A Compact Weak PUF Circuit Based on MOSFET Subthreshold Leakage Current

Yuanfeng Xie¹, Gang Li¹, Pengjun Wang¹) and Ziyu Zhou¹

Abstract Owing to the large area and power consumption of traditional physically unclonable function (PUF) circuits, they are susceptible to interference from environmental factors. A compact PUF circuit design scheme is proposed by analyzing the circuit structure and sub-threshold leakage current deviation characteristics of a bistable PUF. First, the current-voltage sensitive characteristics of a transistor in the sub-threshold operating region are utilized. Next, to improve the output response speed and the uniqueness of the characteristic information of the PUF circuit, the proposed PUF circuit is designed which combines with the positive feedback and RS latch characteristics. Finally, simulation results based on the TSMC 65 nm CMOS process show that the PUF has good uniqueness, randomness, and reliability. The cell layout area, the bit error rate (BER) in the worst case, and the energy consumption are 0.177 μm², 2.8%, and 8.976 fJ/bit respectively.

key words: Physically unclonable function, sub-threshold leakage current, compactness, circuit design

Classification: Integrated circuits

1. Introduction

With the development of Internet of Things (IoT), an increasing number of IoT technologies have been applied in numerous fields, such as smart homes [1], smart logistics [2], and smart medicine [3, 4]. IoT edge devices are mostly deployed in untrusted environments and are vulnerable to security threats, such as surveillance, forgery, and tampering. The existing security protection systems that are based on cryptographic mechanisms require complex computing and excessive storage resources. The information present in nonvolatile storage devices can be easily read and illegally used. Therefore, they no longer meet the low overhead and high security requirements of increasingly miniaturized and lightweight modern IoT intelligent devices.

Existing hardware security technologies include random number generators [5], security layout design, and physically unclonable functions (PUF). As a type of digital fingerprint of a chip, a PUF generates challenge-response pairs (CRPs) with characteristics of randomness and uniqueness by using unavoidable process deviation in the manufacturing process of a chip. PUFs can be used in IoT protection, key security storage [6], and other information security fields. PUFs are typically categorized into two classes: strong PUFs and weak PUFs. The difference between these two types is the ability to generate CRPs. Strong PUFs [7, 8] obtain exponential CRPs through the reconstruction of hardware resources; however, the CRPs are correlated and more vulnerable to machine-learning attacks. Typical strong PUFs include arbiter PUF (APUF) [9, 10] and ring oscillator PUF [11] (RO-PUF). Weak PUFs usually consist of cell arrays of the same design, which utilize the unavoidable process deviation of hardware circuits or hardware electronic components during the manufacturing process as an entropy source. A weak PUF cell typically produces only a one-bit response, and its CRP space has a linear relationship with the chip area. It has best resilience to machine learning attacks, and is more suitable for generating security keys. Typical weak PUFs include the Latch PUF [12] and static random access memory (SRAM) PUF [13]. The chip is easily affected by the environmental noise during its operation, and the PUF cell produces unstable response bits and has a high bit error rate (BER). A resource-constrained system [14] has a limited chip area and cannot effectively use the auxiliary circuits to improve the stability of the weak PUFs. Therefore, the design of lightweight PUF circuits with low BER has become a popular research matter in hardware security.

