IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 27, 2022, accepted February 17, 2022, date of publication February 22, 2022, date of current version March 3, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3153359

Compact SRAM-Based PUF Chip Employing Body Voltage Control Technique

JAE-WON NAM[1], **(Member, IEEE), JU-HYEOK AHN**[2], **AND JONG-PHIL HONG**[3], **(Member, IEEE)**

[1]Department of Electronic Engineering, SeoulTech, Seoul 01811, Republic of Korea
[2]LX Semicon, Daejeon 34027, Republic of Korea
[3]School of Electrical Engineering, Chungbuk National University, Cheongju 28644, Republic of Korea

Corresponding author: Jong-Phil Hong (jphong@cbnu.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) by the Korean Government through the Ministry of Science and ICT (MSIT) under Grant NRF-2021R1A2C2005258, and in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) by the Ministry of Education under Grant 2020R1A6A1A12047945.

ABSTRACT This paper presents an ultra-small physical unclonable function (PUF) chip structure to protect data in compact IoT sensor devices. The proposed PUF has far fewer transistors and a reduced active area compared to the conventional strong PUF with multiple challenge response pairs (CRPs). According to the manufacturing process variations, the conventional SRAM-based PUF uses a switching transistor and a main transistor to implement multiple CRPs, whereas the proposed structure adds the function of a switching transistor to a single main transistor, controlling the body voltage to switch the transistor. This unified and simple PUF structure results in significant silicon area reduction. For a PUF with a 32-bit challenge, the number of transistors is significantly reduced by 40%; the active area of the conventional structure is $57.78\mu m^2$ while the area of the proposed structure is $36.4\mu m^2$. Overall, an active area reduction of 38% is realized with the same number of CRPs. Here, we implemented an SRAM-based PUF system with a 32-bit challenge, a 1024-bit response, and 160 million CRPs. PUF core cell shows energy efficiency of 0.09 pJ/bit. The inter-Hamming distance is 48.89%, while the intra-Hamming distance is 1.2% after data post-processing, i.e., discarding unstable bits. A prototype chip is implemented in the 65nm CMOS process with a supply voltage of 1.2V. Compared to the prior arts, the proposed prototype is shown effective silicon area reduction while maintaining remarkable energy efficiency.

INDEX TERMS PUF, SRAM-based PUF, and body voltage control.

I. INTRODUCTION

The rapidly expanding deployment of IoT devices to remote and isolated areas leaves sensors and edge routers vulnerable to physical security attacks. The hardware itself also requires strong protection algorithms and the circuitry of mobile devices and personal electronics. Unlike existing networks, which simply provide commands from a higher-level system to lower-level sensor devices, the IoT requires bi-directional communication from lower-level devices to a higher-level system. Therefore, it is necessary to defend against security threats from lower-level devices [1]–[4]. With regard to conventional security systems, customized systems have mostly been researched on servers and PCs, where security threats are a major problem. Servers and PCs store considerable amounts of important data, leading to major problems in the event of theft, such as personal information losses. The features of the server and PC security systems are as follows. In order to ensure a high level of security performance, the server is mainly a high-capacity hardware system, and the PC uses a software system that requires a high-performance processor [2]–[4]. As is in an environment where power is always supplied, the burden on power consumption is relatively relaxed. Also, the installation cost of the system is high, but there is no need to move once it has been installed. The characteristics of these existing security systems are not appropriate for application to IoT devices.

In IoT devices, numerous sensors are integrated into a single chip, and because portability is important, batteries are often attached. Due to the characteristics of IoT devices, it is difficult to apply currently researched high-performance

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

security systems. Therefore, an advanced ultra-small security system with low power and a small area suitable for IoT devices is required [1].

As an alternative to the security requirements of IoT devices as described in the earlier section, the physical unclonable function (PUF) has been studied. The PUF is a random number generator that generates a password using random physical features existing in nature. PUFs can be classified according to the physical characteristics used to generate the random numbers [5]. Non-electronic PUFs are classified according to the material type; there are paper PUFs, CD PUFs, magnetic PUFs, acoustical PUFs, and optical PUFs. An optical PUF uses a pattern formed when a laser is irradiated onto a manufactured optical token. In this case, the position of the laser serves as a challenge response pair (CRP) [6] by using the pattern created as a challenge as a response. In contrast, an electronic PUF uses electrical properties, and this category includes coating PUFs and LC PUFs. The coating PUF is used as a CRP that relies on errors in the manufactured capacitor.

The intrinsic PUF is a random number generation circuit that relies on the fact that the operation characteristics differ due to process variations, even when the same circuit is manufactured with a PUF using the process variations in the semiconductor manufacturing process to generate a random output [7]. Because process variations are manufacturing errors that cannot be predicted in advance, reverse engineering can be prevented. There are various causes of process variations, but they are typically caused by differences in operating speeds depending on the position in the wafer, and mismatches in the etching and diffusion processes. For process variations due to etching, if dry etching or wet etching is utilized during the process, etching is performed using a specific material for the process. Even if the same material is used for the same amount of time, the degree of etching will differ, resulting in errors in the width and depth. Although etching has been well described, errors occur in other processes, including etching due to similar reasons. Wafer mismatches affect the operating speeds of chips manufactured at the same location due to mismatches in wafer thicknesses that arise during the process of cutting and polishing the ingot. If there is a process variation, the physical characteristics of the transistor, such as the width (W) and length (L), change. The drain current of a MOSFET transistor is expressed as shown below.

$$I_D = \frac{1}{2}\mu C_{\text{ox}}\frac{W}{L}(V_{GS} - V_{th})^2.$$

Here, as L, W of the transistor vary, the drain current changes accordingly. Therefore, given that the operating characteristics of each transistor constituting the PUF are different, even if the PUF has the same structure, different responses would be generated. The intrinsic PUF is mainly divided into delay-based PUF and Memory-based PUF depending on the operation principle. The strength of the PUF depends on the number of CRPs that can be configured from a single device, and the greater number of CRPs typically demand the larger active area.

