A Survey on Physically Unclonable Function: its Basics and Current Progress

Kentaroh Katoh[1,a,*], Toru Nakura[1,b], and Haruo Kobayashi[2,c]

[1]Dept. of Electronics Engineering and Computer Science, Faculty of Engineering, Fukuoka University, 8-19-1 Nanakuma Jonan-ku, Fukuoka 814-0180, Japan

[2]Emeritus Professor, Gunma University, 1-5-1 Tenjin-cho, Kiryu Gunma 376-8515, Japan

*Corresponding author

[a]<kentarohkatoh@fukuoka-u.ac.jp>, [b]<nakura@fukuoka-u.ac.jp>, [c]<koba@gunma-u.ac.jp>

Keywords: physically unclonable function, basics, current progress, device, entropy source

Abstract. PUF is an important hardware security device that can be used for authentication and encryption key generation. PUFs, also known as device fingerprints, can generate random digital values that can be regenerated using physical quantities that are correlated with manufacturing variations. PUF can be used to prevent the distribution of counterfeit products, to authenticate IoT devices at low cost, and to realize more secure communication technologies. In the academic field, numerous PUFs utilizing different physical properties influenced by manufacturing variations have been proposed. This paper briefly surveys PUFs that have been proposed in the academic field. In this survey, the PUFs are categorized into seven categories. Some of the current research works of each category are introduced after the explanation of the basic working principle of the typical PUFs in each category.

1. Introduction

In recent years, both the US and the global semiconductor industry have witnessed a troubling increase in counterfeit ICs [1]. They say that the globalization of the IC design and manufacturing industry, and changes in the procurement methods of IC users are the background to the distribution [2, 3]. Counterfeit ICs pose serious challenges to global supply chains, particularly for the defense, automotive, and aerospace industries [4]. The distribution of semiconductor counterfeit products causes leakage of personal information and software information in chips, and hacking of devices.

Assignment of unique authentication ID to each device is a conventional countermeasure against semiconductor counterfeits. A unique authentication ID for device authentication is written to the non-volatile memory such as EEPROM and flash memory of each device, and a genuine or imitation product is identified by this information. However, this method has the disadvantage of being vulnerable to side-channel attacks and easy to replicate. On the other hand, the cost of using tamper-resistant memory that is resistant to side-channel attacks is high.

Physically Unclonable Function (PUF) is a circuit technology that complements the drawbacks of conventional authentication technologies and performs individual authentication using variations in the manufacturing of devices that are physically difficult to replicate. Variations in device manufacturing lead to differences in the delay time of electrical signals, leakage currents, the initial state of the memory, and so on. PUFs use these physical quantities to generate device-specific bit strings. This bit string is also called a device fingerprint because it is reproducible and reflects the manufacturing variability inherent in the device.

This paper briefly surveys PUFs that have been proposed in the academic field. In this survey, the PUFs are categorized into seven categories. Some of the current research works of each category are

introduced after the explanation of the basic working principle of the typical PUFs in each category. After reviewing the fundamental concepts of PUF in Section 2, we provide a comprehensive survey the PUFs in Section 3. Finally, we conclude the paper.

2. Basics

This section reviews the basics of PUF. Subsection 2.1 gives a system-level model of PUF which is in common with most of PUFs. Subsection 2.2 shows generation of unique response outputs from a common challenge input. Subsection 2.3 describes classification of Strong PUF and Weak PUF. Finally, subsection 2.4 explains popular evaluation metrics of performance of PUFs.

2.1 System-Level Model of PUF

Fig. 1 shows the system-level model of PUF. PUF can be modeled at the system level as a challenge-response system that is a black box with a challenge input c and a response output r [5]. Conceptually expressed in mathematical terms, output r can be regarded as a function of f with input c. Unlike normal function, output r depends not only on c but also on device-specific manufacturing variations.

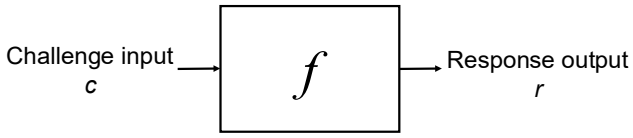


Fig. 1. System-level model of PUF.

2.2 Generation of Unique Response Output

A challenge input common to the PUFs on each device is input to the PUFs to obtain response outputs. Since the output response of the PUF depends on the challenge input and the variation in device manufacturing, the response output is expected to be unique to each device. Let the ith challenge input be c_i and the 1-bit response output of c_i be r_i. The response output $r_1r_2\cdots r_n$ of the challenge input $c_1c_2\cdots c_n$ is expected to be a device-specific n-bit bit string. In Fig. 2, a common challenge input $c_1c_2\cdots c_n$ is input to PUFs on Device 1, Device 2,⋯, Device m to generate n-bit unique response outputs $r_{11}r_{12}\cdots r_{1n}$, $r_{21}r_{22}\cdots r_{2n}$,⋯, $r_{m1}r_{m2}\cdots r_{mn}$.

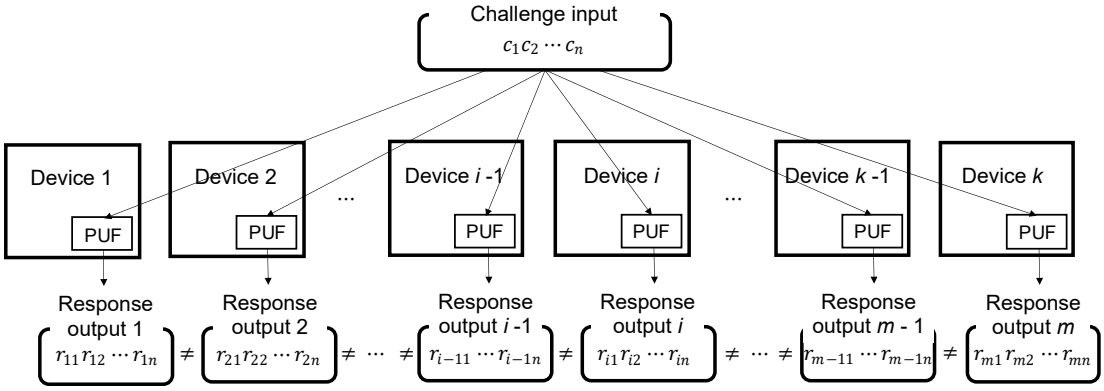


Fig. 2. Generation of unique n-bit response outputs with common challenge input.

2.3 Strong PUF and Weak PUF

PUFs are classified into Strong PUFs and Weak PUFs. Strong PUF supports large number of CRPs that is on the order of exponential. Consequently, it is not possible (in a reasonable time) to read

exhaustively the whole set of CRPs [6]. Therefore, it is strong to tamper and brute force attacks. Mainly, it is used for device authentication. On the other hand, Weak PUF supports small number of CRPs that is on the order of linear or polynomial [7]. That is vulnerable to tamper and brute force attacks, while that has high reliability, which means little error exists in the response outputs. Mainly it is used for private key generation for secure communication or IP protection [5, 8].

