International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2630-2634

Reliable Physical Unclonable Function based on Asynchronous Circuits

Kyung Ki Kim

Department of Electronic Engineering, Daegu University, Gyeongbuk, 38453, South Korea.
E-mail: kkkim@daegu.ac.kr

Abstract

The conventional Physically Unclonable Function (PUF) circuits take advantage of the physical properties of silicon and provide an alternative to storing digital encryption keys in nonvolatile memory, and they output the corresponding digital values as a set of unique digital inputs. However, the conventional PUF circuit is influenced by the temperature and the voltage variation, so that the digital output values can be changed. In addition, the PUF is vulnerable to advanced side-channel attack. In this paper, an asynchronous circuit based PUF circuit with low dependence on temperature and supply voltage has been proposed. A delay-insensitive asynchronous design methodology, named NULL Convention Logic (NCL), has been deployed for low-power robust circuit operation. In this paper, the proposed methodology has been designed using a standard 0.18um CMOS technology, and the experimental results show that the proposed asynchronous PUF circuit improves the robustness and reduces power consumption compared with a conventional Arbiter PUF circuit.

Keywords: Security, PUF, Physical Unclonable Function, Low Power, Reliability

INTRODUCTION

The rapid growth of Internet of things (IoT) including mobile phones, portable devices has imposed both conceptually and technically new challenges. Among them, the most demanding requirements for the widespread realization of many IoT visions are security and low power. In terms of security, IoT applications include tasks that are rarely addressed before such as trusted sensing, secure computation and communication, privacy, and data right management. These tasks ask for new and better techniques for the protection of hardware, software, and data. An integral part of hardware cryptographic primitives are secret keys and unique IDs. Conventional methods rely on digital storage of secret keys in non-volatile memory which is vulnerable to reverse engineering and side channel attacks. Physical Unclonable Functions(PUF) are a unique class of circuits that leverage the inherent variations in manufacturing process to create unique, unclonable IDs and secret keys. Figure 1 shows the basic concept of PUF [1][2].

Different types of PUFs such as Ring-Oscillator PUF, Arbiter PUF, SRAM-PUF, and Butterfly PUF have been proposed [3-6]. MIT's Ring-Oscillator PUF has been reported to have significant advantages in providing more stable performance and a relatively easy manufacturing process as well as being easily implemented in FPGAs and ASICs. Reliability is one of the biggest concerns when designing a PUF. The chip ID should not depend on time or operating environment. Temperature and voltage variation reduce reliability and reliability [7][8]. Therefore, this paper proposes an asynchronous circuit based PUF circuit with low dependence on temperature and supply voltage.

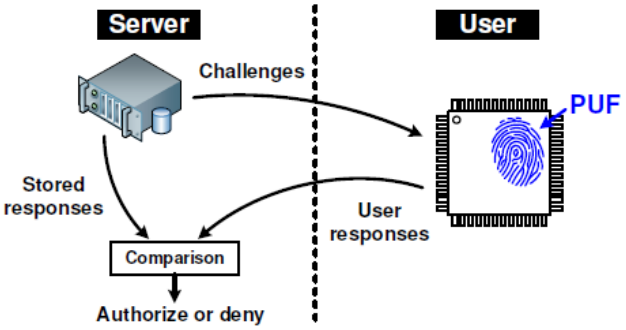


Figure 1: Basic Concept of PUF

Asynchronous circuits are at natural advantage in terms of side-channel attack resistance. The clock-related information leakage can be either eliminated or significantly reduced, which extensively increases the difficulties of attack due to the lack of timing references. In this paper, Null Convention Logic (NCL) as an asynchronous circuit design methodology has been used; NCL is one of the promising delay-insensitive asynchronous circuit design methodologies [9]. To the best of my knowledge, this is the first attempt to implement a PUF circuit based on NCL.

PHYSICALLY UNCLONABLE FUNCTION

In recent years, PUF has become an issue in hardware security research. A meta-stable PUF, a bi-stable element SRAM PUF based on PUF or static random access memory (SRAM), and a Butterfly PUF. An arbiter PUF called a delay-based PUF, a ring oscillator ring oscillator PUF (or RO-PUF) [3] [4].