The SRAM PUF has good scalability and randomness among the various process technologies. This architecture utilizes the mismatch between the cross-coupled inverters to extract the response bits from the physical characteristics of the IC. The traditional SRAM PUF has certain defects, such as a high BER and a large area overhead. Therefore, Shifman et al. [15] adopted the "capacitance bias" preselection mechanism for the unstable cells in a bistable PUF by adding controllable capacitors to any cross-coupled inverter node to reduce the BER to 10⁻⁹. However, the PUF layout area is as high as 3001 F². Li et al. [16] proposed a lightweight bistable weak PUF with a cell feature size of only 215 F² and the lowest BER of 2.05% by using the bistable PUF cell.
sharing and random word-level reading strategies. Zhao et al. [17] proposed a PUF circuit design scheme based on a cross-coupled comparator, which uses complementary to absolute temperature (CTAT) and spatial majority voting (SMV) [18] technology to reduce the BER; however, the cell layout area is as high as 1036 F². At present, many works have proposed different solutions to improve the stability of PUF, such as the use of new material devices [19] (carbon nanotubes), accelerated aging [20], ECC error correction coding [21], etc. Therefore, to further optimize the circuit structure, this study reveals the entropy source mismatch mechanism caused by the leakage current deviation by analyzing the bistable PUF circuit and the subthreshold current characteristics. A design scheme of a compact PUF circuit, i.e., a PUF based on a subthreshold leakage current deviation (SLCD-PUF) is proposed. The influence of the voltage and temperature changes on the stability of the circuit is analyzed by the Monte Carlo simulation, and the experimental results show that the designed circuit considers both the area overhead and stability.

2. Bistable PUF Circuit Structure and Analysis of Subthreshold Current Deviation

2.1 Bistable PUF circuit structure

A bistable PUF [22] is a type of PUF with a cross-coupled circuit structure as its core. The bistable PUF circuit is always in a stable state when not triggered by an external excitation signal and jumps from the current stable state to another stable state when triggered by the challenge signal. As the basic cell of a bistable circuit, the cross-coupling structure has the characteristics of positive feedback, which is conducive to the rapid calculation and storage of data. It is mostly used in latches [23], flip-flops [24], and SRAM. The SRAM PUF is a bistable PUF that has been extensively studied in literature. It uses the random process deviation of the cross-coupled circuit to extract the hardware fingerprints. Taking the traditional 6-transistor SRAM [25] cell circuit structure as an example, a bistable PUF circuit structure is described, as shown in Fig. 1.

\[I_{sat} = \mu C_{ox}\left(\frac{W}{L}\right)^2(V_{gs} - V_{th})^2\]  \hspace{0.5cm} (1)

\[I_{sub} = \mu C_{ox}\left(\frac{W}{L}\right)\exp\left(V_{gs} - V_{th}\right)\left(1 - \exp\left(-\frac{V_{ds}}{V_t}\right)\right)\]  \hspace{0.5cm} (2)

where, \(\mu\) is the carrier mobility, \(C_{ox}\) is the gate oxide capacitance, \(W/L\) is the width-to-length ratio of the transistor, \(V_{th}\) is the threshold voltage, \(V_t\) is the thermoelectric potential, \(I_{sat}\) is the saturation current, and \(I_{sub}\) is the sub-threshold current. \(-\exp(-V_{ds}/V_t)\) can be ignored because \(V_{ds}\) discharges from VDD and \(V_{ds}\) is much larger than \(V_t\). The subthreshold current is exponentially related to \(V_{gs}\) voltage according to equations (1) and (2). Compared with operating in the saturation region, the current changes more significantly with the voltage in the subthreshold region. As shown in

Fig. 1 Traditional 6-transistor SRAM cell

The transistors M1–M4 form two inverter structures connected end-to-end. Transistors M5 and M6 are controlled by the word line (WL) and are connected to the BL and BLB. Ideally, the threshold voltages of M1–M4 are the same. When the SRAM cell is powered on, as the voltages of Q and QB increase, the gate-source voltage of the transistor gradually reaches the threshold voltage, and the node voltage remains at the metastable point. However, the threshold voltage of the transistors is different owing to the process deviation, which results in a voltage difference between Q and QB. This forms a positive-feedback channel. Finally, the node voltage easily transitions from a metastable to a stable point. Q or QB tended to be high. Fig. 2 shows the voltage distribution (100 Monte Carlo simulations) of the initial value of the SRAM PUF cell affected by the noise and process variation. It can be observed that node Q transitions from an initial value of 0 to a stable state of 0/1 after a period of time.