Both PUFs require enough uniqueness. Since Weak PUFs are used for cryptographic application, Weak PUFs must have higher reliability than Strong PUFs. Since Strong PUFs are used for device authentication of numerous products, Strong PUFs must generate longer-length response output. As a result, Strong PUFs must support huge number of CRPs with low chip area [6].

2.4 Evaluation Metrics

This section shows the evaluation metrics widely used to assess the performance of PUFs. Subsubsection 2.4.1 explains uniqueness and reliability which are the most important metrics and therefore, evaluated in almost all of the PUFs. Subsubsection 2.4.2 shows other popular metrics.

2.4.1 Uniqueness and Reliability

A PUF needs uniqueness and reliability. The response output generated by a PUF must be unique to the device. It is uniqueness. Ideally, a PUF must generate a unique response output even when the external environment changes, noise occurs, and time goes. It is reliability.

Inter-chip Hamming distance (HD) is a metric of uniqueness. Inter-chip HD is defined as average HD among response outputs of PUFs. Larger inter-chip HD is desired. The ideal value is 50% of the length of the response outputs. Inter-chip HD HD_{INTER} (%) is expressed as follows [9]:

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

where k is the number of devices, $HD(R_i, R_j)$ is the Hamming distance between the response outputs R_i and R_j, and n is the bit-length of the response outputs. Almost all works use Eq. (1) or the modified ones for evaluation of uniqueness.

To define reliability quantitatively, at first, we define intra-chip HD. Intra-chip HD of a PUF is the average of Hamming distance of response outputs which are generated consecutively under an environment (different from the environment where the device ID is obtained) to the device ID. Smaller intra-chip HD is desired. The ideal value is 0%. Intra-chip HD HD_{INTRA} (%) is expressed as follows [9]:

$$HD_{INTRA} = \frac{1}{N_q} \sum_{j=1}^{N_q} \frac{HD(R_i, R_{i,j})}{n} \times 100.0\%, \quad (2)$$

where N_q is the number of the queries of response outputs. Finally, Reliability (%) is defined as follows [10]:

$$\text{Reliability} = 100 - HD_{INTRA}\ \% \quad (3)$$

Most of works use Reliability of Eq. (3) [7, 11, 12]. Some works use HD_{INTRA} instead of Reliability of Eq. (3) [6, 13].

2.4.2 Other Metrics

Ideally, the proportion of ‘0’s and ‘1’s in the response outputs must be uniform. Uniformity is a quantitative metric that shows how uniform the proportion of ‘0’s and ‘1’s in the response outputs is.

For truly random PUF responses, this proportion must be 50%. Uniformity of a response output of the PUF in chip *i* is expressed as follows:

$$(Uniformity)_i = \frac{1}{n}\sum_{l=1}^{n} r_{i,l} \times 100.0\%, \quad (4)$$

where $r_{i,l}$ is the *l*-th binary bit of an *n*-bit response output of chip *i*.

Bit-aliasing is Hamming weight of a bit of response outputs of PUFs. The ideal value is 50%. When the value is near 0% or 100%, the probability that the response output of a PUF is almost the same as those of the other PUFs increases. Bit-aliasing of *l*-th bit of *n*-bit response output among *k* devices is defined as follows:

$$(Bit-aliasing)_l = \frac{1}{k}\sum_{i=1}^{k} r_{i,l} \times 100.0\% \quad (5)$$

Above four metrics are popular ones. In addition to these, there are various evaluation metrics of PUF such as Randomness, Steadiness, Correctness, Diffuseness, Misidentification, Single-bit probability, and Variety [14-16].

3. Classification of PUF

Some of PUFs are named based on the entropy source used for response output generation. Delay PUF and Current Array PUF are the typical ones. On the other hand, some of PUFs are named based on the implemented device. Memory PUF, ADC PUF, TDC PUF, and FPGA PUF are the typical ones. This section describes the basics and the current progress of these PUFs. Subsections 3.1 and 3.2 describe Delay PUF and Current Array PUF, respectively. Subsection 3.3 describes Memory PUF. Subsections 3.4 and 3.5 describe Analog-to-Digital Converter (ADC) PUF and Time-to-Digital Converter (TDC) PUF, respectively. Subsection 3.6 describes FPGA PUF. Finally, subsection 3.7 summarizes the other PUFs recently proposed.

3.1 Delay PUF

Delay PUF is a PUF that uses the delay variation of the gate circuit as the entropy source. Arbiter PUF and Ring Oscillator (RO) PUF are typical ones.

Arbiter PUF generates response output comparing delay of two identical delay-lines. Fig. 3 (a) shows the basics of the Arbiter PUF. Arbiter PUF consists of two identical delay-lines represented by the left-side two bold lines and an arbiter represented by the right-side rectangle. The outputs of the two delay-lines are connected to the arbiter. A positive transition is launched to the input of the two delay-lines in parallel to generate a 1-bit response output. Ideally, both the transition through the upper delay-line and the transition through the lower delay-line arrive at the arbiter simultaneously. However, the arrival time varies for process variation. The arbiter generates a digital value from the difference of the arrival times. If the upper transition arrives earlier than the lower transition, the response output R is 1, otherwise 0.

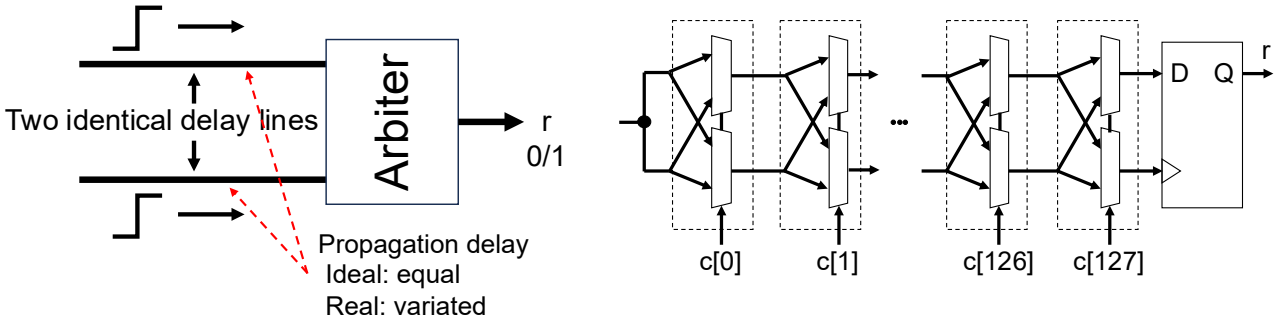
Fig. 3 (b) shows a typical implementation of a 128-bit Arbiter PUF. A Strong Arbiter PUF with 128-bit challenge input is realized with the 128-stage cascaded two-parallel 2-to-1 multiplexers with common control input as 1-bit challenge input.

