IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 12, 2021, accepted May 22, 2021, date of publication May 28, 2021, date of current version June 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3084621

A Reconfigurable SRAM Based CMOS PUF With Challenge to Response Pairs

SEUNGBUM BAEK[1], GUK-HYEON YU[1], JAEWOO KIM[1], CHI TRUNG NGO[1], JASON K. ESHRAGHIAN[2,3], (Member, IEEE), AND JONG-PHIL HONG[1], (Member, IEEE)

[1]School of Electrical Engineering, Chungbuk National University, Cheongju 28644, Republic of Korea
[2]Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48105, USA
[3]School of Medicine, The University of Western Australia, Perth, WA 6009, Australia

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

This work was supported in part by the National Research Foundation of Korea (NRF) Grant 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 a reconfigurable SRAM-based physically unclonable function (PUF) topology with multiple challenge-response pairs (CRPs) per cell. The proposed PUF structure enables a very large CRP space by connecting additional pull-up and pull-down paths to each SRAM cell. These alternate pathways to the supply rail and ground are activated by the challenge inputs, which effectively reconfigure the transfer characteristics of each cross-coupled inverter. A newly proposed response instability detector improves bit error rate (BER) performance by discarding unstable response. In addition, the proposed PUF adds indirect challenges by scrambling the responses using a Galois linear feedback shift register (LFSR). The proposed PUF can be applied to a wider range of applications as a CRP PUF because it has multiple CRPs in addition to the small area and fast operating speed, which are the advantages of the conventional SRAM structure. In order to verify the performance of the proposed architecture, a 32×32-bit reconfigurable SRAM PUF array with 32-bit challenge is implemented in a 65 nm CMOS process. Experimental results show a core area of 88.867 μm^2/bit, energy efficiency of 0.082 pJ/bit, and inter-chip Hamming distance (HD) of 48.93% across 40 chips. By applying an unstable bit discard (UBD) scheme, BER is improved from 13.7% to 0.9%. Compared to the state-of-the-art, the proposed PUF is shown to be highly competitive in area, throughput and energy efficiency.

INDEX TERMS Physically unclonable function, random number generator, authentication, Internet of Things.

I. INTRODUCTION

The rapid growth of Internet of Things (IoT) devices in applications such as mobile and wearable computing, autonomous vehicles, and smart grids, has made two-way wireless communication pervade many aspects of daily life. The benefits of increased connectivity come with heightened data vulnerability issues, such as information leakage and loss of administrative access. With malicious manufacturers being propelled by advances in adversarial attacks, there is a critical need to build resilient security systems against physically invasive and non-invasive attacks [1], [2].

Information security technology, such as entity authentication or digital signatures, are inevitably required to build a trustworthy bidirectional network. Kerckhoffs' principle states that a cryptographic system should be secure even if an opponent knows the entire underlying encryption algorithm but does not know the secret key. Therefore, secret random keys are a crucial element for authentication protocols. Secret keys can be generated via a true random number generator (TRNG). The implementation of a TRNG, however, might be too expensive to embed on chips with stringent design constrains.

Silicon PUFs are a promising technology for security in IoT devices [3]. They utilize naturally occurring physical variations in the chip fabrication process so that the same circuit produces different outputs across different chips. It is arguably impossible to create a perfect duplicate [4]–[6]. In many silicon PUFs the secret key is generated only when needed, so it does not need to be stored in memory. The low

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

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

cost, ultra-small and low power advantages of CMOS technology make silicon PUFs suitable as secret key generators in IoT and other lightweight devices.

Silicon PUFs are generally recognized to come in two strengths: weak and strong. A strong PUF has a CRP space that is large enough to prevent an adversary, after having full access to the PUF for a reasonable duration, is unable to predict an unseen response with an advantage better than random guessing. To satisfy this criterion, (i) the CRP space must be large enough such that the attacker cannot fully model it in the time they have access to the PUF, and (ii) the CRPs must be sufficiently independent from each other to avoid the attacker from predicting unseen responses based on prior observed CRPs. Resource-centric views of PUF strength link the CRP space to chip area [7]. A weak PUF has a CRP space that scales linearly with chip area, while a strong PUF has a large CRP space that increases exponentially with the corresponding area. In other words, the CRP scaling factor in a strong PUF should be capable of preventing a malicious attacker from reading out the full CRP space. Weak PUFs are typically advantageous in resource-constrained devices, while a strong PUF is preferable for authentication. Authentication protocols should avoid reusing CRPs to prevent malicious attacks. As the space of CRPs increases, the probability for a CRP pair to reoccur becomes negligibly small. A system with a small CRP space may need to compensate potential reuse which will require additional overhead [8].

A. RELATED WORKS

Demand on SRAM memory for IoT devices has been driven by its lower standby power dissipation and lower access time compared to DRAM and flash memory, even though SRAM is still thought of as a critical block for resource efficiency [9]. Thus, research on building an SRAM PUF as an IoT security primitive is highly active [10]–[18]. Guajardo *et al.* [11] introduced the use of an input address as the challenge, and the power-up state of the selected cell as the response. Initially, it was thought to be a viable way to improve the security of FPGAs using pre-existing IP blocks, but many FPGAs are designed to force SRAM to a known initial state and could not be relied upon as a PUF. Kumar *et al.* [12] improved the SRAM PUF to a butterfly PUF which alleviated initialization issues on FPGA. This led to advances in ASIC-based SRAM PUFs. Notable examples include Maes *et al.* [15], who discovered that SRAM PUFs and ring oscillator PUFs are able to achieve the highest degree of uniqueness and reliability among such PUFs. Mathew *et al.* [16] demonstrated the high tolerance of SRAM PUFs to process-voltage-temperature (PVT) variation. However, memory-based PUFs are generally limited by their CRP capacity [19]–[21]. Thus far, SRAM and latch-based PUFs have only been implemented as weak PUFs, where each cell is capable of storing only one binary digit. There is a lack of CRPs which depend on the cells rather than the addressing mechanism. Holcomb *et al.* [19] recently demonstrated the use of SRAM in building a native strong PUF by enabling multiple wordlines concurrently at the evaluation stage. Jeloka *et al.* [20] used sequencing to enable multiple wordlines in a given order to increase the number of possible CRPs. But in all cases, wordlines and addressing have been used to generate challenge inputs on a weak SRAM PUF. It may therefore be inappropriate to classify these as true strong PUFs. The proposed design circumvents this issue by using SRAM cells that may independently generate multiple CRPs. This paper presents the first SRAM cell PUF with multiple CRPs.

For a silicon PUF to be utilized in cryptography, reliability of the response on the same PUF chip must be ensured. The reliability is a measure of consistency of the response bits for an identical challenge input across varying environmental conditions such as temperature and voltage. For the same challenge input, it is possible to obtain a varying response bit due to environmental conditions and variations, which reduces the reliability of the PUF. Post-stabilization is often necessary to alleviate this issue [13], [16], [22]–[26]. Error correction codes (ECC), such as the Bose-Chaudhuri-Hocquenghem (BCH) codes, are often required to achieve stability, but ECC is computationally intensive, and the power and area overhead of the ECC logic can be several times larger than the overhead of the PUF itself. It is also susceptible to serious entropy leakage [22], [23]. Mathew *et al.* [16] introduced a temporal majority voting (TMV) circuit to stabilize unstable bits. TMV averages multiple samples of a bitstream within a voting window and has shown to improve error by up to 8%. However, more samples must be taken when the statistical bias of an SRAM PUF cell is weak which increases the cost of TMV. They used burn-in hardening to decrease bit errors which requires high-stress conditions. This additional manufacturing step will add cost in terms of the necessary equipment needed to elevate the voltage and temperature (e.g., a temperature chamber). Yang *et al.* [24] introduced a dynamic thresholding technique based on oscillation collapse, but requires additional overhead to track the number of oscillation cycles for collapse, and is only applicable to oscillator structure. Hiller *et al.* [26] introduced a new error correction scheme based on differential sequence coding which generates a 128-bit key with 974 PUF bits and 1,108 helper bits for an input bit error of 15%, however, it may require massive clock cycles (∼29K) and RAM size (∼10K-bit). There is a need for compact and cost-efficient post-processing methods with fewer testing cycles and redundancy.

B. CONTRIBUTIONS

Extending from the previously presented paper [21], this work introduces a new SRAM-based CRP PUF and its operating principle in order to generate multiple CRPs from a single cell. This is achieved by designing a reconfigurable SRAM cell, the characteristic of which depends upon the challenge input. A newly designed compact response instability detector which improves the reliability of responses, and an output scrambler for optional permutation of the produced response are also presented. The proposed architecture demonstrates that it has a large CRP space while maintaining the

advantages of a fast operating speed (on the order of GHz) and low power dissipation (on the order of pJ/bit) of weak PUF. The proposed PUF chip is fabricated in a 65 nm process and evaluated across 40 chips with a uniqueness index of 1.07% away from the optimal point, and a BER of 0.9% under the worst-case measured condition, within an area occupation of 88.867 μm^2/bit and energy efficiency of 0.082 pJ/bit.

