IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 30, 2019, accepted July 25, 2019, date of publication July 30, 2019, date of current version August 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2932022

An Energy-Efficient Current-Starved Inverter Based Strong Physical Unclonable Function With Enhanced Temperature Stability

YUAN CAO[1], **(Member, IEEE), WENHAN ZHENG**[1], **XIAOJIN ZHAO**[1], **(Member, IEEE), AND CHIP-HONG CHANG**[2], **(Fellow, IEEE)**

[1]College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China
[2]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798

Corresponding author: Xiaojin Zhao (eexjzhao@szu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61601168, in part by the Kongque Technology Innovation Foundation of Shenzhen under Grant KQJSCX20170727101037551, in part by the Fundamental Research Foundation of Shenzhen under Grant JCYJ20170302151209762 and Grant JCYJ20170818101906654, and in part by the Singapore Ministry of Education Tier 2 Grant MOE2015-T2-013.

ABSTRACT As burgeoning hardware security primitive, physical unclonable function (PUF) has aroused the interest of solid-state circuit community on its efficient integration into security-critical applications. This paper presents an energy efficient implementation of classic arbiter PUF design. Current-starved (CS) inverters are inserted at the inputs of each multiplexer cell to reduce the skew and widen the distribution of the delay difference between two symmetric daisy-chained delay paths selectable by the input challenge. The CS-inverters are biased at the zero temperature coefficient (ZTC) point, making the accumulated delays of the two identical paths insensitive to temperature variations. A symmetric two RS latches based arbiter is proposed to overcome the asymmetric input and clock to the output propagation delay of D flip-flop and the metastability problem of RS latch arbiter. By limiting the drain currents of CS-inverters to achieve ZTC, the power consumption of the proposed PUF is also reduced substantially. The performance of the proposed PUF design has been successfully validated by the responses measured from prototype chips fabricated in standard 65 nm CMOS process. The fabricated chips feature a compact silicon area of 3838 μm^2 and low energy consumption of 2.74 pJ per bit at 25 Mbps, with measured uniqueness of 46.8% and native bit error rate (BER) of 0.8%. It is worst-case BER is less than 10.46% measured over an extended ~7x temperature range and ~5x supply voltage range. These physically measured figures of merit have outperformed previously reported measurements of strong PUFs with similar linear additive delay architecture.

INDEX TERMS Strong physical unclonable function, lightweight authentication, low power consumption, current-starved inverter.

I. INTRODUCTION

As forecasted by Gartner [1], 20.4 billion of Internet of Things (IoT) devices will be connected worldwide in 2020. The increasing reliance on IoT devices in autonomous decision making processes gives hackers an open field to exploit vulnerabilities in the physical implementation of on-device cryptographic algorithms that link to protected data storage and private information in distributed networks. Physical unclonable function (PUF) has emerged as an unconventional hardware-oriented security primitive to address this new threat landscape that is taking shape in the domain of IoT [2]. PUF can be used to extract chip-unique and random digital signatures without relying on computationally intractable mathematical problems that are costly or power hungry to implement on chip. As a one-way function, a PUF circuit generates an output in response to an input stimulus through physical disorder, or more precisely, the mismatch parameters of individual nano-scale components of a solid-state circuit inherently existed in their manufacturing process. One central feature of such disorder-based security is that each challenge response pair (CRP) of a PUF can be measured in real time, but the re-fabrication of another PUF with the same set of CRPs is infeasible or prohibitively costly even with the knowledge of the entire circuit down to the atomic level due to the very large entropy of physical disorder

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

in nano-fabrication. The unclonability and high characterization complexity properties have attracted several companies, including *Maxim*, *Intel*, *Xilinx* to invest in the efficient integration of various forms of solid-state PUFs for the new paradigm of security applications [3]–[5].

PUFs are broadly categorized into two classes [2]. Weak PUFs feature linear or polynomial CRP space. Hence, they are more suitable for use as unique and unforgeable serial numbers in supply chain applications, secret key generation, digital rights management and IC anti-counterfeiting. Demonstrated weak PUF solid-state circuit examples include memory-based PUF [6], classic ring oscillator based PUF [7] and current mirror based PUF [8]. In contrast, strong PUFs possess exponential CRP space. As it is practically infeasible to exhaust all the CRPs, strong PUFs are widely used for more versatile applications such as device authentication, cryptographic nonce and random number generation. As freshness of CRPs can be easily assured and the probability of collision decreases exponentially with increasing challenge-response length, strong PUFs can simplify peripheral protection and authentication protocol against replay attacks. The most well-known strong PUF is the arbiter PUF [9]. Owing to its low power dissipation and small footprint, it was first commercialized and integrated into RFID for chip authentication [10]. Arbiter PUF establishes a race condition by launching a pulse into two identical delay paths. Each segment of the two paths is a switch with either parallel or crossover connection selectable by the input challenge. The delays of the parallel and crossover connected segments are comparable and their deviation is solely determined by the manufacturing process variations, resulting in a slight difference in the travelling time of the pulse along the two paths. The response bit is generated by an arbiter at the endpoint, which can be either ‘1’ or ‘0’, depending on which path has a smaller propagation delay.

While more versatile in applications, the huge number of CRPs of strong PUFs also give rise to two major operation issues in arbiter PUF, which are the high bit error rate (BER) and poor uniqueness [11]. The 180 nm CMOS implementation of arbiter PUF is reported to have a native BER of 4.8% within a narrow operating temperature range of 40°C to 60°C and a uniqueness of only 23% [9]. To reduce the skew random distribution, Kumar *et al.* [12] buffers each path segment by current starved (CS) inverters in the arbiter PUF. Unfortunately, no physical implementation has been made to demonstrate the uniqueness of the PUF except that the path delay distribution with CS-inverters is simulated to have ∼3x and ∼15x increase in the mean and standard deviation than those using the regular inverters. Moreover, the simulated BER is still susceptible to temperature variation and remains high at 15% at 100°C. This response stability problem is mitigated in [13] by using CS multiplexers at the expense of doubling the number of transistors. Strong PUF has also been made from inverter ring with an even number of inverters. The bistable ring PUF (BR-PUF) [14] exploits the meta-stability of such an inverter ring, which will theoretically converge into either logic ‘1’ or ‘0’ with equal possibility. The BER of BR-PUF implemented on 9 *Xilinx Virtex-II Pro* FPGA boards is 5.81% with the temperature varying from room temperature to 85°C and the uniqueness is only 14.8% due to the biased layout. Yang *et al* [15] proposed a strong PUF that uses the oscillation collapse in a double edge injected ring oscillator. The output is determined by the accumulated delay that is different in each stage. The prototype implemented with a 40 nm CMOS process shows a good uniqueness of 50.07% but a poor equivalent native BER of as high as 23%. More recently, a low power diode-clamped inverter based strong PUF was proposed in [16]. It exploits the mono-stable status of the parallel diode-clamped inverters whose output is directly connected to the input. The prototype chip implemented by a 40 nm CMOS shows a native BER of less than 8% at 0.9∼1.3 V and −40∼90°C and a good uniqueness of 49.89%.