Since Arbiter PUF is simple and requires only low area, it is suitable for custom design. Thus, Arbiter PUF is often used for PUF-based device authentication of light weight edge devices in IoT systems [17, 18].

However, delay of a stage is independent of all other delays, and the delays add linearly. As a result, one can use standard linear system analysis to intelligently gather data about the gate delays from the response bits [19]. Therefore, it is vulnerable to security attacks. In fact, it is easily modeled with quite

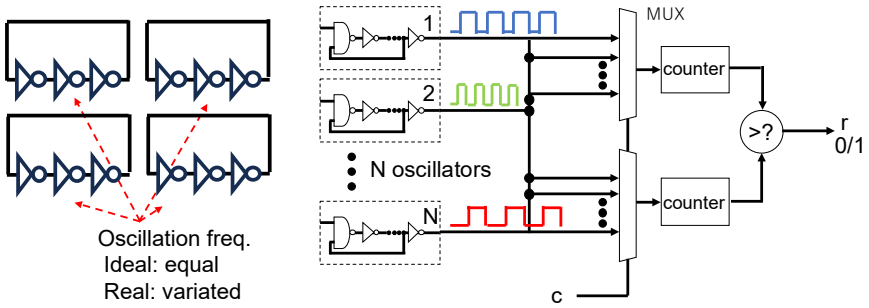
small CRP set as labeled data for machine learning within a second [20]. Consequently, most of the researches about Arbiter PUF is on security attack to it or resilience to the attack to it [21, 22].

Recently, as shown in subsection 3.6, the researches on implementation of Arbiter PUF in FPGA is increasing [12, 23, 24].



(a) Basics (b) Gate-level schematic

Fig. 3. Arbiter PUF: generate a 1-bit response output from polarity of delay difference of slightly variated two identical delay-lines.



(a) Basics (b) Gate-level schematic

Fig. 4. RO PUF: generate a 1-bit response output from polarity of frequency difference of a pair of slightly variated identical ring oscillators.

RO PUF is a PUF that uses the variation of the oscillation frequency of the ring oscillator due to the process variation. We will explain the basic with Fig. 4 (a). In Fig. 4 (a), 2×2 RO array is depicted. Ideally, the oscillation frequencies of the ROs are identical. However, they vary due to process variation. Usually, RO PUF uses the difference of the frequencies of a pair of ROs as an entropy source. In this example, a pair of RO is selected from the four ROs to generate a 1-bit response output. Fig. 4 (b) shows a typical implementation of N/2-bit RO PUF. The challenge input c selects a pair of ROs. The frequencies of the selected two ROs are measured with each upper and lower oscillation counters. A 1-bit response output r is generated with the difference of the frequencies.

The number of the CRPs is on the order of linear or polynomial, which depends on the PUF architecture. Accordingly, most of RO PUFs are classified to Weak PUF. Because the RO array can be notable area overhead when it is implemented with custom design on ASIC, it is implemented on FPGA as a FPGA PUF usually.

Suh et al. were the first to propose RO PUFs [6]. Loop PUF was proposed as a variant of RO PUF [25]. Area efficiency of RO FPGA PUFs has been improved. Maiti et al. improved the area efficiency of RO PUFs by implementing eight ROs in one CLB [26]. Xin et al. further improved area efficiency by implementing 256 ROs in one CLB [27]. Pei et al. improved area efficiency by utilizing the fact that Xilinx CLBs have two outputs, implementing two reconfigurable ROs in one CLB [9]. These days, a Strong RO PUF was proposed, too [28].

Delay PUF is vulnerable to aging. Karimi et al. analyzed the impact of aging on each Arbiter PUF, RO PUF, and Loop PUF [29].

3.2 Current Array PUF (CA PUF)

Subthreshold Current Array (SCA) PUF utilizes variation of characteristics of two identical current arrays as the entropy source. Fig. 5 shows a typical SCA PUF. The PUF is composed of a pair of identical two-dimensional subthreshold current arrays SCA_a and SCA_b, and a comparator. The comparator compares V_{outa} and V_{outb}, which are the lower end voltages of SCA_a and SCA_b. Ideally these voltages are equal.

However, due to manufacturing variation, the voltages V_{outa} and V_{outb} vary for variation of the characteristics of the pair of subthreshold current arrays. The comparator generates 1-bit response output from the difference of the voltages.

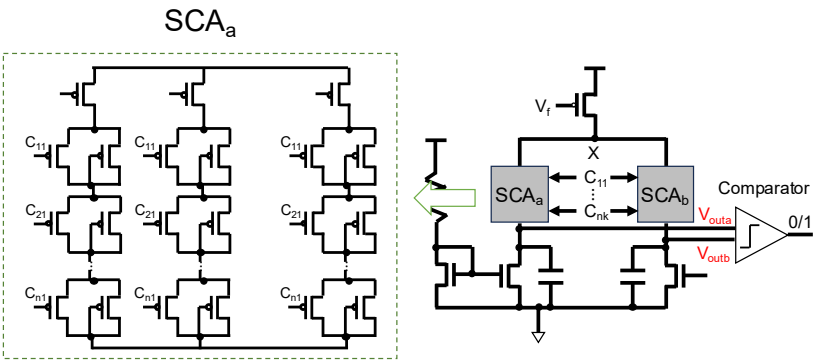


Fig. 5. Typical subthreshold CA (SCA) PUF: generate a 1-bit response output from polarity of slight voltage difference due to slight difference of subthreshold leakage current of two identical current arrays.

To the best of our knowledge, Kalynaraman et al. proposed the first SCA PUF. They shows the effectiveness of the proposed SCA PUF with simulation of the 64-bit SCA PUF with SPICE simulator in a 45nm technology node using a predictive technology [30]. Xi et al. fabricated a 65-bit SCA PUF and showed the effectiveness of the PUF [31]. A weakness of the SCA-PUF design is that a load transistor that does not operate in the strong inversion region causes high impedance and a huge voltage drop across the drain and source nodes, and thus output voltage is relatively low. Therefore, Mispan et al. proposed TCO PUF, an extension of SCA PUF which construct voltage dividers by diode-connected, cascode PMOS and NMOS transistors in an array topology to keep the output voltages higher [32]. Hata et al. proposed Leak Racing PUF (LR PF) which generates a 1-bit response output from the difference of charging time of the output voltages of the identical cascode PMOS and NMOS transistors operating at ultra-low voltage [33]. Georgoulas et al. proposed CAS-PUF which is a low-area CA PUF using a current-mode array applied current mirror circuit instead of subthreshold current arrays. The area is 20-72 % lower than conventional PUFs [7].