C. PAPER ORGANIZATION

The paper is organized as follows: section II introduces the topology of the reconfigurable SRAM PUF, describes its operating principle and provides a calculation for the total CRP space. Section III explains implementation of the entire PUF system in a 1024-bit array, the instability detector and the output scrambler circuits. The work is experimentally validated in section IV by measuring the uniqueness, randomness, and stability, along with a comparison against other comparable state-of-the-art PUFs. The paper is concluded in section V.

II. OPERATING PRINCIPLE OF PROPOSED RECONFIGURABLE SRAM PUF

A. OPERATING PRINCIPLE

Fig. 1 shows a unit cell structure and the voltage transfer characteristics under both ideal and practical conditions in a conventional SRAM PUF. As shown in Fig. 1 (a), the unit cell of the SRAM PUF consists of a cross-coupled pair of inverters with complementary outputs (V_{OUT} and V_{OUT_B}) which are a function of physical mismatch due to process variation. Under idealized conditions where both inverters are perfectly identical, and in the absence of any noise, the metastable point is located at the intersection of the x- and y-axes, indicated by

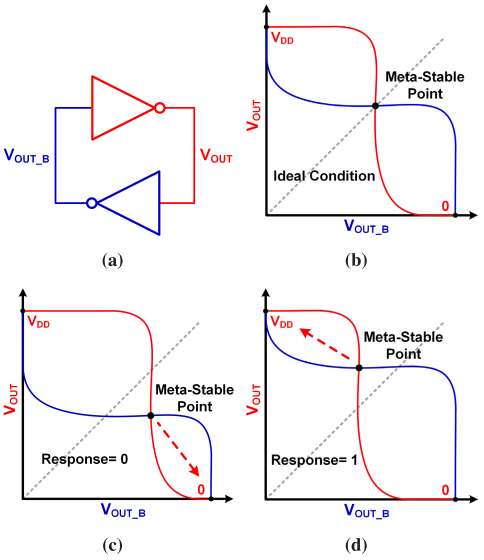


FIGURE 1. Basic structure and voltage transfer characteristics of conventional SRAM PUF. (a) Block diagram of the SRAM PUF, (b) Transfer characteristics under ideal conditions, (c) Transfer curve when response = 0, (d) Transfer curve when response = 1.

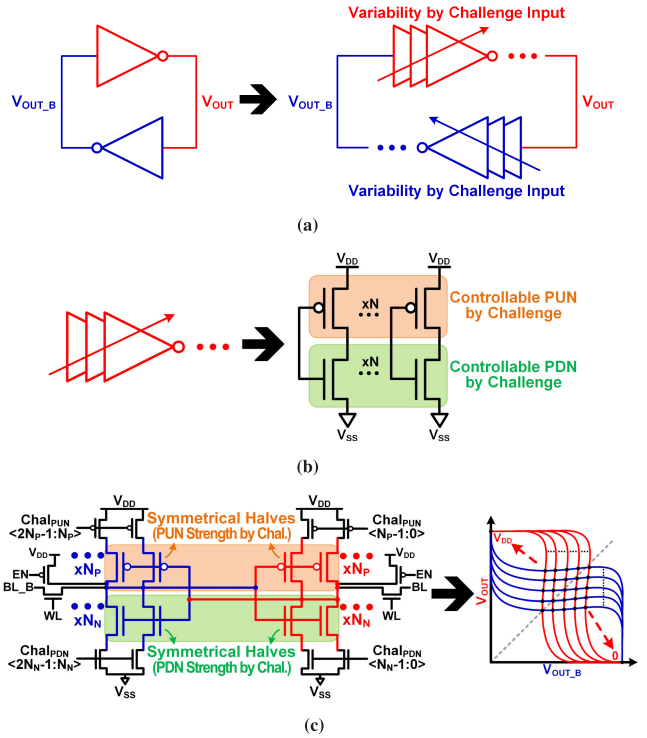


FIGURE 2. Conceptual structure of the proposed reconfigurable SRAM PUF unit (a) enabling variability for cross-coupled inverters by challenge, (b) into pull-up network (PUN) and pull-down network (PDN) separately. (c) Unit cell schematic of the proposed SRAM PUF allowing challenge-response pairs using controllable pull-up/down strength.

the dashed line in Fig. 1 (b). In practice, the situation will be more like in Fig. 1 (c) and (d). The pull-up and pull-down networks of cross-coupled inverters drive the outputs to V_{DD} and ground, respectively, due to a slight offset caused by process mismatch. As a result, even if the SRAM schematic in Fig. 1 (a) is replicated, the output values are random and physically unclonable due to unpredictable process variation. The conventional SRAM cell can generate a response even in absence of a challenge input. Upon initialization, the metastable point diverges from the intersection boundary and the response of the SRAM PUF cell will settle faster, and become more robust against noise and other external variation. This is useful in ID generation. Conversely, for small mismatch, the response is randomly generated by stochastic noise present in the circuit.

A schematic of the proposed reconfigurable SRAM PUF with multiple CRPs is shown in Fig. 2. It consists of multiple cross-coupled inverters (Fig. 2 (a) and Fig. 2 (b)) with challenge inputs applied to cascode pull-up and pull-down transistors. By varying the multi-bit challenge, the relative strength of the pull-up network (PUN) and pull-down network (PDN) can be reconfigured which randomly shifts the point of metastability (Fig. 2 (c)). This mechanism converts the weak PUF to a CRP PUF by enabling multiple CRPs from a single SRAM PUF unit. For each side of the inverters in Fig. 2 (c), there must be corresponding cross-coupled

inverters with an identical strength. This ensures the response is a function of physical mismatch rather than a deterministically applied voltage. The challenge input is connected to gate terminals of the cascode transistors. The gate impedance is theoretically infinite thus the PUF responses are hardly affected by interconnections between the challenge inputs and SRAM PUFs.

A simple example where the number of NMOS and PMOS are $N_N = N_P = 2$ for a given challenge input is shown in Fig. 3. The challenge from C_0 to C_7 reconfigures the SRAM cell properties, generating new mismatch combinations as a result of process variation. The process variation of each inverter accumulates with a compound effect on the PDN/PUN strength, enabling a faster settling time to a stable state. In Fig. 3 (b), if only one PMOS transistor with $C_0 = 0$ and $C_1 = 1$ is turned on, the number of different configurations in the cell is two: $C_2 = 1$ and $C_3 = 0$ or $C_2 = 0$ and $C_3 = 1$, which is the same number of transistors that are turned on to have the identical strength for each side of the inverters. Similarly, for $C_0 = 1$ and $C_1 = 0$, the proposed PUF allows two combinations of challenges input. When both transistors are on, there is only one case in which all PMOS transistors are on. Therefore, the response from the PMOS transistor challenges with $N_P = 2$ in the proposed reconfigurable SRAM PUF can have 5 combinations. Eventually, the proposed SRAM PUF with an 8-bit challenge input ($N_N = N_P = 2$) provides 25 (5×5) CRPs, which is the product of the NMOS and PMOS combinations.

B. CRP SPACE CALCULATION

Equations (1)-(4), as shown at the bottom of the page, represent the general expression for the number of responses from the PDN of the NMOS transistors, total number of challenge inputs, transistors, and CRPs, respectively, when N_N in the proposed SRAM PUF is n. In Eq. (2), the total bit-width of a challenge input is $4\times n$ (i.e., $n\times 2\times 2$). $4\times n$ can be decomposed to $2\times(2\times n)$, where the first factor of 2 represents the two sides of the network (PUN and PDN), and the second factor represents the two inverters in a cross-coupled configuration. From Eq. (3), the total number of transistors required for a cell is $8\times n+4$ consisting of $8\times n$ for PUN and PDN, and 4 for coupled transistors. The total number of CRPs in Eq. (4) is multiplied by both of the responses of the PUN and PDN, and is calculated to be the square of Eq. (1). For instance, if the number of bits of the challenge input are 32, the total number of CRPs of the proposed SRAM PUF is 1.6×10^8, as shown in Eq. (5), as shown at the bottom of the page.

