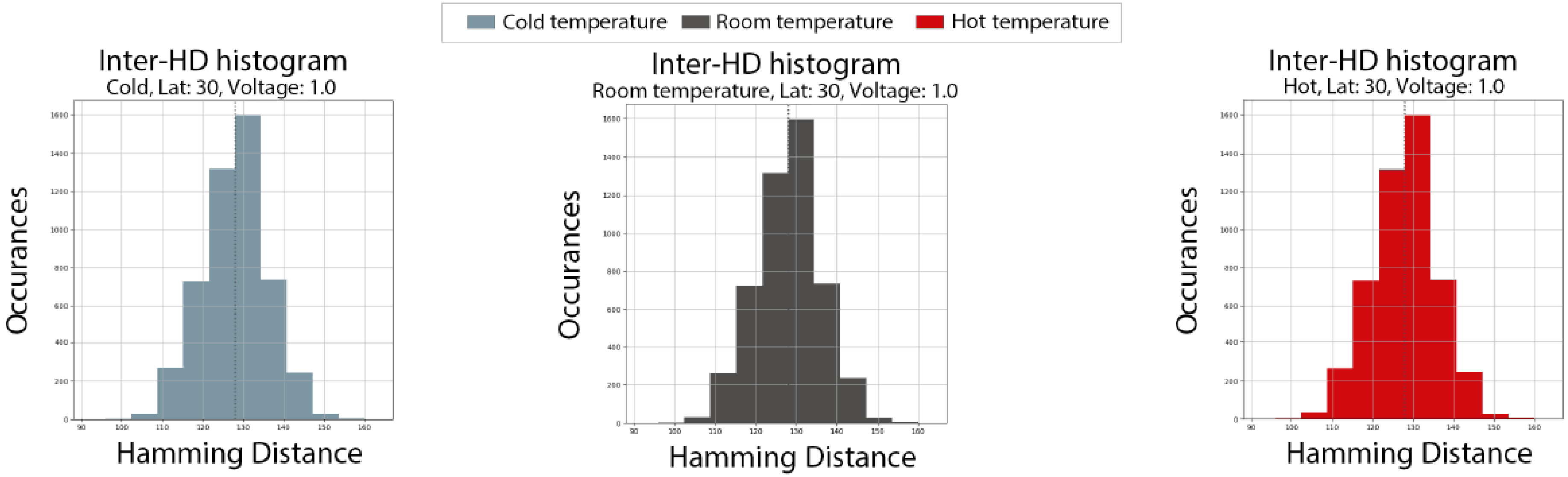
- Average case:
  - Good stability
  - Accepted fail probability 10-15 times higher for latency 30

		Before Aging						After Aging					
Temp.	Lat.	Mean			Max			Mean			Max		
		0.95V	1.0V	1.05V	0.95V	1.0V	1.05V	0.95V	1.0V	1.05V	0.95V	1.0V	1.05V
0°C	10	1.4382	1.3030	1.3445	2.7969	2.8008	3.0781	1.4467	1.3486	1.3744	2.7109	2.5000	2.3281
	30	0.0159	0.0089	0.0078	0.3672	0.2461	0.1094	0.0212	0.0117	0.0104	0.2930	0.2656	0.1445
	50	0.0060	0.0024	0.0020	0.3438	0.1641	0.0781	0.0103	0.0030	0.0020	0.2344	0.1172	0.0391
	70	0.0045	0.0012	0.0005	0.2695	0.0977	0.0117	0.0077	0.0017	0.0012	0.1875	0.0625	0.0312
	90	0.0030	0.0005	0.0005	0.1758	0.0391	0.0195	0.0056	0.0009	0.0003	0.1445	0.0312	0.0156
25°C	10	1.6277	1.5433	1.7142	3.1797	2.9844	3.0234	1.6798	1.6667	1.8098	2.7695	2.9023	2.9023
	30	0.0045	0.0033	0.0062	0.0859	0.0664	0.1367	0.0059	0.0041	0.0077	0.0820	0.0469	0.1602
	50	0.0007	0.0011	0.0014	0.0117	0.0234	0.0820	0.0005	0.0004	0.0011	0.0039	0.0039	0.0391
	70	0.0004	0.0007	0.0010	0.0039	0.0195	0.0547	0.0005	0.0002	0.0004	0.0078	0.0039	0.0156
	90	0.0003	0.0004	0.0003	0.0039	0.0078	0.0117	0.0003	0.0005	0.0005	0.0039	0.0078	0.0156
85°C	10	2.2488	2.2975	2.4457	3.9570	4.4258	4.8398	2.3066	2.3767	2.5170	4.0469	4.4766	4.0391
	30	0.0117	0.0145	0.0280	0.1758	0.2305	0.2461	0.0090	0.0140	0.0284	0.1211	0.1406	0.2188
	50	0.0026	0.0039	0.0062	0.1172	0.1367	0.0938	0.0036	0.0034	0.0073	0.0898	0.0508	0.1836
	70	0.0005	0.0012	0.0045	0.0273	0.0430	0.1211	0.0008	0.0011	0.0039	0.0273	0.0352	0.1328
	90	0.0005	0.0008	0.0020	0.0273	0.0352	0.0625	0.0007	0.0004	0.0027	0.0312	0.0078	0.1016

RESULTS - UNIQUENESS

- Uniqueness parameter *U*
  - *All results "close" to 50%*
  - *No significant outliers in any scenario*
  - *Visible normal distribution*

Latency	~ 0°C			~ 35°C			~ 85°C		
	0.95 V	1.0 V	1.05 V	0.95 V	1.0 V	1.05 V	0.95 V	1.0 V	1.05 V
10	49.92	49.88	49.92	49.90	49.89	49.88	49.80	49.79	49.79
30, 50, 70, 90	49.98	49.98	49.98	49.98	49.98	49.98	49.98	49.98	49.98



RESULTS - RANDOMNESS

- NIST SP 800-22 *selected tests*
  - *After aging the percentage of “failed” tests doubles because all devices that failed the entropy tests were randomly selected for aging*

Temp.	Test	Prop. (NA)	Prop. (A)	Unif. (NA)	Unif. (A)
$\sim 0°C$	Monobit	97%	94%	0.10562	0.12962
	Freq. Block	99%	98%	0.57490	0.69931
	Runs	100%	100%	0.26225	0.73992
$\sim 35°C$	Monobit	97%	94%	0.09372	0.22482
	Freq. Block	99%	98%	0.55442	0.69931
	Runs	100%	100%	0.30413	0.69931
$\sim 85°C$	Monobit	97%	94%	0.10253	0.36692
	Freq. Block	99%	98%	0.55442	0.69931
	Runs	100%	100%	0.41902	0.85138

DISCUSSION

- Evaluation methodology:
  - Can the method be generalized for other PUF designs?
  - Refinement of some of the evaluation parameters
  - Consider side-channel or fault attacks
- Accelerated aging:
  - Was the aging not aggressive enough?
  - Voltage beyond recommendation
  - Extended aging phase, perhaps 1 month
  - Checkpoints every week or day to observe trends
- Target selection:
  - material with larger temperature and voltage range
  - Follow up experiment on ASIC target

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
TAIWAN	sales-TAIWAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

FOLLOW US ON SOCIAL MEDIA