# Unified Analog PUF and TRNG Based on Current-Steering DAC and VCO

Mohammadhadi Danesh, *Graduate Student Member, IEEE*, Aishwarya Bahudhanam Venkatasubramaniyan, Gaurav Kapoor, Naveen Ramesh, Sudarsan Sadasivuni, Sanjeev Tannirkulam Chandrasekaran, *Graduate Student Member, IEEE*, and Arindam Sanyal, *Member, IEEE*

***Abstract*—This work presents a unified weak physical unclonable function (PUF) and a true random number generator (TRNG) based on the current-steering digital-to-analog converter (DAC) and ring voltage-controlled oscillator (VCO). Entropy source for the weak PUF is the mismatch between NMOS and PMOS transistors in a cascode current DAC as well as the mismatch between VCO quantizers, while entropy source for the TRNG is thermal noise in the DAC and VCO and clock jitter. Instead of using spatial entropy sources for the PUF, i.e., multiple unit PUF elements, the proposed architecture utilizes temporal entropy source by capturing the output of unit PUF element over multiple cycles, which reduces area significantly. A unified PUF/TRNG prototype is fabricated in 65-nm CMOS and consumes 0.36 pJ/bit at a throughput of 100 Mb/s. The PUF has a measured intra-HD of 0.0906 and inter-HD of 0.4859, while the raw TRNG bitstream has an entropy of 0.9991 and passes all the NIST statistical randomness tests.**

***Index Terms*—Digital-to-analog converter (DAC), physical unclonable function (PUF), true random number generator (TRNG), voltage-controlled oscillator (VCO).**

## I. Introduction

PHYSICAL unclonable functions (PUFs) and true random number generators (TRNGs) are security primitives that are used for secure key generation, authentication, and cryptography. In silicon implementations, PUFs leverage inherent random manufacturing mismatches in transistors, capacitors, and interconnects/vias to create a unique identifier, while TRNGs derive their randomness from thermal noise and jitter. Both PUF and TRNG circuits require systematic mismatch to be very small such that there is no bias toward “1/0” in the PUF/TRNG response. While both PUF and TRNG outputs are unpredictable, the fundamental difference between PUF and TRNG is that a PUF response should be repeatable when interrogated with the same challenge, and a TRNG’s output varies randomly every time it is interrogated. There are several well-established architectures for both PUF and TRNG. Widely used PUF architectures exploit variations in path delays [1]–[3] or variations in threshold voltages of cross-coupled inverters [4], [5] and current sources [6], [7]. Arbiter PUF [1] is one of the first and most popular architectures, which generates a PUF output by comparing delays of two nominally identical paths. Variants of arbiter PUF includes XOR-ing outputs from multiple PUFs [2], ring-oscillator (RO) PUF [2], or adding feed-forward paths [3]. SRAM-based PUFs [5] use random power-ON state of the SRAM array to create a unique identifier but require calibration to remove bias in the SRAM array. Recent cross-coupled inverter PUF [4] is based on the same principle as SRAM PUF. Analog PUFs leverage threshold voltage mismatch between transistors, as in the cascode current mirror-based weak PUF [6] and the current mirror array-based strong PUF [7]. Another analog PUF is based on a random mismatch in resistances of metal vias in an integrated circuit [8]. Recent works have also reused or repurposed circuit components to develop PUFs, specifically capacitor mismatches in a digital-to-analog converter (DAC) to derive PUF [9]–[11]. While Herkle *et al.* [9] and Duncan *et al.* [11] derive PUF from capacitive DAC in $\Delta\Sigma$ analog-to-digital converter (ADC), Tang *et al.* [10] exploit capacitor mismatches in DAC of successive approximation register (SAR) ADC to form a PUF.

On the other hand, silicon TRNGs primarily leverage thermal noise and jitter as entropy sources. Petrie and Connelly [12] digitize thermal noise in a resistor to generate a TRNG sequence but require high-bandwidth amplifiers that are power-hungry. Laurenciu and Cotofana [13] use thermal noise in transistors biased in the linear region and an inverter amplifier to produce a probability modulated TRNG sequence but require an OTA which can bias the TRNG sequence. Digital TRNGs use metastable latches [14]–[16] to generate a TRNG sequence but require calibration, and often postprocessing, to suppress bias. ROs are another popular digital TRNG that uses phase noise of oscillator and clock jitter as entropy sources. There are several variants of RO-based TRNG, such as edge-chasing TRNG [17] and

Manuscript received March 25, 2020; revised June 25, 2020; accepted July 20, 2020. *(Corresponding author: Arindam Sanyal.)*

Mohammadhadi Danesh was with the Department of Electrical Engineering, University at Buffalo, Buffalo, NY 14260 USA. He is now with Cirrus Logic, Austin, TX 78701 USA (e-mail: mdanesh@buffalo.edu).