Strong PUFs based on linear additive delay architecture are generally vulnerable to machine learning attacks. At circuit level, the modeling complexity of arbiter PUF can be increased by, e.g., XOR arbiter PUF [7], feed-forward arbiter PUF [17], lightweight arbiter PUF [18] and multi-PUF [19], etc., without revamping the basic underlying PUF structure. Machine learning attacks can also be thwarted effectively at protocol level as exemplified by techniques such as slender PUF [20], noise bifurcation [21], reconfigurable latent obfuscation [22], [23] and lockdown [24]. The latter approaches [23], [24] turn the disadvantage of machine learnable arbiter PUF into an advantage for lightweight model-based authentication by making the strong PUF easy to learn during enrollment but infeasible upon deployment and/or restricting the number of authentication events to limit the number of CRPs from being learned by the attackers. However, they require the native strong PUF to be more reliable in the field to minimize the hardware overheads on error correction.

In this paper, we focus specifically on addressing the two main operational issues encountered by current physical implementation of the core arbiter PUF circuit. The uniqueness and reliability problems are solved simultaneously by a strong PUF that employs bias-controlled CS-inverters to boost the signal along the two symmetric delay paths and a new arbiter circuit. The CS-inverters are biased in the zero temperature coefficient point (ZTC) to make their propagation delay insensitive to temperature variation. As the charging/discharging current of CS-inverter is smaller than the regular inverter, the propagation delay difference in each stage of the arbiter PUF due to the manufacturing process variation is magnified while the power consumption is reduced with their active current limited by the biasing circuitry. Finally, a dedicated arbiter circuit is proposed to minimize the system bias. The proposed strong PUF improves the reliability and uniqueness of an existing strong PUF structure without introducing a new entropy source like [16]. The entropy source of [16] is introduced by the monostable output voltage of feedback stabilized single inverter ring.

Unlike the CS-inverter, the inverter used in [16] has a header and a footer diode-connected transistor. It is used to limit the large short circuit current of partially turned on PMOS and NMOS transistors of the monotstable inverter. The monostable strong PUF of [16] enhances its reliability by filtering out potentially unreliable response bits while this work biases the CS-inverters in the ZTC region to mitigate temperature induced delay deviations. The proposed PUF is taped out in a 65 nm CMOS process and their responses are measured to validate the performance improvements against existing physical implementation of strong PUFs based on similar linear additive delay architecture.

The rest of the paper is structured as follows. The temperature induced instability of arbiter PUF is analyzed in Section II. Section III presents the design and operations of the proposed strong PUF. The experimental results of the proposed PUF are shown and discussed in Section IV. Finally, the conclusion is drawn in Section V.

II. TEMPERATURE INDUCED INSTABILITY ANALYSIS OF ARBITER PUF

Temperature is an important environmental factor that has great influence on the performance of CMOS circuitries. It has been reported that every 15°C increase in local temperature will cause a 10∼15% increase in delay or skew locally [25]. While SKITTER (SKew+jITTER) circuit and guard band can be embedded into digital signal processors to address the timing uncertainty due to temperature fluctuation, they are not helpful in resolving the reliability problem on PUF circuits that explicitly utilize the random delay difference at minuscule scale for secret generation and protection. The responses of strong PUFs are particularly susceptible to temperature induced instability in view of the inordinate number of different combinations of pairs of comparable delay paths. In the classic arbiter PUF [9], the accumulated delay of each path is determined by the individual delay of every inverter stage. The propagation delay t_d of each inverter stage can be expressed as:

$$t_d = \frac{C_L V_{DD}}{\eta I_D} \tag{1}$$

where C_L and V_{DD} are the load capacitance and power supply voltage, respectively. η is a fixed parameter for a given inverter and I_D is the saturation current of MOSFET transistor. ηI_D defines the average output current of the inverter.

I_D can be expressed as:

$$I_D = \frac{\mu C_{OX} W}{2L}(V_{GS} - V_t)^2 \tag{2}$$

where W, L, V_{GS}, C_{OX}, V_t and μ are the effective channel width and length, gate-to-source voltage, gate capacitance, threshold voltage and charge carrier mobility, respectively.

From Eq. (2), the temperature coefficient of switching current (TCC) can be derived as follows [26]:

$$T_{CC} = \frac{1}{I_D}\frac{dI_D}{dT} = \frac{1}{\mu}\frac{d\mu}{dT} - \frac{2}{V_{GS} - V_t}\frac{dV_t}{dT} \tag{3}$$

Two parameters in Eq. (3) are temperature-dependent.

$$V_t(T) = V_t(T_0) - \sigma(T - T_0) \tag{4}$$

$$\mu(T) = \mu(T_0)(\frac{T_0}{T})^{\kappa} \tag{5}$$

where T_0 is the reference temperature, κ and σ are the mobility temperature exponent (1.2∼2) and the threshold voltage's temperature coefficient (0.5∼3mV/°C), respectively.

The threshold voltage $V_t(T)$ decreases with increasing temperature, resulting in an increased drain saturation current. On the other hand, the mobility of charge carriers also decreases with increasing temperature, which in turn reduces the drain saturation current. The reduction of carrier mobility is more prominent than the reduction of threshold voltage in the super-threshold operation region. Consequently, the delay of a regular inverter gate exhibits a positive correlation with temperature. Particularly, the relationship between the delay and temperature can be well-modelled by a linear function [27]. The arbiter PUF becomes unreliable as the linear functions of the two delay paths intercept at some temperature different from the reference temperature during response enrollment. As illustrated in Fig. 1(a), a reliable bit can be generated in the temperature range where the delay difference between the two paths in comparison is significantly large despite the fact that both path delays increase with temperature at different rates. Unfortunately, as shown in Fig. 1(b), the two delay paths can intersect over the working temperature range if their path delay difference is small. When this happens, the response bit generated by the two paths selected by the challenge can flip when the temperature varies. Due to the many different possible challenges of an arbiter PUF, this is very likely to happen, and the best solution is to make the delay of all paths after chip fabrication insensitive to temperature change.

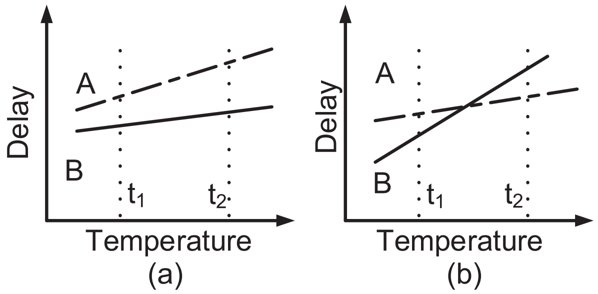

FIGURE 1. (a) Stable and (b) unreliable responses generated from the comparison of two timing paths over the operating temperature range.