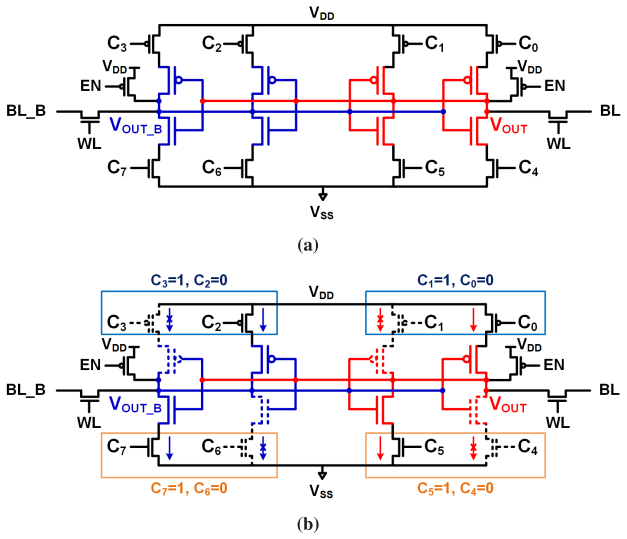


FIGURE 3. (a) Unit cell schematic of the proposed reconfigurable SRAM PUF when $N_P = N_N = 2$, (b) the pull-up/down path as determined by challenge input (C_X).

$$N_N \text{ (or } N_P) = \text{No. of NMOS (or PMOS) making up the inverter on each side}$$
$$N_N \text{ (or } N_P) = 1,\ \text{No. of CRPs} = 1$$
$$N_N \text{ (or } N_P) = 2,\ \text{No. of CRPs} = 2 \times 2 + 1 = 5$$
$$N_N \text{ (or } N_P) = n \text{ (or } p),\ \text{No. of CRPs} = \left({}^nC_1\right)^2 + \left({}^nC_2\right)^2 + \ldots + \left({}^nC_{n-1}\right)^2 + \left({}^nC_n\right)^2 = \sum_{k=1}^{n}\left({}^nC_k\right)^2 \quad (1)$$
$$\text{Bitwidth of challenge in a cell} = (2\times N_N + 2\times N_P) \text{ bits}$$
$$\text{Assuming } N_N = N_P,\ \text{Bitwidth of challenge} = (4\times N_N) \text{ bits} \quad (2)$$
$$\text{No. of transistors in a cell} = 8\times N_N + 4 \quad (3)$$
$$\text{Total No. of CRPs} = \left(\sum_{k=1}^{N_N}\left({}^{N_N}C_k\right)^2\right)^2 \quad (4)$$
$$\text{Actual value for } N_N = N_P = 8,\ \text{Bitwidth of challenge} = 32 \text{ bits}$$
$$\text{Total No. of CRPs} = \left(\sum_{k=1}^{8}\left({}^8C_k\right)^2\right)^2 \approx 1.6 \times 10^8 \quad (5)$$

III. IMPLEMENTATION OF OVERALL PROPOSED PUF ARCHITECTURE

A. IMPLEMENTATION OF OVERALL RECONFIGURABLE SRAM PUF SYSTEM

Fig. 4 illustrates the system architecture and its timing diagram of the proposed PUF chip, where the reconfigurable SRAM PUF cell comprises of 32-bit challenges and $N_N = N_P = 8$, depicted in Fig. 2 (c). The PUF chip consists of a 1024-bit (32×32) array which includes a response instability detector, a scrambler to optionally permutate the response to improve complexity, and a controller to switch between 3 operating modes: reset, evaluation, and scramble. To generate CRPs, all blocks are initialized by synchronously resetting all signals except for the challenge inputs to either '1' or '0' during reset mode. This is followed by an array evaluation stage that generates 32-bit output from the challenge inputs. A single CRP generation consumes a minimum two clock cycles for PUF reset and evaluation, shown in Fig. 4 (b). The challenge can be generated through an external input signal using a serial to parallel interface circuit. The other way to generate challenge input can be designed for random bitstream input meeting the challenge constraint by using pseudorandom number generator (PRNG). The circuit may include a shift register and a binary counter. Once a random bitstream is obtained through PRNG, challenge strength of each side is compared by the counter and a new random bit from PRNG is injected using the shift register for a challenge part having weaker strength. It can repeat until the circuit detects each side of challenge has the same strength and the configured challenge is transferred to the PUF circuit. The responses are screened by a response instability detector. For the identical challenge input, the same chip should ideally reproduce the same response, while a random response must be generated across different chips during evaluation mode. The response instability detector detects occurrences of bit-flipping under identical challenges. Bit-flipped cells have a high probability of generating an unstable response for a given challenge, and so the addresses of susceptible cells are passed to the Stability signal. These cell responses are discarded during evaluation. In scramble mode, the scrambler optionally converts the input string of the 32-bit response (PUF_OUT) into an XOR-ed output string of the same length. In the proposed structure, the scrambler implemented with Galois-configuration LFSR randomizes or bypasses the response according to the S_REF signal. The S_REF signal also determines the number of permutations of the response to be performed.

Fig. 5 (a) shows a transistor-level schematic of the implemented SRAM PUF cell unit when $N_P = N_N = 8$ in Fig. 2 (c), consisting of 16 inverters and a 32-bit challenge input. From Eq. (5), when $N_P = N_N = 8$, the total capacity of CRPs is 1.6×10^8. The associated timing diagram to read-out the response from the bitline (BL) is shown in Fig. 5 (b). The cascode transistors are multi-purposed to not only provide the challenge signal to the inverters, but to also initialize the cell during the reset phase. Initialization is performed by entering

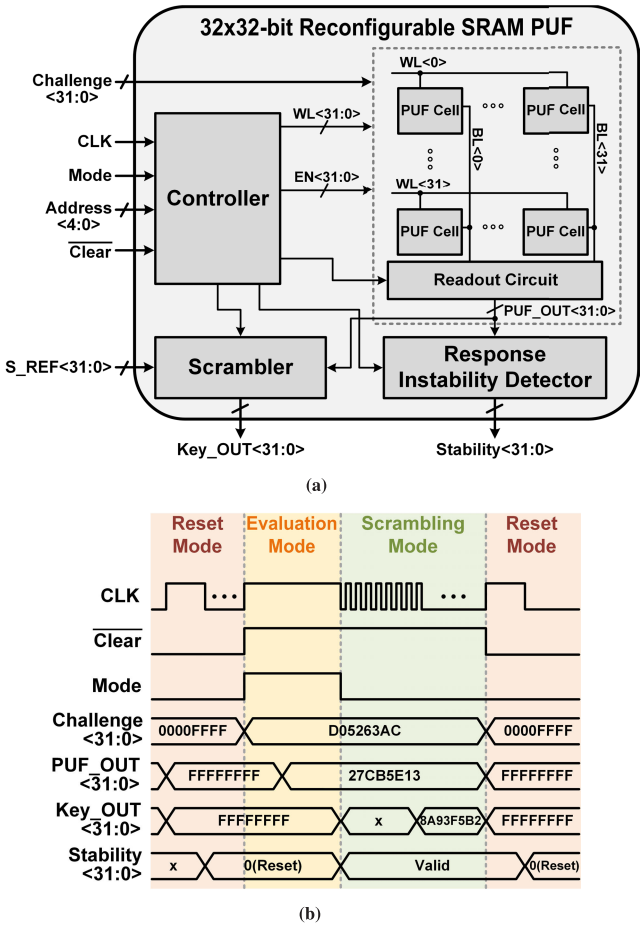


FIGURE 4. (a) Top-level architecture and (b) waveforms of the proposed reconfigurable SRAM PUF chip.

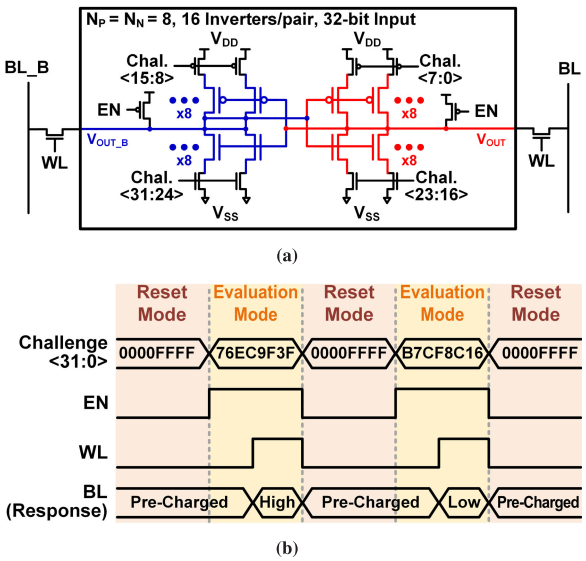


FIGURE 5. (a) Unit cell architecture of the proposed reconfigurable SRAM PUF when $N_P = N_N = 8$, and (b) its operational timing diagram.

a challenge that turns off the cascode transistor to block V_{DD} and V_{SS} from being passed to the output nodes. The two output nodes are safely pre-charged to '1' with an active-low signal applied to EN. The bitline can also be pre-charged in the same manner. When the pre-charge phase is completed, the evaluation phase commences by applying the challenge bits which drives the SRAM unit to its metastable point. The positive feedback from the cross-coupled inverter network will then stabilize the output which are transferred to BL and BL_B through WL.