Aishwarya Bahudhanam Venkatasubramaniyan was with the Department of Electrical Engineering, University at Buffalo, Buffalo, NY 14260 USA. She is now with Intel Corporation, Folsom, CA 95630 USA.

Gaurav Kapoor was with the Department of Electrical Engineering, University at Buffalo, Buffalo, NY 14260 USA. He is now with Intel Corporation, Hillsboro, OR 97124 USA.

Naveen Ramesh was with the Department of Electrical Engineering, University at Buffalo, Buffalo, NY 14260 USA. He is now with Qualcomm, San Jose, CA 95110 USA.

Sudarsan Sadasivuni, Sanjeev Tannirkulam Chandrasekaran, and Arindam Sanyal are with the Department of Electrical Engineering, University at Buffalo, Buffalo, NY 14260 USA (e-mail: arindams@buffalo.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2020.3011648

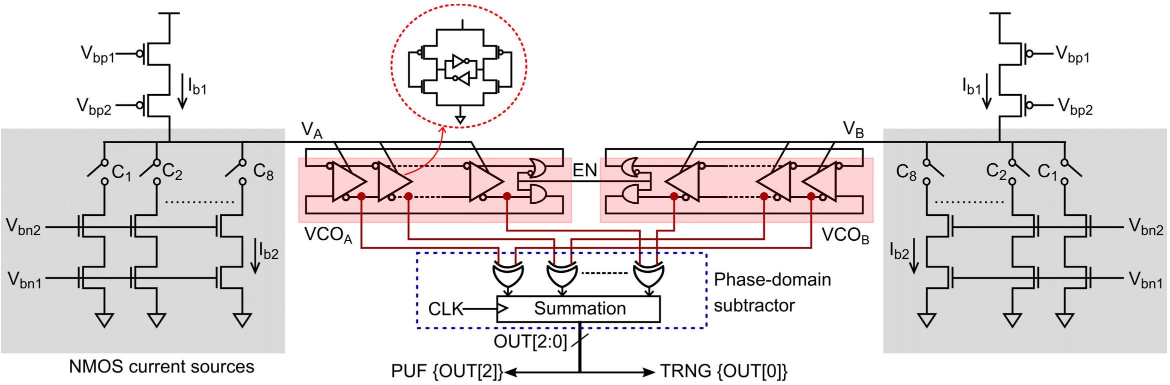


Fig. 1. Proposed unified analog weak PUF and TRNG architecture.

beat frequency-detection TRNG [18]. In edge-chasing TRNGs, edges are inserted at different points in the oscillator, which leads to the collapse of oscillation. The time between injection of the edges and collapse of oscillation is digitized, and the least significant bits (LSBs) of the digitized time act as TRNG. In beat-frequency-detection TRNG, time taken by one RO to catch up with another is digitized with a counter and LSBs of the counter act as TRNG. The trend in silicon security primitive design so far has been to use different dedicated circuits for PUF and TRNG, with only the work in [16] and [19] presenting a unified PUF and TRNG based on the metastable latch that reuses discarded PUF candidates as TRNG source.

In this work, we present a unified PUF+TRNG circuit comprising a current-steering cascode DAC and ring voltage-controlled oscillator (VCO), as shown in Fig. 1. The cascode DAC provides amplification of mismatch between NMOS and PMOS transistors due to the high impedance of cascode current sources. The DAC output is quantized by a ring VCO, and the PUF output is generated from the most significant bit (MSB) of the VCO output, while the LSB acts as a TRNG. By running the VCO for a long time, we can generate long PUF and TRNG bitstreams, i.e., the proposed architecture tradeoff speed for the area. This is in contrast to conventional PUF design that requires multiple unit PUF elements to generate a long PUF bitstream. The proposed unified PUF+TRNG architecture is discussed in more detail in Section II. A test chip is fabricated in 65-nm CMOS and consumes 0.36 pJ/bit for generating 1-bit PUF and 1-bit TRNG responses. The proposed PUF and TRNG performances are validated through lab measurements that are discussed in Section III. Finally, the conclusion is broughtup in Section IV.

## II. Unified PUF+TRNG Design

### A. Circuit Architecture

The proposed unified PUF+TRNG architecture is shown in Fig. 1. A pair of cascode DACs generate output voltages ($V_A/V_B$ in Fig. 1) that drive two seven-stage ring VCOs (VCO$_A$ and VCO$_B$). The bias voltages $V_{\mathrm{bp1}}$, $V_{\mathrm{bp2}}$, $V_{\mathrm{bn1}}$, and $V_{\mathrm{bn2}}$ are generated using high swing cascode current mirrors. The cascode DAC has eight nominally identical NMOS current sources that are selectable through the bits $C_1, \ldots, C_8$. The VCOs quantize the voltages $V_A/V_B$, and an XOR-based subtractor extracts the difference between the quantized phase outputs of the two VCOs [20]. An enable signal (EN in Fig. 1) ensures that both VCOs start with the same phase. In the absence of mismatch and noise, both VCOs would run at the same frequency, and the quantized output would be zero. Assuming a nominal DAC output voltage of $v_{\mathrm{in}}$ and a nominal VCO tuning gain of $k_{\mathrm{vco}}$, the sampled phase difference between the two VCOs in presence of mismatch can be written as