The SRAM PUF is shown in Fig. 2, which is based on SRAM (6T-SRAM), which is composed of six transistors, and the threshold voltage of a small inverter transistor due to the variation of parameters due to manufacturing process variability to provide one bit of output data in each SRAM cell. The SRAM PUF can be implemented using a field programmable gate array (FPGA) or a microcontroller. However, not all SRAMs are suitable for implementing PUF.

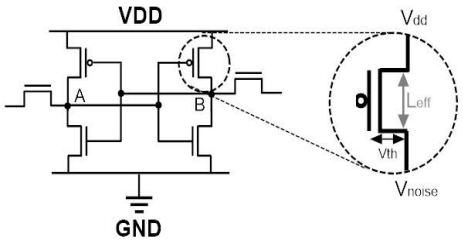


Figure 2: Architecture of SRAM PUF

Arbiter PUF [3][4] shown in Fig. 3 compares delays between two digital paths. The delay time generated in the logic gate is different for each gate due to the process variation even if the same design and technology have been used.

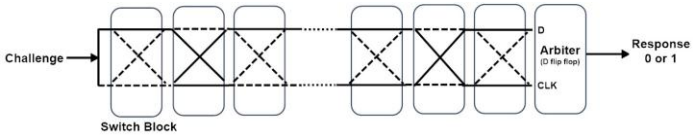


Figure 3: Arbiter PUF

The ring oscillator PUF deploys the frequency variation of ring oscillators due to manufacturing process variation [5]. The ring oscillator method uses only a simple standard logic gate as shown Fig. 4, which makes it easier to implement in FPGAs than other methods. These PUFs are called silicon PUFs or unique PUFs because no additional processing steps are required for this kind of PUF. In recent years, more and more configurable PUFs have been proposed [6] and new applications have been proposed.

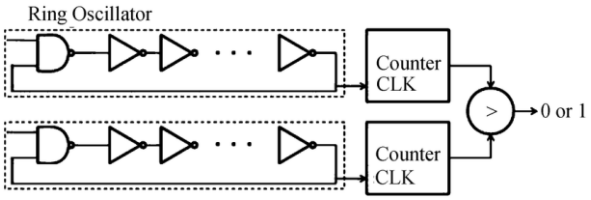
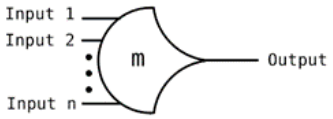


Figure 4: Ring Oscillator PUF

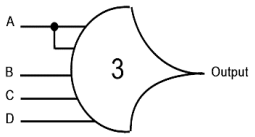
NULL CONVENTION LOGIC (NCL) :

In the reliable ultra-low power design, asynchronous circuits have recently been re-considered as a solution for scaling issues [9]. Null Convention Logic (NCL) is one of the promising delay-insensitive asynchronous circuit design methodologies. NCL circuits utilize threshold gates with hysteresis to maintain delay insensitivity. NCL uses delay-insensitive codes for data communication, alternating between set and reset phases. NCL uses threshold gates with hysteresis for its logic elements. One type of threshold gate is the THmn gate as shown in Fig. 5 (a), where $1 \leq m \leq n$. A THmn gate means that at least m of the n inputs has to be asserted before the output will become asserted. For example, Figure 5 (b) shows TH34w2 threshold gate. Threshold gate inputs and outputs can be in of two states, DATA or NULL [9].

A threshold gate starting with its output in a NULL state will remain in the NULL state until the specified numbers of inputs are placed in the DATA state. Once the gate reaches the DATA state, it remains in this state until all of the inputs return to the NULL state. A dual-rail signal, D, consists of two wires, D0 and D1, which may assume any value from the set DATA0, DATA1, NULL. The DATA0 state (D0 = 1, D1 = 0) corresponds to logic zero, the DATA1 state (D0 = 0, Dl = 1) corresponds to logic one, and the NULL state (D0 = 0, D1 = 0) corresponds to the empty set meaning that the value of D is not yet available. The two rails are mutually exclusive, so that both rails can never be asserted simultaneously; this state is defined as an illegal state as shown in Table 1. Figure 6 (a) presents the NCL pipeline structure based on local handshaking flow, and Figure 6 (b) presents the DATA/NULL cycle in the NCL pipeline structure.



