# A 1036 $F^2$/bit High Reliability Temperature Compensated Cross-Coupled Comparator Based PUF

Qiang Zhao, Yiheng Wu, Xiaojin Zhao, *Member, IEEE*, Yuan Cao, and Chip-Hong Chang, *Fellow, IEEE*

***Abstract*—In this paper, a compact physical unclonable function (PUF) based on cross-coupled comparator is presented. Featuring a positive feedback response generation mechanism, the mismatch in analog signals between the cross-coupled transistor pair is quickly amplified to prevent its polarity from flipping by the temporal noise. The rapid enlargement of noise margin by the sense amplifier also contributes to stabilizing the response against supply voltage variations. To improve its temperature stability, the counteracting effect of complementary-to-absolute-temperature (CTAT) and proportional-to-absolute-temperature (PTAT) drives are considered in sizing the bit cell transistors. The proposed design is fabricated in standard 65 nm CMOS process. The bit cell occupies an area of only 4.38 $\mu m^2$ (i.e. 1036 $F^2$), and the overall PUF chip consumes 2.98 pJ/bit at the throughput of 8 Mb/s, of which only 1.61 pJ/bit is due to the PUF's core. With the uniqueness measured to be 49.53%, the unpredictability of the fabricated PUF chips is validated by auto-correlation function and NIST randomness tests. Compared with the state-of-the-art implementations, the proposed PUF has the lowest native response instability of 1.46% with 500 repeated PUF readouts at 27°C and 1.2 V. By varying the operating temperature from −50°C to 150°C in step size of 10°C and the supply voltage from 1.0 V to 1.4 V in step size of 0.1 V simultaneously, the average reliability of the proposed PUF obtained from the 2D plot of all operating conditions is found to be 96.87% without correction and 99.31% with spatial majority voting (SMV).**

***Keywords*—Physical unclonable function, cross-coupled comparator, temperature compensation, low native instability, wide operating temperature range.***

## I. Introduction

THE evolution of hardware security research has recently moved away from chip identities generated and protected by key-based cryptographic algorithms towards hardware intrinsic root-of-trust. The manufacturing process variability of nano-scale devices, which used to have negative impact on circuit performance, is now leveraged for the generation of secure chip-unique identity without the need for the persistence presence of an on-chip secret key. As opposed to the speckle pattern based identity of optical physical unclonable function (PUF), where measurement and digitalization are performed externally, the response of solid-state circuit based PUF can be easily digitized and evaluated internally. As a security primitive, this promises the advantages of lightweight, low-power, fast response enrollment and low measurement cost [1]–[3]. The tamper-evident property of PUF and its ability to securely identify a device by interrogation without a permanent secret residence or well-defined algorithmic support largely reduce the risks of a number of powerful hardware attack vectors such as reverse engineering, probing and fault injection attacks on smart cards and security tokens [4]–[6]. In fact, PUF has been increasingly used with logic locking to avoid the security problem of key distribution [7], where the key for unlocking the circuit functionality is assumed to be stored locally in anti-tamper memory and protected by passive and active mesh against reverse engineering or externally input through secure communication link.

PUF is characterized by its challenge-response mapping mechanism. A PUF is useless once all its challenge-response pairs (CRPs) can be exhaustively extracted or predicted with high accuracy by the attackers. Therefore, from application and challenge-response interface protection perspectives, existing PUFs can be broadly categorized into strong PUF [8]–[17] and weak PUF [18]–[25] based on the growth of CRP space with the number of basic cells. It is in principle impossible to exhaust the challenges of a strong PUF within reasonable time of query due to its exponential CRP space. Hence, strong PUFs have been widely considered for secure lightweight device authentication before many of them were reported to be mathematically cloneable by emerging modeling attacks [26]. The relatively limited CRP space of weak PUFs makes modeling attacks irrelevant but also restricts their usage for authentication. Weak PUFs are typically adopted in key generation and device tagging applications. Until recently, weak PUF has become a popular mechanism to individualize ICs for logic and scan-chain locking, IC metering and pay-per-use IP licensing schemes [7], [27]–[29] that used to share a global chip key. The use of weak PUF as a key preprocessor in these design-for-trust techniques allows the designer of each IC (or even each IP) to derive an individual chip key for processing the unlocking information internally. Even the designer with the knowledge of the common key is not able to dictate the actual individual key of a specific chip until it is fabricated.

Unfortunately, real PUF circuits can produce erroneous responses upon deployment due to the change in environmental conditions. In [18], a logic gate structure based on the transistor offset voltage is used to construct a 128-bit chip ID using

This work was supported by Kongque Technology Innovation Foundation of Shenzhen (KQJSCX20170727101037551), Fundamental Research Foundation of Shenzhen (JCYJ20190808151819049), Singapore Ministry of Education Tier 1 grant MOE2018-T1-001-131 (RG87/18), and Natural Science Foundation of Jiangsu Province (BK20191160). *Corresponding author: Xiaojin Zhao.*

Q. Zhao, Y. Wu and X. Zhao are with the College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: eexjzhao@szu.edu.cn).

Y. Cao is with the College of IoT Engineering, Hohai University, Changzhou, China.

C. H. Chang is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798.

0.13 $\mu$m CMOS process. Based on the reported measurement results, even under the normal working temperature and supply voltage, up to 3% of instability (native unstable bits based on the PUF's raw output without any correction) were reported due to the random noise, and approximately 5.47% (7b) of error bits were detected over the temperature range of 0°C∼80°C. A cascode current mirror based PUF was proposed in [20]. Due to the inherent difference between NMOS and PMOS transistors of the current mirrors, the outputs are biased although the native instability has improved to 1.73%. Until recently, measurement results of physically fabricated weak PUF chips still suffer from a relatively high native instabilities of ∼27% [23], 5.62% [24] and 2.55% [25].

In order to mitigate the influence of temporal noise on the PUF's native reliability at a lower hardware cost than resorting to expensive and sophisticated error correction codes (ECC), temporal majority voting technique (TMV) is proposed in [19], [21]. Specifically, for the PUF based on voltage-compensated proportional-to-absolute-temperature (PTAT) voltage generators [21], bit error rates (BER) of 3.5% and 1.0% were reported over an operating temperature range of 0°C∼80°C and a supply voltage range of 0.6 V∼1.2 V [21], respectively. Due to the low native voltage mismatch between PTAT pairs (∼0.09 mV), an instability of as high as 6.54% was reported even at normal temperature and supply voltage. After 11 times of TMV, its instability at normal temperature/supply voltage condition has reduced to 2.00%. In [19], besides TMV, aging hardening and bit-masking are also introduced to further reduce the instability at normal condition by 10 folds (from 30% to 3%). Nevertheless, the abovementioned reliability improvements in [19] and [21] were achieved at the expense of significantly higher energy consumption per bit. Specifically, the energy consumptions of [19] and [21] were increased by ∼10× from 0.013 pJ/bit and 0.548 pJ/bit to 0.19 pJ/bit and 6.02 pJ/bit, respectively.

In this paper, the raw response stability problem of the aforementioned implementations is overcome by pre-amplifying the weak mismatched analog voltage/current signals of our proposed cross-coupled comparator PUF [30], which can be easily overwhelmed by the temporal noise before they are fed into the following digitizing circuitries. Meanwhile, the combined effect of complementary to absolute temperature (CTAT) and proportional to absolute temperature (PTAT) is also leveraged in the bit cell design to increase the immunity of PUF response generation process against thermal fluctuation. Specifically, with a small number of additional transistors per cell, the tiny mismatched voltages of the cross-coupled transistor pair that dictates the response bit state are boosted up by increasing the overall loop gain of the comparator. Together with the sense amplifier, the difference between the mismatched analog values enlarges instantaneously to a large noise margin. A 16×16 array of the proposed PUF cells is fabricated using a standard 65 nm CMOS process to validate the randomness, uniqueness and reliability of its raw response against temperature and supply voltage variations. The effectiveness of further reliability improvement by independent application of existing temporal majority voting (TMV), dark-bit detection (DBD) [23] and spatial majority voting (SMV) [31] error correction techniques with different controlling parameters are also evaluated and compared. In addition, due to the proposed optimized bit addressing scheme, the energy consumption of the entire circuitry is limited to 2.98 pJ/bit (of which 1.61 pJ/bit is contributed by the PUF core) at a throughput of 8 Mb/s.

The rest of this paper is organized as follows. Section II presents the proposed PUF implementation based on cross-coupled comparator with temperature compensation. The chip measurement results are presented, discussed and compared with the previous implementations in Section III. The paper is concluded in Section IV.