Fig. 1 describes the structure and operational principle of two representative delay-based PUFs: the arbiter PUF and ring oscillator PUF. First, the arbiter PUF generates output by comparing which input arrives at the arbiter first among two paths using the operation speed error of the signal path [8]–[11]. The CRP increases as more paths are configured, but one disadvantage is the reduced operating speed. The ring oscillator (RO) PUF measures the speed of a square wave generated from a RO by selecting two from among several Ros [12], [13]. Like the arbiter PUF, it generates its output by comparing which of the two ROs is faster.

The memory-based PUF is a PUF that uses the metastable state of memory devices and has the advantage of a small area per bit and rapid response generation. [6], [7] However, because it is difficult to increase the CRP, it is used as the chip ID of the circuit rather than for entity authentication [14]. The latch PUF and SRAM PUF are mainly used as memory-based PUFs [7], [15], [16]. The latch PUF connects two latches as a cross-coupling, and the remaining inputs tie together as a reset signal. The reset signal is then applied as the input first to set the two latch outputs to "high," after which, when the reset signal is cut off, the latch operates to invert the output. Although both latches have the same input and output, the latch with the higher operating speed determines the response first due to process deviations. Similarly, the SRAM PUF has a structure in which two inverters compete to determine the output when the gate input is set to "high" and then operated.

Among non-electronic PUFs, the electronic PUF and the intrinsic PUF described above, integration is impossible, except in the intrinsic PUF, meaning that it is difficult to apply this type to the low-area security system mentioned earlier. Therefore, the intrinsic PUF, especially memory-based PUF, is suitable as a security alternative for IoT systems applicable to strong and low-area security systems. For higher security systems, we can apply an error correction circuit (ECC) to existing SRAM-based PUF. This is related to a bi-stability of the SRAM memory cell, thus PUF output becomes more stable and unique code over the operating condition changes. By employing a temporal voting, an increasing entropy, or a discarding technique, a bit error rate (BER) can be enhanced by scarifying multiple cycle of computation time [17], scrambling PUF output [18], [19], or masking out few SRAM bit cells [20]. Since the effectiveness of ECC is proportional to the complexity of the SRAM-based PUF associated with CRPs, it is important to have a higher number of CRPs. However, it is difficult to apply large number of CRPs due to the proportionally increased silicon area [18]. Hereby, we conducted research on a method to dramatically reduce the increase in chip area while maintaining large number of CRP and compensated for the structural disadvantages of the conventional SRAM-based PUF system by controlling the body voltage of the transistor.

For similar prior method, there is a current integrated differential NAND structure PUF that employs different body

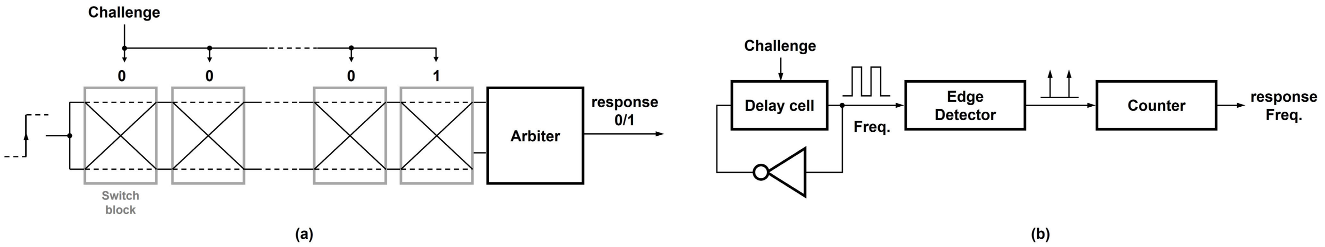


FIGURE 1. Block diagram of (a) Arbiter PUF and (b) Ring oscillator PUF.

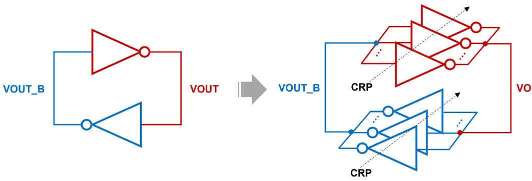


FIGURE 2. SRAM-based PUF with multiple CRPs [18].

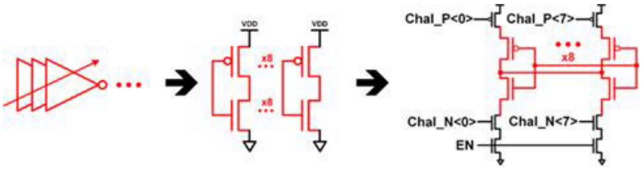


FIGURE 3. Schematic of multiple CRP inverter.

biases in the word-line PUF cell [21]. Since the effective resistance of the transistor changes depending on the threshold voltage according to the applied body potential, it is expected that the number of CRP will increase. However, in NAND-structured cells, more transistors need to be connected in series to increase the overall PUF size. Therefore, the overall resistance of a single bit-line circuit is much higher and the final single transistor threshold voltage fluctuations caused by various body biases are negligible. Therefore, there is a limit to implement a larger PUF.

This paper is organized as follows: section II explains existing technical issues related to the conventional SRAM-based PUF structure as designed with multiple CRPs. Section III explains the proposed SRAM-based PUF, and section IV shows the circuit implementation of the entire PUF system in a 1024-bit array. The work is experimentally validated in section V by measuring the uniqueness, randomness, and stability of the outcome, with a comparison presented with comparable prior state-of-the-art PUFs. The paper is concluded in section VI.