Fig. 2 SRAM-PUF cell power-on process
Fig. 3, the basic cell is composed of two NMOS transistors, and the gate voltage $V_{gs}$ controls the current in transistors M1 and M2. A total of 1000 Monte Carlo simulations were performed for each value of $V_{gs}$ and the coefficient of variation of the difference between $I_1$ and $I_2$ ($CV=\sigma/\mu$, where $\sigma$ and $\mu$ represent the standard deviation and average value of the difference between $I_1$ and $I_2$). The simulation diagram of the current mismatch in the subthreshold region, saturation region, and linear region of the transistor is shown in the curve in Fig 3. As shown in Fig. 3, when the PUF circuit works in the subthreshold region, the coefficient of variation is the largest, and the subthreshold current deviation is the largest [26]. Therefore, the subthreshold current deviation as the entropy source is more stable, which is conducive to enhancing the stability of the PUF.

![Simulated results of the two NMOS transistors](image_url)

**Fig. 3** Simulated results of the two NMOS transistors. Curve 1 reveals the standard deviation of the difference between $I_1$ and $I_2$, curve 2 reveals the average value of the difference between $I_1$ and $I_2$, and curve 3 reveals the CV of the difference between $I_1$ and $I_2$.

3. SLCD-PUF circuit structure design

Traditional bistable PUF circuit design schemes generally use six or more transistors as switches and bias entropy sources. They have large overheads in terms of area and power consumption. The 6-transistor SRAM PUF cell in which M5 and M6 transistors are used for row selection and M1–M4 transistors are used as deviation entropy source transistors is shown in Fig. 1. Without considering the SRAM storage function and considering only the PUF characteristics, the 2-transistor cell in Fig. 3 can be used to replace the 6-transistor SRAM PUF cell in Fig. 1. Its function is to realize the switching control through the gate voltage of the NMOS transistors, take the leakage current deviation of the NMOS transistors as the entropy source, reduce the four transistors, and propose the SLCD-PUF circuit framework shown in Fig. 4. The SLCD-PUF circuit is primarily composed of a timing control circuit, decoder circuit, shared head, PUF cell array, and an RS latch. The timing control and decoder modules are shown in Fig. 4 (a). The timing control circuit is primarily used to generate the timing information of the decoder and the PUF circuit and to provide them with the required pre-charging signal. The decoder adopts two-stage decoding: the first stage adopts 2-4 decoding and the second stage adopts 3-8 decoding. Address sequence of decoder is the challenge input of the PUF. The output of decoder is the 16-bit WL [0:15]. The signal WL [0:15] is the cell-chosen signal of PUF cell. PUF cell structure is shown in Fig. 4 (b). In the PUF module, the PMOS transistors are directly connected to the power supply, the NMOS transistors array is isolated from the power supply through the P-type shared head, and the charging speed of the PMOS transistors array is lower than that of the NMOS transistors array.

![Structure block diagram of the proposed PUF circuit](image_url)

**Fig. 4** Structure block diagram of the proposed PUF circuit: (a) Clock control and decoder module, (b) Basic structure diagram of PUF cell.
The proposed cell array is constructed using NMOS transistors to ensure stability and working speed. Here, the shared head selects the process size \( W_p/L_p = 2 \mu m/60 \) nm to avoid the bias of the PUF response output (the overall bias is 0 or 1). Transistors P5, P6, N5, and N6 formed cross-coupled bistable structures. Transistors N1 and N2 are used as the gate switches, and currents \( I_1 \) and \( I_2 \) flowing through N1 and N2 are used as the deviation sources. N1 and N2 are set to work in the subthreshold region to maximize the sensitivity of the drain-current deviations of N1 and N2.