## II. Proposed Cross-Coupled Comparator Based PUF with Temperature Compensation

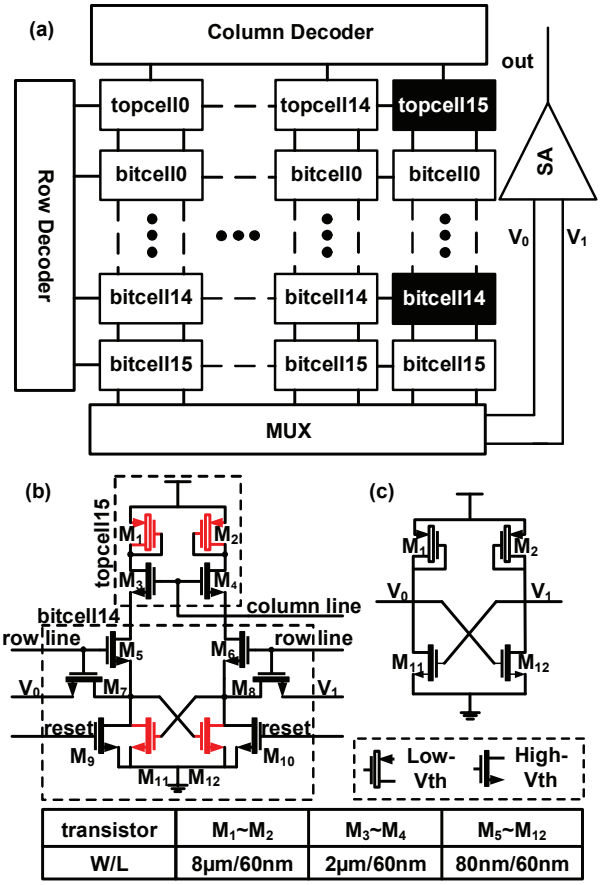


Fig. 1. (a) Architecture of the proposed PUF; (b) schematic of the top cell and bit cell; (c) simplified model of the PUF cell.

As shown in Fig. 1(a), the overall architecture of our design comprises a column decoder, a row decoder, 16 column units (CU), a sense amplifier (SA) and an analog multiplexer (MUX). Specifically, each column unit contains one top cell and 16 bit cells. To generate a response bit, the bit cells are selected in turn by the MUX, with the two output voltages ($V_0$, $V_1$) being compared by the sense amplifier. Fig. 1(b)

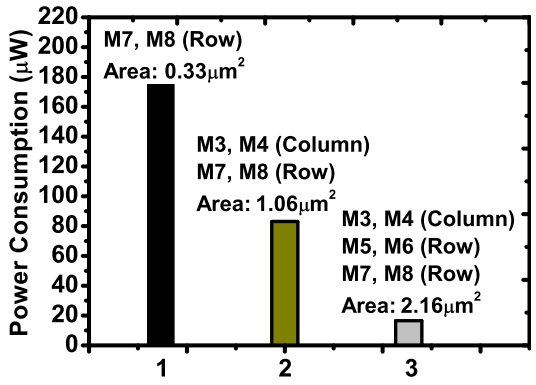


Fig. 2. Simulated static power consumptions: 1) with $M_7$ and $M_8$ only (174.88 $\mu$W); 2) with $M_3$, $M_4$, $M_7$ and $M_8$ only (88.62 $\mu$W); 3) with $M_3 \sim M_8$ (16.52 $\mu$W).

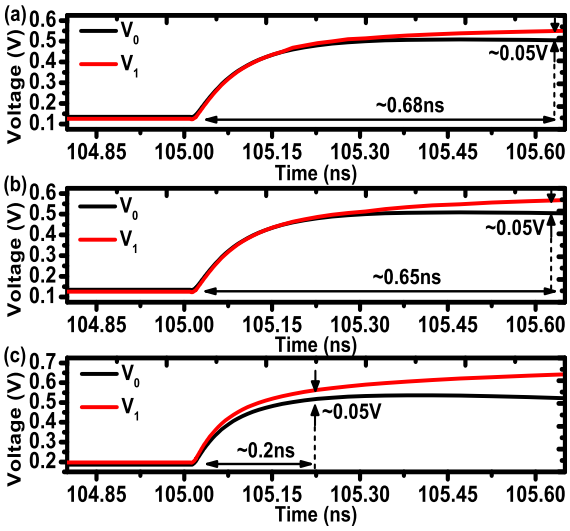


Fig. 3. (a) Regeneration process with $M_7$ and $M_8$ only; (b) regeneration process with $M_3$, $M_4$, $M_7$ and $M_8$ only; (c) regeneration process with $M_3 \sim M_8$.

illustrates the schematic of each bit cell, which has a compact footprint of 4.38 $\mu$m$^2$ (i.e. 1036 $F^2$). It includes 8 minimum-sized NMOS transistors ($M_5 \sim M_{12}$), where $M_5 \sim M_8$ are access transistors, $M_9$ and $M_{10}$ are reset transistors, and the cross-coupled transistors with positive feedback $M_{11}$ and $M_{12}$ are the main entropy source.

Typically, only $M_7$ and $M_8$ in Fig. 1(b) are needed as the access transistors for row selection. However, with only $M_7$ and $M_8$, the cross-coupled structure adopted in this design dissipates a substantially high static power consumption of 174.88 $\mu$W, as shown in Fig. 2. In addition, the current flowing through each top cell is equally divided by the 16 bit cells in the same column, resulting in a slow regeneration process. By adding $M_3$ and $M_4$, the static power consumption can be reduced to 88.62 $\mu$W, as shown in Fig. 2. However, the regeneration speed is not improved, as illustrated in Fig. 3(a) and (b). To address this issue, we introduce two more access transistors, $M_5$ and $M_6$. High threshold voltage (HVT) transistors are used for $M_3 \sim M_6$. As depicted in Fig. 2 and Fig. 3(c), with $M_3 \sim M_6$ added, the regeneration process is 3.3$\times$ faster, and the static power consumption has been dramatically reduced from 174.88 $\mu$W to 16.52 $\mu$W. In fact, these added transistors ($M_3 \sim M_6$) serve as both access transistors and power gating transistors, which account for the reduced power consumption with only one bitcell activated to produce one PUF bit.

As presented in Fig. 1(c), the simplified model of the PUF structure, without reset and access transistors, is composed of the cross-coupled transistors $M_{11}/M_{12}$ and a pair of top cell PMOS transistors $M_1/M_2$. The cross-coupled structure with two stable $V_0/V_1$ states (i.e., $V_0$ $XOR$ $V_1$ = 1) can be initialized into metastable states using a pair of top cell PMOS transistors $M_1$ and $M_2$ with the same size. Due to the inherent current mismatch of transistors $M_{11}$ and $M_{12}$, the metastable states are eventually resolved into stable states. Specifically, the process variation of the four transistors, $M_1$, $M_2$, $M_{11}$ and $M_{12}$, introduces an intrinsic bias that converts the metastable state to a stable state of either ($V_0$ = 0, $V_1$ = 1) or ($V_0$ = 1, $V_1$ = 0) [32]. Meanwhile, the cross-coupled structure also provides a positive feedback to speed up the stabilization process. When a bit cell is selected, the top cell starts to charge the bit cell. At this stage, the gate voltages of the transistors, $M_{11}$ and $M_{12}$, are close to 0. So the transistors $M_{11}$ and $M_{12}$ are biased at the subthreshold region. As the bit cell is charged continuously, the rise of $V_0$ and $V_1$ corresponds to a drop in $|V_{gs}|$ of the top cell transistors, which pushes the top cell transistors to the subthreshold region and eventually turns off one of them. Suppose $M_1$ is turned off, $M_2$ continues to charge the serially connected transistor $M_{12}$ to increase $V_{ds12}$ = $V_1$ until $M_{11}$ is turned on ($V_{ds12}$>$V_{th11}$). Then $V_0$ and $V_1$ are well separated as shown in Fig. 4. Before $M_1$ is turned off, the values of $V_0$ and

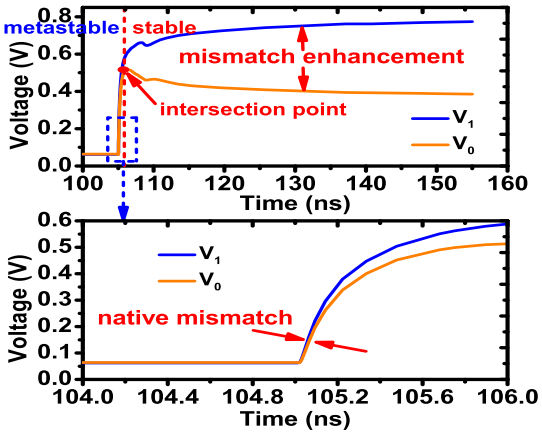


Fig. 4. Positive feedback based native reliability enhancement mechanism of the proposed PUF implementation.