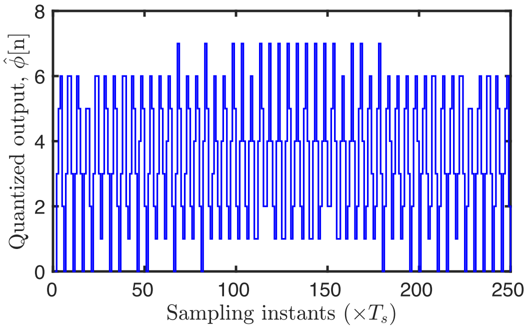
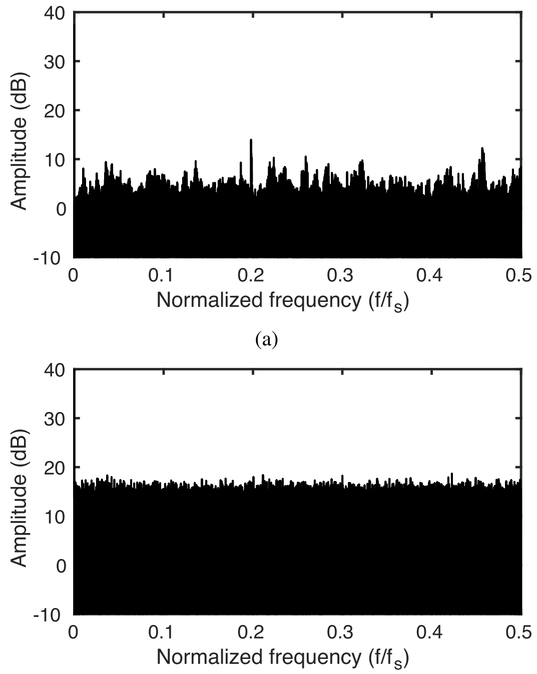


Fig. 2. Simulated quantized phase output versus time.

$$\begin{aligned}\phi[n] &= \mathrm{mod}(2\pi k_{\mathrm{vco}}(1+\Delta k_{\mathrm{vco}})v_{\mathrm{in}}(1+\Delta v_{\mathrm{in}})nT_s \\ &\quad - 2\pi k_{\mathrm{vco}} v_{\mathrm{in}} nT_s, 2\pi) \\ &\approx \mathrm{mod}(2\pi f_{\mathrm{vco}} nT_s(\Delta k_{\mathrm{vco}} + \Delta v_{\mathrm{in}}), 2\pi) \qquad (1)\end{aligned}$$

where $T_s$ is the sampling period, $\Delta k_{\mathrm{vco}}$ is the fractional random mismatch in VCO gain, $\Delta v_{\mathrm{in}}$ is the fractional random mismatch in DAC output voltage, $f_{\mathrm{vco}} = k_{\mathrm{vco}} v_{\mathrm{in}}$, and the mod operator represents the modulo phase-domain integration performed by the VCO. The modulo integration causes the VCO phase to wrap over after it crosses $2\pi$. The quantized phase output is given by $\hat{\phi}[n]$ and has values in the range of [0, 7] for this design. Fig. 2 shows the simulated $\hat{\phi}[n]$ assuming 30-mV mismatch in $v_{\mathrm{in}}$ and 1% mismatch between the VCOs. No noise or jitter is included in the simulation model. The two VCOs start with "0" phase difference, and they run at slightly different frequencies. "0"s of $\hat{\phi}[n]$ correspond to the sampling instants when the two VCO phases align again. In the absence of any noise or jitter, $\hat{\phi}[n]$ is a deterministic signal that depends only on the mismatch between the DACs, mismatch between the VCOs and sampling frequency, and is repeatable. Hence, $\hat{\phi}[n]$ is unique to a DAC-VCO pair and can be used to create a weak PUF sequence by sampling $\hat{\phi}[n]$ over multiple time periods.

In the presence of noise and jitter, the LSB of $\hat{\phi}[n]$ starts varying dynamically with time. Hence, in this work, we have selected only the MSB of $\hat{\phi}[n]$ for generating PUF bitstream,



(a)

(b)

Fig. 3. Measured $2^{19}$ point FFT for (a) MSB of $\hat{\phi}[n]$ and (b) LSB of $\hat{\phi}[n]$.

while the LSB acts as a TRNG sequence. Fig. 3(a) and (b) shows measured $2^{19}$-point FFT of MSB and LSB of $\hat{\phi}[n]$, respectively, at 1-V power supply and room temperature. While the MSB spectrum shows some tones due to quantization error, the LSB has a flat frequency response that is a necessary condition for randomness. In subsequent sections, we will present detailed measurement results that validate both PUF and TRNG operations.