The working process of the SLCD-PUF circuit is as follows. It can be divided into two stages: pre-charging and evaluation. In the precharge stage, Q and QB are charged to high values when the PRE is low. The switch signal SW is kept at a low level to prevent leakage current during charging. In addition, the bias voltage decreases from VDD to VBB. In the evaluation stage, the mismatched voltages of N1 and N2 are rapidly amplified owing to the process variation and the cross-coupling structure of the shared head. In addition, a stable output response is achieved. If \( I_1 > I_2 \), then \( QB = \text{VDD} \) and \( Q = 0 \); otherwise, \( QB = 0 \) and \( Q = \text{VDD} \).

The working sequence of the SLCD-PUF circuit is illustrated in Fig. 5. CLK, PRE, WL[0], WL[1], WL[2],...WL[15] are the clock, precharge, and word-line signals, respectively. The decoding output terminal is connected to the inverter. The inverter adopts an NMOS source connected to the VBB instead of VSS so that the WL signal is at a high level or VBB. Finally, the PUF signal ID is produced after the output signal of the PUF is locked by the RS latch.

![Working sequence of PUF circuit](image)

Fig. 5 Working sequence of PUF circuit.

4. Experimental results and analysis

The proposed PUF circuit module diagram is constructed using the TSMC 65 nm CMOS process. The custom layout of the PUF circuit is shown in Fig. 6, and the whole layout area is 25.80 \( \mu m \times 20.70 \mu m \). The layout area of the PUF’s basic cell is 0.177 \( \mu m^2 \). The deviation circuit is located on the left side of the layout, the decoder circuit is located on the upper right side, and the timing control circuit is located on the lower right side. The entire layout design shares four layers of metals (MT1–MT4). MT1 and MT2 are used for the internal signal of the cell circuit, MT3 is used to enable the signal wiring, and MT4 is used to connect the decoder with the PUF cell. Vertical wiring is utilized for the metal wires of each layer to reduce the capacitive coupling.

![Layout of the proposed PUF circuit](image)

Fig. 6 Layout of the proposed PUF circuit.

4.1 Stability

The stability of the PUF refers to the ability to maintain the output characteristic of the PUF circuit unchanged when environmental factors, such as temperature and power supply voltage, change. The stability of a PUF is usually measured by the BER and the unstable bits (bits with at least one error during N tests). The PUF output stability is primarily affected by the power supply noise, voltage, and temperature changes. To evaluate the PUF stability under different operating conditions, the proposed PUF was measured across a wide range of supply voltage from 1.0–1.4 V and temperature from -40–125°C. The response outputs were then compared against the golden CRPs generated under the nominal condition to estimate BER. Fig. 7 shows the measured BER in the worst case is 2.8%, demonstrating the excellent supply and temperature scalability of the proposed PUF.

![Measured BER under different conditions](image)

Fig. 7 Measured BER under different (a) supply voltage and (b) temperature conditions.
4.2 Randomness
Randomness characterizes the uniformity of the PUF output response, which is primarily measured by the probability distribution of logic 0 and logic 1 in the PUF circuit output response. Ideally, logical 0 and logical 1 obey a uniform distribution, both close to 50%, which can be expressed as follows:

\[
\text{Randomness} = (1 - |2P(R = 1) - 1|) \times 100\% \tag{3}
\]

where, \(P(R=1)\) represents the probability of a logical 1 in the output data.

The randomness test typically uses a grayscale map to map the PUF response to the gray-scale map. The black pixels represent the response as logic "1," and the white pixels represent the response as logic "0." A PUF is randomly selected, and a grayscale image of the output response is shown in Fig. 8. The probability of generating a logical "1" (49.6 %) is close to the ideal value of 50%. Similar statistical results are observed for the remaining PUF instances. The average grayscale map values of the 50 PUF output responses are concentrated at approximately 0.5.