The TCC in the super-threshold region has been analyzed above. Alternatively, if an inverter operates in the subthreshold region, its drain current $I_{D,sub}$ can be expressed as:

$$I_{D,sub} = \mu C_{OX}\frac{W}{L}\left(\frac{\kappa_B T}{q}\right)^2 (n-1)e^{\frac{q(V_{GS}-V_t)}{n\kappa_B T}}\left(1 - e^{-\frac{qV_{DS}}{\kappa_B T}}\right)$$

$$n = \frac{1 + (C_S + C_{it})}{C_{OX}} \tag{6}$$

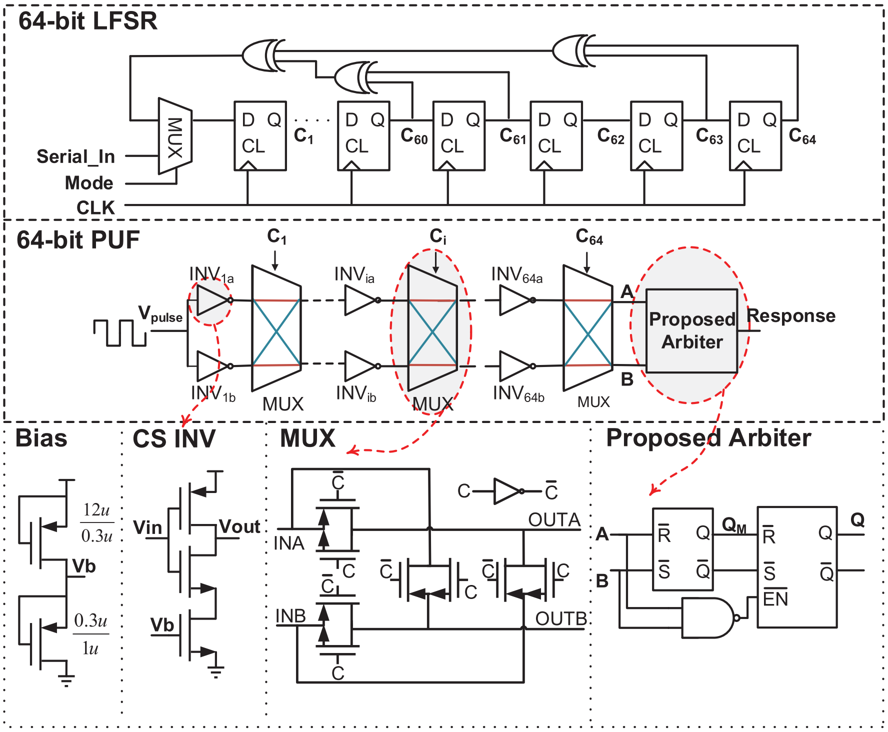

FIGURE 2. Schematic of the proposed strong PUF.

where C_S, C_{it} and C_{OX} are the capacitances of the semiconductor, the fast surface states and the oxide layer, respectively [26].

Then the TCC in the subthreshold region can be written as:

$$T_{CC,sub} = \frac{1}{\mu}\frac{d\mu}{dT} + \frac{2}{T} - \frac{q}{nk_BT}\left(\frac{dV_t}{dT} + \frac{V_{GS}-V_t}{T}\right) \tag{7}$$

Since the decrease in threshold voltage dominates the decrease in charge carrier mobility with increasing temperature in the subthreshold region, the value of $T_{CC,sub}$ is positive [26]. All in all, the delay of an inverter is positive in the super-threshold region and negative in the subthreshold region, which indicates a zero TCC can be achieved by appropriate biasing of the inverter. From [26], [28], the proper V_{GS} for ZTC can be approximated by:

$$V_{GS,ZTC} = V_t + 2\frac{dV_t}{dT}/\left(\frac{1}{\mu}\frac{d\mu}{dT}\right) \tag{8}$$

By substituting (8) and (2) into (1), the inverter delay at $V_{GS,ZTC}$ is given by:

$$t_{d,ZTC} = \frac{C_LV_{DD}L}{2\eta\mu C_{ox}W\alpha^2} \tag{9}$$

where $\alpha = \frac{dV_t}{dT}/(\frac{1}{\mu}\frac{d\mu}{dT})$. When the V_{GS} is biased at $V_{GS,ZTC}$, the inverter delay is almost immune to temperature variation. When the bias voltage is larger than $V_{GS,ZTC}$, TCC becomes negative and the delay increases with temperature. Conversely, when V_{GS} is smaller than $V_{GS,ZTC}$, TCC becomes positive and increase in temperature will shorten the delay.

III. PROPOSED STRONG PUF DESIGN

In this section, we propose an arbiter PUF that uses CS-inverters to alleviate the influence of temperature on response stability regardless of input challenges. Fig. 2 shows the schematic of the proposed design, which includes a linear feedback shifter register (LFSR), symmetric delay paths implemented with CS-inverters and a customized arbiter.

The LFSR serves as a stream cipher to randomize and obfuscate the input challenge C [29]. A 64-bit Fibonacci LFSR is implemented for a lightweight 64-bit strong PUF. Its reciprocal characteristic polynomial is $h(x) = x^{64} \oplus x^{63} \oplus x^{61} \oplus x^{60} \oplus 1$. Therefore, bit numbers 63, 61 and 60 are feedback to the input. The control signal *mode* is used to shift the seed into the LFSR through the external *Serial_In* port or enable the feedback loop to generate the internal challenges. For enhanced security, a multiple-input signature register (MISR) with reconfigurable feedback polynomial coefficients as in [23] can be used instead.

Each delay stage in the delay path is realized using two CS-inverters and a multiplexer (MUX). The MUX is used to keep or swap the path segment of the racing edge according to the input challenge bit. The delay of the MUX is ∼4.8 ps according to the simulation results obtained using the 65 nm process design kit (PDK) in Cadence Environment, while the delay from the CS-inverter is simulated to be ∼858.7 ps. As the stage delay is dominated by the CS-inverter, the delay deviation of the MUX is negligible and can be omitted. Hence the contributor of temperature induced instability of the path delay has been shifted from the MUX to the CS-inverter,

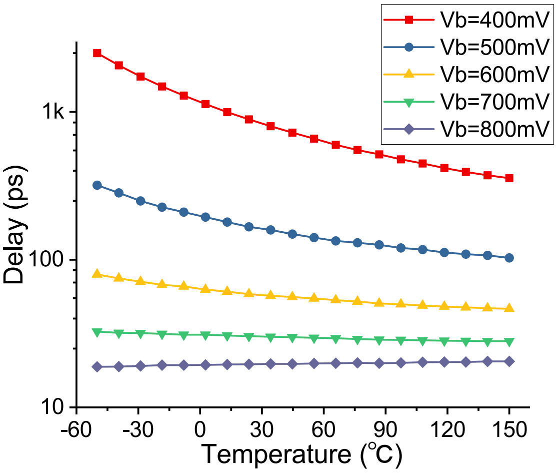

FIGURE 3. Simulated delay versus temperature for different V_b.

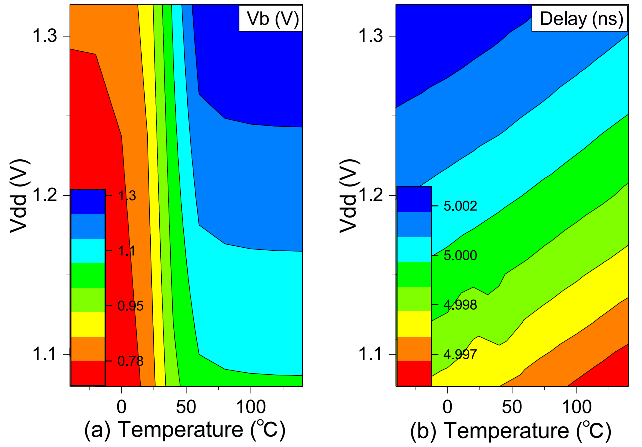

FIGURE 4. Monte Carlo simulation results of average V_b and delay of CS inverter against changes in temperature and supply voltage variations for 100 instances of CS inverter with biasing circuit.