II. TECHNICAL ISSUES OF CONVENTIONAL SRAM-BASED PUF SYSTEMS

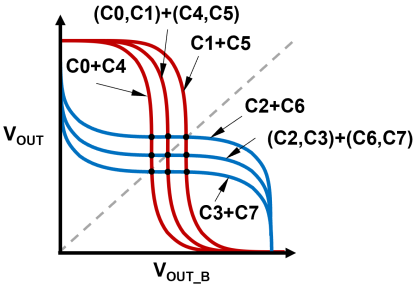
A. EXISTING TECHNICAL ISSUES

To reduce the active area and the power consumption of a security system targeting IoT applications, the intrinsic PUF approach appears to be the best choice due to the compactness of the intrinsic PUF. Among PUFs, research on the SRAM PUF, occupying the smallest silicon area, is actively underway. Although the SRAM PUF has the advantages of a rapid response and a small area, there is a disadvantage related to the number of CRPs required for authentication of an entity.

Intrinsic PUFs can be further categorized into the strong PUF and weak PUF types depending on the number of CRPs. The strong PUF has multiple CRPs and can thus be used for various purposes, such as authentication and authorization. On the other hand, the weak PUF has only a single CRP, meaning a single chip ID, and thus cannot be used for authentication; in fact, the uses of this type are limited. As a result, the strong PUF with multiple CRPs is suitable for entity authentication. Figure 2 shows SRAM-based PUFs with multiple CRPs and Figure 3 illustrates a schematic of multiple-CRP inverter. The multiple-CRP inverter configures the SRAM differently according to the challenge, which is selected from among the multiple-CRP sets [18]. This method improves the hardware security of the conventional SRAM PUF. However, for simply configured inverters that work in parallel to connect switching transistors, the entire area of the SRAM PUF increases by as much as the number of CRPs. To resolve this issue, the switching transistor is connected to the PMOS and NMOS of the inverter in parallel without the inverter selected as the switching transistor. With this structure, the number of PMOS and NMOS components in the inverter can be determined according to the challenge. For example, two PMOS and one NMOS components can be selected to configure a new inverter.

B. OPERATING PRINCIPLE OF THE CONVENTIONAL APPROACH

Fig. 4 describes the operation principle of the existing SRAM-based PUF with multiple CRPs. Depending on the challenge, the operation characteristics of the inverter change for each inverter selected and the metastable point changes, accordingly, resulting in different responses. The existing SRAM-based PUF with multiple CRPs has the advantage of compactness, though with an increase in the number of CRPs. However, a structure with a 32-bit challenge requires 80 transistors. Although it has a small area, it can be reduced furthermore. In the following section, we describe in more detail the proposed SRAM PUF topology to minimize the silicon area by reducing the number of transistors in the existing SRAM-based PUF with multiple CRPs.



Note: C0, C1, … , C7 stands for challenge bits

FIGURE 4. Operating principle of multiple CRP SRAM-based PUF.

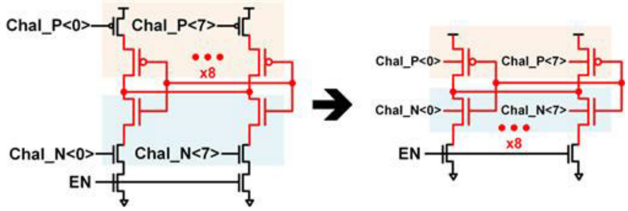


FIGURE 5. Schematic of the conventional and proposed SRAM-based PUF.

III. PROPOSED SRAM-BASED PUF SYSTEM

A. ACTIVE AREA AND CRP SPACE CALCULATION

Fig. 5 shows a schematic of the conventional PUF and the proposed SRAM-based PUF. To reduce the area of the conventional structure, the switching transistor shown in light red, and the main transistor of the inverter shown in light blue can be operated as a single transistor. Conventionally, to increase the CRP, the PMOS and NMOS are connected in parallel, and a connected switching transistor is required to determine whether or not each transistor is used. Because the main transistor cannot operate independently and an additional switching transistor is required, two or more transistors are desired to increase a 1-bit challenge. However, the proposed structure requires only one transistor, in which the switching transistor and the main transistor are combined to increase the 1-bit challenge. The numbers of transistors used in the PUF with a 32-bit challenge are as follows: in the conventional structure, 16 switching PMOSs, 16 main PMOSs, 16 switching NMOSs, 16 main NMOSs, and 16 current flow prevention NMOSs, for a total of 80 transistors, are required. On the other hand, in the proposed structure, 48 transistors in total are required with 16 switching, main PMOS, and NMOS each, and 16 NMOSs for current flow prevention. The number of transistors required is reduced by 40% from 80 to 48 transistors. In general, the overall degree of transistor reduction represents a decrease in active area, and considering the chip manufacturing process, the actual area reduction would be 40% or less due to unscalable layout factors.

Here, we count the number of CRPs in the proposed PUF structure; NMOS and PMOS transistors are counted separately for simplification. The SRAM-based PUF, which has back-to-back connected and balanced inverters, is ideally in a metastable state. However, owing to process mismatches, a biased output is produced. With or without the CRP, whichever SRAM-PUF remains in metastable state cannot be used for entity authentication due to possible bit flipping. This issue can be resolved by embedding an extra circuit, which can avoid problematic challenges or can change such challenges into other, more viable challenges.