$V_1$ can be calculated using the subthreshold region equation:

$$I = \mu C_{ox}\frac{W}{L}(m-1){V_t}^2 exp\left(\frac{V_{gs}-V_{th}}{mV_t}\right) \times\left(1-exp\left(-\frac{V_{ds}}{V_t}\right)\right) \tag{1}$$

where $\mu$ is the carrier mobility, $C_{ox}$ is the sheet oxide-capacitance density, $W/L$ is the width to length ratio of the transistor, $m$ is the sub-threshold slope factor, $V_{gs}$ and $V_{ds}$ are the gate-source and drain-source voltages, respectively, $V_{th}$ is the threshold voltage and $V_t$ is the thermal voltage.

Since the top cell and the bit cell are connected in stack, the values of $V_0$ and $V_1$ can be calculated as follows:

$$V_0 = V_{dd} - V_{al} + \underbrace{\left(\frac{m_1}{m_{11}}V_{th11} - |V_{th1}|\right)}_{CTAT} - \frac{m_1}{m_{11}}V_1 + \underbrace{\left(m_1 V_t ln\frac{(\mu C_{ox}\frac{W}{L}(m-1))_1}{(\mu C_{ox}\frac{W}{L}(m-1))_{11}}\right)}_{PTAT} \tag{2}$$

$$V_1 = V_{dd} - V_{ar} + \underbrace{\left(\frac{m_2}{m_{12}}V_{th12} - |V_{th2}|\right)}_{CTAT} - \frac{m_2}{m_{12}}V_0 + \underbrace{\left(m_2 V_t ln\frac{(\mu C_{ox}\frac{W}{L}(m-1))_2}{(\mu C_{ox}\frac{W}{L}(m-1))_{12}}\right)}_{PTAT} \tag{3}$$

where $V_{al}$ and $V_{ar}$ are the drain-source voltages of the left and right access transistors, $M_5$ and $M_6$, respectively. According to our simulation results, $V_{al}$ and $V_{ar}$ are close to each other with a difference of around 10 mV. Considering that $V_{ds}$ of the device is typically larger than 200 mV, the dependence of subthreshold drain current on $V_{ds}$ can be ignored. Besides, $M_{11}$/$M_{12}$ are designed with minimum size HVT transistors to maximize the native entropy. With optimized transistor size for the top cell transistors, the CTAT and PTAT terms in Eq. (3) counteract each other to minimize the temperature dependence of $V_0$ and $V_1$. Except for $M_5$∼$M_{12}$, whose W/L were kept at 80nm/60nm to minimize the PUF cells area, $M_1$∼$M_4$ in the top cell were sized for the minimum temperature instability. To determine the sizes of these transistors, *Monte Carlo* (MC) simulations were conducted for different transistor sizes at each temperature point to extract sufficient PUF bits. The temperature coefficient (TC) and BER for each transistor width were calculated and shown in Fig. 5. The sizes of $M_1$∼$M_4$ that have the lowest TC and BER were selected.

Let $\Delta V_{out}$ be the difference between $V_0$ and $V_1$. It can be calculated as follows:

$$\Delta V_{out} = \underbrace{(V_t \Delta K)}_{PTAT} - (V_{al} - V_{ar}) - (\frac{m_1}{m_{11}}V_1 - \frac{m_2}{m_{12}}V_0) + \underbrace{\left(\underbrace{\left(\frac{m_1}{m_{11}}V_{th11} - \frac{m_2}{m_{12}}V_{th12}\right)}_{Bias_{bitcell}} - \underbrace{(|V_{th1}| - |V_{th2}|)}_{Bias_{topcell}}\right)}_{CTAT} \tag{4}$$

$$\Delta K = m_1 V_t ln\frac{(\mu C_{ox}\frac{W}{L}(m-1))_1}{(\mu C_{ox}\frac{W}{L}(m-1))_{11}} - m_2 V_t ln\frac{(\mu C_{ox}\frac{W}{L}(m-1))_2}{(\mu C_{ox}\frac{W}{L}(m-1))_{12}} \tag{5}$$

Eq. (4) indicates that the temperature dependent terms are well compensated and the dependence of $\Delta V_{out}$ on the supply voltage is largely reduced. Moreover, $\Delta V_{out}$ is dominated by the difference between the threshold voltages of $M_{11}$ and $M_{12}$ instead of the top cell transistors, $M_1$ and $M_2$, which are shared by each column. To further minimize the mismatch originating from the top cell transistors, $M_1$ and $M_2$, we upsize the top cell transistors ($M_1$∼$M_4$), then split them into smaller sizes and connect them together in a common-centroid layout style.

Device parametric variation due to fabrication process, such as threshold voltage of the transistor, is typically modelled by normal distribution $N(\mu,\ \sigma^2)$ with mean and variance governed by the process technology [33]. Theoretically, as the $V_{th}$ distributions of the two bottom transistors, $M_{11}$ and $M_{12}$, are the same, $\Delta V_{out}$ also follows a normal distribution with zero mean and twice the variance. However, the mismatched voltages/currents generated by the two adjacent transistors are very small initially, and can be easily perturbed by noise. $\Delta V_{out}$ becomes stable when the difference between

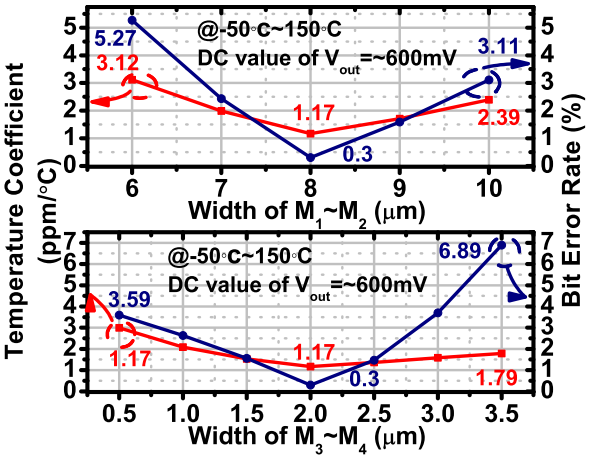


Fig. 5. The simulated temperature coefficient and bit error rate versus different transistor sizes of $M_1$∼$M_4$.

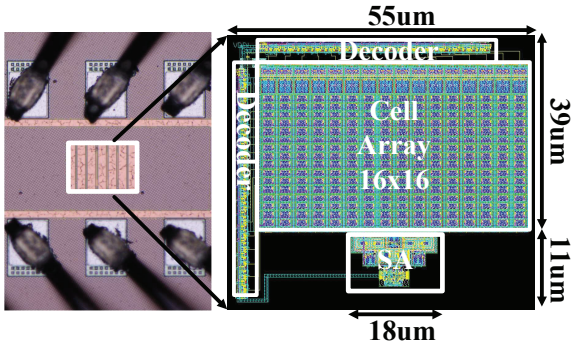


Fig. 6. Microphotograph and layout of the fabricated PUF chip prototype.

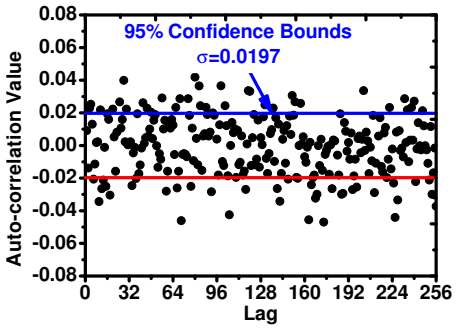


Fig. 7. Auto-correlation results of 2560 consecutive bits obtained from 10 PUF chips.

$V_0$ and $V_1$ increases beyond the noise. As shown in Fig. 4, the proposed positive feedback mechanism quickly amplifies this mismatch induced metastable $\Delta V_{out}$ before it can be overturned by temporal noise to improve the robustness of the entire structure. As temporal noise is a random process with time-varying amplitude and phase, by ramping up the noise margin of $\Delta V_{out}$ fast enough during the PUF bit generation cycle, the probability of temporal noise inflicted error bit is significantly reduced. Finally, a sense amplifier is used to generate the rail-to-rail digital output at the earliest, according to the stable output state of the cross-coupled comparator structure. The sense amplifier adopted in our design is formed by three cascaded differential amplifiers, which has a gain of 64.5dB and a bandwidth of 9.73MHz.