3.3 Memory PUF

Memory PUFs use a specification of memory cells as the entropy source. SRAM PUF is based on the fact that the initial value of the SRAM cell, which stores the value in a cross-coupled loop, depends on the variation (Fig. 6) [34, 35]. Several variantions of SRAM PUF have been proposed. In SPUF [36], Lu et al. proposed a modified 6T SRAM cell, with split wordlines, where whenever a group of four adjacent cells in the array is concurrently activated, process dependent bitflips may occur due to

cell collisions. Xynos et al. proposed Strong in-Cache Bitflip PUF (SiCBit-PUF), where whenever two cells in the same bitline written different values is concurrently activated, process dependent bitflip may occur due to cell collisions [37]. Zhang et al. presented that analog read current value for a codeword is a good entropy source for a PUF [38]. Chen et al. proposed Compute In- Memory PUF (PUF-CIM) that uses a modified SRAM that supports in-memory computing, where the read currents of multiple activated cells in two bitlines are used for the response output generation [39].

DRAM PUFs use variations in the capacitance of memory cells. Variations in memory cell capacitance surface in various ways. As a result, various DRAM PUFs have been proposed [40]. Memory cells are discharged after data are written (Fig. 7). Sometimes, some of data are corrupted for that. These failures are called retention failures. The time of a memory cell keeping correct data is called retention time. The distribution of retention failures is unique in each chip. Retention-based DRAM PUF utilizes the uniqueness of the distribution [41-43]. Latency-based DRAM PUF utilizes the variation of activation time of data read or time for pre-charge in each memory cell [44, 40]. Start-up-based DRAM PUF uses the uniqueness of the initial values after power-up like SRAM PUF [45, 46]. Rowhammer is a memory vulnerability that impacts system-level security across a range of memory technologies [47]. This vulnerability occurs when the same row is accessed frequently. The frequent accesses result in bit flips in physically adjacent rows. Rowhammer DRAM PUF uses the uniqueness of the flipped bit patterns [48, 49]. Yoo et al. proposed a DRAM PUF which generates 1-bit response output through differential mismatch between two identical memory cells. The PUF consists of two identical 64×64 DRAM arrays arranged around a sense amplifier array. The outputs of the symmetrical two identical memory cells with the same distance from the target sense amplifier are connected to BL and BL_b of the amplifier, respectively. The 1-bit response output is generated from the output of the amplifier [50].

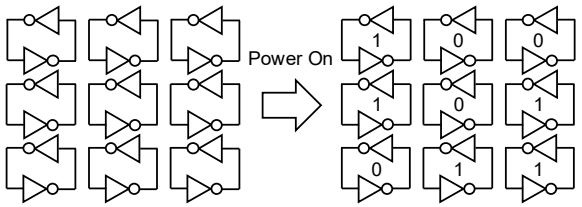


Fig. 6. Basic idea of SRAM PUF: generating a muti-bit response output from unique initial bit pattern of SRAM cells after power-on.

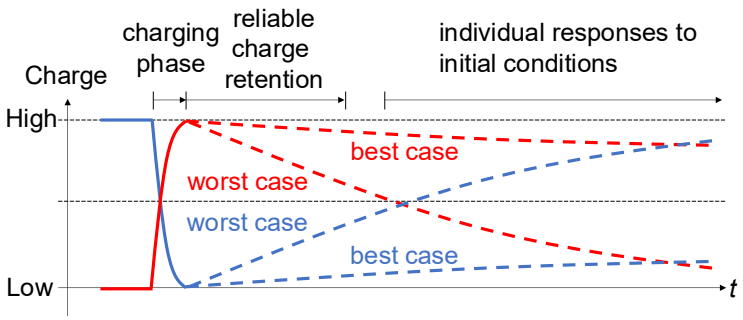


Fig. 7. Charge decay of DRAM cell over time Charge decay of DRAM cell over time: unique in each DRAM cell.

PUFs using emerging non-volatile memory have also been proposed [51, 52]. These PUFs take advantage of the variation in the resistance value of the memory cell. In particular, STT MRAM PUF has the advantages of high security, high power efficiency, and high bit density [52]. On the other hand, it also has the disadvantage of low reliability. In general, memory-based PUFs are used as Weak PUF.

3.4 ADC PUF

ADC PUFs which are PUFs embedded in ADC have been proposed. As far as we know, all the proposed ADC PUFs are Successive Approximation Register (SAR) ADC PUF. SAR ADC PUFs have normal operation mode and PUF mode. In normal operation mode, the PUFs work as normal SAR ADC, otherwise they work as a PUF.

SAR ADC PUFs utilize the mismatch of the unit capacitors inside the charge redistribution CDAC as the entropy source. Some unit capacitors of the CDAC construct two symmetrical capacitor arrays in PUF mode as shown in Fig. 8. The comparator compares V_U and V_L which are lower end voltages of upper and lower capacitor arrays, respectively.

Because the same switching operation of S_0 to S_N is applied to both of the upper and lower capacitor arrays, the ideal synthesized capacitances are always the same. So ideally, V_U and V_L are always the same. However, the mismatch of V_U and V_L occurs for variation of the upper and lower capacitor arrays due to manufacturing variation. The comparator generates 1-bit response output from the mismatch of the voltages.

Tang et al. proposed SAR ADC PUF harnessing variation of metal-oxide-metal capacitors through a charge redistribution operation. The evaluation shows the inter-chip Hamming distance is 50.80%, intra-chip HD is 0.46%, and uniformity is 50.59% [53]. Shylendra et al. showed SAR ADC can be modified for back-end capacitor-based authentication in addition to its regular functionality. The evaluation shows that the power overhead is 3.2% and the active-area overhead is 75% [54]. Chen et al. proposed a PUF embedded in a 10-bit SAR ADC, whose reliability 97.69% and uniqueness is 48.01%, respectively [55]. Tian et al. proposed a strong SAR ADC PUF based on SMIC 18nm CMOS process, which utilizes the combination of capacitor array structure in SAR ADC, shared capacitor array to reduce the chip area, and gate-voltage bootstrap switch as a sampling switch to reduce the SAR ADC power consumption. The evaluation shows that the inter-chip HD is within 46% to 52%. The reliability is 97% [56].

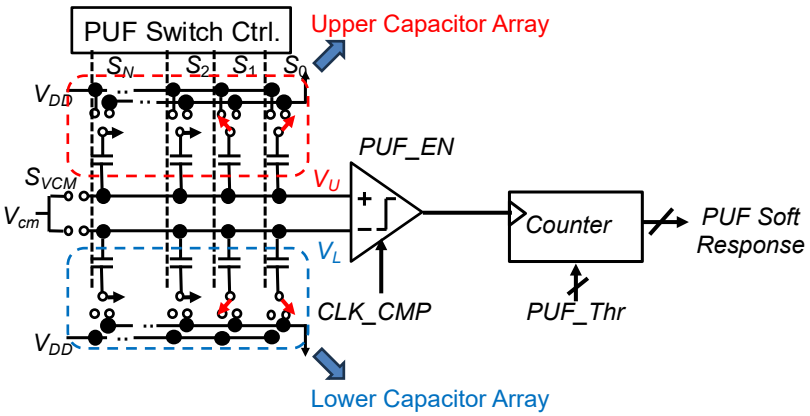


Fig. 8. Typical SAR ADC PUF: generate a 1-bit response output from the capacitor mismatch between two identical capacitor arrays configured in PUF mode.