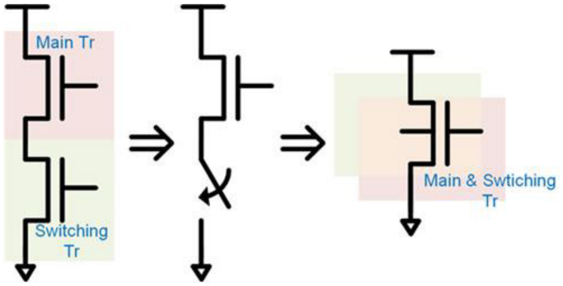


FIGURE 6. Schematic of the conventional and proposed SRAM-based PUF.

$$\text{Number of NMOS CRP} = ({}_{n}\mathrm{C}_1)^2 + ({}_{n}\mathrm{C}_2)^2 + \ldots + ({}_{n}\mathrm{C}_n)^2$$
$$\text{Number of PMOS CRP} = ({}_{p}\mathrm{C}_1)^2 + ({}_{p}\mathrm{C}_2)^2 + \ldots + ({}_{p}\mathrm{C}_p)^2$$
$$\text{Total Number of CRP} = \sum_{k=1}^{n} ({}_{n}\mathrm{C}_k)^2 \cdot \sum_{m=1}^{p} ({}_{p}\mathrm{C}_m)^2$$

Given that the number of PMOSs (p) and the number of NMOSs (n) are independent, the total number of CRPs is calculated as the product of the NMOS cases and the PMOS cases. As a result, the number of CRPs in the proposed structure is approximately 160 million according to the above calculation.

B. OPERATING PRINCIPLE

The operating principle of the proposed SRAM-based PUF structure is described in this section. The key idea of the proposed structure is to allow one transistor to act as a switching transistor and as a main transistor simultaneously. Fig. 6 shows a schematic of the proposed SRAM-based PUF cell combining two roles into a single transistor. The first schematic in Fig. 6 illustrates the main and selected transistors for configuring the inverter and for connecting the branch to an activation function. The second schematic in Fig. 6 is a symbolic expression of a merged transistor performing the main and activation functions at once. Note that the body voltage potential may change the strength of the transistor in terms of drain current control; in such a case, we can adjust the operating point of the transistor using the body voltage. In other words, we can enable multiple CRPs from the different body voltage control schemes.

Fig. 7 shows the drain current change resulting from a device threshold voltage shift from the body voltage control. In general, the body voltage of the NMOS is tied to the lowest potential, such as 0V, and the body terminal is often connected to the source terminal to diminish the body effect. In this 65nm CMOS process, we varied the body potential from 0V to 1.2V and observed the changes in the drain current.

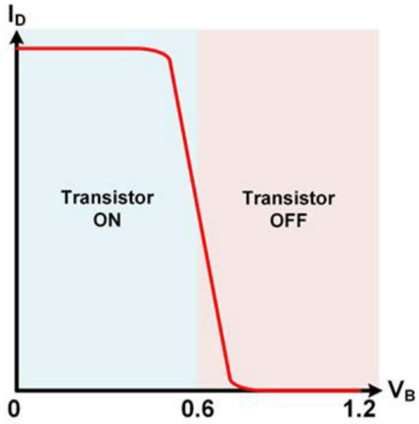


FIGURE 7. I/V response between a drain current and a body voltage.

When 1.2V is applied to the gate terminal of the transistor, an electric field is formed due to the difference relative to the body voltage, with the electrons in the body moving toward the gate and creating a channel. However, when the body voltage increases, the voltage difference is reduced, and the electric field becomes weaker. Thus, the number of electrons moving toward the gate decreases and no channel is formed. Similarly, an increase in the body voltage turns off the transistor despite the application of non-zero gate input potential. As a result, the body voltage of the transistor takes over the role of the switching transistor in the conventional SRAM-based PUF structure. As shown in the Figure 7, when body voltage of 1.2V is applied, the transistor is strongly turned off. However, in the proposed structure, we chose to use body voltage of 0.6V to deactivate the transistor because this approach induces minimum leakage current while also turning off the transistor at the given CMOS process.

Fig. 8 shows the operational principle of the proposed SRAM-based PUF according to an 8-bit challenge. Figure 8 (a) illustrates the enabled transistors (T0, T2, T5, and T7) at the given challenge input. For each transistor, the operating speed caused by a process variation is simply expressed as “Fast” and “Slow.” In the inverter marked in red, two fast transistors are selected, while in the inverter marked in blue, two slow transistors are selected. When the operation of the SRAM PUF is started by the enable signal (EN), the inverters operate to change both gate nodes from “High” to “Low.” Because both inverters have different operating speeds, the inverter with the “Fast” transistor selected operates first; as a result, VOUT and VOUT_B become “High” and “Low,” respectfully. Figure 8 (b) illustrates the enabled transistors (T0, T2, T4, and T7) at different challenge inputs. In the inverter indicated in red, “Fast” and “Slow” transistors are selected, and in the inverter marked in blue, two “Slow” transistors are selected. As in the case described in Fig. 8 (a), when the operation starts, VOUT becomes “High” because the inverter with “Fast” and “Slow” transistors selected operates first. Although the operating speed is indicated as “Fast” and “Slow” for clarity, it is not actually divided into only two settings but is more detailed. Therefore, even in the comparison between “Slow” and “Slow,” the output can be determined as either “High” or “Low.”