## III. Experimental Results

The proposed implementation was fabricated using standard 65 nm CMOS process. Fig. 6 shows both the microphotograph and layout of the fabricated prototype, which features a compact overall silicon area of 2533 $\mu m^2$. Each bit cell occupies an area of 4.38 $\mu m^2$. Including all the peripheral circuitries such as the decoders, sense amplifier and the top cells shared by each column, the chip area per PUF bit is calculated to be 9.89 $\mu m^2$. In the following subsections, the proposed PUF implementation is evaluated based on the widely-adopted figures of merit, including unpredictability/randomness, uniqueness and reliability/instability. TMV, DBD and SMV are commonly used lightweight error correction schemes for reliability improvement of PUF. To evaluate the extent of reliability enhancement achievable by our proposed PUF by these schemes, they are implemented off-chip on FPGA board and Matlab program on PC as in [19]–[24].

TABLE I. NIST SP800-22 test results based on the outputs generated by the fabricated PUF chips.

| Test Item | Stream length | No. of runs | P_VALUE | Pass (%) | Pass? |
|---|---|---|---|---|---|
| Frequency | 256 | 10 | 0.911413 | 100 | YES |
| Block Frequency | 256 | 10 | 0.213309 | 100 | YES |
| Cumulative Sums | 256 | 10 | 0.739918 | 100 | YES |
| Runs | 256 | 10 | 0.534146 | 100 | YES |
| Longest Run | 256 | 10 | 0.350485 | 100 | YES |
| FFT | 256 | 10 | 0.122325 | 100 | YES |
| Approximate Entropy | 256 ( $m$ = 3 ) | 10 | 0.350485 | 100 | YES |
| Serial | 256 ( $m$ = 3 ) | 10 | 0.739918 | 100 | YES |

### A. Unpredictability

The widely-adopted auto-correlation function (ACF) and NIST SP800-22 test suite [34] for entropy test are used to evaluate the unpredictability of the proposed implementation. As shown in Fig. 7, a 2560-bit (10 chips×256 bit) data stream obtained from 10 test chips was sent for ACF test, and the auto-correlation result $\sigma$ was calculated to be 0.0197 with 95% confidence interval. The small $\sigma$ value obtained from the auto-correlation test results implies that the data stream generated by our proposed PUF has high randomness [32], and is less vulnerable to correlation analysis attacks.

In addition, the 2560 raw CRPs without any pre- and post-processing were also input to NIST test suite to further evaluate their randomness. The results are summarized in Table I. The P-value of each test must be greater than 0.01 in order for the bitstream to be considered as random. Due to the limited number of test chips and CRP space of weak PUF, the size of the raw response bit stream collected from the PUF chips is insufficient to carry out some NIST tests such as "*Binary Matrix Rank*", "*Linear Complexity*", "*Overlapping Template Matching*", "*Universal Statistical*", "*Random Excursions*" and "*Random Excursions Variant*", which require much larger data bit stream. Given the results of Table I from the raw PUF responses for all NIST tests that can be conducted with this length of bitstream, it demonstrates that the response generated by each bit cell is independent and identically distributed.

Moreover, the spatial uniformity of the response bits due to the combined effect of inter- and intra- die variations is visualized by the 2D map in Fig. 8. Each pixel of a 2D map represents the average value of the response bits of a cell measured from 20 different chips for Fig. 8(a), 20 MC simulated cell instances for Fig. 8(b) and over 1000 MC simulated cell instances for Fig. 8(c). The average response bit value between 0 and 1 of each cell is quantized into 10 equal intervals and represented by 10 different color intensities. The mean $\mu$ and standard deviation $\sigma$ of each of the array of 16×16 cells are computed to be ($\mu$, $\sigma$) = (0.498, 0.063) for 20 chips, (0.507, 0.073) for 20 MC instances and (0.5006, 0.0142) for 1000 MC instances. The cells that fall outside the 95% confidence interval are marked in each plot by using

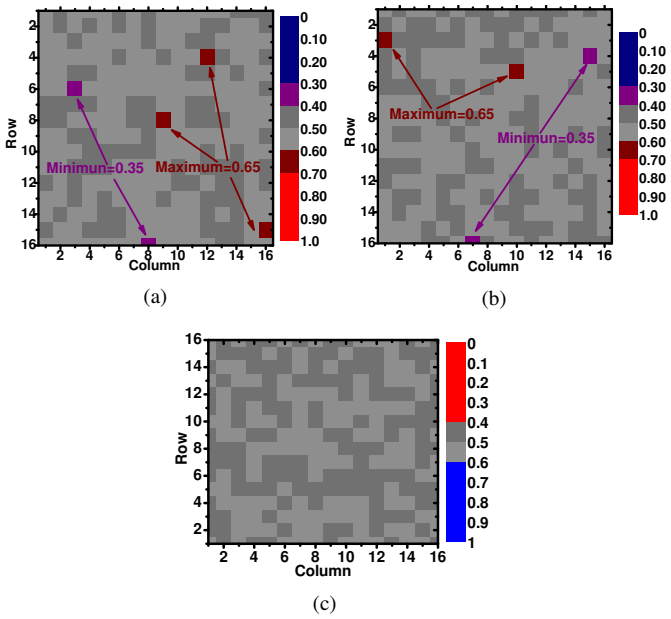


Fig. 8. (a) Average outputs of the PUF arrays of 20 test chips; (b) average outputs of the PUF arrays based on 20 pre-layout MC simulation runs; (c) average outputs of the PUF arrays based on 1000 pre-layout MC simulation runs.

different intensities of red color for average cell response bit values that fall in the range from 0 to $\mu - 2\sigma$ and different intensities of blue color for average cell response bit values that fall in the range from $\mu + 2\sigma$ to 1. The percentages of cells that fall within $\pm 2\sigma$ are equal to 98.0%, 98.4% and 95.7% for 20 chips, 20 and 1000 MC instances, respectively. The results indicate the measured average response bit values are not significantly deviated from the simulation results with good uniformity as more than 95% of the cells have deviation bounded within $2\sigma$. MC simulation with larger sample size has a more uniform distribution across all cells in the array and better approximates the population mean. To check if there is significant difference between the 256 average response bits measured from the 20 chips and those simulated by the 1000 MC instances, a two-tails Welch's T test is conducted with the null hypothesis $H_0$ of $\mu_1 = \mu_2$, the significant level $\alpha = 0.05$ and outliers included. Since the $p$-value equals $0.197835 > \alpha$, $H_0$ is accepted, signifying that the difference between the average response bits of the two populations is not big enough to be statistically significant.

Meanwhile, the row and column averages of the digital outputs of 20 test chips and 20 MC simulated instances are plotted in Figs. 9(a) and (b), respectively. For a binomial distribution with $p$ = 0.5, $n$ = 320 for $20 \times 16$ rows/columns. The standard deviation can be calculated as $\sqrt{np(1-p)}$ = 8.944, which correspond to 2.80% of 320 bits. The dashed lines on each plot mark the boundaries 0.5±0.028. The variations of the row and column averages of both plots are bounded by the calculated standard deviation, which show an excellent statistical agreement between the measured and simulation results.

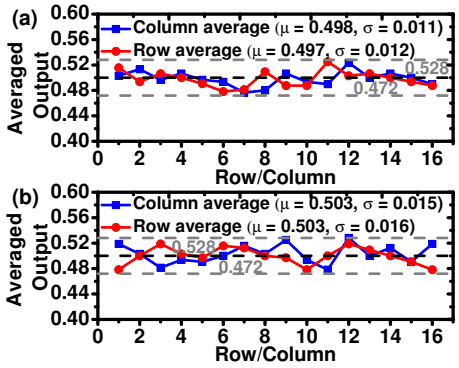


Fig. 9. Average digital output values per row and per column generated from (a) 20 test chips; (b) 20 pre-layout MC simulation runs.

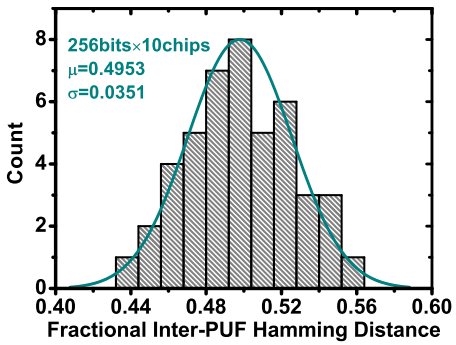


Fig. 10. Measured inter-PUF HDs across 10 PUF chips.

The absence of strong gradient change in the row average and the column average shows that systematic deviation has been greatly reduced. The insignificant fluctuation of these average values around 0.5 indicates that the effect of the mismatch in the top cell transistors has been successfully eliminated by the optimized size and common-centroid layout. It corroborates that the term $Bias_{topcell}$ in Eq. (4) is negligible compared with $Bias_{bitcell}$ and can thus be ignored.