![Grayscale mapping](image)

**Fig. 8** Output response distribution of PUF: (a) Grayscale mapping (b) Average grayscale mapping.

4.3 Uniqueness
The Uniqueness is used to identify the degree of discrimination between different PUFs, which reflects the ability of a PUF to distinguish itself from other PUFs. The response of the same excitation to different PUFs is different, which is usually measured by the average inter-Hamming Distance (inter-HD). Ideally, with a uniqueness of 50%, the HD-Inter of k PUF individuals is depicted as follows:

\[

d_{\text{inter}} = \frac{1}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{D(R_i, R_j)}{N} \times 100\%
\]

where, \(R_i\) and \(R_j\) represent the n-bit responses generated by the \(i^{th}\) and \(j^{th}\) PUF circuits under the same excitation.

To test the accuracy of the PUF, 100 Monte Carlo simulations are performed on the PUF circuit, which can obtain 25,600 output responses. The HD between each response is calculated. The intra-PUF HD is measured by applying the same challenges to the same chip for 100 times and the response of each time are compared. The results are shown in Fig. 9. The fitting curve for the average interslice HD of the proposed PUF is shown in Fig. 8 (solid line). The expectation and variance of the normal distribution after fitting are 0.5062 and 0.0329, respectively, after normalization. And their corresponding uniqueness is close to the ideal value of 50%, with good uniqueness.

![Fitting curve](image)

**Fig. 9** Fitting curve of intraslice Hamming Distance and interslice Hamming Distance.

4.4 Performance comparison
The performance comparison results between the proposed compact PUF and other PUFs of the same type are shown in Table I. The proposed PUF is simulated under the optimal bias voltage (VBB=0.375V). In terms of area power consumption, the power consumption is reduced by 1.7 times compared with the PUF proposed in the literature [30] due to its great advantages in the number of cells and cell size. Compared with the PUF proposed by [27], it still has an advantage of 1.09 times.

In terms of reliability, it has a 1.44 times advantage over literature [28] in BER.

| Comparative literature | [27]JSSC’16 | [28]TCAS’17 | [29]JSSC’18 | [30]JSSC’21 | This work |
|------------------------|------------|------------|------------|------------|----------|
| Technology(nm)     | 65         | 180        | 45         | 130        | 65       |
| Cell transistor counts | 6          | 12         | 30         | 8          | 2        |
| Cell area(\(\mu^2\)) | 3.07       | 17.91      | 5.83       | 8          | 0.177    |
| Cell feature size(\(\mu^2\)) | 548       | 553        | 57.5       | 497        | 41.91    |
| Voltage range(V)   | 0.6-1.2    | 0.8-1.8    | 0.8-1.0    | 0.8-1.8    | 1.0-1.4  |
| Temperature range(°C) | 0.80       | -40-120   | -40-125    | -40-120    | 125      |
| ACF @ 95% confidence | 0.0188     | 0.0173     | 0.00735    | 0.0334     | 0.012    |
| BER in worst case(%) | 6.64       | 4.7        | 2.31       | 6.74       | 2.8      |
| Energy efficiency(fJ/bit) | 548       | 91.1       | 57.5       | 15.39      | 8.976    |

6. Conclusion
In this study, a novel bistable compact PUF circuit is constructed by combining a bistable PUF and a sub-threshold current bias sensing mechanism. The PUF obtains a compact array structure under the premise of considering randomness, uniqueness, reliability, and other properties by comparing the difference in the sub-threshold leakage current of MOS transistors and using shared-bistable multiplexing technology. The experimental results show that the PUF cell can generate a 256-bit response in only one working cycle, and the energy consumption is about 8.976 fJ/bit at 1.2 V/5.6 MHz, the randomness is 49.6%, and the cell layout area...
is 0.177 μm². It can be observed that the proposed PUF circuit has the characteristics of low hardware resource consumption and high output response quality, and provides a new solution for the generation and storage of security keys in low-power hardware security chip systems.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB2202100; in part by the National Natural Science Foundation of China under Grant 62174121, Grant 61904125, and Grant 61874078; in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY22F040004.