### B. Length of PUF Sequence

In order to use the MSB of $\hat{\phi}[n]$ as PUF response, we need to determine the sequence length of $\hat{\phi}[n]$, which contains unique information. If the VCOs are kept running, the MSB bit will eventually start showing temporal correlation with previous bits in the sequence, and the amount of secure information contained in the MSB sequence will not increase with bit lengths. This is because quantization error in a VCO is deterministic and can exhibit periodic behavior [21], which can limit the number of secure bits that can be extracted from the proposed PUF. Even though thermal noise dithers quantization error, MSB of $\hat{\phi}[n]$ still exhibits some tones, as shown in Fig. 3(a). To evaluate correlation between bits in the PUF response, we calculate joint entropy by considering two adjacent $M$-bit sequence of PUF segments. Let us denote the two adjacent segments by $X_1$ and $X_2$ with outcomes $x \in [0, 1]$ and probability mass function $P(x) = P(X = x)$. The joint Shannon entropy [9], [22] is then defined as

$$H(X_1, X_2) = -\sum_{x_1=0}^{1}\sum_{x_2=0}^{1} P(x_1, x_2) \cdot \log_2 P(x_1, x_2). \quad (2)$$

The joint entropy is an indicator of local temporal correlation between adjacent sequences, and for a truly random sequence, the joint entropy in (2) will be 2. Fig. 4 shows joint entropy versus sequence length calculated on measured PUF responses from eight PUFs. For small sequence lengths till 128 bits, all the PUFs show joint entropy greater than 1.9 corresponding to an upper bound of 0.1 on correlation factor [23], [24], and the joint entropy value starts dropping once the sequence length exceeds 256 bits. Hence, the PUF sequence contains unique information in the first 128 bits, and the entropy source starts getting depleted as the sequence length is increased.

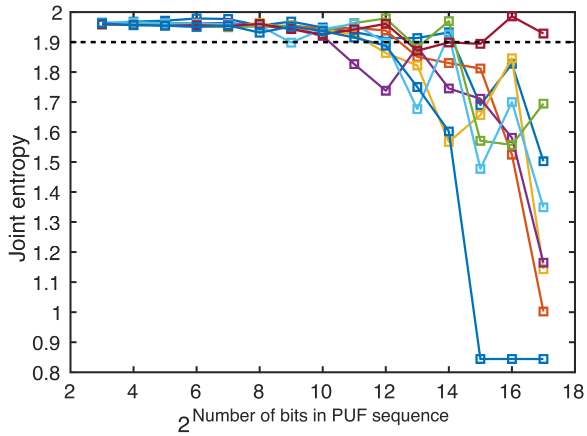


Fig. 4. Joint entropy versus PUF sequence length for eight PUFs.

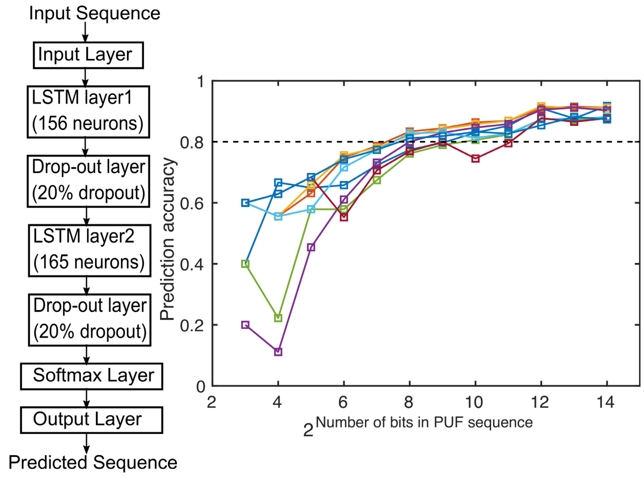


Fig. 5. LSTM prediction accuracy versus PUF sequence length for eight PUFs.

To further investigate the temporal correlation, we used a recurrent-neural network (RNN) with long-short term memory (LSTM) from MATLAB's deep-learning toolbox to model the PUF. The LSTM model is optimized using grid search of the following hyperparameters: number of layers, number of neurons in each layer, learning rate, and dropout rates. The LSTM model accepts an $M$-bit PUF sequence and predicts the next 0.2 $M$ bits. Fig. 5 shows the LSTM model used and prediction accuracies versus sequence length for eight PUFs. The LSTM model has dropout layers to prevent overfitting. The prediction accuracy is less than 80% for sequence lengths less than 128 bits and exceeds 90% for sequence lengths greater than 4096 bits. The LSTM model results verify that the PUF sequence has low temporal correlation for sequence lengths up to 128 bits.