In perspective of layout technique, to minimize layout effects other than physical variations, parasitic components should be carefully considered to make the left and right side of the PUF core balanced by drawing the layout in a symmetric form including metal, via and contact. The connection between SRAM and transistors making up the challenge input should also be drawn symmetrically. While the proposed SRAM PUF pursues low systematic components, its layout is drawn with the minimum size devices for large random variations [13]. Furthermore, it includes dummy gates for across-chip linewidth variation (ACLV) improvement during device fabrication [27], which is a contributor for the systematic variation through layout patterns.

B. RESPONSE STABILITY IMPROVEMENT

To prevent intrinsic or environmentally induced failures, many silicon PUFs use integrated post-processing techniques [16], [24]–[26]. The proposed PUF includes a response instability detector to perform this task. In silicon PUFs, process mismatch determines the stability and settling time of the response. In general, most SRAM PUF cells converge to digitally distinguishable states from initialization in hundreds of picoseconds. However, cells with small physical mismatch coefficients have a higher probability of unexpected bit-flipping due to sensitivity to environmental conditions (e.g., voltage supply fluctuations and temperature variation).

The response instability detector in the proposed PUF evaluates the proportion of bit-flipping by comparing successively generated responses under identical challenge conditions. The first response generated is used as the reference, and is stored in a register of the instability detection circuit. Under identical operating conditions, a second response is generated by the PUF circuit and compared with the reference response. This comparison is repeated for 5K operations per challenge. A CRP is discarded if any of the 5K responses differ. Fig. 6 introduces the architecture of the proposed compact response instability detector which only requires 4 basic logic gates to make comparisons between repeated responses. The instability evaluation method is designed using 2 registers, an XOR-based comparator, and a buffer (delay). The first stage register stores the reference response at the rising edge of the Ready_Ref signal. Then the XOR-based comparator determines whether bit-flipping has occurred from the successive input, and the result is sampled by the following register. The instability detector obviously consumes

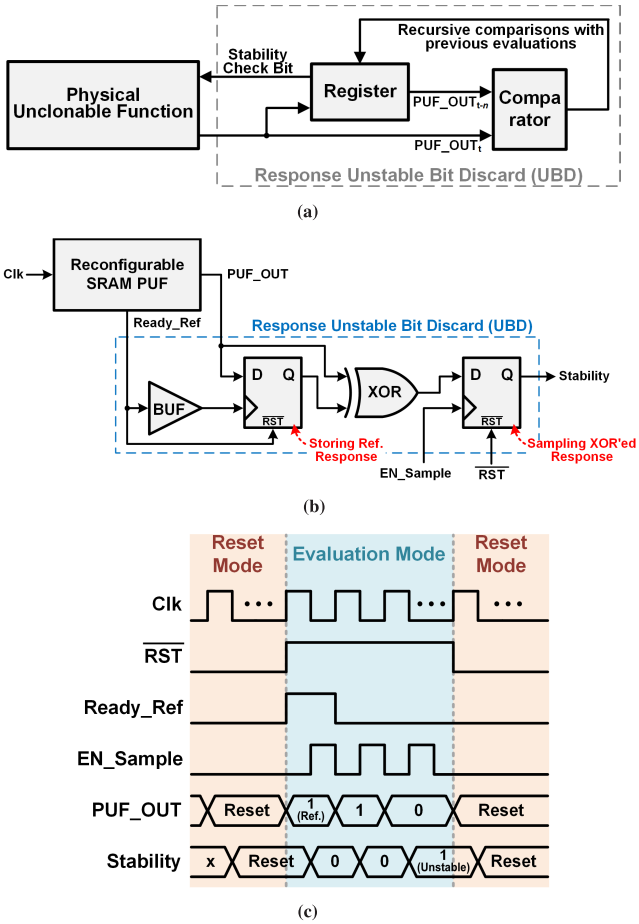


FIGURE 6. (a) Overview of the proposed response instability detector based on multiple comparison, (b) schematic and (c) its operational waveform.

additional clock cycles than typical PUF operation. At least a PUF operation is required for generating a reference response. The EN_Sample signal which samples the comparison result per PUF operation is made by the controller block to run half a cycle behind the clock. Thus, two clock cycles at least are required for a comparison, and the clock cycles are linearly increased for further multiple comparisons.

The proposed post-processing algorithm may also contribute to building a trustworthy authentication protocol. A general authentication protocol using CRPs may include two stages: enrollment and authentication. In the enrollment stage, unstable CRPs are filtered through the instability detection circuit, and a robust stable CRPs are stored and enrolled in the server and PUF chip as secret keys. Thus, 8.48×10^7 stable pairs per chip after discarding 47% (i.e., unstable bit rate at worst case) from the total 1.6×10^8 pairs can be stored on the server. During the authentication stage, verification is performed between the server and the PUF chip using the enrolled CRPs. This type of post-processing is successfully implemented with the SRAM array and its effect on reliability improvement is analyzed in the following section.

C. RESPONSE SCRAMBLER DESIGN

The input (or output) scrambler provides the option to permutate challenge (or response) bits, adding an additional layer of complexity [13], [28], [29]. In general, the PUF core should operate as the primary source of entropy, while the contribution of the scrambler is limited from a security perspective. Pseudorandom number generators or encryption algorithms can be employed as a scrambler, thus the proposed PUF adopts Galois-configuration LFSR (G-LFSR) as the optional response scrambler because of its simple and fast bitwise encryption. Moreover, the ability to bypass without any bit-shuffling is included within the scrambler structure to benchmark the native PUF performance. Fig. 7 elucidates how the scrambler operates in conjunction with the PUF, thus enabling additional indirect challenges by the S_REF signal which determines the number of permutations to perform within the maximum possible states. The G-LFSR in the proposed PUF has been modified by including a 32-bit counter to perform clock-gating according to the S_REF signal. Moreover, the implemented LFSR has 4 taps: 32, 30, 26, and 25, the positions of which are known to achieve the maximum cycle size in the 32-bit LFSR [30]. When the PUF generates the output and the scrambler is activated, the produced response is transferred to the scrambler to be utilized as a seed. The received response is then scrambled using as many cycles as the value of S_REF, and the same-length output is shown at the output node. Furthermore, if the value of the S_REF signal is set to zero, then the scrambler would not permutate the input bits and instead, transfer the input directly to the output node. However, the scrambler is susceptible to unreliable CRPs generated by a PUF. This is because if a produced response is not identical to the previously generated response, then the scrambled response will also differ.

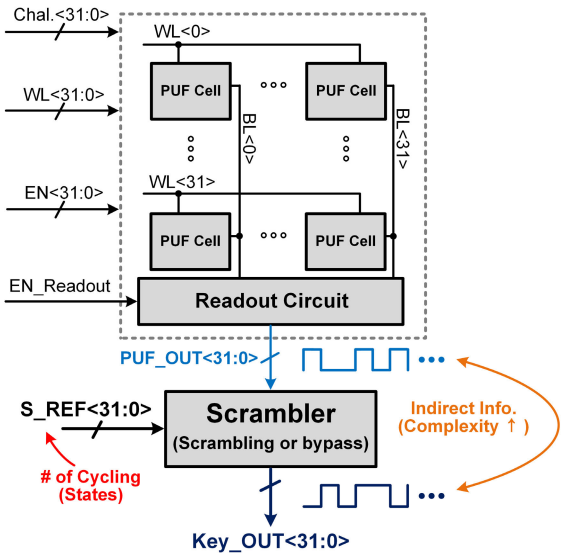


FIGURE 7. Scrambler utilization with the proposed SRAM PUF for improving complexity.

Thus, when an embedded instability detector decides a CRP to be unreliable, it would be discarded thus bypassing the scrambler.

For a scrambler implementation with robust algorithms if enlarged area constraint is allowed, ISO/IEC 29192 standard recommends several cryptographic algorithms such as Enocoro and Trivium [31]. Moreover, the eSTREAM project portfolio contains couples of stream ciphers such as Salsa20 and Grain which may be suitable for a scrambler implementation [32].

IV. MEASUREMENT RESULTS

A. EVALUATION SETUP

The prototype of the proposed reconfigurable SRAM PUF with 32-bit challenges and 1024-bit array is fabricated in a 65 nm CMOS process. Fig. 8 shows a die micrograph of the proposed PUF with the instability detector and output scrambler, which occupy an area of 0.1121 mm^2. The measurement setup to verify the performance of the PUF is shown in Fig. 9, which uses a chip evaluation board with a Xilinx FPGA, and a memory scan chain for massively iterative testing under varying operation conditions. The system clock frequency is tested up to 100 MHz under varying operating conditions. Uniqueness, randomness (CRP unpredictability), stability (CRP reproducibility) and chip performance for a CRP PUF are measured using 40 samples of the fabricated PUF, and are compared against state-of-the-art PUF structures.