(a)

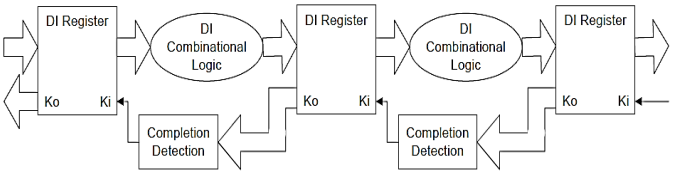


(b)

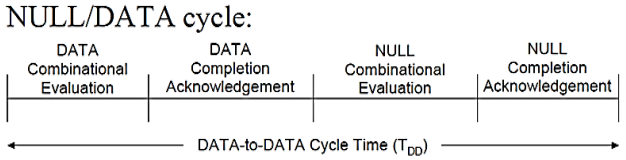
Figure 5: (a) Thmn NCL gate symbol, (b)TH34w2 threshold gate: Z = AB + AC + AD + BCD

Table 1: Dual-rail encoding

	DATA 0	DATA 1	NULL	Illegal
Rail0	1	0	0	1
Rail1	0	1	0	1



(a)



(b)

Figure 6: (a) NCL pipeline structure, (b) DATA/NULL cycle

INTERFACING BLOCK BETWEEN SYNCHRONOUS AND ASYNCHRONOUS CIRCUITS:

ASYNCHRONOUS PUF

For example, in a ring oscillator-based PUF, the frequencies of the two ring oscillators are matched closely, so the environment can cause the oscillator to switch output, causing the temperature to rise or fall, resulting in inaccurate responses.

It can also be observed that a large array of ring oscillators can cause local chip temperature changes. This temperature stability problem is depicted on the left side of Fig. 7. The ideal scenario is that the frequency difference should be sufficient to ensure consistent operation for temperature and voltage, as shown on the right in Fig. 7. The approach to solve this problem in the PUF has been to use error correction methods that are expensive in terms of silicon area and add additional complexity to the challenge-response protocol.

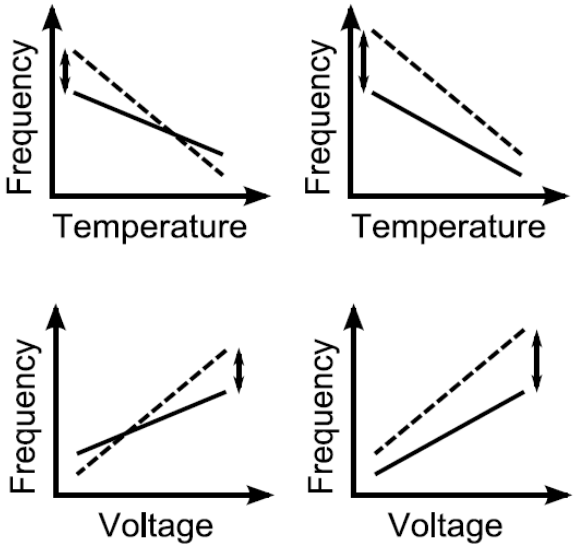


Figure 7: Temperature and voltage effects on a ring oscillator based PUF

In this paper, we propose a highly reliable PUF based on NCL asynchronous circuit with low cost which does not depend on temperature and voltage variation on a chip as shown in Fig. 8.

The proposed PUF consists of NCL registers, NCL MUXs, and exclusive ORs, and a razor filp-flop. The NCL registers are conventional NCL registers, and the NCL MUXs select the inputs according to challenge values received from a server as shown in Fig. 9. In order to make it difficult to predict the final response value, the inputs are crossed before the NCL-MUX in the middle of the path and used Exclusive OR in the final output.

In addition, to solve the metastability problem of conventional D flip-flops, Razor flip-flip [10] has been used. The output of the conventional D flip-flop goes to a metastable state when setup or hold time violation occurs). The Razor flip-flop can solve the metastability by using a metastability detector as shown in Fig. 10.