whose delay dependence on temperature can be modeled more accurately and easily. As shown in the bottom left subfigure of Fig. 2, a CS-inverter is constructed by inserting an NMOS transistor into a regular inverter. The voltage V_b can be used to make the inverter work in different regions (e.g., subthreshold region or super-threshold region). Section II derives the existence of zero *TCC* for a CS inverter with an appropriate V_b bias. Fig. 3 shows the simulation results for the CS inverter's delay versus temperature plot when it is biased with different V_b. It is observed that the flattest delay over the entire range of temperature simulated is achieved at V_b of around 750 mV. This verifies that the ZTC operating point of the CS inverter is located between the superthreshold and subthreshold regions. The schematic of the common biasing circuit of the CS-inverters is also shown in the bottom subfigure of Fig. 2. It is biased at the ZTC point and shared with all the CS-inverters to minimize the silicon area. The width and length of the PMOS is 12 μm and 0.3 μm, respectively. The width and length of the NMOS is 0.3 μm and 1 μm, respectively. No post-manufacturing trimming is used to avoid extra control circuit, calibration program and operation costs. We also performance 100 runs of Monte Carlo simulation to verify the effect of PVT on the bias circuitry and the CS-inverter. The parameters for the simulation are extracted from the same PDK used for chip fabrication. The results are shown in Fig. 4. The results show that V_b can change with temperature and voltage but it saturates at the top-right corner (140 °C, 1.32 V). Nevertheless, the CS-inverter simulated together with the biasing circuit still exhibits a good stability against temperature and supply voltage variations. The maximum deviation is 7.05 ps, which is only 0.14% of its nominal delay.

In the classic arbiter PUF implementation, the arbiter is realized with the D flip-flop [9], which is illustrated in Fig. 5(a). However, this may not be a fair arbiter. A system bias is introduced into the design since the paths from D to Q and from CLK to Q are asymmetrical in the D flip-flop.

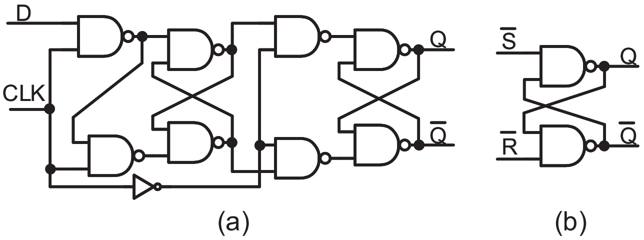

FIGURE 5. Schematic of the (a) D-flipflop, and (b) R-S latch.

In [30], the design is improved by using a RS latch as shown in Fig. 5(b), which has symmetric propagation delay between both inputs to the output and is area efficient. Nevertheless, the RS latch based on NAND gate has a forbidden state when $\overline{R} = \overline{S} =$ '0'. As both inputs may go high simultaneously thereafter. When a transition from the forbidden state to the rest state occurs, the state of the output will be unknown and unstable due to the propagation time difference between the two NAND gates (i.e., a race condition). This metastability problem can be mitigated by the proposed arbiter shown in the bottom right subfigure of Fig. 2, which employs two RS latches and a NAND gate.

Different from the RS latch in the first stage, the RS latch in the second stage has an extra active low enable input $\overline{EN}$. The truth table of the proposed arbiter is shown in Table 1. The latch in the second stage is enabled only when both inputs of the first latch are high simultaneously. Fig. 6 shows the timing diagram for the comparison of two raising pulses of width t_w using a conventional RS latch and the proposed arbiter. For high response throughput, t_w of the launching pulse should be kept short but long enough to cover the largest delay difference between the two timing paths. The proposed arbiter has significantly improved the reliability issues caused by the forbidden state of conventional RS latch arbiter while keeping t_w as small as possible. From Fig. 6, it is evident that the conventional RS latch arbiter has a narrow read window as the response flips during t_4, whereas stable

TABLE 1. Truth table of the proposed arbiter.

$\overline{R}$	$\overline{S}$	Q_M (Latch 1 output)	Q (Latch 2 output)
0	0	Forbidden state	Previous State
1	0	Set	Previous State
0	1	Reset	Previous State
1	1	Previous State	Q_M

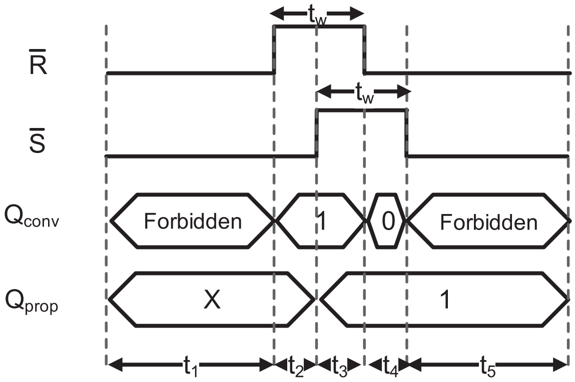

FIGURE 6. Timing diagrams of the RS latch and proposed arbiter.

response bit can be read by the proposed arbiter over the entire period between the rising edge of the late pulse in the current challenge till the rising edge of the early pulse of the next challenge. Besides, the RS latch is metastable when the two pulses arrive at both its inputs about the same time. The time required to resolve the metastable state and the final resolved state is unpredictable as it depends on both gate mismatch (due to process variation) and noise. This results in degraded reliability if noise dominates or increases systematic bias if process variation dominates. Our proposed arbiter mitigates the reliability degradation by enabling the second latch after a NAND gate delay in this case. This allows the small voltage difference built up by the mismatched gates to be amplified to a more reliable output by the second cross-coupled gate pair. As the NAND gate to the $\overline{EN}$ input of the second latch is lightly loaded and the transistors driven by the $\overline{EN}$ input is placed closer the output node, when one of $\overline{R}$ or $\overline{S}$ goes low at t_3, the second latch will be disabled before the output of the first latch Q_M changes. To reduce the systematic bias, the layout of the proposed arbiter is carefully designed (see Fig. 7(b)).

The timing waveforms of the PUF are plotted in Fig. 8. With reference to Fig. 2, when the *mode* signal is asserted high, the input challenge C_{in} is shifted serially through the *Serial_In* port into the LFSR as a seed in 64 clock cycles. After that, the *mode* signal is asserted low. An internal challenge C is produced by clocking the LFSR for N cycles. C is then parallelly output to the MUX select input of the PUF core to configure the two delay paths. A pulse is then launched simultaneously into the two paths through the first CS-inverter stage of the PUF. The pulses propagate along the two paths race against each other and the proposed arbiter is used to decide the winner and generate the random response bit ‘1’ or ‘0’ accordingly. A multi-bit response can be generated from an n-bit input challenge by generating multiple internal challenges through the LFSR. The number of cycles N used to generate the first internal challenge is an arbitrary user-defined integer. For a more latent obfuscation, the number of cycles to clock the LFSR to generate the next internal challenge for multi-bit response can be determined by a non-linear function of N and the response bit to the current internal challenge C.

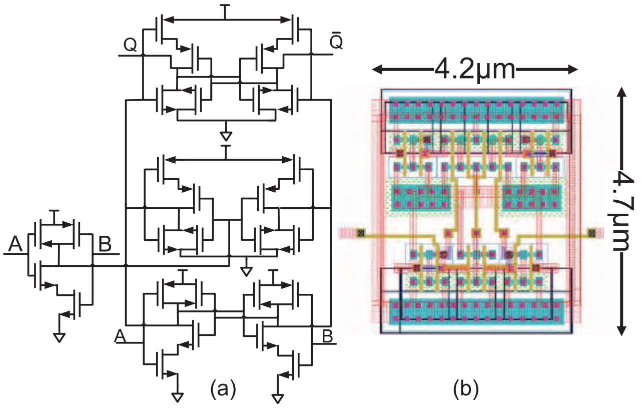

FIGURE 7. (a) Schematic, and (b) symmetrical layout of the proposed arbiter.