3.5 TDC PUF

TDC is a circuit that converts a time interval into a digital value. It has various applications such as Time-of-Flight (ToF) systems, light detection and imaging, position emission tomography, ultrasonic measurement, and diffuse optical tomography [57].

TDC PUF is a PUF embedded in TDC. Like ADC PUF, it has normal operation mode and PUF mode. In normal operation mode, it works as a normal TDC, otherwise it works as a PUF. Like ADC PUF, the variation of some of the components of the circuit is used as an entropy source of the PUF.

We have proposed two TDC PUFs. The first proposal is the TDC PUF using linearity self-calibration. The PUF uses a Single Delay-Line (SDL) TDC with linearity self-calibration. The PUF uses the difference of a pair of buffer delays of the TDC as an entropy source. Each buffer delay is measured with on-chip delay measurement using the linearity self-calibration [58].

The second proposed TDC PUF uses SDL TDC, too. The proposed PUF uses the difference of the outputs of the two identical TDCs input common time intervals as the entropy source of the PUF [13].

Both ADC PUF and TDC PUF reuse the pre-existing circuits. Therefore, hardware and design overheads are lower than those of usual PUFs.

3.6 FPGA PUF

FPGAs can reconfigure digital circuits. Consequently, PUFs composed of digital elements can be configured on FPGAs for FPGA device authentication and cryptographic key generation (FPGA PUFs). Most of Delay PUFs such as RO PUF, Arbiter PUF, and Loop PUF are used as FPGA PUF.

PUFs with array of cross-coupled circuits composed of digital elements used as entropy sources are also used as FPGA PUF. The most well-known one is Butterfly PUF [8]. Butterfly PUF is composed of the array of the identical cross-coupled loops of latches. Fig. 9 (a) shows a cross-coupled loop of a typical Butterfly PUF. When 1-bit response output is generated with a loop, one latch is set to 1 and another latch is set to 0 to fall them into metastable state. After that, the difference in the strength of the latches leads to stable 0 or 1.

NAND PUF is an improved low-area one proposed by Sala et al. [11, 59]. It is composed of the array of the identical cross-coupled loops of 2-input NAND gates. Fig. 9 (b) shows a cross-coupled loop of NAND PUF. The control input of each NAND gate is start. When 1-bit response output is generated with a loop, a positive transition is input to start to fall them into metastable state. After that, the difference in the strength of the latches leads to stable 0 or 1.

The structure of DD PUF, XOR PUF, and PICO PUF and the principle of the generation of a 1-bit response output are similar to those of NAND PUF [60-67]. XOR PUF can be used as a latch and a ring oscillator with controlling the control lines, too [11, 63]. A good point of NAND PUF, DD PUF, and XOR PUF proposed by Sala et al. is that they require only a half slice per bit for the implementation on AMD FPGA, while others require more than one slice [11, 60].

The Transient Effect Ring Oscillator (TERO) PUF, is a variant of ring oscillator (RO) PUF. Unlike RO PUF, TERO PUF has stable state in addition to oscillation state. To generate 1-bit response output, TERO PUF is forced to oscillation state. After that, it moves into stable 0 or 1.

The Single Slice (SS) RO PUF is a ring oscillator PUF which can fit in one Slice of the seven-series FPGA devices. Fig. 9 shows the gate-level schematic. Unlike usual RO PUF, it is used as a 1-bit cell of a PUF.

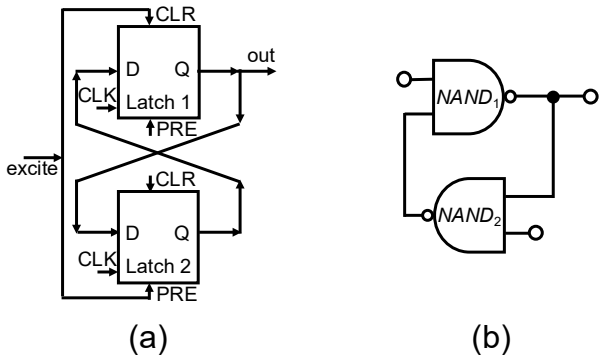


Fig. 9. (a) A cross-coupled loop of Butterfly PUF. (b) A cross-coupled loop of NAND PUF.

3.7 Other PUFs

Various other PUFs have been proposed. Chowdhury et al. proposed a Weak PUF using the characteristic variation of the null convention logic gate utilized as the entropy source, which is a logic gate in an asynchronous circuit [68]. The inverter/amplifier analog PUF, which is a Weak PUF, uses the variation of threshold voltage and switching voltage of inverter and inverting amplifier as the entropy source [69, 70]. Chatterjee et al. proposed a RF-PUF using variations in analog and RF characteristics due to process variations in wireless transmitters (Tx) as the entropy source [71].

Table 1 shows the comparison of the performance of major PUFs. The 1st column is the class of the PUFs. The 2nd column is the detailed type of the PUFs. The 3rd column shows whether the PUF is a Weak PUF (W) or a Strong PUF (S). The 4th column to the 8th column are the performance metrics of the PUFs. A double circle represents high performance, a circle represents mid. performance, and a triangle represents low performance.

Usually, all the PUFs are optimized to keep high uniqueness. Reliability of Delay PUFs and CA PUFs is high. In general, reliability of memory PUFs is low due to their vulnerability to environmental noises. Reliability of ADC PUFs utilizing their embedded CDAC is high. Future work of our TDC PUF is to enhance its reliability [13]. Reliability of an FPGA PUF depends on the reliability of the implemented PUF. Generally, area overhead of Weak PUF is high, while that of Strong PUF is low. Area overhead of memory PUFs and all the FPGA PUFs is zero. Power consumption of all the PUFs except FPGA PUFs is almost in proportion to the power consumption. Power consumption of FPGA PUFs depends on that of implemented PUFs. Power consumption of FPGA PUFs depends on that of implemented PUFs. Resilience to security attacks of Delay PUF, ADC PUF, and TDC PUF is low in general. That of Memory PUF and CA PUF is high. Resilience to security attacks of FPGA PUFs depends on that of the implemented PUFs.

Table 1. Comparison of performance of major PUFs.

Class	Type	W/S	Uniqueness	Reliability	Area Overhead	Power Consumption	Resilience to Attacks
Delay	Arbiter	S	4	4	4	4	2
	RO	W	4	5	2	2	2
CA	-	S	4	4	3	3	4
Memory	SRAM	W	4	3	5	5	4
	DRAM	W	4	3	5	5	4
	Emerging	W	4	3	5	5	4
ADC	-	S	4	4	4	4	2
TDC	-	S	4	3	4	4	3
FPGA	Arbiter	S	4	4	5	4	2
	RO	W	4	5	5	2	2
	Butterfly	W	4	4	5	4	4

5: Excellent, 4: Good, 3: Fair, 2: Poor

4. Conclusion

This paper has briefly surveyed PUFs that have been proposed in the academic field. The performance of PUFs tends to increase as device progress and brand-new PUFs of emerging devices are proposed continuously. This trend will continue in the next decade, too.