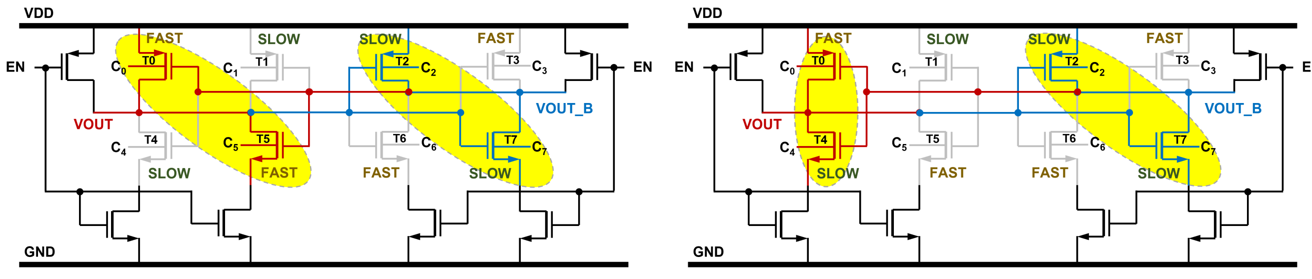
IV. CIRCUIT IMPLEMENTATION

A. OVERALL SYSTEM ARCHITECTURE

The proposed PUF system includes a control circuit for operating a PUF cell and a PUF array, as shown in Fig. 9. The PUF array consists of a total of 1024 bits (32 rows and 32 columns). The reason why the PUF output is set to 1024 bits is as follows. There is a circuit that uses the secret key as input in the protocol used for entity authentication. The secret key input of the circuit requires approximately 80 bits to 256 bits. When implementing a PUF that generates a single bit, 256 CRPs must be used to generate 256 bits, and the response time is accordingly reduced by 256 times. Therefore, it is necessary to design a PUF that can generate more than 256 bits in a single operation. Ideally, the PUF response should always have an output that matches the input; however, the manufactured chip may not produce the same output depending on the operating conditions, such as the operating supply voltage, temperature, and noise. Therefore, we allocate spare bits in addition to 256 bits to compensate for the discarding of unstable bits (called the unstable bit discard technique).

B. CONTROL CIRCUIT

The control circuit consists of three blocks. First, the reset and clock signal are used as inputs, and enable (EN), word-line (WL), and pre-charge signals are generated accordingly. EN is the signal for charging a SRAM cell to “high” and initializing the PUF cell. WL is used to pass the generated PUF response to the final output. Finally, the pre-charge signal is used to charge the word-line to “High” when the WL remains at “Low.” Each instance of the signal timing is described in a timing diagram shown in Fig. 10. The second block of the control circuit (shown in Fig. 9) is a 5-to-32 decoder and is used to decode the signal generated in the first block of the control circuit into 32 bits according to the address signal. The PUF array operates in units of rows, and it is necessary to control each row separately. Here, the 1-bit signal is decoded into 32 bits using the address signal and the decoder. However, because a pre-charge signal is not applied to each row or column of the PUF array but is connected to the buffer of the PUF array, only a 1-bit pre-charge signal is sufficient. Therefore, it is transferred directly to the next block without going through the decoder. The third block of the control circuit (shown in Fig. 9) amplifies the signal generated by the first and second blocks. Because the PUF array consists of 32 rows and 32 columns and many cells need to be operated at once, the unamplified signal cannot easily drive 32 cells. Therefore, a buffer is used to amplify the signal. The challenge signal is directly applied to the PUF array without going through the control circuit. In addition,



(a)

(b)

FIGURE 8. Example of proposed structure operation with the cases of (a) "Fast/Fast" and "Slow/Slow" and (b) "Fast/Slow" and "Slow/Slow" transistors.

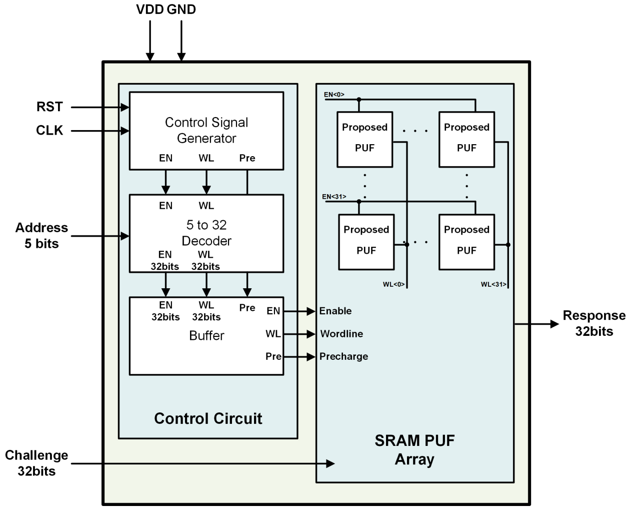


FIGURE 9. Overall block diagram of the proposed SRAM-based PUF system.

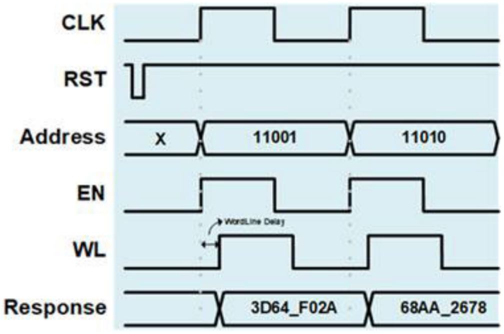


FIGURE 10. Timing diagram of the proposed PUF system.

the response is generated at the output terminal through the buffer in the PUF array.

C. SYSTEM TIMING PLAN

Fig. 10 illustrates the operation timing of the signals described above. The reset signal (RST) has the highest priority, and when RST becomes "Low," all circuits are reset during any operation. Next, the EN, WL, and pre-charge signals are generated in sync with the master clock signal. Note that there is a fixed delay time between WL and EN shown in the timing diagram. The reason why WL is flagged later than EN signal is to ensure the established PUF output by process variations of solely the internal PUF cell. If WL and EN are flagged at the same time, a load line and associated external load circuits contribute the final output, which is not desired. Thus, we propose a delay of WL against EN to resolve this issue. As the address signal changes, EN and WL are toggled, and as the operating row changes, the response also changes accordingly. To generate all 1024 bits, the address must be updated 32 times from 00000$_{(2)}$ to 11111$_{(2)}$.