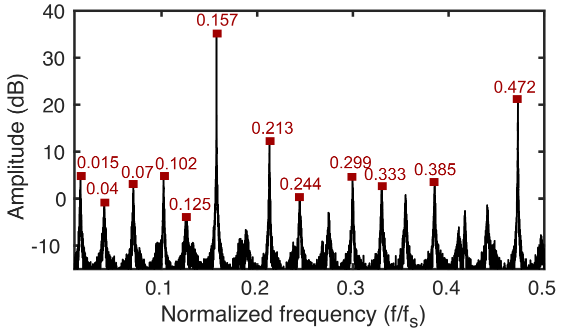


Fig. 6. Simulated $2^{15}$ point FFT for MSB of $\hat{\phi}[n]$ without thermal noise.

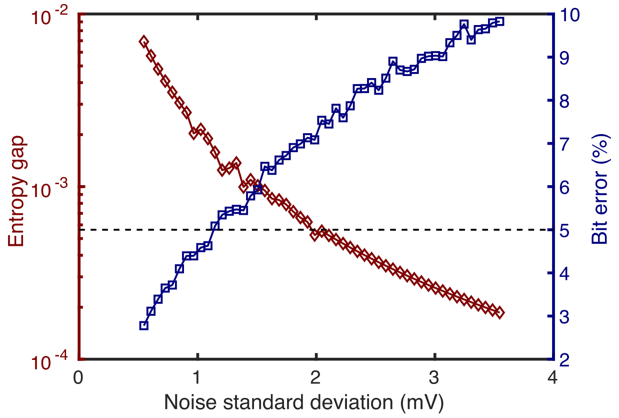
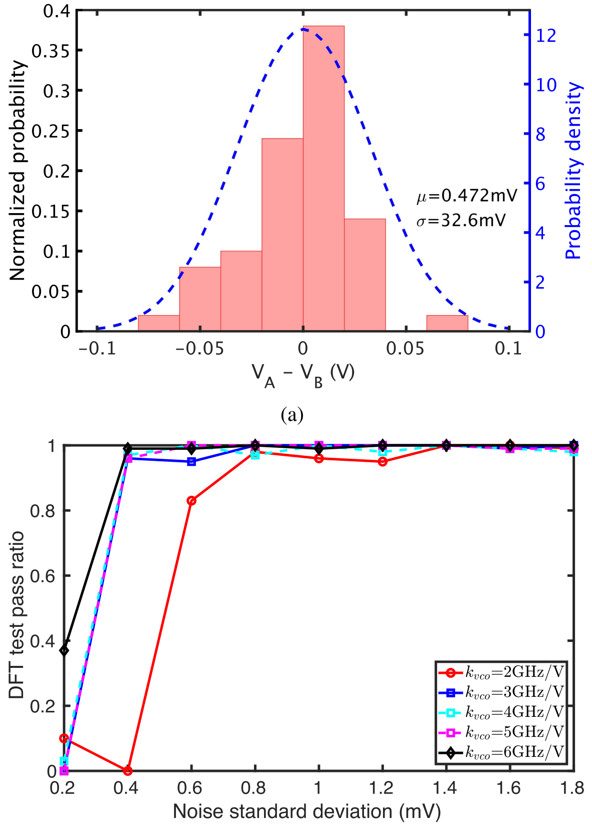


Fig. 7. Simulated PUF BER and TRNG entropy gap versus thermal noise.



(a)

(b)

Fig. 8. (a) Simulated DAC mismatch distribution and (b) simulated DFT test pass ratio for TRNG output versus noise standard deviation for a different nominal $k_{\text{vco}}$.

Fig. 6 shows the simulated $2^{15}$ point FFT plot of PUF output without thermal noise. The FFT plot shows many peaks, arising out of pulse-frequency modulated VCO quantization error [21], and also verifies the periodicity observed through joint entropy and LSTM prediction results. Thermal noise dithers the quantization error resulting in a frequency spectrum with less observable peaks, as shown in Fig. 3(a).