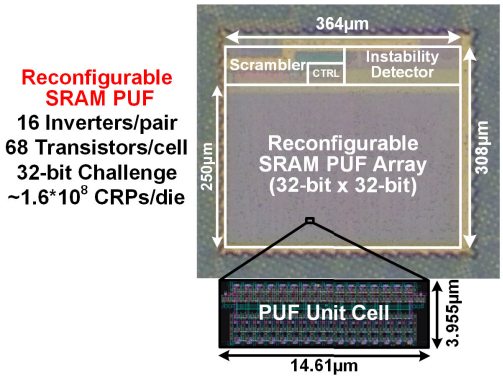


FIGURE 8. Die micrograph of the reconfigurable SRAM PUF.

B. CRP UNPREDICTABILITY ANALYSIS

The inter-PUF Hamming distance is used to estimate the average distinguishability, or uniqueness, by applying identical challenges across different chips and measuring the difference between the bitstream responses [4]. Conversely, the intra-PUF Hamming distance indicates the average noise of responses for identical challenges on a single PUF instantiation. Fig. 10 displays a histogram of the measured inter-PUF Hamming distance without the unstable bit discard method and the output scrambler, which is shown to be a Gaussian distribution with a mean of 48.93% and a standard deviation

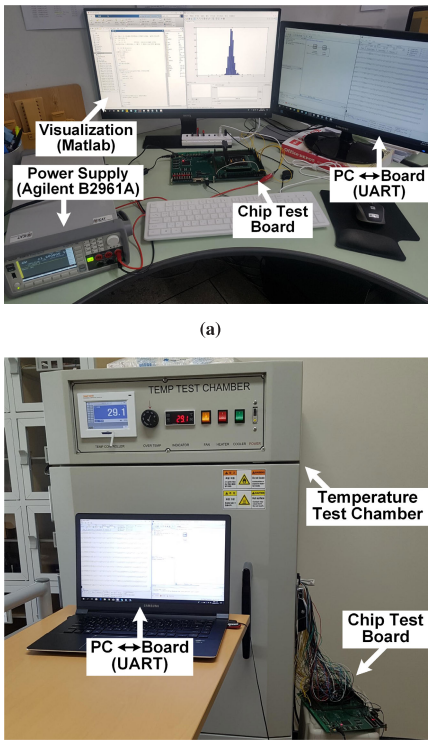


FIGURE 9. (a) Overall chip measurement environment and (b) chip operation under temperature variation.

of 1.9% over 120K bits responses evaluated across 40 chips. The reconfigurable SRAM PUF shows competitive uniqueness metrics as its measured value is very close to the golden standard of 50%.

The potential as a random number generator is evaluated by various metrics. Fig. 11 illustrates the Hamming weight distribution under two conditions to analyze binary proportions between the measured responses without any post-processing (i.e., scrambling) [33]: (a) the distribution across 75 different challenges within a single instantiation of the PUF, and (b) the distribution for a single challenge across 40 chips. This metric indicates the likelihood of undesirable bit-aliasing which may generate closely correlated (or biased) bitstreams across different chips. The analysis shows a mean of 50.76% ($\sigma = 6.28\%$) and 51.21% ($\sigma = 2.45\%$), which shows close to ideal uniformity and a low risk of bit-aliasing.

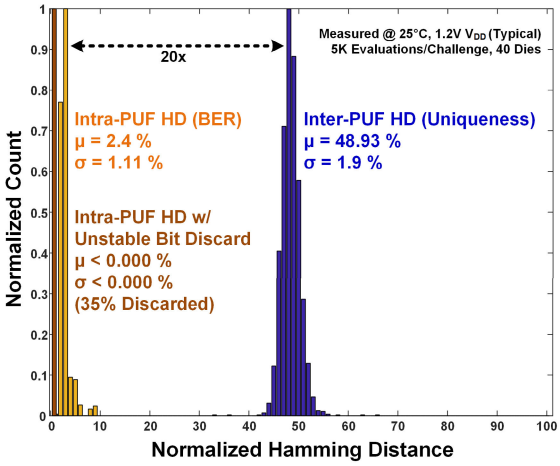


FIGURE 10. Measured inter/intra-PUF Hamming distance distribution.

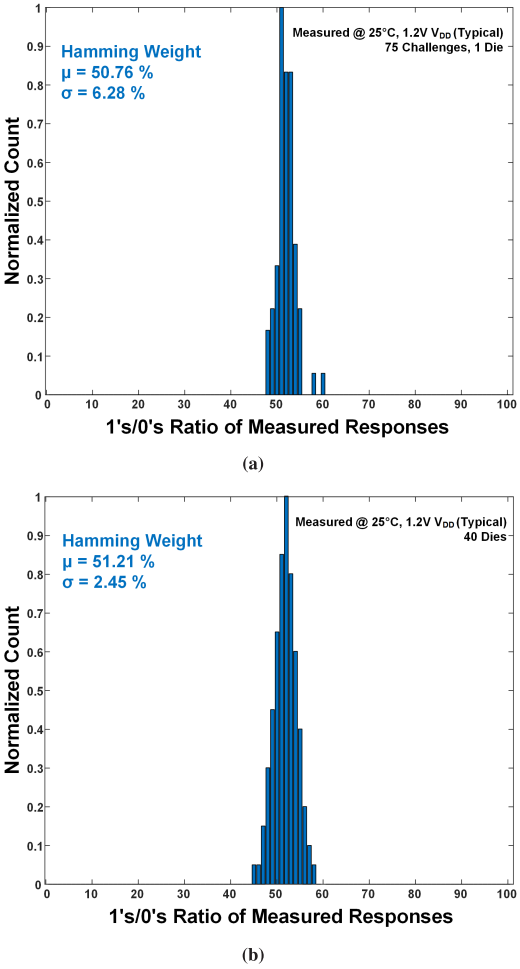


FIGURE 11. Measured Hamming weight distribution. (a) Distribution across 75 challenges within a die, (b) Distribution across a challenge between 40 chips.

The auto-correlation of responses is measured to show repeated bitstream patterns for any given lag. A lag n autocorrelation estimates the spatial correlation between responses that are n bits apart [14]. Systematic variations in SRAM PUFs will be susceptible to model-building attacks due to impact by neighboring cells, layout or gradients. Therefore, influence from neighboring cells should also be considered to ensure high entropy responses [14], [34]. Fig. 12 quantifies the auto-correlation factor (ACF) using the lag between 120K bits native responses, extracted from the entire core area. The lag represents bit intervals among the extracted responses. The measured ACF waveform shows negligible correlation at any bit interval with a mean of 6.804×10^{-6} and a standard deviation of 3.3×10^{-3}, falling within 95%

confidence bounds. Therefore, this confirms effective rejection of layout-dependent variations.

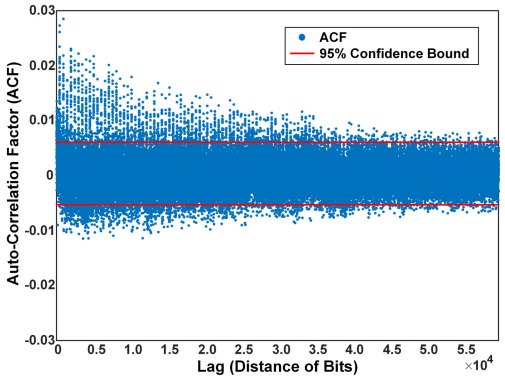


FIGURE 12. Measured auto-correlation waveform showing negligible spatial correlation within 95% bounds.

C. MODELING ATTACK ANALYSIS

Resilience to model-building attacks is measured to further analyze CRP unpredictability. While the PUF exploits naturally occurring physical variations, an attacker may attempt to build a software model rather than physical replication after obtaining access to a sufficiently large sample of CRPs. Thus, CRPs need to be sufficiently independent from each other. At the very least, unseen CRPs need to be unpredictable enough to prevent false authentication. Digital PUFs based on competing symmetric circuits (such as arbiters or ring oscillators) have conditional dependencies between CRPs, as different challenge combinations may reuse the same transistors and/or pathways [4]. A PUF with a cascade structure such as nonlinear current PUF might increase machine learning attack resilience, however, it may suffer from hardware overhead (e.g., large area occupation and slow key generation speed) [35], [36]. This lack of independence between CRPs can be modeled using machine learning techniques [37]–[41]. Becker [37] proposed a machine learning attack using a divide-and-conquer approach for attacking XOR PUFs. Recently, Shi *et al.* [38] introduced two approximation attacks with the perspective of logical and global approximation using artificial neural networks that can build an accurate model particularly for variants of multiplexer and XOR arbiter PUFs. The work in [40] described that bias and correlation exist in memory-based PUFs thus may be utilized for response prediction.