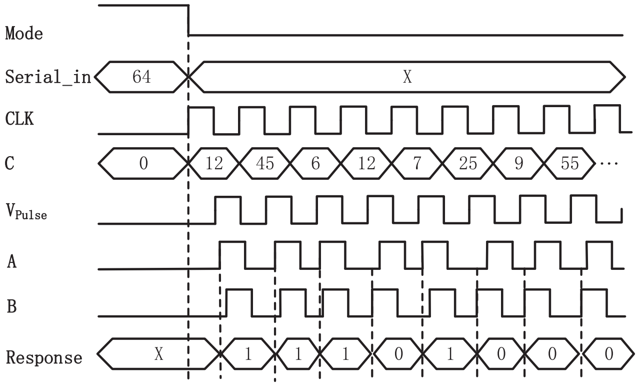

FIGURE 8. Simulated waveforms of proposed PUF.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

The proposed CS-inverter based strong PUF was successfully implemented using a standard 65 nm CMOS process. Ten dies were measured with the test setup shown in Fig. 9. Specifically, the temperature chamber (*Espec SU262*) is used to vary the temperature from −40°C to 150°C, and the different supply voltages are provided by the DC power supply (*Keysight E3631A*). The *Altera DE2* FPGA board is configured to generate the control signals to the PUF and capture the responses from the PUF. The raw response bitstreams are post-processed by the MATLAB scripts. Fig. 10 shows the microphotograph and the layout of the prototype chip, where the active area of the PUF design is reported to be 3838 μm^2. In the following subsections, the important

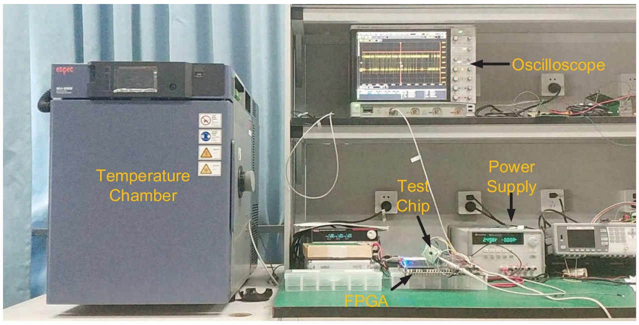

FIGURE 9. Chip measurement setup.

figures of merit (FoMs) for evaluating the PUF, including randomness, uniqueness, reliability, power/energy consumption and speed, are measured and analyzed.

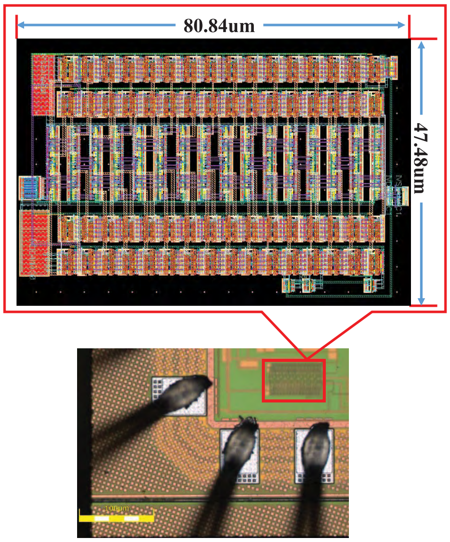

FIGURE 10. Microphotograph and layout of the proposed PUF.

A. UNIQUENESS

Uniqueness represents how distinguishable is the CRP of a PUF instance from those of other PUF instances. It is usually measured by the inter-chip Hamming distance (HD). The same challenge is applied to different PUF instances to generate different responses under the same environmental condition. The uniqueness is defined as [16]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \qquad (10)$$

where R_u and R_v are the response sets of the chips u and v, respectively. n is the number of response bits and m is the number of chip instances. The ideal value of uniqueness is 50%. Fig. 11(a) presents the measured HDs from 10 PUF chips under the nominal condition (1.2V and room temperature). A response bit stream of 128 bits is generated from each test chip. The histogram has a best-fit Gaussian of $\mu = 46.8\%$ and $\sigma = 18.3\%$. The measured σ is larger than the ideal value of $\frac{1}{2\sqrt{n}} = 4.42\%$ [31]. This insinuates the inherent difficulty in achieving good uniqueness from arbiter-PUF like structure. The average inter-die HD is calculated to be 46.86%, which is close to the ideal value, and significantly better than the uniqueness of 23.0% reported for classic arbiter PUF [9]. This higher uniqueness implies a smaller false acceptance rate (FAR), i.e., the chance of accepting a fake ID is lower [32]. To have a better statistical estimate of the uniqueness, Monte Carlo simulation is performed on 100 PUF design instances using the same technology PDK as that of the fabricated chips. As shown in Fig. 11(b), the uniqueness of these 100 instances is calculated to be 49.85%.

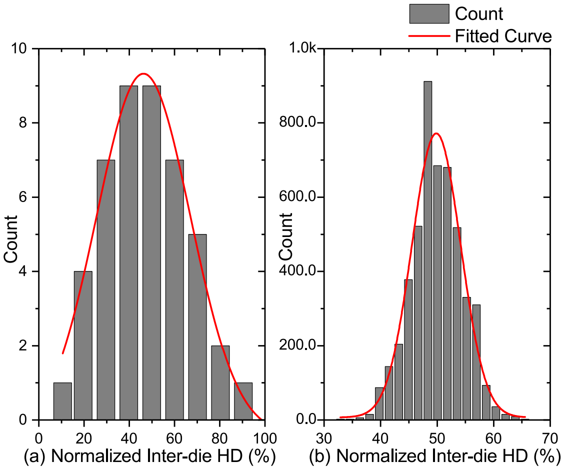

FIGURE 11. Frequency distribution of (a) measured and (b) simulated HD distances.

B. RANDOMNESS

Randomness measures the unpredictability of PUF's response. Standard randomness test suites, including NIST [33], DIEHARD [34], AIS.31 [35], ACF [36], etc. are available to evaluate the randomness of the sequence of response bits. NIST and ACF test suites are chosen for the evaluation of the generated PUF responses.

Table 2 lists the NIST test results of a 10 Mb random bitstream collected from the raw responses of ten test chips operating at 1.2 V and room temperature. The bit stream is grouped into ten data sets each of 1M bits. In NIST test, a P-value greater than 0.01 for each test is required to pass an arbitrary information source as random with a confidence level of 99% [33]. Most of the tests for the raw bit streams fail due to inevitable systematic bias of different delay stages, which is common for the raw response bits generated by most delay-based PUFs. Random extractor such as XOR post-processing, parity-based von Neumann entropy extractors [37], [38], LFSR-based hashing [39], [40], or keyed message digest, e.g., HMAC, CMAC or CBC-MAC is typically required to post-process the raw response bits to obtain a full-entropy key. We have also performed the NIST tests on the post-processed data using

TABLE 2. NIST test results for raw response data and post-processed data.