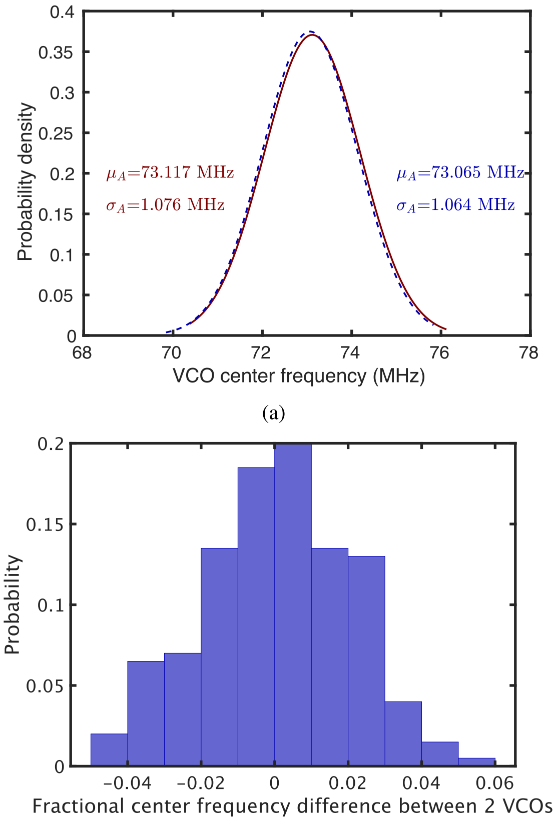
### C. Effect of Noise

There is an intrinsic tradeoff between the performance of PUF and TRNG. To ensure the high quality of random bits from the TRNG, thermal noise should be high. On the other hand, thermal noise should be low to ensure that the PUF output is reproducible when repeatedly interrogated. We simulated the tradeoff between TRNG and PUF performance by sweeping thermal noise at the output of the DAC (nodes A and B in Fig. 1). We interrogated a 1000-bit PUF sequence 500 times for each thermal noise step and repeated the same experiment ten times. Fig. 7 shows the simulated PUF and TRNG performance versus thermal noise. As expected, the PUF bit-error rate (BER) increases with noise, while the TRNG entropy improves. For this design, the target PUF BER is 5% for a corresponding TRNG entropy of 0.9994.

In order to get a high-quality TRNG output, the systematic mismatch between DACs and VCOs should be minimum such that difference in phase between the two VCOs is set by random noise. On the other hand, if the two DACs and VCOs are matched very well such that the random mismatch is small, then the PUF output will be unreliable due to noise. Hence, for both PUF and TRNG outputs to work, the mismatch and noise have to be carefully balanced. Fig. 8(a) shows the histogram of $V_A - V_B$ for 500 Monte Carlo runs across process and mismatch corners. $V_A - V_B$ has a standard deviation $\sigma_{\text{mis}} = 32.6$ mV.

In order to assess the amount of noise required for high-quality TRNG output, we sweep noise at nodes A and B and perform DFT test on the TRNG output for different $k_{\text{vco}}$ values. DFT test is one of the tests in the NIST randomness test suite that tests for periodic features in a sequence and computes a $p$-value. If the computed $p$-value is greater than 0.01, the sequence is considered to be statistically random. While passing the DFT test is a necessary but not sufficient condition for randomness, it can provide important insights during the design phase. For each noise standard deviation value $\sigma_n$, we repeat the simulation 100 times and calculate the pass ratio. Fig. 8(b) shows the pass ratios for different $k_{\text{vco}}$ and noise values. As expected, for small values of $\sigma_n$, the TRNG output fails most of the time, and the pass ratio is low. If $k_{\text{vco}} \geq 3$ GHz/V, the TRNG output passes DFT test with high pass ratio close to 1 if $\sigma_n > 1$ mV. The pass ratio improves with the increase in $k_{\text{vco}}$ because a high $k_{\text{vco}}$ reduces quantization error compared with thermal noise when referred to the VCO input.

For this design, we set $k_{\text{vco}}$ to 4 GHz/V. Fig. 9(a) shows the simulated distribution of center frequencies of the two VCOs without any DAC mismatch for 300 Monte Carlo



(a)

(b)

Fig. 9. (a) Simulated distribution of the VCO frequencies. (b) Histogram of simulated fractional difference between center frequencies of the two VCOs.

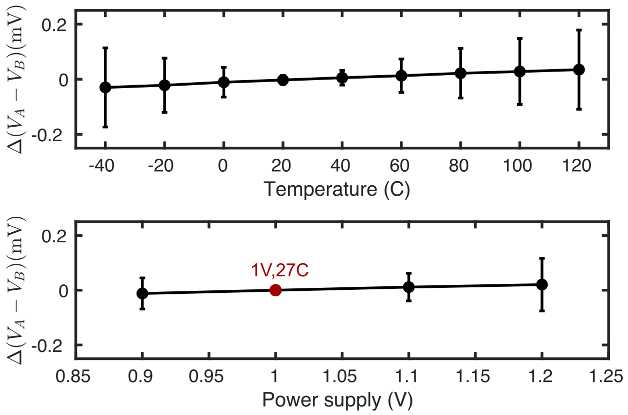


Fig. 10. Simulated change in $V_A - V_B$ from nominal condition across VT corners.

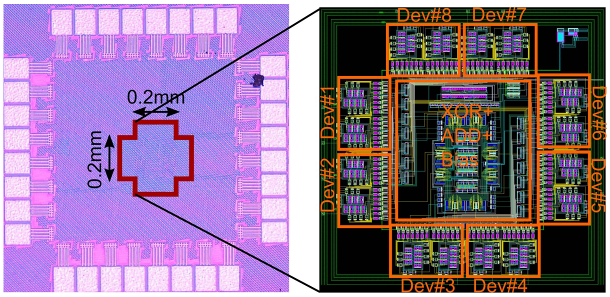


Fig. 11. Die microphotograph and layout.