To test how resilient our proposed PUF is to models built using machine learning, we train a support vector machine (SVM) on a randomized training set of CRPs (of varying dataset size), and examine how well it predicts the response of a challenge input from the unseen test set [42]. This is implemented using the open-source library LIBSVM [42]. We performed 5-fold cross-validation and a best kernel parameter search, which determined the radial basis function (RBF) kernel outperformed all other tested kernels. A variety of machine learning attacks were applied (e.g., regression, tree-based methods, CMA-ES), each performed with a hyperparameter and/or kernel sweep where relevant, and the strongest attack of these proved to be a support vector machine using a RBF kernel [37].

Fig. 13 illustrates the prediction error as a function of the size of the training set with both native and scrambled CRPs. Responses are extracted from a single cell in the same location across 40 chips to ensure fair testing conditions. Moreover, the control input (S_REF) of the LFSR was set to a fixed value. The prediction error when 10^4 training samples are used shows 0.166 on natively generated CRPs, and 0.239 for scrambled CRPs. The ideal error for prediction is 0.5, which is equivalent to the probability using a random guess. We expect the prediction error of the scrambled topology shows better performance than that of the native case because of the multi-dimensional nature of the XOR operation of the G-LFSR for scrambler. However, the implemented LFSR structure should be assumed to be open to the public thus, the prediction error through the ML algorithm should be considered mainly with native PUF responses while the LFSR performs the post-XOR subordinately. Compared to a conventional arbiter PUF [41], the SRAM PUF requires ten-fold more CRPs to be trained to achieve a prediction error of 0.1. Moreover 10^3 CRPs can break the arbiter PUF with an error of less than 0.1 while the SRAM PUF model demonstrates errors of 0.191 and 0.256 which are twice as high for the native and the scrambled CRPs, respectively.

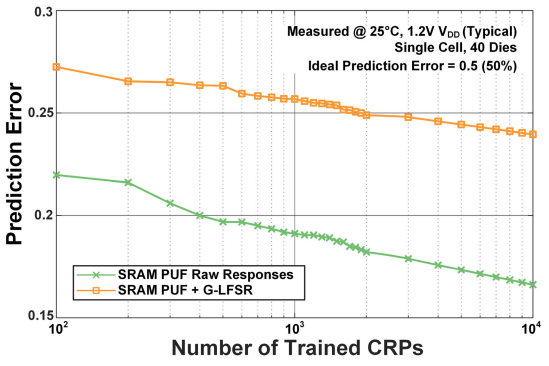


FIGURE 13. Measured prediction error through training CRPs on machine learning algorithm.

D. CRP RELIABILITY ANALYSIS

For a given challenge input, consistency of responses is a crucial metric for a PUF to be usable as a secret key generator for authentication. The BER for a PUF instantiation can be measured as a function of the intra-Hamming distance of a PUF response under identical challenge inputs with different operating conditions. Fig. 10 illustrates the distributions of intra- and inter-Hamming distance under identical operating conditions. 5,000 iterative evaluations over 40 chips are used to measure stability. The intra-Hamming distance is classified under two cases: (i) the distance from the native PUF

response, and (ii) the distance after post-processing using the unstable bit discard method. Both cases do not consider usage of the output scrambler. As shown in Fig. 10, the measured intra-Hamming distances from native and post-processing have a mean of 2.4% ($\sigma = 1.11\%$) and 0.000% ($\sigma = 0.000\%$), respectively. The BER in both cases shows that the proposed reconfigurable SRAM PUF produces stable random bits with an acceptable distribution. Fig. 14 (a) displays the native BER under different combinations of supply voltage from 1.0 V to 1.4 V with a 0.2 V step, and operating temperature from 0°C to 75°C in 25°C steps. In practice, all bits that are unstable at either extreme must be discarded. The lowest BER of 2.4% occurs for 1.2 V and 25°C. Post-stabilized BER under the measured different combinations of operating conditions are explained in Fig. 14 (b). The BER is less than 1% over the entire measured range of supply voltages and temperatures.

The proportion of discarded CRPs for satisfying a given BER requirement under corner cases must also be considered, since over-discarding CRPs without a proper bound can significantly reduce the CRP capacity of a chip. Fig. 14 (c) quantifies this issue by showing how worst-case corners have a smaller number of usable CRPs based on the instability detector. Under typical operating conditions, discarding all bits determined to be unstable (i.e., 35% of all bits) reduced the post-processed BER to 0%. This threshold is extremely strict, and for many practical applications may be relaxed. For instance, a stringent threshold would be used where BER is critical, and a relaxed threshold may be used where the CRP capacity is critical.

E. AUTHENTICATION FEASIBILITY

For feasibility analysis as a secret key source for practical identification, a false acceptance and rejection rate (FAR and FRR) are computed. The FAR and FRR metrics estimate the ability for true identification without acceptance and rejection mistakenly due to insufficient security and robustness of a PUF [43]. An authentication threshold adjusts the trade-off between the FAR and FRR, so the equal error rate (EER) indicates the intersecting point of the two measures. The FAR and FRR for the proposed SRAM PUF, along with other approaches in Table 1 under the fair identification threshold condition, is shown in Fig. 15. The FAR and FRR for the proposed PUF is relatively close to the analog PUF [36] while it is better than the SRAM PUF [20] and the arbiter PUF [44], within an acceptable range among the state-of-the-art. Depending upon authentication requirements, either a more secure or more robust authentication process can be developed.

F. ENERGY CONSUMPTION

Energy consumption is an important indicator for employing a PUF in lightweight devices. Fig. 16 describes the energy consumption per a single response bit generation as a function of the clock frequency. The energy is considered without the post-processing methods for PUF energy comparison fairly. It shows the inverse proportional relationship to the clock

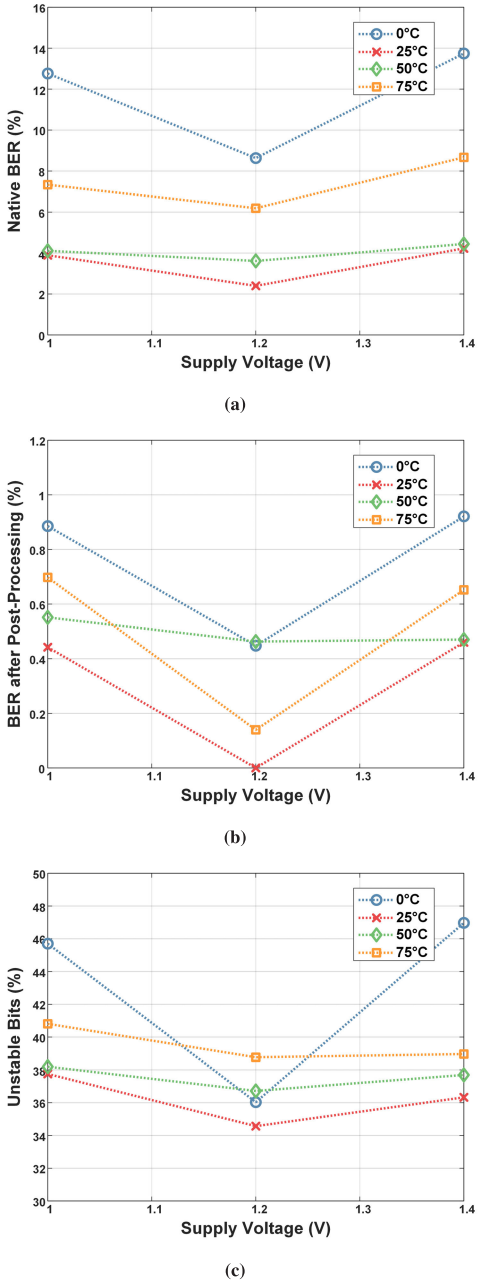


FIGURE 14. (a) Bit error rate without post-processing method, (b) stabilized bit error rate using the unstable bit discard method and (c) discarded CRPs analysis under operating environment changes.

frequency and the most efficient consumption of 0.082 pJ/bit at a maximum measured frequency of 100 MHz. SRAM-based fast response generation without a need of multi-stage operation compared to the conventional CRP generating PUF such as RO, arbiter and addressing based SRAM PUF contributes to achieving the low energy consumption [20]. Modern CMOS technology e.g., 28 nm process may further improve the efficiency as the typical supply voltage decreases.

G. PERFORMANCE SUMMARY AND COMPARISON

Table 1 describes and compares several significant performance metrics of similar competitive PUF instantiations.

TABLE 1. Performance Comparison Results with State-of-the-Art.