References

[1] W. D. S. Costa, et al.: “Power Line Communication based Smartplug Prototype for Power Consumption Monitoring in Smart Homes,” IEEE LAT AM J T 19 (2021) 1849 (DOI: 10.1109/TLA.2021.9475618).

[2] Y. Song, et al.: “Applications of the Internet of Things (IoT) in Smart Logistiques: A Comprehensive Survey,” IEEE INTERNET THINGS 8 (2020) 4250 (DOI: 10.1109/JIOT.2020.3034385).

[3] K. K. Coello, et al.: “LORENA: Low memOry symmEtirc-Key geNerAtion Method for Based on Group Cryptography Protocol Applied to the Internet of Healthcare Things,” IEEE Access, 10, (2022), 12564. (DOI:10.1109/ACCESS.2022.3143201).

[4] V. Selamneni, et al.: “Low-Cost, Disposable, Flexible, and Smartphone Enabled Pressure Sensor for Monitoring Drug Dosage in Smart Medicine Applications,” IEEE SENS J 19 (2019) 11255 (DOI:10.1109/JSEN.2019.2935383).

[5] C. S. Petrie, et al.: “A noise-based IC random number generator for applications in cryptography,” IEEE T CIRCUITS-I 47 (2000) 615 (DOI: 10.1109/TCSI.2000.846772).

[6] P. Mall, et al.: “PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey,” IEEE INTERNET THINGS 9 (2022) 8205 (DOI: 10.1109/JIOT2022.3142084).

[7] R. Ali, et al.: “A Machine Learning Attack-Resilient Strong PUF Leveraging the Process Variation of MRAM,” IEEE T Circuits-II, 69, (2022), 2712 (DOI:10.1109/TCSI.2022.3144497).

[8] S. Hou, et al.: “A lightweight and secure-enhanced Strong PUF design on FPGA,” IEICE Electron. Express 16 (2019) 20190695 (DOI: 10.1587/exle.16.20190695).

[9] D. P. Sahoo, et al.: “A Multiplexer-Based Arbiter PUF Composition with Enhanced Reliability and Security,” IEEE T Comput 67 (2018) 403 (DOI: 10.1109/TC.2017.2749226).

[10] W. Ge, et al.: “FPGA implementation of a challenge pre-processing structure arbiter PUF designed for machine learning attack resistance,” IEICE Electron. Express 17 (2020) 20190607 (DOI: 10.1587/exle.16.20190607).

[11] M. T. Rahman, et al.: “An Aging-Resistant RO-PUF for Reliable Key Generation,” IEEE T Emerg Top Com 4 (2016) 335 (DOI: 10.1109/TETC.2015.2474741).

[12] J. L. Danger, et al.: “Analysis of Mixed PUF-TRNG Circuit Based on SR-Latches in FD-SOI Technology,” Euromicro Conference on Digital System Design (2018) 508 (DOI: 10.1109/DSD.2018.00090).

[13] Y. C. Chiu, et al.: “A 4-Kb 1-to-8-bit Configurable 6T SRAM-Based Computation-in-Memory Unit-Macro for CNN-Based AI Edge Processors,” IEEE J. Solid-State Circuits 55 (2020) 2790 (DOI: 10.1109/JSSC.2020.3005754).

[14] A. D. Vita, et al.: “A Partially Binarized Hybrid Neural Network System for Low-Power and Resource Constrained Human Activity Recognition,” IEEE T CIRCUITS-I 67 (2020) 3893 (DOI: 10.1109/TCSI.2020.3011984).

[15] Y. Shifman, et al.: “An SRAM-Based PUF With a Capacitive Digital Preselection for a 1E-9 Key Error Probability,” IEEE T Circuits-I 67 (2020) 4855 (DOI: 10.1109/TCSI.2020.2996772).

[16] G. Li, et al.: “A 215-F F Bisstable Physically Unclonable Function With an ACf of <0.005 and a Native Bit Instability of 2.05% in 65-nm CMOS Process,” IEEE T VLSI SYST 28 (2020) 2290 (DOI: 10.1109/TVLISI.2020.3014892).