### *B. Uniqueness Measurement*

The uniqueness of the proposed PUF design is evaluated by the inter-PUF Hamming distance (HD). The inter-PUF HD is defined as the HD between the outputs of two different PUF chips operating at the reference temperature and supply voltage (which is 27 °C and 1.2 V for our tests). The ideal inter-PUF HD is 50%. Let $R_u$ and $R_v$ be the $n$-bit responses of two different chips to the same challenge, respectively, the uniqueness can be calculated by taking the average HD of $n$-bit responses between different pairs of $m$ PUF chips normalized by the response bit length $n$ as follows [2]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \qquad (6)$$

For 10 test chips, $m$ = 10. Since a 256-bit response is generated by each test chip, $n$ = 256. The histogram of the

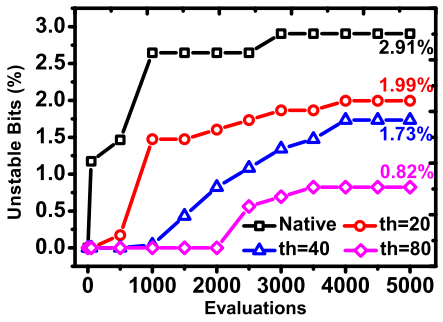


Fig. 11. Fraction of native unstable bits detected by different error thresholds.

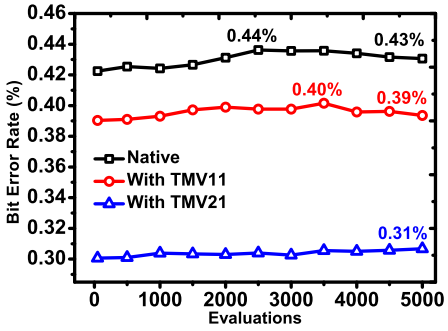


Fig. 12. Measured native BER with/without TMV under normal condition.

fractional HD values calculated from ${}^{10}C_2$ = 45 pairs of 256-bit response is plotted in Fig. 10. The distribution of the fractional inter-PUF HDs measured from 10 PUF chips exhibits a binomial distribution. The mean $\mu$ and standard deviation $\sigma$ of the best-fit Gaussian curve to the histogram are found to be 49.53% and 3.51%, respectively.

### C. Reliability Characterization

Reliability is characterized by the cumulative instability (i.e., proportion of locations that have at least one error occurred across all evaluations) and the instantaneous instability (i.e., the BER) in previous implementations [22], [25]. In order to quantify the PUF's instability against temporal noise, the outputs of 10 PUF chips are read up to 5000 times and averaged under normal operating condition.

As shown in Fig. 11 and Fig. 12, the worst-case fraction of unstable bits of the native PUF is measured to be at most 1.46% for 500 evaluations and 2.91% for 5K evaluations, and the worst-case BER is 0.44%. By setting the threshold (th) in the number of errors over 5K evaluations to 20, 40 and 80 to classify a bit location as unstable, the unstable bits are further reduced to 1.99% (th = 20), 1.73% (th = 40) and 0.82% (th = 80), respectively, as shown in Fig. 11.

In a $v$-way TMV (TMV-$v$), the PUF bit is computed by the mean response within a voting window $v$, where $v$ is an odd integer determined by the non-zero response bit flip probability. TMV-$v$ is implemented as follows: 1) The PUF bit is read out $v$ times by applying the same challenge. 2) The $v$ output bits ('1' or '0') are accumulated by a counter. The PUF response bit is 1 if the counter output is larger than $(v-1)/2$, and 0 otherwise. 3) The steps are repeated for 256 different challenges to form a 256-bit PUF response. The BERs at different environmental conditions are calculated based on the majority-voted PUF bit strings. Fig. 12 shows that with TMV, the worst-case BER of the native response has been reduced to 0.40% and 0.31% for TMV11 and TMV21, respectively. For comparison, the BER for TMV31 is also calculated, which is very close to that for TMV21. It shows that the reliability improvement saturates with the increase in frequency for majority voting.

In order to measure the reliability of the proposed PUF against temperature variation, the fabricated PUF chips were challenged under various operating temperature and the digital responses were recorded to calculate the BER:

$$BER = 1 - Reliability = \frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i, R_{i,j})}{n} \times 100\% \quad (7)$$

where $R_i$ is an $n$-bit response produced by a PUF chip $i$ under normal operating condition (27°C) and a set of input challenges, $C$. Then the same set of challenges is applied $k$ times to the same PUF under varying operating temperature ranging from $-50$°C to 150°C to obtain the responses $R_{i,j}$ for $j = 1, 2, \cdots, k$. Each bit of the reference $n$-bit response $R_i$ of Eq. (7) is obtained by a single measurement under normal operating condition. The average of multiple measurements was only adopted for TMV based error correction. In TMV-$v$, each bit of the reference response $R_i$ is obtained by the average of $v$ measurements with the same challenge at normal operating condition. As shown in Fig. 15, the average native BER measured from 10 PUF chips is found to be 3.91% for the worst-case scenario (i.e., $-40$ °C). With the temperature changes in a step size of 10°C, the BER per 10°C is calculated to be 0.26%. TMV scheme is applied to further improve the BER per 10°C. The fact that the BER per 10°C can only be reduced to 0.21% even with TMV31 implies temporal noise is not the main contributor of the error bits at adverse operating condition.

DBD is another effective way for locating the unstable bits with multiple evaluations by sweeping temperature/voltage [23]. In particular, during the chip measurement, we found that the locations of some cells that generate error bits are always fixed. For instance, the cell corresponding to the challenge (0x08) generates an error bit at 30°C, and for other operating temperature including $-30$°C, 50°C, 70°C, 100°C, the error bit is always detected for the same challenge. These error bits with fixed locations cannot be completely eliminated by TMV scheme. DBD scheme is applied to prune the unreliable responses from these cells. For DBD, the response of PUF under normal condition (27°C, 1.2V) and the responses under varying conditions are compared to prune the dark bits. It

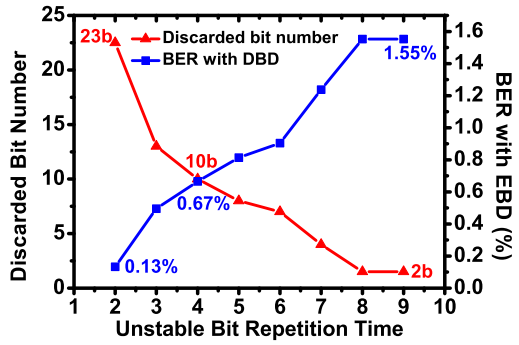


Fig. 13. Improved BER with DBD based correction scheme.

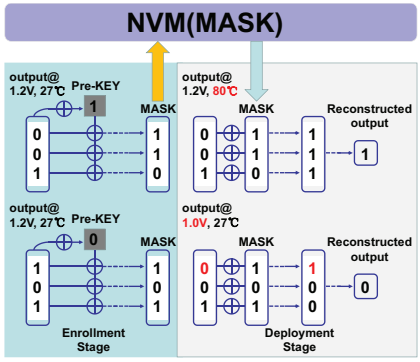


Fig. 14. Operation principle of the SMV based correction scheme.

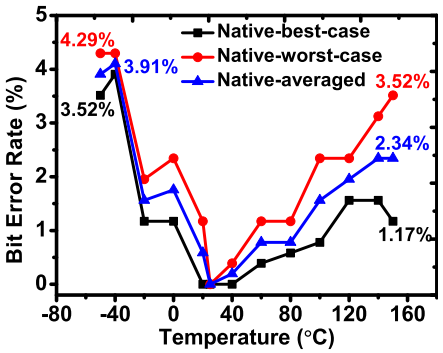


Fig. 15. Measured native BER for 10 test PUF chips with the operating temperature ranging from −50°C to 150°C.