V. MEASUREMENT RESULTS

A. SIZE COMPARISON

The conventional SRAM-based PUF and the proposed structure are fabricated as shown in Fig. 11. The conventional structure has an area of 57.78μm^2(14.61$\mu m \times 3.96\mu m$). On the other hand, the cell of the proposed structure has an area of 36.4μm^2(20.8$\mu m \times 1.75\mu m$), and it achieves an active area reduction of 38% due to the reduced number of transistors.

B. INTER-INTRA HAMMING DISTANCE

Fig. 12 shows the measurement results (intra- and inter-Hamming distances) of the proposed structure. The fabricated prototype in the 65nm CMOS process was evaluated under a room temperature of 25 °C and with a supply voltage of 1.2V. The measured Inter-HD is 0.4889, which is quite close to the ideal value of 0.5. To measure Inter-HD, we used the same challenge to 60 chips, and the output responses were measured and calculated for each chip [12,22]. The statistical result of Inter-HD has a mean value of 0.4889 and standard deviation of 0.0224. Intra-HD was measured by comparing the responses obtained by the same challenge to the same chip and iterating the test 3000 times. In addition, in order to increase the reliability of the measurement, the result was derived by evaluating four different chips instead of testing a single chip. The measured Intra-HD showed a mean value of 0.031 and a standard deviation of 0.0171.

C. HAMMING WEIGHT

Fig. 13 shows the Hamming weight (HW), which is an index used to determine whether the ratio of 0 and 1 outcomes at the single response of the PUF are evenly distributed. To measure

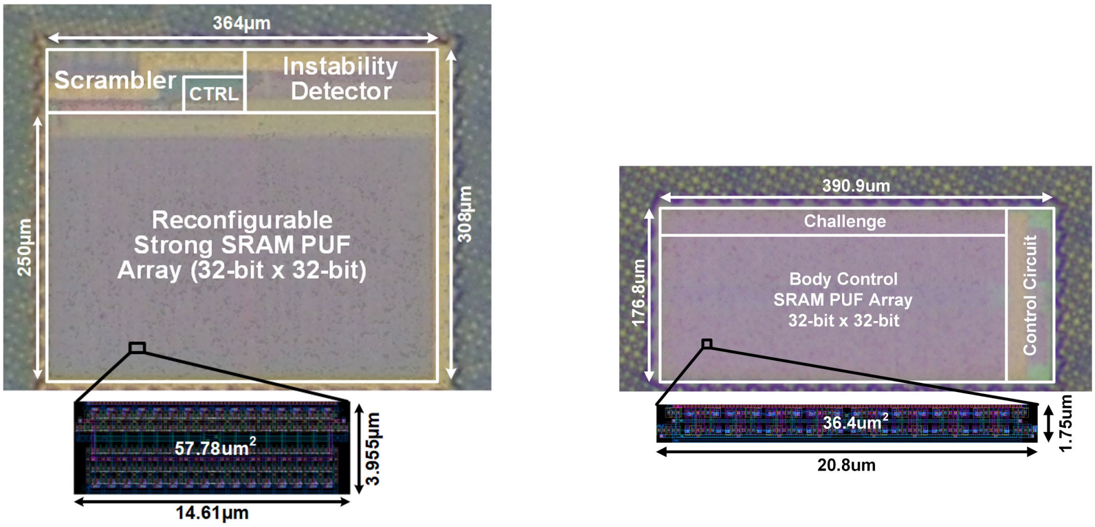


FIGURE 11. Chip micrograph.

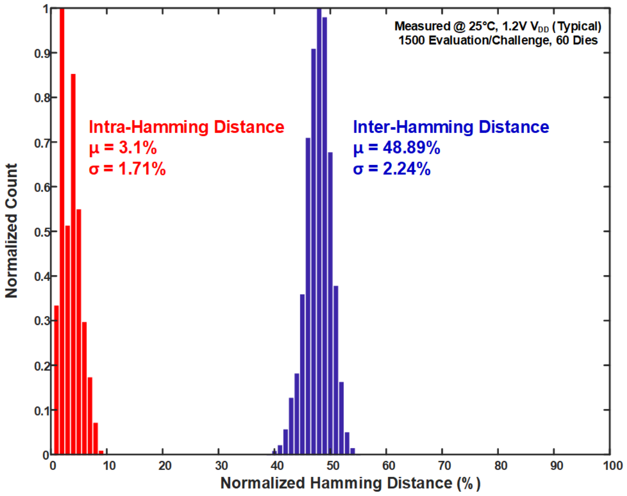


FIGURE 12. Measured inter/intra-PUF hamming distance distribution.

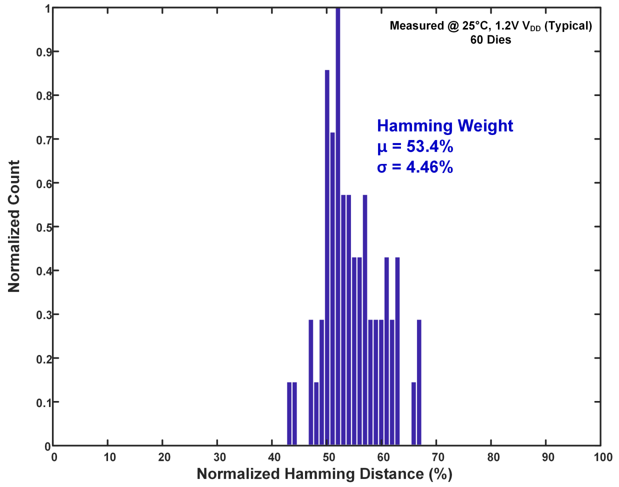


FIGURE 13. Measured hamming weight.

the HW, it was evaluated through the responses obtained by the same challenge to 60 chips, similar to the Inter-HD case.