		ISSCC'15 [24]	VLSI'17 [20]	Access'19 [44]	TCAS-I'20 [36]	**This Work**
CMOS Technology		40 nm CMOS	28 nm FDSOI	65 nm CMOS	130 nm CMOS	65 nm CMOS
PUF Topology		Delay(RO)	Bi-Stable(SRAM)	Delay(Arbiter)	Analog	Bi-Stable(SRAM)
Bit-Width of Challenge [bit]		96	256[c]	64	65	32
Output Length [bit]		1	64	1	1	1024
Number of CRPs		5.5×10^{28}	1.17×10^{11}	1.8×10^{19}	3.7×10^{19}	$\mathbf{1.6 \times 10^{8}}$[d]
Measured Operating Conditions	Temp. [°C]	$-25 \sim 125$	$0 \sim 80$	$-40 \sim 150$	$-20 \sim 80$	$0 \sim 75$
	V_{DD} [V]	$0.7 \sim 1.2$	$0.5 \sim 0.9$	$1.08 \sim 1.32$	$1.08 \sim 1.32$	$1.0 \sim 1.4$
Worst Case BER [%]	Native	9	12	10.46	9	13.7
	per 10°C (Norm.)	0.6	1.5	0.55	0.9	1.83
	per 0.1V (Norm.)	1.8	3	4.36	3.75	3.43
	After Stabilizing	0 (34% Discarded)	-	-	0.4 (42% Discarded)	**0.9 (47% Discarded)**
Inter-PUF HD		0.5007	0.483	0.468	0.499	**0.4893**
ML Prediction Error	10^4 CRPs Trained	-	0.106	-	0.4	**0.166 (Native) 0.239 (Scrambled)**
Core Area	Area [μm^2/bit]	845	0.7605	3838	6240	**88.867**
	Normalized Area[a]	8.37	6E-3	21.59	8.64	1.00
Energy Consumption	Energy [pJ/bit]	17.75	0.097	2.74	11	**0.082**[e]
	Normalized Energy[a]	309.62	1.85	16.71	8.26	1.00
Throughput [Mb/sec]		1.6[b]	1100	25	0.006	**1600**
Post-Processing Method		Thresholding	-	-	Calibration	Unstable Bit Discard

[a] Normalized with CMOS technology and challenge bit-width
[b] Effective throughput = Clock frequency × (1−Percentage of CRPs discarded during evaluation in the worst-case)
[c] Challenge bit-width = # of Rows × (Sequence−1), Sequence = 5 in this comparison
[d] 1.03×10^{27} with expanded challenge of 96 bits and 5.46×10^{26} after discarding 47% of the CRPs
[e] PUF energy consumption without post-processing for fair comparison

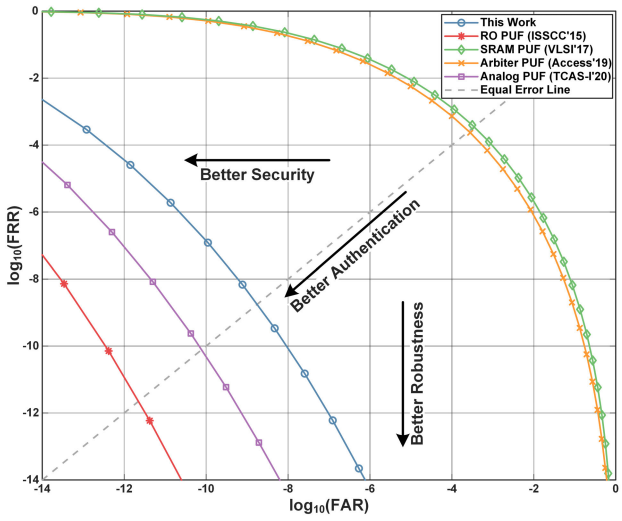


FIGURE 15. Comparison of false acceptance and false rejection rate under the fair identification threshold condition.

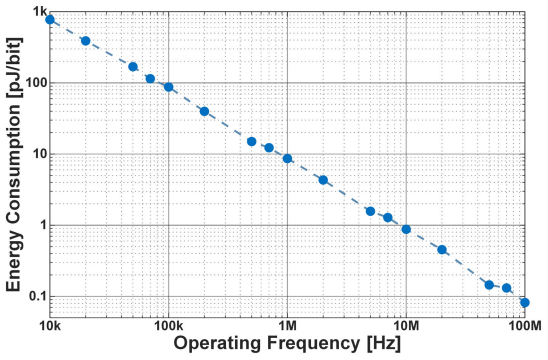


FIGURE 16. Energy consumption per a response bit generation as a function of the operating frequency.

The proposed reconfigurable PUF shows a small area of 88.867 μm^2/bit and energy efficiency of 0.082 pJ/bit compared to other state-of-the-art topologies. To compare the performance under fair conditions, the normalized core area and energy consumption are also presented in Table 1. The normalized values are calculated by using the minimum gate length of the CMOS process to scale area and energy by a factor of $1/S^2$ and $1/S^3$, respectively [45]. The challenge bit-width is linearly normalized. In Table 1, the proposed PUF has the lowest normalized energy dissipation and falls within the lower class of area occupation among state-of-the-art structures. The fastest throughput index of 1.6 Gbps allows for high-speed key generation. Although the number of CRPs of the proposed PUF is comparatively low, if our chip area is normalized to allow for 96-bit challenges, this allows for a capacity of 1.03×10^{27} CRPs, or 5.46×10^{26} if the unstable 47% of CRPs are discarded. These values are comparable to state-of-the-art designs [20], [24], [36], [44]. The expanded CRP space with 96-bit challenges also contributes to increasing required time for full CRP read-out by an attacker with full access. The total read-out time can be estimated by a function of the total number of CRPs, required clock cycles for generating a single CRP and clock

frequency. Under a condition for a single CRP generation speed (minimum 2 cycles) and the system clock frequency (100 MHz as maximum measured frequency), it may require up to 2.06×10^{19} seconds for full read-out, making it difficult to attempt an attack.

The CRP relation of the proposed PUF demonstrates strong resilience to model-building attacks with prediction errors of 0.166 on native CRP generation, and 0.239 when scrambled using the G-LFSR on a training set of 10^4 CRPs using a SVM to perform classification. The prediction error of the proposed PUF is higher than that of comparable SRAM based PUFs [20]. The analog PUF [36] has the best resilience to machine learning attacks, though it comes at the cost of larger area occupation, higher power consumption, and slower key generation speed than SRAM based PUFs.

In addition, the proposed SRAM PUF demonstrates comparable uniqueness (48.93%) and a BER (0.9%) across a measured operating range. To compensate the different operating ranges among the state-of-the-art, the worst case native BER is normalized per 10°C and per 0.1 V, resulting in 1.83% and 3.43% respectively. The implemented SRAM PUF shows slightly worse BER performance than the other PUFs. This result is expected to be due to the 1K-bit large-scale array implementation, which may degrade reliability via cross-talk between densely connected cells [34], [46]. However, this trade-off is justifiable as the proposed chip is the only one to surpass the ISO/IEC 29192 standard which recommends a minimum of 80-bit or 112-bit security strength for lightweight cryptography [31]. Security-critical systems are likely to require multiple security services within a single die, such as confidentiality, authentication, and non-repudiation. Thus, several sets of secret keys would be required for different algorithms. A large-scale array, such as the presented chip, would therefore be fully utilized.

V. CONCLUSION

This paper presents a reconfigurable SRAM-based PUF with 160M CRPs. The proposed architecture is the first to integrate multiple CRPs per cell by cascoding pull-up and pull-down transistors into cross-coupled inverters within each SRAM cell. The proposed response instability detector is shown to improve BER performance by discarding unstable responses, and the output scrambler adds indirect challenges by using a Galois-LFSR to scramble the response. The proposed PUF is implemented in a 65 nm CMOS process and was measured to evaluate the performance of uniqueness, randomness, and stability under various supply voltages and temperature. Compared with other state-of-the-art designs, the proposed PUF shows high-speed, high power efficiency, and compact area while maintaining good CRP density and performance. To the best of our knowledge, this is the first experimental demonstration where multiple CRPs are attained within an individual SRAM cell. The proposed topology, which merges the advantages of weak and strong memory-based PUFs, can be used as a practical information security system for a highly robust and unpredictable bi-directional authentication.