runs over mismatch and process corners. The two VCOs are relatively well-matched and have similar center frequencies close to 73 MHz. Fig. 9(b) shows a histogram of the fractional difference between center frequencies of the two VCOs simulated over 100 mismatch and process corners. The two VCOs show a worst case ($3\sigma$) difference of 6% in the center frequencies, which is equivalent to a 1.1-mV voltage difference referred to as the VCO inputs. Thus, the cascode DACs are the major contributors to a mismatch in the design. Based on the simulation results, the noise referred to nodes A and B has a standard deviation of $\sigma_n = 1.2$ mV. Fig. 10 shows the simulated variation in $V_A - V_B$ with respect to nominal conditions due to variation in the bias current mirrors across VT corners. Since the same cascode current mirrors are used to generate the biasing voltages for both DACs, VT variations do not produce a differential change in $V_A - V_B$, and all changes in $V_A - V_B$ across VT corners are due to noise in current mirrors. The simulations for each VT corner in Fig. 10 are repeated 1000 times, and the worst case variations in $V_A - V_B$ are less than ±0.2 mV, which is 6× less than $\sigma_n$.

The probability that the PUF mismatch, $v_{\text{mis}} = V_A - V_B$, is less than $3\sigma_n$ is given by

$$P_1 = P(-3\sigma_n \leq v_{\text{mis}} \leq 3\sigma_n) = \text{erf}\left(\frac{3\sigma_n}{\sqrt{2}\sigma_{\text{mis}}}\right). \quad (3)$$

For the simulated values of $\sigma_n = 1.2$ mV and $\sigma_{\text{mis}} = 32.6$ mV, $P_1 = 0.088$, implying that the PUF mismatch will be less than 3× noise standard deviation for 8.8% of times. Since we have eight-unit NMOS current sources, the probability that PUF mismatch will be less than $3\sigma_n$ for all eight NMOS current sources is $P_1^8 = (0.088)^8 \approx 0$. Thus, the PUF mismatch will always exceed $3\sigma_n$ for at least one of the NMOS current sources. The NMOS current sources that result in a stable PUF can be selected through measurements on the PUF during initial registration and the configuration inputs $C_1$–$C_8$ can be restricted to only the useful space. For our measurements, we used the configuration inputs $\{C_1, C_2, \ldots, C_8\}$ of {00000010} and {00000100} for all the PUFs.

## III. Measurement Results

### A. PUF Measurement Results

A test chip of the proposed unified PUF+TRNG circuit is fabricated in 65-nm CMOS. Fig. 11 shows the die microphotograph and layout of the test chip. Each test chip has eight devices and occupies a core area of 0.04 mm$^2$. Each device consumes 36-$\mu$W power from a 1.2-V power supply, and the PUF/TRNG responses are sampled using a 100-MHz clock. The 36-$\mu$W power includes power consumed in converting sine-wave clock signal to square wave and distributing the clock across the chip to the PUF devices.

Fig. 12 shows the measured intra- and inter-HD values. Intra-HD is measured over 0.9–1.2-V power supply and 0 °C–50 °C for four PUFs. Inter-HD is measured at a 1.2-V power supply at 27 °C for 16 PUFs. The 2048-bit PUF response is used for intra- and inter-HD calculations. The measured intra- and inter-HDs are 0.0906 and 0.4859, respectively. To perform stability tests under nominal conditions, we inter-

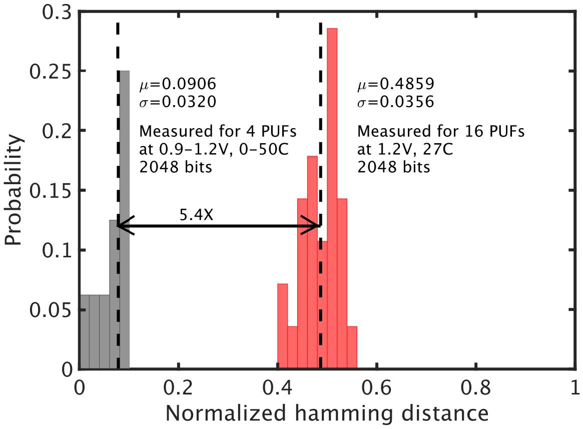


Fig. 12. Measured PUF intra- and inter-HD plots.

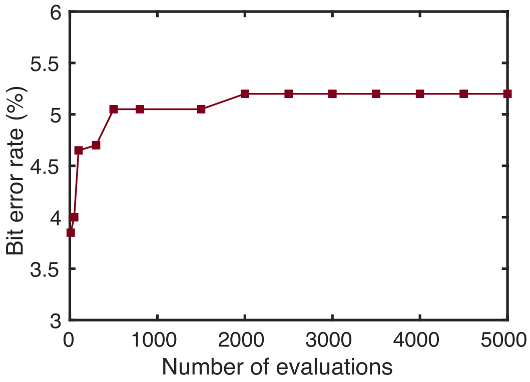


Fig. 13. Measured BER versus number of evaluations.