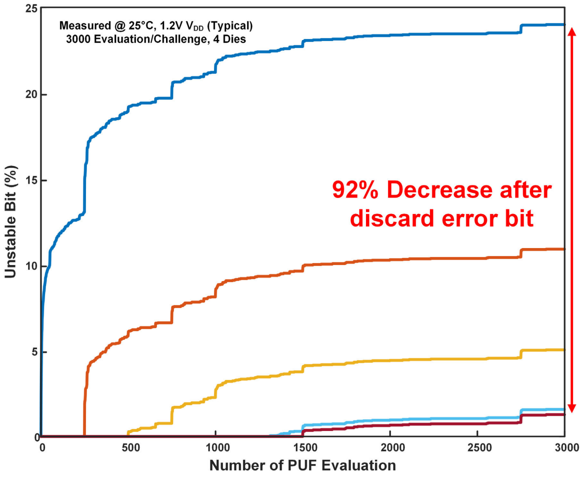


FIGURE 14. Unstable bit error ratio with the post processing.

The measured mean value is 0.534 and the standard deviation is 0.0446.

D. CRP RELIABILITY IMPROVEMENT AND ANALYSIS

Fig. 14 shows the measurement results of unstable bits to improve the stability of the proposed structure. According to the measured unstable bits of four different chips with the same challenge, 24.1% bits are detected as unstable through 3000 evaluations. If unstable bits are used continuously, the stability of the response generated by the PUF is degraded; thus, a technique by which to remove the unstable bits is used to increase the credibility of the PUF. If the unstable bits obtained through 1500 trials are removed, the unstable bits of the PUF are reduced to 1.2%. In this case, it is possible to discard 92% of the unstable bits.

Fig. 15 shows the measurement results when assessing the degree of error in the response due to the external environment. Including the room temperature and reference voltage, this was measured in 25 °C increments from 0 degrees to

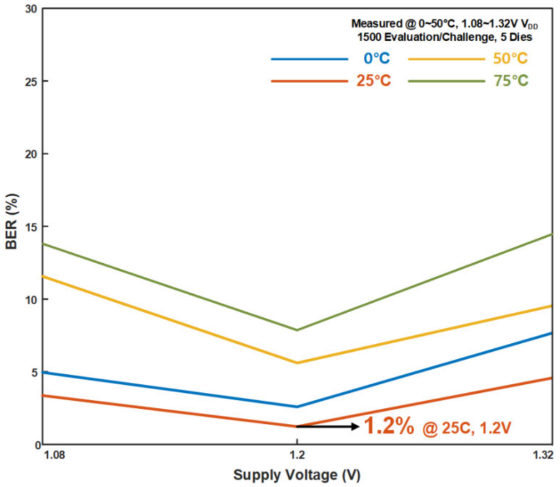


FIGURE 15. Measured bit error rate (BER) after post-processing.

TABLE 1. Performance summary and comparison with prior works.

	This work	[23]	[20]	[25]	[24]
Tech node	65nm	28nm	40nm	40nm	90nm
PUF type	Bi-stable	Bi-stable	Bi-stable	Digital	Analog
Bit-width of challenge	32	256	-	96	256
Bit-width of response	1024	64	-	1	31
Operating condition (V)	1.08-1.32	0.5-0.9	0.7-1.2	0.7-1.2	0.64-0.66
$\text{BER}_{\text{worst}}$ (%)	20.8	8	8.41[a]	<1.8E-8	<0.1
Inter-HD	0.4889	0.483	0.4964	0.5007	-
Intra-HD	0.0311	0.0317	-	0[b]	0.1
Core area (F^2/bit)	8,615	22,720	987	528,125	139,382
Energy Efficiency (pJ/bit)	0.09	0.097	0.127	17.75	6080
No. of CRPs	1.6E8	1.17E11	5.5E28	1E25	4.01E15

[a] 29.76% of CRPs are dynamically masked.
[b] 34% of CRPs are discarded.

75 °C, and the supply voltage of the circuit was measured by increasing it from 1.08V to 1.32V, which is ±10% of the reference voltage. The most error-prone environment arose when 75 °C and 1.32V were applied, and the bit error rate was 14.8%. The above result is the calculated result after removing any unstable bits that were found. The bit error rate can be lowered even further by removing additional unstable bits.

VI. CONCLUSION

In this paper, we proposed an ultra-small SRAM-based PUF that reduces the area of the conventional structure with multiple CRPs. Through the idea of reducing the switching transistor and the main transistor of the conventional structure to one transistor by controlling the body voltage, the number of transistors of the PUF with the same CRP was reduced by 40% and the area was reduced by 38%. While reducing the active area, the performance remained at a level similar to that of the conventional structure. The core 1-bit cell area of the prototype is 36.4μm^2, and the number of CRPs is 160 million. The performance outcomes when measured using a test board with an FPGA are as follows: Inter-HD = 0.4889, Inter-HD = 0.0311 and energy efficiency of 0.09pJ/bit. The proposed switching transistor reduction technique using the body voltage control technique can be applied to PUFs with other structures. The overall performance summary and a comparison with the prior works are given in Table 1.

REFERENCES

[1] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.

[2] Y. Zheng, S. S. Dhabu, and C.-H. Chang, "Securing IoT monitoring device using PUF and physical layer authentication," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Florence, Italy, May 2018, pp. 1–5.

[3] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. S. Chakraborty, D. Mahata, and M. M. Prabhu, "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 3, pp. 424–437, May/Jun. 2019.

[4] T. Idriss, H. Idriss, and M. Bayoumi, "A PUF-based paradigm for IoT security," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Reston, VA, USA, Dec. 2016, pp. 700–705.