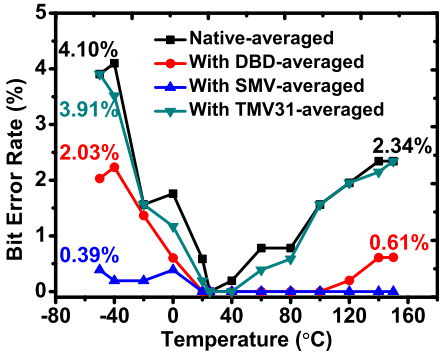


Fig. 16. BER improved by different correction schemes with the operating temperature varied from −50°C to 150°C.

is evaluated by the following procedure: 1) The reference response bit of a cell is read out at normal condition (27°C, 1.2V). 2) The response bit of the same cell is also read out at each other condition with the temperature varying from −50°C to 150°C in step size of 10°C, and supply voltage varying from 1V to 1.4V in step size of 0.1V. 3) A counter is used to count the number of differences in the response bits of the same cell generated at other conditions from that at the reference condition. 4) If the counter output is larger than the threshold $v$, the PUF cell will be marked as a dark bit and discarded. As shown in Fig. 13, DBD can reduce the BER significantly. By discarding the output bit of a cell that repeatedly generates error for $v$ times over the sweeping temperature range, 23 bits (9%) are discarded if $v$ is set to 2, and the BER can be reduced to as low as 0.13%. In order to strike a good balance between the number of discarded bits and the BER, $v$ is set to 4 to discard only 10 bits (4%) to reduce the BER to 0.67%, as illustrated in Fig. 13.

SMV [31] is similar to TMV except that the majority voting is performed spatially instead of temporally. In SMV, the responses from a group of affiliated cells (i.e., responses to different challenges) are used to determine the response bit of a cell in the group. It uses $v$ output bits to reconstruct a new output bit (called the pre-key) with fault-tolerance up to $(v-1)/2$ bits, where $v$ is an odd integer determined by the non-zero probability of response bit flip. By majority voting, the reconstructed response bit is erroneous only when the number of bit errors within the group exceeds half of the votes. The process is carried out in two stages, as shown in Fig. 14. The pre-key is generated under normal condition (27°C, 1.2V) by the following steps: 1) Response bits from $v$ PUF bit cells are XORed to obtain a pre-key. The $v$ bit cells can be arbitrarily selected by $v$ successive outputs generated from a linear feedback shift register (LSFR) seeded by the challenge. 2) The pre-key is XORed with the $v$ PUF response bits to obtain a $v$-bit mask. The mask will be stored in a non-volatile memory without leaking the response bit. The response bit is reconstructed from the PUF under different operating conditions (−50°C∼150°C, 1 V∼1.4 V) as follows: 1) The response bits are read out from $v$ bit cells selected by successive outputs of the LSFR seeded by the applied challenge. 2) The $v$-bit mask stored in the NVM corresponding to the challenge are XORed with the $v$ response bits to obtain a $v$-bit word. 3) The number of 1s in the $v$-bit word are accumulated by a counter. The PUF response bit is 1 if the counter output is larger than $(v-1)/2$, and 0 otherwise. The improved BER per 10°C of the response reconstructed by SMV is compared with the TMV and DBD schemes in Fig. 16.

The BER of the PUF output against the supply voltage

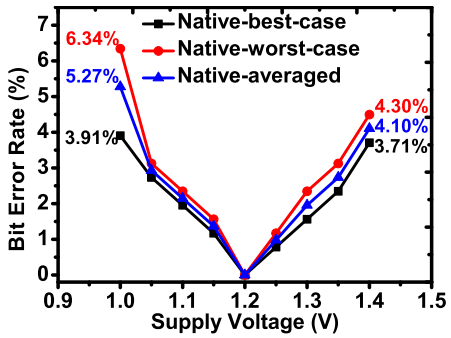


Fig. 17. Measured native BER for 10 test PUF chips with the supply voltage ranging from 1.0 V to 1.4 V.

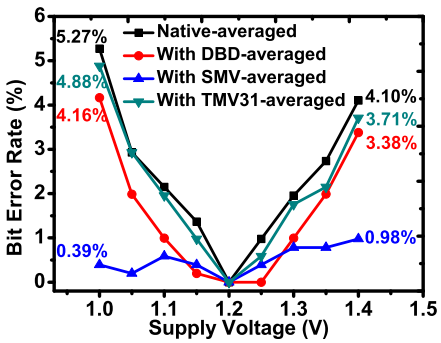


Fig. 18. BER improved by different correction schemes with the supply voltage ranging from 1.0 V to 1.4 V.

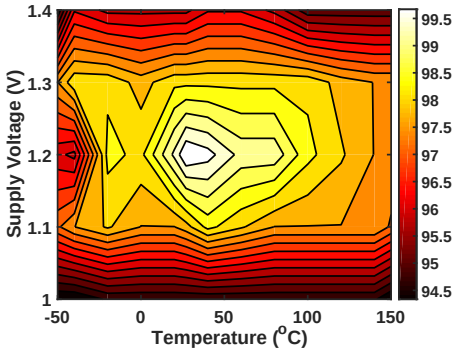


Fig. 19. Native reliability across all different operating conditions without any correction.

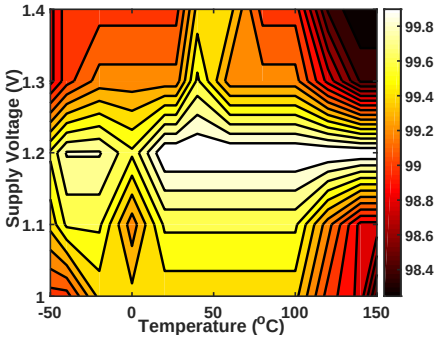


Fig. 20. Improved reliability across all different operating conditions with SMV.

variations from 1.0 V to 1.4 V (i.e. ±17%) is also evaluated, with the reference voltage at 1.2 V. As depicted in Fig. 17, the native BER of 10 PUF chips is 5.27% in the worst-case scenario at 1.0 V. With a step size of 0.1 V, the BER per 0.1 V is calculated to be 2.34%. With TMV31, DBD ($v = 4$, 12b) and SMV ($v = 3$) schemes, the BER per 0.1 V can be lowered to 2.15%, 1.89% and 0.34%, respectively, as shown in Fig. 18.

The PUF reliability are also evaluated against simultaneous temperature and supply voltage variations. The 2D plot in Fig. 19 shows the native reliability across all different combinations of changes in these two environmental factors. The measured average reliability is 96.87%, and the worst-case reliability is 94.34%, which occurs at (−50°C, 1 V) and (150°C, 1 V). With SMV correction scheme, the average reliability and the worst-case reliability have been raised to 99.31% and 98.25%, respectively, as shown in Fig. 20.

The ratio of the mean inter-PUF HD to mean intra-PUF HD is also calculated. As expressed in Eq. (7), the intra-PUF HD is defined as the number of mismatch bits with the same challenge applied to the same PUF instance under different environmental conditions. The output responses of the chip are read under the reference supply voltage and temperature repeatedly for ∼5000 times, and two output sets are randomly selected to calculate the HDs. As shown in Fig. 21, based on the best-fit Gaussian curves plotted for both the inter-PUF HD and the intra-PUF HD, the mean inter-PUF HD is calculated to be around 118× the mean intra-PUF HD. By randomly selecting two output streams generated under different operating temperature/supply voltage conditions, the intra-PUF HDs are plotted with the operating temperature varied from −50°C to 150°C and the supply voltage varied from 1.0 V to 1.4 V in Fig. 22. Then the ratios of the inter-PUF to intra-PUF HDs corresponding to the operating temperature and supply voltage variations are calculated to be around 18 and 13, respectively. The inter/intra-PUF HD ratios for the PUF readout with DBD and SMV based correction schemes are also determined. As illustrated in Fig. 23, with DBD correction, the ratios of inter-PUF to intra-PUF HDs have been elevated to 38 and 20 for the operating temperature and supply voltage variations, respectively. In stark contrast, with SMV based correction scheme, the inter-PUF HDs have been significantly elevated to 127× and 59× those of the intra-PUF HDs for the same ranges of temperature and supply voltage variations, respectively, as illustrated in Fig. 24.

### D. Comparison

Table II provides a full comparison of our proposed PUF against the reported state-of-the-art weak PUF implementations

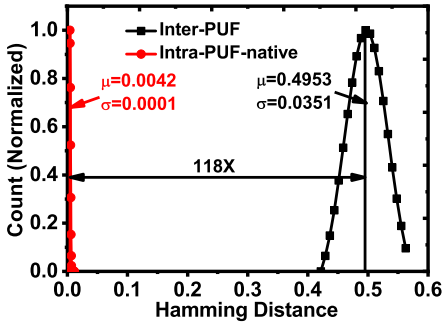


Fig. 21. Separation of inter/intra-PUF HD at the normal condition (27°C, 1.2V).