PUF is useful to secure low power and low computational power devices connected to wireless network, such as IoT devices for telemedicine, smart agriculture, smart factory, and smart logistics,

drones, and connected electric cars. It is expected as an essential security primitive for security of future broad-band huge wireless systems.

References

[1] M. Barekatain, J. Lee, A. Sengupta, K. S. Esfahani, A. Roy and E. S. Kim, "PREATS: Passive RFID-based embedded anti-tampering sensor for authentication in semiconductor supply chain", ***IEEE Sensors Journal to appear***.
https://doi: 10.1109/JSEN.2025.3605555

[2] Serious semiconductor counterfeit product problem, blockchain to deal with it (Website), https://eetimes.itmedia.co.jp/ee/articles/2205/25/news084.html

[3] O.H.A. Shaikh, S. Saha, K. Zamiri Azar, F. Farahmandi, M. Tehranipoor and F. Rahman, "Re-pen: Reinforcement learning-enforced penetration testing for SoC security verification", ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***, Vol.33, No.3, pp.853-866, 2025.
https://doi.org/10.1109/TVLSI.2024.3510682

[4] M. S. I. Shovon, S. Ghosh, P. J. Craig, C. -C. Huang, C. -Y. Pai and N. Asadizanjani, "A Novel Framework for Identifying Counterfeit ICs via Pinhole Evaluation", ***Proceedings of IEEE RAPID2025*** (Miramar Beach, FL, USA), August 2025.

[5] C. Herder, M.-D. Yu, F. Koushanfar and S. Devadas, "Physical unclonable functions and applications: A tutorial", ***Proceedings of the IEEE***, Vol.102, No.8, pp.1126-1141, 2014.
https://doi.org/10.1109/JPROC.2014.2320516

[6] G.E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", ***Proceedings of IEEE DAC2007*** (San Diego, CA, USA), June 2007.

[7] D. Georgoulas, Y. Tsiatouhas and V. Tenentes, "CAS-PUF: Current-mode array-type strong PUF for secure computing in area constrained SoCs", ***Proceedings of IEEE DATE2025*** (Lyon, France), March-April 2025.
https://doi.org/10.23919/DATE64628.2025.10992979

[8] S.S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA", ***Proceedings of IEEE HOST2008*** (Anaheim, CA, USA), June 2008.
https://doi.org/10.1109/HST.2008.4559053

[9] S. Pei, J. Zhang and R. Wang, "A Low-overhead RO PUF design for Xilinx FPGAs", ***IEICE Electronics Express***, Vol.15, No.5, pp.20180093-20180093, 2018.
https://doi.org/10.1587/elex.15.20180093

[10] A. Maiti, V. Gunreddy and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions", ***IACR Cryptology ePrint Archive***, 2011.
https://eprint.iacr.org/2011/657.pdf

[11] R.D. Sala and G. Scotti, "Evaluation and comparison of physical unclonable functions suitable for FPGA implementation", ***Proceedings of IEEE DCIS*** (Catania, Italy), November 2024.
https://doi.org/10.1109/DCIS62603.2024.10769166

[12] C.P. G and A.P. Shah, "Fredkin gate-based feed-forward arbiter PUF design on FPGA", ***Proceedings of IEEE ICM2024*** (Doha, Qatar), December 2024.
https://doi.org/10.1109/ICM63406.2024.10815789

[13] K. Katoh, T. Nakura and H. Kobayashi, "A strong physical unclonable function using dual time-to-digital converters for AMD FPGAs", ***Proceedings of ICCCAS2025*** (Wuhan, China), May 2025.

[14] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs", ***Proceedings of IEEE ReConFig2010*** (Cancun, Mexico), January 2010.
https://doi.org/10.1109/ReConFig.2010.24

[15] Y. Su, J. Holleman and B. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations", ***IEEE Journal of Solid-State Circuits***, Vol.43, No.1, pp.69-77, 2008.
https://doi.org/10.1109/JSSC.2007.910961

[16] D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, T. Ochiai, M. Takenaka and K. Itoh, "Variety enhancement of PUF responses using the locations of random outputting RS latches", ***Journal of Cryptographic Engineering***, Vol.3, pp.197-211, 2013.
https://link.springer.com/content/pdf/10.1007/s13389-012-0044-0.pdf

[17] S.S. Mehjabin, M.F. Younis, A. Tekeoglu, M. Ebrahimabadi, T. Sookoor and N. Karimi "PETIT: PUF-enabled trust evaluation framework for IoT networks", ***Computer Networks***, Vol.254, 110772, 2022.
https://doi.org/10.1016/j.comnet.2024.110772

[18] P. Mall, R. Amin, A.K. Das, M.T. Leung, and K.-K.R. Choo, "PUF-based authentication and key agreement protocols for IoT, WSNs, and Smart Grids: A comprehensive survey", ***IEEE Internet of Things Journal***, Vol.9, No.11, pp.8205-8228, 2022.
https://doi.org/10.1109/JIOT.2022.3142084

[19] D. Lim, "Extracting secret keys from integrated circuits", ***Journal of M.S. thesis,*** Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, May 2004.

[20] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas and J. Schmidhuber, "Modeling attacks on physical unclonable functions", ***Proceedings of ACM CCS2010*** (Chicago, IL, USA), October 2010.
https://doi.org/10.1145/1866307.1866335

[21] T. Kroeger, W. Cheng, S. Guilley, J.-L. Danger and N. Karimi, "Cross-PUF attacks on arbiter-PUFs through their power side-channel", ***Proceedings of IEEE ITC2020*** (Washington, DC, USA), November 2020.
https://doi.org/10.1109/ITC44778.2020.9325241

[22] S. Yu, K. Park and Y. Park, "A machine learning attack-resistant PUF-based robust and efficient mutual authentication scheme in fog-enabled IoT environments", ***IEEE Internet of Things Journal***, Vol.12, No.12, pp.20652-20669, 2025.
https://doi.org/10.1109/JIOT.2025.3544443

[23] N.N. Anandakumar, M.S. Hashmi, and M.A. Chaudhary, "Implementation of efficient XOR arbiter PUF on FPGA with enhanced uniqueness and security", ***IEEE Access***, Vol.10, pp.129832-129842, 2022.
https://doi.org/10.1109/ACCESS.2022.3228635

[24] S. Rajput, J. Dofe and K. Sood, "Exploring efficient implementation of delay-based PUF design on FPGA", ***Proceedings of IEEE ICCNS2023*** (Valencia, Spain), June 2023.
https://doi.org/10.1109/ICCNS58795.2023.10193305