Asynchronous circuits are at natural advantage in terms of side-channel attack resistance. The clock-related information leakage can be either eliminated or significantly reduced, which extensively increases the difficulties of attack due to the lack of timing references. For example, the balanced delay insensitive method introduced a power-balance gate design that could improve the resistance of asynchronous RTZ protocol; Globally-Asynchronous Locally-Synchronous (GALS) module is a module that uses a synchronous circuit wrapped around by an asynchronous circuit to gain the benefits of both design methodologies. 1-of-n data encoded speed independent (SI) circuit has been proved to be more resistant against timing attack, DPA attack, and clock/power glitch attack. With the development of systematic design flows for asynchronous circuits, certain commercial asynchronous crypto-processors also emerge in the market.

EXPERIMENTAL RESULTS

The proposed circuit have been designed and evaluated

using a 0.18 μm MOSFET technology model (VDD=1.8V), and is a circuit of Physical Unclonable Function in which one bit of response is transmitted through 8 switches and one Razor flip-flop. Fig. 11, the Arbiter PUF using the existing D flip-flop cannot output the correct output, but the proposed Arbiter PUF showed the correct output value.

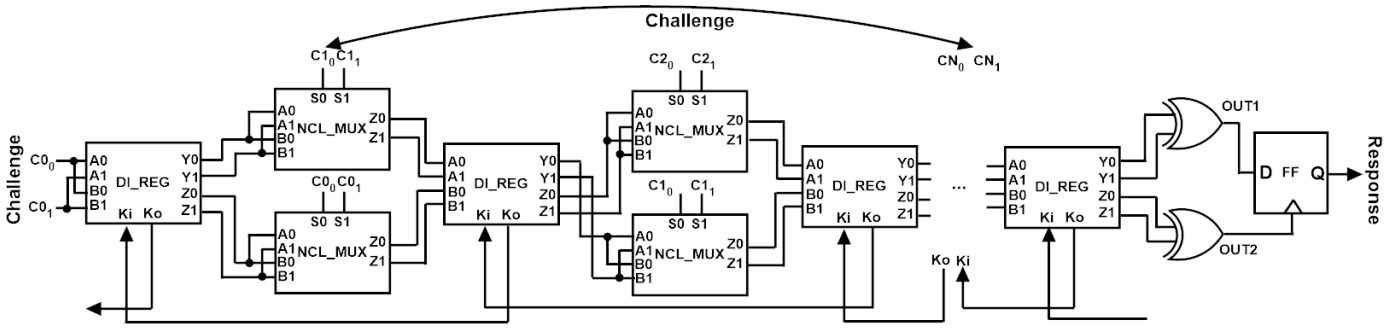


Figure 8: Proposed Arbiter PUF

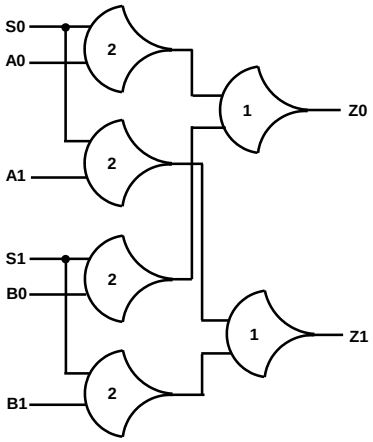


Figure 9: NCL MUX

The temperature and voltage stability are shown in shown in Fig. 11. In this simulation, the temperature is changed from 0 to 125℃, and the supply voltage is changed from 1.6V to 2.0V. The simulation result shows that the proposed PUF based on NCL asynchronous circuit with low cost does not depend on temperature and voltage variation on a chip

Therefore, it is confirmed that the proposed PUF compensates for the existing problems and has a reliable physical copy protection function for the resultant values.