REFERENCES

[1] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.
[2] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Autom. Conf.*, Jun. 2015, pp. 1–6.
[3] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems—A comparative analysis," in *Data Privacy Management and Autonomous Spontaneous Security*, J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, Eds. Berlin, Germany: Springer, 2014, pp. 333–349.
[4] 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: Foundations and Practice*, A.-R. Sadeghi and D. Naccache, Eds. Berlin, Germany: Springer, 2010, pp. 3–37.
[5] T. Idriss, H. Idriss, and M. Bayoumi, "A PUF-based paradigm for IoT security," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 700–705.
[6] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electron.*, vol. 3, no. 2, pp. 81–91, 2020.
[7] 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.
[8] A. Babaei and G. Schiele, "Physical unclonable functions in the Internet of Things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, Jul. 2019.
[9] J. R. D. Kumar, C. G. Babu, V. R. Balaji, K. Priyadharsini, and S. P. Karthi, "Performance investigation of various SRAM Cells for IoT based wearable biomedical devices," in *Inventive Communication and Computational Technologies*, G. Ranganathan, J. Chen, and Á. Rocha, Eds. Singapore: Springer, 2021, pp. 573–588.
[10] K. Agarwal and S. Nassif, "Statistical analysis of SRAM cell stability," in *Proc. 43rd ACM/IEEE Design Autom. Conf.*, Jul. 2006, pp. 57–62.
[11] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems—CHES*, P. Paillier and I. Verbauwhede, Eds. Berlin, Germany: Springer, 2007, pp. 63–80.
[12] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 67–70.
[13] M. Bhargava, C. Cakir, and K. Mai, "Attack resistant sense amplifier based PUFs (SA-PUF) with deterministic and controllable reliability of PUF responses," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 106–111.
[14] C. Böhm, M. Hofer, and W. Pribyl, "A microcontroller SRAM-PUF," in *Proc. 5th Int. Conf. Netw. Syst. Secur.*, Sep. 2011, pp. 269–273.
[15] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," in *Proc. ESSCIRC (ESSCIRC)*, Sep. 2012, pp. 486–489.
[16] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2014, pp. 278–279.
[17] A. Alvarez, W. Zhao, and M. Alioto, "14.3 15fJ/b static physically unclonable functions for secure chip identification with <2% native bit instability and 140× inter/intra PUF Hamming distance separation in 65nm," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 256–257.
[18] K.-U. Choi, S. Baek, J. Heo, and J.-P. Hong, "A 100% stable sense-amplifier-based physically unclonable function with individually embedded non-volatile memory," *IEEE Access*, vol. 8, pp. 21857–21865, 2020.
[19] D. E. Holcomb and K. Fu, "Bitline PUF: Building native challenge-response PUF capability into any SRAM," in *Cryptographic Hardware and Embedded Systems—CHES*, L. Batina and M. Robshaw, Eds. Berlin, Germany: Springer, 2014, pp. 510–526.
[20] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," in *Proc. Symp. VLSI Circuits*, Jun. 2017, pp. C270–C271.

[21] S. Baek, J.-H. Ahn, K.-U. Choi, and J.-P. Hong, "A reconfigurable challenge-response generating SRAM PUF in 65nm CMOS," in *Proc. IEEE Hot Chips Symp. (HCS)*, Aug. 2019. [Online]. Available: https://old.hotchips.org/hc31/HC31.ChungbukNationalUniversity.Seungbum Baek.v02.pdf

[22] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[23] M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Des. Test. Comput.*, vol. 27, no. 1, pp. 48–65, Jan. 2010.

[24] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "14.2 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. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 254–255.

[25] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "8.7 physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Jan. 2016, pp. 158–160.

[26] M. Hiller, M.-D. Yu, and G. Sigl, "Cherry-picking reliable PUF bits with differential sequence coding," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2065–2076, Sep. 2016.

[27] S. Muddu, "Auxiliary pattern-based optical proximity correction for better printability, timing, and leakage control," *J. Micro/Nanolithography, MEMS, MOEMS*, vol. 7, no. 1, Jan. 2008, Art. no. 013002.

[28] M. Bhargava. (May 2013). *Reliable, Secure, Efficient Physical Unclonable Functions*. [Online]. Available: https://kilthub.cmu.edu/articles/thesis/Reliable_Secure_Efficient_Physi%cal_Unclonable_Functions/6721310

[29] Y. Chen, Z. Wang, A. Patil, and A. Basu, "A 2.86-TOPS/W current mirror cross-bar-based machine-learning and physical unclonable function engine for Internet-of-Things applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 6, pp. 2240–2252, Jun. 2019.

[30] R. Ward and T. Molteno. (2007). *Table Linear Feedback Shift Registers*. [Online]. Available: https://cdn.hackaday.io/files/1630346975246656/lfsr_table.pdf

[31] *Information Technology—Security Techniques—Lightweight Cryptography—-Part 1: General*, Standard ISO/IEC 29192-1:2012, Jun. 2012.

[32] M. Robshaw and O. Billet, *New Stream Cipher Designs: The eSTREAM Finalists*, vol. 4986. Berlin, Germany: Springer, 2008.

[33] 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)*, Jun. 2010, pp. 94–99.

[34] M. T. Rahman, A. Hosey, Z. Guo, J. Carroll, D. Forte, and M. Tehranipoor, "Systematic correlation and cell neighborhood analysis of SRAM PUF for robust and unique key generation," *J. Hardw. Syst. Secur.*, vol. 1, no. 2, pp. 137–155, Jun. 2017.

[35] A. Vijayakumar, V. C. Patil, C. B. Prado, and S. Kundu, "Machine learning resistant strong PUF: Possible or a pipe dream?" in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2016, pp. 19–24.

[36] H. Zhuang, X. Xi, N. Sun, and M. Orshansky, "A strong subthreshold current array PUF resilient to machine learning attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 1, pp. 135–144, Jan. 2020.

[37] G. T. Becker, "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in *Cryptographic Hardware and Embedded Systems—CHES*, T. Güneysu and H. Handschuh, Eds. Berlin, Germany: Springer, 2015, pp. 535–555.

[38] J. Shi, Y. Lu, and J. Zhang, "Approximation attacks on strong PUFs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2138–2151, Oct. 2020.

[39] J. Zhang and C. Shen, "Set-based obfuscation for strong PUFs against machine learning attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 1, pp. 288–300, Jan. 2021.

[40] F. Wilde, B. M. Gammel, and M. Pehl, "Spatial correlation analysis on physical unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1468–1480, Jun. 2018.

[41] L. Lin, S. Srivathsa, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.

[42] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, Apr. 2011.

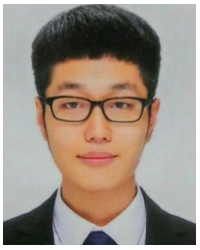
[43] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[44] Y. Cao, W. Zheng, X. Zhao, and C.-H. Chang, "An energy-efficient current-starved inverter based strong physical unclonable function with enhanced temperature stability," *IEEE Access*, vol. 7, pp. 105287–105297, 2019.

[45] N. H. E. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*, 4th ed. Reading, MA, USA: Addison-Wesley, 2010.

[46] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 101–106.

SEUNGBUM BAEK received the B.S. and M.S. degrees in information and communication engineering from Chungbuk National University, Cheongju, South Korea, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree in electrical engineering. His current research interests include VLSI design for security services targeting resource-constrained devices, microprocessor-controlled embedded systems, and bio-medical engineering.



GUK-HYEON YU received the B.S. and M.S. degrees in electrical engineering from Chungbuk National University, Cheongju, South Korea, in 2016 and 2018, respectively. He is currently working in Key Foundry, Cheongju. His current research interest includes CMOS true random number generator design.

JAEWOO KIM received the B.S. degree in electrical engineering from Chungbuk National University, Cheongju, South Korea, in 2020, where he is currently pursuing the M.S. degree. His current research interest includes CMOS true random number generator design for the IoT devices.

CHI TRUNG NGO received the B.Sc. degree in electronic-electrical engineering from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with Chungbuk National University, Cheongju, South Korea. His research interests include digital domain security service integrated circuits design and verification for lightweight devices.

JASON K. ESHRAGHIAN (Member, IEEE) received the Bachelor of Engineering degree in electrical and electronic and the Bachelor of Laws degree from The University of Western Australia, WA, Australia, in 2017, and the Ph.D. degree from The University of Western Australia. He is jointly appointed as a Postdoctoral Researcher with the Department of Electrical Engineering and Computer Science, University of Michigan, in Ann Arbor, USA, and a Forrest Research Fellow with the Schools of Medicine and Computer Science, The University of Western Australia. His current research interests include neuromorphic computing and spiking neural networks. He is a member of the IEEE Neural Systems and Applications Committee. He was awarded the 2019 IEEE Very Large Scale Integration Systems Best Paper Award, the Best Paper Award at the 2019 IEEE Artificial Intelligence Circuits and Systems Conference, and the Best Live Demonstration Award at the 2020 IEEE International Conference on Electronics, Circuits and Systems. He was a recipient of the 2021 Fulbright Postdoctoral Fellowship, the 2021 Forrest Research Fellowship, and 2019 Endeavour Research Fellowship.

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 main research interests include RF integrated circuits, such as LNA, mixer, VCO, and frequency synthesizer for wireless and wire-line communication systems. His current research interests are toward high frequency (THz) circuit design and integrated security chip based on CMOS technology.