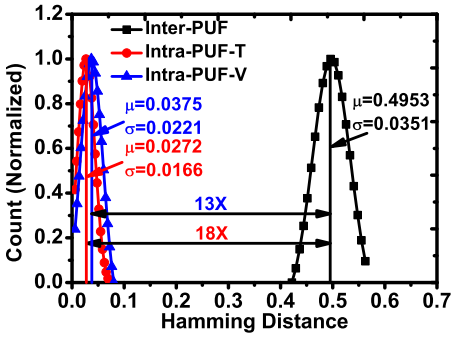


Fig. 22. Separations of inter/intra-PUF HD with operating temperature variation (−50 °C∼150 °C) and voltage variation (1.0 V∼1.4 V).

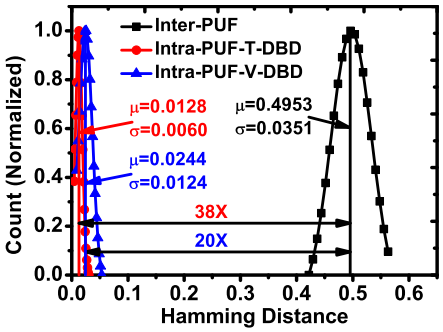


Fig. 23. Improved separations of inter/intra-PUF HD with DBD.

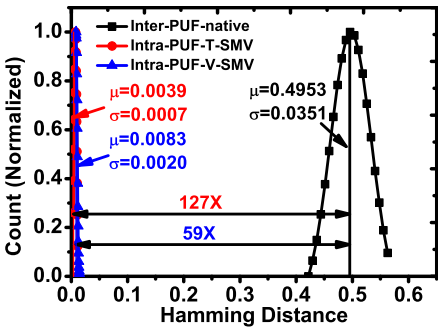


Fig. 24. Improved separations of inter/intra-PUF HD with SMV.

[19]–[25]. It shows that our proposed PUF design is highly reliable with BER per 10°C as low as 0.16%, even under the widest operating temperature range of −50°C∼150°C. The normalized bit cell size is as compact as 1036 $F^2$, which are 9.29×, 5.82×, 9.06× and 3.52× smaller than the previously reported designs of [19], [20], [23] and [25], respectively. With the same number of repeated PUF readouts under the normal condition, our PUF design outperforms the reported native unstable bits/BER of [19] by 10.3×/19.3× (5K readouts), [20] by 1.18× (400 readouts), [21] by 4.48× (500 readouts), [23] by 9.28× (5K readouts), [24] by 2.13×/1.60× (1K readouts), and [25] by 1.75×/1.88× (500 readouts), respectively. It should be noted that the above Gb/s throughputs reported in some PUF implementations are actually achieved by directly outputting the digital PUF bits in parallel (e.g., 64 bit width in [22]), whereas the PUF bits in this and other works with much lower throughputs are generated and output in series by using a cross-coupled comparator and sense amplifier shared by the whole PUF array. As acknowledged by the authors of [22], the parallel readout that is widely adopted for mainstream memory (e.g., SRAM) can significantly elevate the throughput at huge expense of silicon area and power consumption, including those dedicated to the additional I/O pads for chip testing.

## IV. Conclusion

In this paper, we have successfully demonstrated a PUF implementation based on the cross-coupled comparator with temperature compensation. It features a compact bit cell size of 1036 $F^2$. Due to the positive feedback mechanism provided by the cross-coupled structure, the proposed implementation is capable of minimizing the unstable raw response bits to at most 1.46% (500 evaluations) ∼ 2.91% (5K evaluations) and achieving a native BER of 0.44% at normal operating temperature/supply voltage condition. With the operating temperature ranging from −50°C to 150°C and the supply voltage ranging from 1.0 V to 1.4 V, the native BER per 10°C and BER per 0.1 V are evaluated to be 0.26% and 2.34%, respectively without any correction. By using the DBD and SMV based error correction schemes, the above native BER per 10°C and BER per 0.1 V can be further reduced to 0.11% (DBD)/0.016% (SMV) and 1.89% (DBD)/0.34% (SMV), respectively. Across all different operating conditions, the average BER is measured to be 3.13% without correction and 0.69% with SMV. From the inter-PUF HD measured from 10 fabricated PUF chips, an excellent uniqueness of 49.53% is achieved. The superior unpredictability of this design is also validated by ACF and NIST randomness tests. The measured average power consumption of the PUF chip is 23.83 $\mu$W at the throughput of 8 Mb/s, corresponding to an energy efficiency of 2.98 pJ/bit (and 1.61 pJ/bit for the PUF core). Compared with

TABLE II. PERFORMANCE COMPARISON WITH THE STATE-OF-THE-ART IMPLEMENTATIONS.

| | [19] ISSCC'14 | [20] ISSCC'15 | [20] ISSCC'15 | [21] JSSC'16 | [22] ISSCC'17 | [23] JSSC'17 | [24] ISSCC'18 | [25] JSSC'18 | This Work |
|---|---|---|---|---|---|---|---|---|---|
| **Technology (nm)** | 22 | 65 | 65 | 65 | 180 | 14 | 180 | 40 | 65 |
| **Structure** | SRAM | RO | INV | PTAT Volt. Generator | 2T-Amp. | SRAM | Leakage-based | Current Mirror | Cross-coupled Comp. |
| **Correction scheme** | Burn-in, TMV, Masking | N/A | Burn-in, TMV | TMV, Masking | TMV, Masking | TMV, Burn-in SBD[7] | Remapping, TMV | Hysteresis, T-Comp. | TMV, DBD SMV |
| **Norm. bitcell size ($F^2$)** | 9628 | 39000 | 6030 | 726 | 782 | 9387 | 890 | 3643 | 1036 |
| **Unstable bits under normal condition (%) (No. of Evaluations)** | ∼30<br>∼3[1]<br>(5K) | 69.53 | 1.73<br>(400) | 6.54<br>2.00[2]<br>(500) | 1.73<br>0.69[2]<br>(2K) | ∼27<br>(5K) | 5.62<br>1.76[2]<br>(1K) | 2.55/3.48<br>(500/5K) | **1.46/2.64/2.91**<br>(500/1K/5K) |
| **BER under normal condition (%)** | 8.3<br>0.97[1] | N/A | N/A | N/A | 0.18<br>0.08[2] | N/A | 0.69<br>0.019[2] | 0.81 | 0.44 |
| **Temp. range (°C)** | 25∼50 | N/A | 25∼85 | 0∼80 | −40∼120 | 25∼110 | 0∼80 | −40∼125 | **−50∼150** |
| **Supply volt. range (V)** | 0.7∼0.9 | N/A | 0.7∼1.0 | 0.6∼1.2 | 0.8∼1.8 | 0.55∼0.75 | 1.2∼1.8 | 0.8∼1.0 | 1.0∼1.4 |
| **Averaged BER across all temp. &volt. conditions (%)** | N/A | N/A | N/A | N/A | N/A | 5.76<br>1.46[8] | N/A | N/A | **3.13**<br>**0.69**[5] |
| **BER per 10°C (%)** | N/A | N/A | 0.47 | 0.44[3] | 0.21[4] | N/A | N/A | ∼0.32 | **0.26**<br>**0.016**[5] |
| **BER per 0.1V (%)** | N/A | N/A | 1.3 | 0.13[3] | 0.29[4] | N/A | N/A | ∼0.72 | 2.34<br>0.34[5] |
| **Uniqueness (%)** | 49 | N/A | 50.14 | 50.01 | 49.9 | 48.6 | 50.001 | 49.07 | 49.53 |
| **ACF@95% confidence** | 0.0088 | 0.125 | 0.0363 | 0.0188 | 0.0167 | N/A | 0.0221 | 0.00735 | 0.0197 |
| **Entropy** | 0.9997 | 0.8671 | 0.9966 | 0.9998 | N/A | 0.99993 | N/A | 0.9972 | 0.9999 |
| **Energy efficiency (pJ/bit)** | 0.013[9]<br>0.19[6] | 0.475 | 0.015 | 0.548<br>6.02[2] | 0.0911 | 0.004[9] | 3.6 | 0.0565 | 1.61[9]<br>2.98 |
| **Throughput (Mb/s)** | 2000 | N/A | N/A | 10.2 | 4832 | 750 | 0.018 | 24000 | 8 |
| **Data Output Scheme** | N/A | N/A | Serial | Serial | Parallel (64-bit) | N/A | N/A | N/A | Serial |

[1] Bit-error rate after TMV, with aging hardening and bit-masking applied; [2]With TMV11; [3]With off-chip ADC/comparator and manual re-calibration at each temperature point; [4]With TMV, not native; [5]With SMV to increase the rate of fault tolerance; [6]With TMV15; [7]Selective Bit Destabilization; [8]With TMV15 and dark bits discarded; [9]Energy efficiency of PUF core.

the state-of-the-art implementations, the unstable bits and BER of the native responses measured at the normal condition have been improved by 1.18∼10.3× and 1.60∼19.3×, respectively.