[25] Z. Cherif, J.-L. Danger, S. Guilley and L. Bossuet, "An easy-to-design PUF based on a single oscillator: The loop PUF", ***Proceedings of IEEE DSD2012*** (Cesme, Turkey), Decemeber 2012. https://doi.org/10.1109/DSD.2012.22

[26] A. Maiti and P. Schaumount, "Improved ring oscillator PUF: An FPGA-friendly secure primitive", ***ACM Journal of Crptography***, Vol.24, No.2, pp.375-397, 2011. https://doi.org/10.1007/s00145-010-9088-4

[27] X. Xin, J.-P. Kaps, K. Gaj, "An experimental study of the state-of-the-art PUFs implemented on FPGAs", ***Proceedings of IEEE DESEC2017*** (Taipei, Taiwan), October 2017. https://doi.org/10.1109/DESEC.2017.8073844

[28] A. Gupta, S.F. Naz, and A.P. Shah, "Configurable RO-PUF with improved thermal stability for lightweight applications", ***Proceedings of IEEE ICM2024*** (Doha, Qatar), December 2024. https://doi.org/10.1109/ICM63406.2024.10815902

[29] N. Karimi, J.-L. Danger and S. Guilley, "Impact of Aging on the Reliability of Delay PUFs", ***Journal of Electronic Testing***, Vol.34, pp.571-586, 2018.

[30] M. Kalyanaraman and M. Orshansky, "Novel strong PUF based on nonlinearity of MOSFET subthreshold operation", ***Proceedings of IEEE HOST2013*** (Austin, TX, USA), June 2013. https://doi.org/10.1109/HST.2013.6581558

[31] X. Xi, H. Zhuang, N. Sun, M. Orshansky, "Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130nm CMOS", ***Proceedings of IEEE VLSIC2017*** (Kyoto, Japan), June 2017. https://doi.org/10.23919/VLSIC.2017.8008503

[32] M.S. Mispan, B. Halak, Z. Chen, and M. Zwolinski, "TCO-PUF: A subthreshold physical unclonable function", ***Proceedings of IEEE PRIME2015*** (Glasgow, UK), July 2015. https://doi.org/10.1109/PRIME.2015.7251345

[33] S. Hata and K. Usami, "Leakage-based strong PUF operating at ultra-low voltage using a leakage control approach", ***Proceedings of IEEE ITC-CSCC*** (Okinawa, Japan), July 2024. https://doi.org/10.1109/ITC-CSCC62988.2024.10628304

[34] D.E. Holcomb, W.P. Burleson and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers", ***IEEE Transactions on Computers***, Vol.58, No.9, pp.1198-1210, 2008.

[35] J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection", ***Proceedings of CHES2007*** (Vienna, Austria), September 2007. https://link.springer.com/content/pdf/10.1007/978-3-540-74735-2.pdf

[36] L. Lu, T. Yoo and T.T.-H. Kim, "A 6T SRAM based two-dimensional configurable challenge-response PUF for portable devices", ***IEEE Transactions on Circuits and Systems I: Regular Papers***, Vol.69, No.6, pp.2542-2552, 2022. https://doi.org/10.1109/TCSI.2022.3156983

[37] A. Xynos, V. Tenentes, and Y. Tsiatouhas, "SiCBit-PUF: Strong in-cache bitflip PUF computation for trusted SoCs", ***Proceedings of IEEE ETS2023*** (Venezia, Italy), May 2023. https://doi.org/10.1109/ETS56758.2023.10173941

[38] F. Zhang, S. Yang, J. Plusquellic and S. Bhunia, "Current based PUF exploiting random variations in SRAM cells", ***Proceedings of IEEE DATE2016*** (Dresden, Germany), March 2016. https://ieeexplore.ieee.org/document/7459321

[39] Z. Chen, M. Wu, Y. Zhou, R. Li, J. Tan, and D. Ding, "PUF- CIM: SRAM-based compute-in-memory with zero bit-error-rate physical unclonable function for lightweight secure edge computing", ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***, Vol.31, No.8, pp.1234-1247, 2023. https://doi.org/10.1109/TVLSI.2023.3277517

[40] B.M.S.B. Talukder, B. Ray, D. Forte and M. T. Rahman, "PreLatPUF: Exploiting DRAM latency variations for generating robust device signatures", ***IEEE Access***, Vol.7, pp.81106-81120, 2019. https://doi.org/10.1109/ACCESS.2019.2923174

[41] C. Keller, F. Gürkaynak, H. Kaeslin and N. Felber, "Dynamic memory-based physically unclonable function for the generation of unique identifiers and true random numbers", ***Proceedings of IEEE ISCAS*** (Melbourne VIC, Autralia), June 2014. https://doi.org/10.1109/ISCAS.2014.6865740

[42] S. Sutar, A. Raha, D. Kulkarni, R. Shorey, J. Tew and V. Raghunathan, "D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication and random number generation", ***ACM Transactions on Embedded Computing Systems (TECS)***, Vol.17, No.1, pp.1-31, 2017. https://doi.org/10.1145/3105915

[43] W. Xiong, A. Schaller, N. A. Anagnostopoulos, M. U. Saleem, S. Gabmeyer, S. Katzenbeisser, and J. Szefer, "Run-time accessible DRAM PUFs in commodity devices", ***Proceedings of CHES2016*** (Santa Barbara, CA, USA), August 2016. https://doi.org/10.1007/978-3-662-53140-2_21

[44] J.S. Kim, M. Patel, H. Hassan and O. Mutlu, "The DRAM latency PUF: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity DRAM devices", ***Proceedings of IEEE HPCA2018*** (Vienna, Auria), March 2018.

[45] F. Tehranipoor, N. Karimian, K. Xiao and J. Chandy, "DRAM based intrinsic physical unclonable functions for system level security", ***Proceedings of GLSVLSI2015*** (Pittsburgh, Pennsylvania, USA), 2015. https://doi.org/10.1145/2742060.2742069

[46] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "DRAM-based intrinsic physically unclonable functions for system-level security and authentication", ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***, Vol.25, No.3, pp.1085-1097, 2016. https://doi.org/10.1109/TVLSI.2016.2606658

[47] E. Ortega, J. Kwak, S. Yu and K. Chakrabarty, "Runtime security analysis of monolithic 3D embedded DRAM with oxide-channel transistor", ***Proceedings of IEEE DATE2025*** (Lyon, France), March-April 2025. https://doi.org/10.23919/DATE64628.2025.10993204

[48] A. Schaller, W. Xiong, N.A. Anagnostopoulos, M.U. Saleem, S. Gabmeyer, S. Katzenbeisser and J. Szefer, "Intrinsic rowhammer PUFs: leveraging the rowhammer effect for improved security", ***Proceedings of IEEE HOST2017*** (Mclean, VA, USA), May 2020. https://doi.org/10.1109/HST.2017.7951729