Tests	Raw Data		Post-processed Data	
	Pval	Prop	Pval	Prop
Frequency	Fail	0.2	0.534146	1.0
Block Frequency	Fail	0.4	0.350485	1.0
Cumulative Sums	Fail	0.2	0.066882	1.0
Runs	Fail	0.2	0.350485	1.0
Longest Run	Fail	0.4	0.350485	1.0
Rank	0.534146	1.0	0.534146	1.0
FFT	Fail	0.5	0.534146	1.0
Nonoverlapping Temp	Fail	0.3	0.350485	0.9
Overlapping Template	Fail	0.4	0.739918	1.0
Universal	Fail	0.4	0.350485	1.0
Approximate Entropy	Fail	0.3	0.534146	1.0
Random Excursions	-	1/1	-	4/5
Rand. Excursion Var.	-	0/1	-	4/5
Serial	Fail	0.4	0.350485	1.0
Linear Complexity	0.534146	1.0	0.911413	1.0

Neumann entropy extractor. The results in Table 2 show that the processed data pass all fifteen tests with P-values all larger than 0.01.

Autocorrelation function (ACF) is a mathematical tool capable of detecting the repetitive pattern of a target signal. Fig. 12 shows the auto-correlation result of 10,000,000 responses collected from the proposed PUF design. The maximum auto-correlation value does not exceed 0.2% with the confidence bound equal to 95%, which indicates its resilience against correlation analysis attack [36].

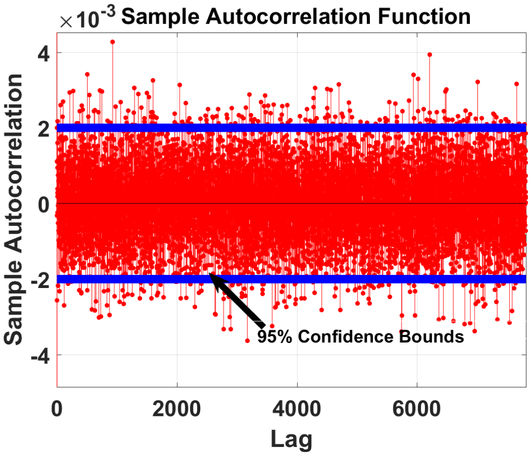

FIGURE 12. Auto-correlation measurements of 10M consecutive bits.

Another means to demonstrate the unpredictability of the PUF is to measure its min-entropy from the generated response bits. The min-entropy is a measure of the lower bound of the unpredictability of the response, i.e., the worst-case entropy. The min-entropy of a random variable X is defined as [41]:

$$H_\infty(X) = H_{\min}(X) = -\log p_{\max} \quad (11)$$

where $p_{max} = max(p_0, p_1)$ is the most likely outcome of a binary random variable X. p_0 and p_1 are the probabilities of occurrence of '0' and '1' bits, respectively. The min-entropy is calculated from a reasonably large sampling of 1,000,000 randomly generated CRPs across the ten test chips. Fig. 13 shows the measured min-entropy for all the ten dies. The average value of the min-entropy is calculated to be 0.77. It has been greatly improved from the min-entropy of classic arbiter PUF, which is reported to be around 0.01 for the ASIC implementation using TSMC 65nm CMOS process [41]. The low min-entropy of classic arbiter PUF is due to the systematic bias introduced by the arbiter and the correlation between the CRPs. The systematic bias has been significantly reduced by the larger process variability of the dominant delay of inverters in weak inversion operation.

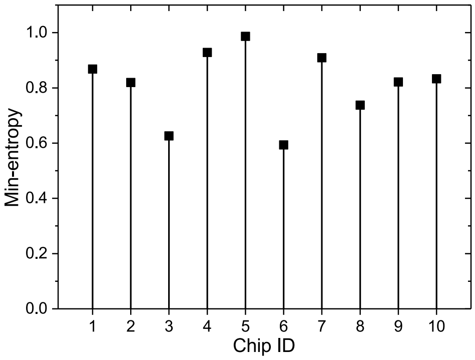

FIGURE 13. Min-entropy measured from ten PUF chips.

C. RELIABILITY

Reliability is an important quality that measures how reproducible or reliable are the CRPs generated by a PUF under different environmental conditions, which is typically formulated as:

$$R = 1 - BER = 1 - \frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i, R_{i,j})}{n} \times 100\% \quad (12)$$

where k is the number of times the same set of challenges are applied to the same PUF chip under different environmental conditions. The BER is calculated by the intra-die HD. R_i is the reference response measured at nominal working condition, while $R_{i,j}$ is a set of responses obtained by varying the temperature or supply voltage for the same chip and the same applied challenge. Fig. 14 presents the measurement results of the average BERs of the 10 PUF chips at temperature ranging from −40°C to 150°C, and the supply voltage ranging from 1.08 V to 1.32 V. The intra-die HD is calculated to be 0.8% by measuring the reference response 1000 times at the reference condition (i.e., 1.2 V and 27 °C). The worst-case BER is as low as 8.41% for the above-mentioned large temperature and supply voltage variations. These ranges of temperature and supply voltage are ∼ 7x and 5x larger than the temperature and supply voltage ranges, respectively for similar worst case BERs reported in the arbiter PUF in [9]. Compared with the BER of 4.8% at 40∼67°C and 3.7% at ± 2% power supply variation of the arbiter PUF in [9], our proposed design for the same temperature and supply voltage

TABLE 3. Summary of the measurement results and comparison with the state-of-the-art strong PUFs.

Metric	This work	TCAS-I'18 [16]	TVLSI'18 [42]	VLSI'17 [43]	ISSCC'15 [15]	JSSC'11 [44]	VLSI'04 [9]
Technology (nm)	65	40	180	130	40	90	180
Number of possible CRPs	$1.8\text{x}10^{19}$	$1.8\text{x}10^{19}$	$4.3\text{x}10^{9}$	$3.7\text{x}10^{19}$	$5.5\text{x}10^{28}$	$1\text{x}10^{25}$	$1.8\text{x}10^{19}$
Core area ($\mu m^2/L^2$)	0.91	2.94	0.16	2.64	0.52	4.32	45.33
Power (μW)	68.63	3.85	-	0.068	28.4	38	-
Native Energy/Bit (pJ/bit)	2.74	7.7	-	11	17.75	6080	-
Uniqueness	0.468	0.4989	0.4995	0.4990	0.5007	-	0.23
Intra-die HD	0.8%	0.85%	3.23%	-	1.01%	-	0.7%
Inter/Intra HD Ratio (Native)	60.75	58.7	15.5	-	49.6	-	32.86
ACF@95%	0.002	0.0089	-	-	0.0283	-	-
Bit Rate (Mb/s)	25	0.5	-	0.006	1.6	0.00625	20
Native worst case BER	10.46%	6.1%	8.1%	9.0%	9%	-	4.8%
Temperature Range (°C)	−40∼150	−40∼90	−40∼125	−20∼80	−25∼125	25∼125	40∼67
BER per 10°C	0.44%	0.47%	0.49%	0.9%	0.6%	NA	1.78%
Voltage Range (V)	1.08∼1.32	0.9∼1.3	1.5∼2.1	1.08∼1.32	0.7∼1.2	±10%	±2%

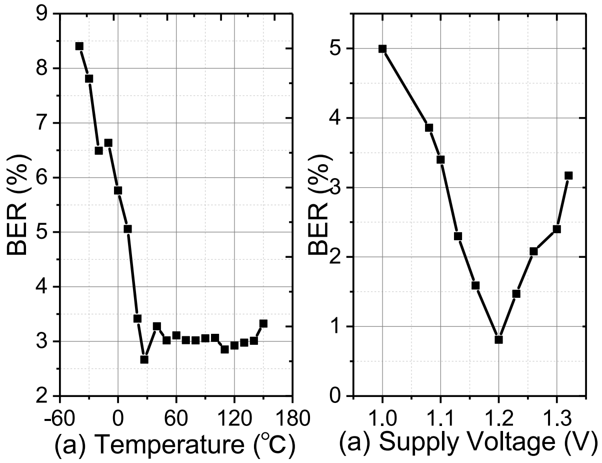

FIGURE 14. Measured average BERs of PUF responses against (a) temperature, and (b) voltage variations.