## REFERENCES


[1] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE,* vol. 102, no. 8, pp. 1126-1141, 2014.

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

[3] Z. Wang, Y. Chen, A. Patil, J. Jayabalan, X. Zhang, C. H. Chang and A. Basu, "Current Mirror Array: A Novel Circuit Topology for Combining Physical Unclonable Function and Machine Learning," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 4, pp. 1314-1326, 2018.

[4] F. Courbon, S. Skorobogatov, and C. Woods, "Reverse engineering flash EEPROM memories using scanning electron micoscopy," *in Proc. Int. Conf. Smart Card Research and Advanced Applications (CARDIS 2016)*, pp. 57-72, Springer 2016. 7(2):292C299, 2017.

[5] C. Helfmeier, et al., " Breaking and entering through the silicon," *in Proc. 2013 ACM SIGSAC Conf. Computer and Communications Security (CCS)*, Berlin, Germany, pp. 733-744, Nov. 2013.

[6] N. F. Ghalaty, B. Yuce, M. Taha, and P. Schaumont, "Differential fault intensity analysis," in *Proc. 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC),* Busan, South Korea, pp. 49-58, Sept. 2014.

[7] Chakraborty et al., "Keynote: A disquisition on logic locking," *IEEE Trans. Computer-Aided Design*, 2019, DOI: 10.1109/TCAD.2019.2944586.

[8] 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 *Proc. IEEE Symp. VLSI Circuits*, Jun. 2004, pp. 176-179.

[9] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann and U. Rhrmair, "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.

[10] 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 *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2015, pp. 1-3.

[11] 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, 2017.

[12] R. Kumar and W. Burleson, "On design of a highly secure PUF based on non-linear current mirrors," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May. 2014, pp. 38-43.

[13] D. E. Holcomb, W. P. Burleson and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," *Proc. Conf. RFID Secur.*, vol. 7. 2007, pp. 1-12.

[14] D. Sahoo, D. Mukhopadhyay, R. Chakraborty and P. Nguyen, "A Multiplexer-Based Arbiter PUF Composition with Enhanced Reliability and Security," *IEEE Transactions on Computers*, vol. 67, no. 3, pp. 403-417, 2018.

[15] 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. Asia and South Pacific Design Automation Conference (ASP-DAC)*, Jan. 2018, pp. 97-104.

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

[18] Y. Su, J. Holleman and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 69-77, Nov. 2008.

[19] S. K. Mathew et al., "A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2014, pp. 278-279.

[20] A. Alvarez, W. Zhao and M. Alioto, "15 fJ/b static physically unclonable functions for secure chip identification with $<2\%$ native bit instability and $140\times$ inter/intra PUF hamming distance separation in 65 nm," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2015, pp. 256-257.

[21] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute temperature voltage generators," *IEEE J. Solid-State Circuits*, vol. 51, no. 9, pp. 2192-2202, Sep. 2016.

[22] K. Yang, Q. Dong, D. Blaauw and D. Sylvester, "A $553F^2$ 2-transistor amplifier-based Physically Unclonable Function (PUF) with 1.67% native instability," in *Proc. IEEE Int. Solid-State Circuits Conf.*, 2017, pp. 146-147.

[23] S. Satpathy et al., "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, Sep. 2017.

[24] J. Lee, D. Lee, Y. Lee and Y. Lee, "A $445F^2$ leakage-based physically unclonable Function with Lossless Stabilization Through Remapping for IoT Security," in *Proc. IEEE Int. Solid-State Circuits Conf.*, 2018, pp. 132-134.

[25] S. Taneja, A. B. Alvarez and M. Alioto, "Fully Synthesizable PUF Featuring Hysteresis and Temperature Compensation for 3.2% Native BER and 1.02 fJ/b in 40 nm," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2828-2839, Sep. 2018.

[26] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability," in *Proc. 2012 IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Tenerife, Spain, pp. 37-42, Dec. 2012.

[27] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in *Proc. 16th USENIX Security Symp.,* Bosten, USA, pp. 291-306, Aug. 2007.

[28] P. Sun and A. Cui, "A new pay-per-use scheme for the protection of FPGA IP," in *Proc. 2019 IEEE Int. Symp. Cir. Syst. (ISCAS)*, Sapporo, Japan, p. 5, May 2019.

[29] A. Cui, C. H. Chang, W. Zhou, and Y. Zheng, "A new PUF based lock and key solution for secure in-field testing of cryptographic chips," in *IEEE Trans. Emerging Topics in Computing*, 2019, DOI: 10.1109/TETC.2019.2903387.

[30] Q. Zhao, Y. Cao, X. Zhao and C. H. Chang, "A Current Comparator Based Physical Unclonable Function with High Reliability and Energy Efficiency," in *Proc. IEEE International Conference on Digital Signal Processing (DSP)*, pp. 1-4, 2018.

[31] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh and S. Lee, "Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," in *Proc. IEEE Int. Solid-State Circuits Conf.*, 2016, pp. 158-160.

[32] S. K. Mathew and S. Srinivasan, "2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 11, pp. 2807-2821, 2012.

[33] V. C. Patil, A. Vijayakumar, D. E. Holcomb and S. Kundu, "Improving reliability of weak PUFs via circuit techniques to enhance mismatch," in *Proc. IEEE International Symposium on Hardware Oriented Security and Trust*, 2017, pp. 146-150.

[34] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," in *NIST Special Publication 800-22,* 2010.

**Qiang Zhao** received the B.Eng. degree from College of Electronic Science and Technology, Shenzhen University, China, in 2017. He is now pursuing the M.S. degree in the College of Electronics and Information Engineering, Shenzhen University. His research interests mainly focus on hardware security and the physical unclonable function design with high reliability.

**Yiheng Wu** is currently pursuing Bachelor degree in the College of Electronics and Information Engineering, Shenzhen University. His research interests include the novel physical unclonable function and true random number generator design.

**Xiaojin Zhao** (S'07-M'10) received his B.Sc. degrees in both Microelectronics and Applied Mathematics from Peking University in 2005 and Ph.D. degree in Electrical and Electronic Engineering from the Hong Kong University of Science and Technology (HKUST) in 2010. From 2010 to 2011, he worked as a post-doctoral Research Associate in HKUST. In 2012, he joined Shenzhen University and is currently an Associate Professor in the College of Electronics and Information Engineering. He has published over 80 international journal papers and refereed conference papers. His research interests include CMOS monolithic polarization image sensor, gas sensor and their related hardware security techniques (e.g., physical unclonable function and true random number generator) when applied to the field of "Smart Internet of Things (IoT)". Dr. Zhao served as the vice chair and chair of IEEE Electron Devices and Solid-State Circuits (EDSSC) Shenzhen Joint Chapter from 2015 to 2019. He also served as the organizing and technical committee members in various IEEE conferences.

**Yuan Cao** (S'09-M'2014) received his B.S. degree from Nanjing University, M.E. degree from Hong Kong University of Science and Technology and Ph.D. degree from Nanyang Technological University in 2008, 2010 and 2015, respectively. Currently he works as a full professor in College of Internet of Things Engineering of Hohai University. His research interests include hardware security, silicon physical unclonable function, and analog/mixed-signal VLSI circuits and systems.

**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) of Singapore in 1993 and 1998, respectively. He served as a Technical Consultant in industry prior to joining the School of Electrical and Electronic Engineering (EEE) of NTU in 1999, where he is currently an Associate Professor. He holds joint appointments with the university as Assistant Chair of Alumni of the School of EEE from 2008 to 2014, Deputy Director of the Center for High Performance Embedded Systems from 2000 to 2011, and Program Director of the Center for Integrated Circuits and Systems from 2003 to 2009. He has coedited five books, published thirteen book chapters, more than 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.

Dr. Chang serves as the Associate Editor of IEEE Transactions on Very Large Scale Integration (VLSI) Systems since 2011, IEEE Access since 2013, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems from 2016-2019, IEEE Transactions on Information Forensic and Security since January 2016, IEEE Transactions on Circuits and Systems-I since 2020 and from 2010-2013, Integration, the VLSI Journal from 2013-2015, Springer Journal of Hardware and System Security since June 2016 and Microelectronics Journal since May 2014. He was the editorial advisory board member of Open Electrical and Electronic Engineering Journal from 2007 to 2013 and Journal of Electrical and Computer Engineering from 2008 to 2014. He guest edited several special issues and served in the organizing and technical program committee of more than 60 international conferences (mostly IEEE). He is an IET Fellow, IEEE Fellow, and 2018-2019 Distinguished Lecturer of IEEE Circuits and Systems Society.