[5] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Appl. Phys. Rev.*, vol. 6, no. 1, Mar. 2019, Art. no. 011303.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2002, pp. 148–160.

[7] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Vienna, Austria, Sep. 2007, pp. 63–80.

[8] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Evadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *IEEE Symp. VLSI Circuits Dig. Tech. Papers*, Honolulu, HI, USA, Jun. 2004, 176–179.

[9] M. Bhargava, C. Cakir, and K. Mai, "Comparison of bi-stable and delay-based physical unclonable functions from measurements in 65 nm bulk CMOS," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, San Jose, CA, USA, Sep. 2012, pp. 1–4.

[10] G. T. Becker, "On the pitfalls of using Arbiter-PUFs as building blocks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 8, pp. 1295–1307, Aug. 2015.

[11] J. Delvaux and I. Verbauwhede, "Fault injection modeling attacks on 65 nm arbiter and RO sum PUFs via environmental changes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 6, pp. 1701–1713, Jun. 2014.

[12] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Anaheim, CA, USA, Jun. 2010, pp. 94–99.

[13] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.

[14] N. Ahmed and C. D. Jensen, "Definition of entity authentication," in *Proc. 2nd Int. Workshop Secur. Commun. Netw. (IWSCN)*, Karlstad, Sweden, May 2010, pp. 1–7.

[15] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[16] J. H. Ahn, "Design of SRAM based compact physical unclonable function security chip using controllable body bias," M.S. thesis, School Elect. Eng., Chungbuk National Univ., Cheongju, South Korea, 2020.

[17] J.-H. Kim, H.-J. Jo, K.-K. Jo, S.-H. Cho, J.-Y. Chung, and J.-S. Yang, "Reliable and lightweight PUF-based key generation using various index voting architecture," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 352–357.

[18] S. Baek, G.-H. Yu, J. Kim, C. T. Ngo, J. K. Eshraghian, and J.-P. Hong, "A reconfigurable SRAM based CMOS PUF with challenge to response pairs," *IEEE Access*, vol. 9, pp. 79947–79960, 2021.

[19] S. Taneja, V. K. Rajanna, and M. Alioto, "36.1 unified in-memory dynamic TRNG and multi-bit static PUF entropy generation for ubiquitous hardware security," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2021, pp. 498–500.

[20] L. Lu and T. T.-H. Kim, "A programmable 6T SRAM-based PUF with dynamic stability data masking," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2021, pp. 1–3.

[21] J. Lee and Y. Lee, "A current-integrated differential NAND-structured PUF for stable and V/T variation-tolerant low-cost IoT security," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2021, pp. 1–3.

[22] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Berlin, Germany: Springer, Oct. 2010.

[23] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response PUF using 28 nm SRAM 6T bit cell," in *Proc. IEEE Symp. VLSI Circuits*, Kyoto, Japan, Jun. 2017, pp. C270–C271.

[24] S. Stanzione, D. Puntin, and G. Iannaccone, "CMOS silicon physical unclonable functions based on intrinsic process variability," *IEEE J. Solid-State Circuits*, vol. 46, no. 6, pp. 1456–1463, Apr. 2011.

[25] K. Yang, D. Blaauw, and D. Sylvester, "A physical unclonable function with BER <10E-8 for robust chip authentication using oscillator collapse in 40 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Mar. 2015, pp. 254–255.

JAE-WON NAM (Member, IEEE) received the B.S. and M.S. degrees from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2006 and 2008, respectively, and the Ph.D. degree in electrical engineering with the University of Southern California (USC), Los Angeles, CA, USA, in 2019. From 2008 to 2012, he was with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, as a full-time Researcher. Since Fall 2017, he has been a Graduate Intern with the Data Center Group, Intel Corporation, Santa Clara, CA, USA, worked on the next generation high-speed I/O architectures. From July 2019 to July 2020, he was an Analog Engineer at Intel Corporation Ltd., I/O Circuit Technology Team. He is currently an Assistant Professor with the Department of Electronic and Information Engineering, Seoul National University of Science and Technology (SeoulTech). His research interests include designing low-power high-speed high-resolution analog-to-digital data converters and high-speed I/O interface circuits.

He was a recipient of the President Award from the Korea Advanced Institute of Science and Technology IT Convergence Campus (KAIST-ICC), in 2006, and the Outstanding Employee Award from ETRI, in 2009, and a co-recipient of the Silver Prize from the Tenth Korea Intellectual Property Office (KIPO) Circuit Design Contest, in 2009. He was also a recipient of the Ph.D. Fellowship from the Viterbi-USC Graduate School of Engineering, from 2012 to 2014. He received the Best Student Paper (Third Place) Award at IEEE Custom Integrated Circuits Conference (CICC), in 2019.

JU-HYEOK AHN received the B.S. and M.S. degrees in electrical engineering from Chungbuk National University, Cheongju, South Korea, in 2018 and 2020, respectively. He is currently working with LX Semicon (Former Silicon Works), Deajeon, South Korea.

JONG-PHIL HONG (Member, IEEE) received the B.Sc. degree in electronic engineering from Korea Aerospace University, Seoul, South Korea, in 2005, and the M.S. and Ph.D. degrees from the Department of Information and Communications Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2007 and 2010, respectively. In 2010, he joined the Mixed-Signal Circuit Design Team, Samsung Electronics, Giheung, South Korea, as a Senior Engineer. Since 2012, he has been a Professor with the Department of Electrical Engineering, Chungbuk National University, Cheongju, South Korea. His current research interests include the design of lightweight security SoC with physically unclonable function, sub-THz signal source based on CMOS technology, and insulation monitoring device for EV and IT systems.