[17] Q. Zhao, et al.: “A 1036-F/Bit High Reliability Temperature Compensated Cross-Coupled Comparator-Based PUF,” IEEE T VLSI SYST 28 (2020) 1449 (DOI: 10.1109/TVLISI.2020.2980306).

[18] X. Xu, et al.: “Bimodal Oscillation as a Mechanism for Autonomous Majority Voting in PUFs,” IEEE T VLSI SYST 26 (2018) 2431 (DOI: 10.1109/TVLISI.2018.2861328).

[19] N. Kumar, et al.: “Multigated Carbon Nanotube Field Effect Transistors-Based Physically Unclonable Functions As Security Keys,” IEEE INTERNET THINGS 6 (2018) 325 (DOI: 10.1109/JIOT.2018.2838580).

[20] M. N. Islam, et al.: “An SRAM-Based PUF With a Capacitive Digital Preselection for a 1E-9 Key Error Probability,” IEEE T CIRCUITS-I 65 (2018) 960 (DOI: 10.1109/TCSI.2017.2766073).

[21] A. Miller, et al.: “A Highly Reliable SRAM PUF with a Capacitive Preselection Mechanism and pre-ECC BER of 7.4E-10,” IEEE Custom Integrated Circuits Conference (2019) (DOI: 10.1109/CICC.2019.8780246).

[22] M. Thirumooorthi, et al.: “Design and Evaluation of a Hybrid Chaotic-Bistable Ring PUF,” IEEE T VLSI SYST 29 (2021) 4855 (DOI: 10.1109/TVLISI.2021.311588).

[23] D. Patel, et al.: “Hybrid Latch-Type Offset Tolerant Sense Amplifier for Low-Voltage SRAMs,” IEEE T CIRCUITS-I 66 (2019) 2519 (DOI: 10.1109/TCSI.2019.2899314).

[24] D. Hayashi, et al.: “Bit Error Rate Measurements of All-Optical Flip-Flop Operations of a 1.55-μm Polarization Bistable VCSEL,” J LIGHTWAVE TECHNOL 32 (2014) 2671 (DOI: 10.1109/JLT.2014.2332535).

[25] L. Lu, et al.: “A 6T SRAM Based Two-Dimensional Configurable Challenge-Response PUF for Portable Devices,” IEEE T CIRCUITS-I 69 (2022) 2542 (DOI: 10.1109/TCSI.2022.3156993).

[26] J. Lee, et al.: “A current-integrated differential NAND-structured PUF for stable and V/T variation-tolerant low-cost IoT security,” IEEE Asian Solid-State Circuits Conference (2021) (DOI: 10.1109/A-SSCC3895.2021.9634806).

[27] J. Li, et al.: “Ultra-Compact and Robust Physically Unclonable Function Based on Voltage-Compensated Proportional-to-Absolute-Temperature Voltage Generators,” IEEE J. Solid-State Circuits 51 (2016) 2192 (DOI: 10.1109/JSSC.2016.2586498).

[28] J. Liu, et al.: “A 0.04% BER Strong PUF With Cell-Bias-Based CRPs Filtering and Background Offset Calibration,” IEEE T CIRCUITS-I 67 (2020) 3853 (DOI: 10.1109/TCSI.2020.3008683).

[29] S. Taneja, et al.: “Fully Synthesizable PUF Featuring Hysteresis and Temperature Compensation for 3.2% Native BER and 1.02 fΩ in 40 nm,” IEEE J. Solid-State Circuits 53 (2018) 2828 (DOI: 10.1109/JSSC.2018.2865584).

[30] K. Liu, et al.: “A 0.5-V Hybrid SRAM Physically Unclonable Function Using Hot Carrier Injection Burn-In for Stability Reinforcement,” IEEE J. Solid-State Circuits 56 (2021) 2193 (DOI: 10.1109/JSSC.2020.3035207).