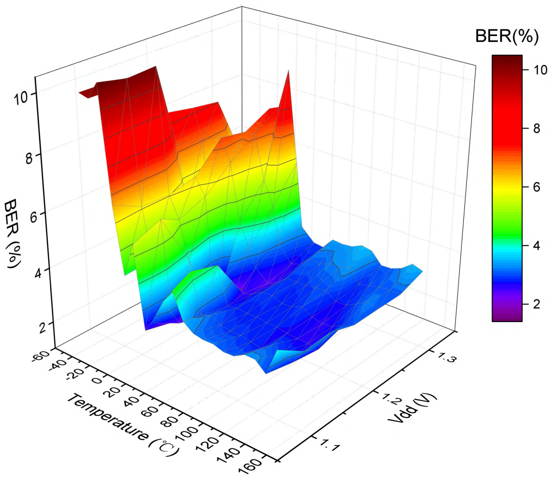

FIGURE 15. Measured BER over the temperature range from −40 to 150°C and supply voltage range of V_{DD} ±10%.

ranges has lower worst case BERs of around 3.2% and 0.8%, respectively.

We have also conducted more experiments to provide a 3D contour map for the BER over the temperature range from −40 to 150 °C and supply voltage range of V_{DD} ±10% as shown in Fig. 15. The measured worst-case BER is 10.46%, which occurs at −20°C and 1.08 V.

D. ENERGY EFFICIENCY

The power and energy consumption as a function of throughput are measured and presented in Fig. 16. The measured power consumption includes the PUF core and the peripheral circuitries such as I/O pads, buffers, etc. It is observed that the power consumption is proportional to the throughput, and the maximum working frequency is measured to be ∼25MHz. The minimum energy consumption converges at 2.74 pJ/bit at the maximum throughput.

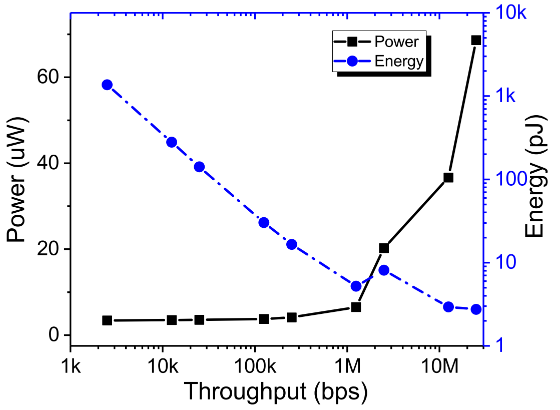

FIGURE 16. Measured power and energy consumptions versus throughput.

E. COMPARISONS

The performance of the proposed PUF are summarized and compared with the state-of-the-art strong PUFs in Table 3. Its core area normalized by the process technology is only slightly higher than [42] and [15], but otherwise it operates at a much faster bit rate and consumes much lower energy per bit than [15] and has orders of magnitude larger CRP space than [42] (bit rate and energy consumption are not reported in [42]). With a low raw response BER of 8.41% over a broader temperature range, it has the lowest normalized raw BER per 10°C of 0.44%. From the BER per 10°C, our design has the slowest BER degradation against temperature change. The proposed strong PUF is advantageous in terms of energy consumption and reliability. The chip consumes only 2.74 pJ/bit on average at the frequency of 25 MHz with the largest inter/intra die Hamming distance ratio of 60.75%. The energy efficiency could be further improved if more advanced process such as the 40 nm process is used. In addition, the proposed arbiter PUF implementation significantly improves the uniqueness of classic arbiter PUF implementation [9] of only 23.0%. Due to the inherent difficulty to fully eliminate the systematic bias from the delay elements of arbiter PUF, the improvement is closing in but not exceeding the uniqueness of other structures of strong PUFs in Table 3.

V. CONCLUSION

This paper presents a low power arbiter PUF design with high temperature stability. The delay cell in the PUF is implemented with the CS-inverter. The temperature reliability is greatly enhanced by biasing the inverter for ZTC. Besides, the working current is also limited by this requirement to exhibit an optimized energy efficiency of 2.74 pJ/bit. The proposed arbiter PUF design featuring low power consumption and high reliability is attractive for use in model-based authentication protocol [24] that requires a lightweight machine learnable arbiter PUF with better uniqueness and reliability. As hundreds of bits are generated per authentication, the two-stage RS latch arbiter has also significantly reduced the latency of each authentication by a more reliable read out of response bits to consecutive challenges input at a fast rate.

REFERENCES

[1] (Feb. 2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. [Online]. Available: https://goo.gl/UnHLV5

[2] C.-H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Circuits Syst. Mag.*, vol. 17, no. 3, pp. 32–62, 3rd Quart., 2017.

[3] C. Young. (Jan. 2018). *PUF Technology Protects Against Invasive Attacks*. [Online]. Available: https://www.maximintegrated.com/en/design/blog/puf-technology.html

[4] S. Satpathy, S. K. Mathew, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, R. K. Krishnamurthy, and V. K. De, "A 4-fJ/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS," *IEEE J. Solid-State Circuits*, vol. 52, no. 4, pp. 940–949, Apr. 2017.

[5] N. Menhorn. (Jun. 2018). *External Secure Storage using the PUF*. [Online]. Available: https://www.xilinx.com/support/documentation/application_notes/xapp1333-external-storage-puf.pdf

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

[7] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Automat. Conf. (DAC)*, San Diego, CA, USA, Jun. 2007, pp. 9–14.

[8] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9 –5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm," *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, Mar. 2016.

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

[10] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 58–64.

[11] Y. Cao, L. Zhang, S. S. Zalivaka, C.-H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for coherent sensor-level authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 11, pp. 2629–2640, Nov. 2015.

[12] R. Kumar, V. C. Patil, and S. Kundu, "Design of unique and reliable physically unclonable functions based on current starved inverter chain," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Jul. 2011, pp. 224–229.

[13] S. Wang, Y. Cao, and C. Chang, "A low-power reliability enhanced arbiter physical unclonable function based on current starved multiplexers," in *Proc. 14th IEEE Int. Conf. Solid-State Integr. Circuit Technol. (ICSICT)*, Oct./Nov. 2018, pp. 1–4.

[14] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2011, pp. 134–141.

[15] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A physically unclonable function with BER $< 10^-8$ for robust chip authentication using oscillator collapse in 40 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2015, pp. 1–3.

[16] Y. Cao, C. Q. Liu, and C. H. Chang, "A low power diode-clamped inverter-based strong physical unclonable function for robust and lightweight authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 11, pp. 3864–3873, Nov. 2018.

[17] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Identification and authentication of integrated circuits: Research articles," *Concurrency Comput., Pract. Exper.*, vol. 16, no. 11, pp. 1077–1098, Sep. 2004.