[49] N.A. Anagnostopoulos, T. Arul, Y. Fan, C. Hatzfeld, A. Schaller, W. Xiong, M. Jain, M.U. Saleem, J. Lotichius, S. Gabmeyer, J. Szefer and S. Katzenbeisser, "Intrinsic run-time row hammer PUFs: Leveraging the row hammer effect for run-time cryptography and improved security", ***Cryptography***, Vol.2, No.3, 13, 2018.
https://doi.org/10.3390/cryptography2030013

[50] M. Yoo *et al.*, "DRAM physically unclonable function (PUF) using dual word-line activated twin-cells", ***IEEE Transactions on Circuits and Systems II: Express Briefs***, Vol.72, No.3, pp.514-518, 2025.
https://doi.org/10.1109/TCSII.2025.3530514

[51] S M Mojahidul Ahsan, Tanvir Hossain, Md Sakib Hasan, and Tamzidul Hoque, "Resistive RAM-based PUF: Challenges and opportunities", ***Proceedings of IEEE DAS2023*** (Denton, TX, USA), Vol.4, No.1, pp.36-47, April 2023.
https://doi.org/10.1109/DCAS57389.2023.10130179

[52] Y. Hu, L. Wu, Z. Chen, Y. Huang, X. Xu, K. Li and J. Zhang, "STT-MRAM-based reliable weak PUF", ***IEEE Transactions on Computers***, Vol.71, No.7, pp.1564-1574, 2022.

[53] Q. Tang, W.H. Choi, L. Everson, K.K. Parhi and C.H. Kim, "A physical unclonable function based on capacitor mismatch in a charge-redistribution SAR-ADC", ***Proceedings of IEEE ISCAS2018*** (Florence, France), May 2018.
https://doi.org/10.1109/ISCAS.2018.8351601

[54] A. Shylendra, S. Bhunia and A.R. Trivedi, "An Intrinsic and database-free authentication by exploiting process variation in back-end capacitors", ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***, Vol.27, No.6, pp.1253-1261, 2019.
https://doi.org/10.1109/TVLSI.2019.2903807

[55] Y.-Y. Chen and S.-J. Chang, "A physically unclonable function embedded in a SAR ADC", ***Proceedings of IEEE ITC-Asia2022*** (Taipei, Taiwan), August 2020.
https://doi.org/10.1109/ITCAsia55616.2022.00025

[56] R. Tian and L. Dai, "A Strong Physical Unclonable Function Based on SAR ADC", ***Proceedings of IEEE ECIE2024*** (Hangzhou, China), May 2020.
https://doi.org/10.1109/ECIE61885.2024.10626434

[57] J. Szyduczynski, D. Koscielnik and M. Miskowicz, "Time-to-digital conversion techniques: a survey of recent developments", ***Measurement***, Vol.214, 112762, 2023.
https://doi.org/10.1016/j.measurement.2023.112762

[58] K. Katoh, S. Yamamoto, Z. Zhao, Y. Zhao, S. Katayama, A. Kuwana, T. Nakatani, K. Hatayama, H. Kobayashi, K. Sato, T. Ishida, T. Okamoto and T. Ichikawa, "A physically unclonable function using time-to-digital converter with linearity self-calibration and its FPGA implementation", ***Proceedings of IEEE ITC-Asia2023*** (Matsue, Japan), September 2023.
https://doi.org/10.1109/ITC-Asia58802.2023.10301181

[59] R.D. Sala and G. Scotti, "A novel FPGA implementation of the NAND-PUF with minimal resource usage and high reliability", ***Crpyptography***, Vol.7, No.2, 18, 2023.
https://doi.org/10.3390/cryptography7020018

[60] R.D. Sala, D. Bellizia and G. Scotti, "A novel ultra-compact FPGA PUF: The DD-PUF", ***Cryptography***, Vol.5, No.3, 23, 2021.

[61] R.D. Sala and G. Scotti, "The DD-Cell: a double side entropic source exploitable as PUF and TRNG", ***Proceedings of IEEE PRIME2022*** (Villasimius, SU, Italy), June 2022. https://doi.org/10.1109/PRIME55000.2022.9816824

[62] R.D. Sala and G. Scotti, "Exploiting the DD-Cell as an ultra-compact entropy source for an FPGA-based re-configurable PUF-TRNG architecture", ***IEEE Access***, Vol.11, pp. 86178-86195, 2023. https://doi.org/10.1109/ACCESS.2023.3304901

[63] R.Della Sala, D. Bellizia, and G. Scotti, "A lightweight FPGA compatible weak-PUF primitive based on XOR gates", ***IEEE Transactions on Circuits and Systems II: Express Briefs***, Vol.69, No.6, pp.2972-2976, 2022.

[64] C. Gu, J. Murphy and M. O'Neill, "A unique and robust single slice FPGA identification generator", ***Proceedings of IEEE ISCAS2014*** (Melbourne, VIC, Australia), June 2014. https://doi.org/10.1109/ISCAS.2014.6865362

[65] C. Gu and M. O'Neill, "Ultra-compact and robust FPGA-based PUF identification generator", ***Proceedings of IEEE ISCAS2015*** (Lisbon, Portugal), May 2015. https://doi.org/10.1109/ISCAS.2015.7168788

[66] C. Gu, N. Hanley and M. O'Neill, "Improved reliability of FPGA-based PUF identification generator design", ***ACM Transactions on Reliable Technology and Systems (TRETS)***, Vol.10, No.3, pp.1-23, 2017. https://doi.org/10.1145/3053681

[67] C. Gu, C.H. Chang, W. Liu, N. Hanley, J. Miskelly and M. O'Neill, "M. A large-scale comprehensive evaluation of single-slice ringoscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs", ***Journal of Cryptographic Engineering***, Vol.11, pp.227-238, 2021. https://link.springer.com/content/pdf/10.1007/s13389-020-00244-5.pdf

[68] S. Chowdhury, R. Acharya, W. Boullion, A. Felder, M. Howard, J. Di and Domenic Forte, "A weak asynchronous RESet (ARES) PUF using start-up characteristics of null conventional logic gates", ***Proceedings of IEEE ITC2020*** (Washington, DC, USA), Vol.4, No.1, pp.36-47, November 2020. https://doi.org/10.1109/ITC44778.2020.9325278

[69] S. Taneja, "Energy-efficient and low-cost hardware security primitives for secure ubiquitous computing", ***MWCAS2022***, August 2020.

[70] D. Li and K. Yang, "A self-regulated and reconfigurable CMOS physically unclonable function featuring zero-overhead stabilization", ***IEEE Journal of Solid-State Circuits***, Vol.55, No.1, pp.98-107, 2020. https://doi.org/10.1109/JSSC.2019.2938133

[71] B. Chatterjee, D. Das, and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning", ***Proceedings of IEEE HOST2018*** (Washington, DC, USA), April-May 2018. https://doi.org/10.1109/HST.2018.8383916