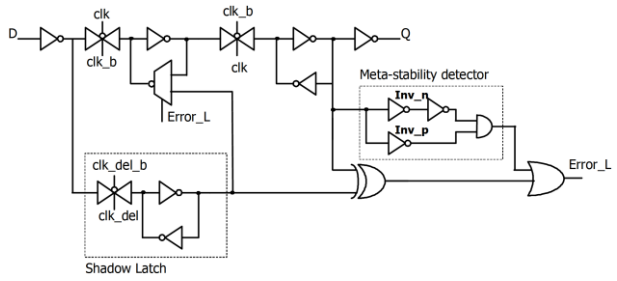


Figure 10: Reliable D Flip-Flop without Metastability

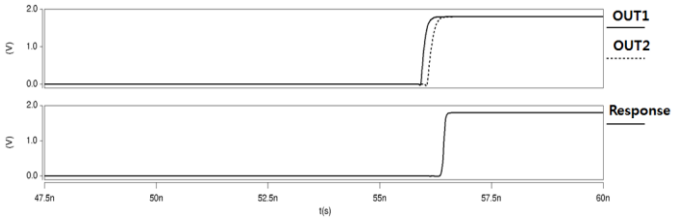


Figure 11: Simulation Waveform on Outputs

Table 2 shows the comparison between the conventional arbiter PUF and the proposed PUF, and the simulation result shows the power reduction rate of 60% compared to the conventional Arbiter PUF.

Table 2: Comparison of Power Consumption.

	Arbiter PUF	Proposed PUF
Power Consumption	9.51E-02W	3.2743E-02 W

CONCLUSIONS

Recently, the importance of security has been emphasized since IoT era has become one of the most important areas of security. Existing security algorithms are done through a complex process, but if they know only algorithms, they are vulnerable to security. Therefore, in this paper, we propose a reliable Arbiter PUF circuit based on an asynchronous circuit methodology with lower error rate and higher reliability than the conventional arbiter PUF. Experimental results show that the proposed PUF improves the reliability and reduces the power consumption of the PUF compared to the conventional Arbiter PUF.

The proposed PUF is expected to be used in systems requiring low power consumption and high reliability such as low power cryptographic processors and low power biomedical systems.

ACKNOWLEDGEMENT

This research was supported by the Daegu University Research Grant, 2014.

REFERENCES

[1] G. Suh & S. Devadas (2007). Physical unclonable functions for device authentication and secret key generation. Design Automation Conference. DAC ’07. 44th ACM/IEEE, San Diego, CA, USA.

[2] D. Lim, (2004) Extracting secret keys from integrated circuits. M.S. thesis, Dept. Elect. Eng. Computer Science, Massachusetts Inst. Technol., Cambridge, USA.

[3] K. Yang, Q. Dong, D. Blaauw, D. Sylvester, “A physically unclonable function with BER <10−8 for robust chip authentication using oscillator collapse in 40nm CMOS,” in IEEE Int. Solid-State Circuits Conf. Dig. Tech., pp. 254-255, 2015.

[4] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” Science, vol. 297, no. 5589, 2026–2030, 2002.

[5] G. Suh & S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” Design Automation Conference. DAC’07. 44th ACM/IEEE, San Diego, CA, USA. 2007.

[6] X. Lu, L. Hong, and K. Sengupta, “An integrated optical physically unclonable function using process-sensitive sub-wavelength photonic crystals in 65 nm CMOS,” in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech., pp. 272–273, 2017..

[7] C. Q. Lin, Y. Cao, C. H. Chang, "ACRO-PUF: A Low-power, Reliable and Aging-Resilient Current Starved Inverter-Based Ring Oscillator Physical Unclonable Function," IEEE Transactions on Circuits and Systems I: Regular Papers. vol. 64, no. 12, pp. 3138-3149, 2017.

[8] Y. Taur and T. H. Ning, "Fundamentals of Modern VLSI Devices," Press, Cambridge Univ. Cambridge, 1998.

[9] Scott C. Smith, Jia Di, "Designing Asynchronous Circuits using NULL Convention Logic (NCL)," Morgan & Claypool Publishers, 2009.

[10] Shidhartha Das, Carlos Tokunaga, et al., "Razor II: In Situ Error Detection and Correction for PVT and SER Tolerance," IEEE Journal of Solid-State Circuits (JSSC), Vol. 44, No. 1, pp. 32–48, 2010.