[18] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, Nov. 2008, pp. 670–673.

[19] Q. Ma, C. Gu, N. Hanley, C. Wang, W. Liu, and M. O'Neill, "A machine learning attack resistant multi-PUF design on FPGA," in *Proc. 23rd Asia South Pacific Design Automat. Conf. (ASP-DAC)*, Jan. 2018, pp. 97–104.

[20] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," in *Proc. IEEE Symp. Secur. Privacy Workshops*, May 2012, pp. 33–44.

[21] M.-D. Yu, D. M'Raïhi, I. Verbauwhede, and S. Devadas, "A noise bifurcation architecture for linear additive physical functions," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 124–129.

[22] Y. Gao, S. F. Al-Sarawi, D. Abbott, A. Sadeghi, and D. C. Ranasinghe, "Modeling attack resilient reconfigurable latent obfuscation technique for PUF based lightweight authentication," *CoRR*, vol. abs/1706.06232, pp. 1–14, Jun. 2017. [Online]. Available: http://arxiv.org/abs/1706.06232

[23] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, "Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 1109–1123, Apr. 2019.

[24] M. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A lockdown technique to prevent machine learning on pufs for lightweight authentication," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 3, pp. 146–159, Jul./Sep. 2016.

[25] M. Santarini. (Sep. 2005). *Thermal Integrity: A Must for Low Power IC Design*. [Online]. Available: http://www.edn.com/article/CA6255052.html

[26] E. Socher, S. M. Beer, and Y. Nemirovsky, "Temperature sensitivity of SOI-CMOS transistors for use in uncooled thermal sensing," *IEEE Trans. Electron Devices*, vol. 52, no. 12, pp. 2784–2790, Dec. 2005.

[27] E. Boemo and S. Lopez-Buedo, *Thermal Monitoring on FPGAs using Ring-Oscillators* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 1997.

[28] C. Q. Liu, Y. Cao, and C. H. Chang, "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 12, pp. 3138–3149, Dec. 2017.

[29] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 7, pp. 1143–1147, Jul. 2015.

[30] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in *Proc. ACM/IEEE Int. Symp. Low-Power Electron. Design (ISLPED)*, Aug. 2010, pp. 43–48.

[31] K. Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 2325–2328.

[32] C. Bhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York, NY, USA: Springer, 2012.

[33] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications, version revision 1a" NIST, Gaithersburg, MR, USA, Tech. Rep., 2010.

[34] G. Marsaglia. (2008). *The Marsaglia Random Number CDROM Including the Diehard Battery of Tests of Randomness*. [Online]. Available: http://www.stat.fsu.edu/pub/diehard/

[35] W. Killmann and W. Schindler, "A proposal for: Functionality classes for random number generators," BDI, Bonn, Germany, Tech. Rep. AIS 20/AIS 31, 2011.

[36] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[37] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, "A low-power true random number generator using random telegraph noise of single oxide-traps," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2006, pp. 1666–1675.

[38] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 12, pp. 3124–3137, Dec. 2010.

[39] D. J. Kinniment and E. G. Chester, "Design of an on-chip random number generator using metastability," in *Proc. 28th Eur. Solid-State Circuits Conf.*, Sep. 2002, pp. 595–598.

[40] M. Bucci and R. Luzzi, "Fully digital random bit generators for cryptographic applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 3, pp. 861–875, Apr. 2008.

[41] J. Delvaux, D. Gu, and I. Verbauwhede, "Upper bounds on the min-entropy of RO sum, arbiter, feed-forward arbiter, and S-ArbRO PUFs," in *Proc. IEEE Asian Hardw.-Oriented Secur. Trust (AsianHOST)*, Dec. 2016, pp. 1–6.

[42] Z. He, M. Wan, J. Deng, C. Bai, and K. Dai, "A reliable strong PUF based on switched-capacitor circuit," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 6, pp. 1073–1083, Jun. 2018.

[43] X. Xi, H. Zhuang, N. Sun, and M. Orshansky, "Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130 nm CMOS," in *Proc. Symp. VLSI Circuits*, Jun. 2017, pp. 268–269.

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

YUAN CAO (S'09–M'14) received the B.S. degree from Nanjing University, the M.E. degree from The Hong Kong University of Science and Technology, and the Ph.D. degree from Nanyang Technological University, in 2008, 2010, and 2015, respectively. His research interests include hardware security, silicon physical unclonable function, and analog/mixed-signal VLSI circuits and systems.

WENHAN ZHENG received the B.Eng. degree from the College of Electronics and Information Engineering, Shenzhen University, in 2017, where he is currently pursuing the M.S. degree. His current research interests include hardware security, physical unclonable function, and digital circuits and systems.

XIAOJIN ZHAO (S'07–M'10) received the B.Sc. degree from the Department of Microelectronics, Peking University, in 2005, and the Ph.D. degree from the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology (HKUST), in 2010, respectively. After one year of postdoctoral research work with HKUST, he joined Shenzhen University, in 2012, where he is currently an Associate Professor with the College of Electronics and Information Engineering. He has published over 75 international journal papers and refereed international conference papers. His research interests include CMOS monolithic polarization image sensor, gas sensor and their related hardware security when applied to the field of "Smart Internet of Things (IoT)." He has served as the Vice Chair and the Chair of the IEEE EDSSC Shenzhen Joint Chapter, from 2015 to 2019. He also served as the organizing and technical committee members in various IEEE conferences.

CHIP-HONG CHANG (S'92–M'98–SM'03–F'18) received the B.Eng. (Hons.) degree from the National University of Singapore, in 1989, and the M.Eng. and Ph.D. degrees from Nanyang Technological University (NTU), Singapore, in 1993 and 1998, respectively.

He has served as a Technical Consultant in industry prior to joining the School of Electrical and Electronic Engineering (EEE), NTU, in 1999, where he is currently an Associate Professor. He holds joint appointments with the university as the Assistant Chair of Alumni of the School of EEE, from 2008 to 2014, the Deputy Director of the Center for High Performance Embedded Systems, from 2000 to 2011, and the Program Director of the Center for Integrated Circuits and Systems, from 2003 to 2009. He has coedited four books, published ten book chapters, 100 international journal papers (two thirds are IEEE), and more than 170 refereed international conference papers (mostly in IEEE), and delivered over 40 colloquia. His current research interests include hardware security and trustable computing, low-power and fault-tolerant computing, residue number systems, and application-specific digital signal processing algorithms and architectures. He is a Fellow of the IET. He serves as the Associate Editor of the IEEE Transactions on Very Large Scale Integration (VLSI) Systems, since 2011, IEEE Access, since 2013, the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, the IEEE Transactions on Information Forensic and Security, since January 2016, the IEEE Transactions on Circuits and Systems-I, from 2010 to 2013, the *Integration, the VLSI Journal*, from 2013 to 2015, the *Springer Journal of Hardware and System Security*, since June 2016, and the *Microelectronics Journal*, since May 2014. He was the editorial advisory board member of the *Open Electrical and Electronic Engineering Journal*, from 2007 to 2013, and the *Journal of Electrical and Computer Engineering*, from 2008 to 2014. He has guest edited several special issues and has served in the organizing and technical program committee of more than 60 international conferences (mostly IEEE). He is a Distinguished Lecturer of the IEEE Circuits and Systems Society (2018–2019).