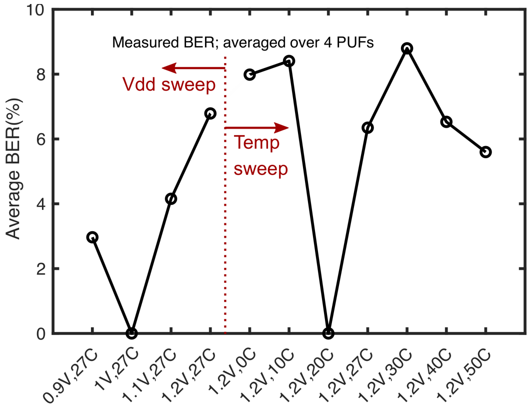


Fig. 14. Measured average BER across corners.

rogated a PUF chip repeatedly for 5000 times [25], [26]. Fig. 13 shows the native BER versus the number of evaluations. The BER is 5.3% for 5000 evaluations.

Fig. 14 shows the measured average BER across voltage and temperature corners. The BER is averaged across four PUFs. For voltage corners, BER is calculated with respect to (1 V, 27 °C), and for temperature corners, BER is calculated with respect to (1.2 V, 20 °C). The worst case BER is 8.8%. The BER is high since the entropy source of the PUF is a random mismatch in threshold voltage and mobility of transistors that vary significantly with voltage and temperature. We performed NIST SP 800-22 randomness tests [27] on 16 devices from two different test chips at the 1-V power supply and room temperature. For each device, we recorded the response for 25 different times. Thus, the NIST tests are performed on 400 PUF response streams. The PUF bitstream is considered to pass a NIST test with a confidence of 0.99 if the $p$-value for that test exceeds 0.01. Fig. 15 graphically shows the results of the NIST tests. For comparison, Fig. 15 also shows the results of NIST tests performed on the TRNG bitstreams obtained from the same devices. The PUF bitstreams pass 12/15 NIST tests with high pass rates almost close to 1, while the TRNG bitstreams pass all 15 NIST tests with a minimum pass rate of 0.9825. The failure of approximate entropy and cumulative sum tests is most likely due to uneven distribution of “0” and “1” in the PUF sequence [28].

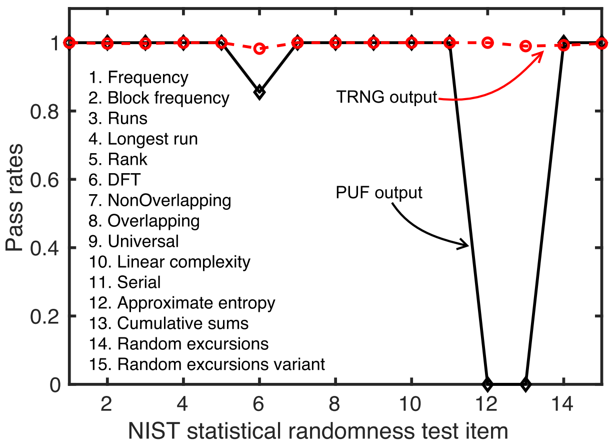


Fig. 15. NIST randomness test results for PUF and TRNG bitstreams at nominal condition.

Table I compares our work with state-of-the-art weak PUFs. For a 128-bit response, the proposed PUF has an area/bit of $1360^2$, which compares favorably to state-of-the-art designs and has an energy consumption, which is comparable with the state of the art.

### *B. TRNG Measurement Results*

The quality of randomness of the TRNG output is evaluated by performing NIST tests across the power supply range of 0.9–1.2 V and temperature range of 0 °C–50 °C. Fig. 16 shows the NIST test results across voltage and temperature corners. The TRNG outputs pass all the NIST tests with a pass ratio of 1 except for the 1-V, 20 °C corner in which the pass ratio for approximate entropy test drops to 0.9375. Fig. 17 shows the plots of the histogram of the Shannon entropy of TRNG output measured across 16 devices and voltage and temperature corners. For a random variable $X$ with outcomes $x \in [0, 1]$ and probability mass function $P(x)$, the Shannon entropy is defined by

$$H_{\text{shannon}} = -P(0) \cdot \log_2\{P(0)\} - P(1) \cdot \log_2\{P(1). \quad (4)$$

The TRNG output has a mean Shannon entropy of 0.9991 with a standard deviation of 0.0017. Fig. 18 shows the measured bias in 1-M TRNG output stream at nominal conditions for ten chips. The worst case $P(1)$ is 0.5004 for chip 10.

TABLE I

COMPARISON WITH STATE-OF-THE-ART WEAK PUFs

| | [26]<br>ISSCC'17 | [5]<br>JSSC'08 | [29]<br>TCAS–I'15 | [4]<br>ISSCC'14 | [30]<br>ISSCC'15 | [6]<br>JSSC'16 | [6]<br>JSSC'16 | This<br>work |
|---|---|---|---|---|---|---|---|---|
| **Process(nm)** | 180 | 130 | 180 | 22 | 40 | 65 | 65 | **65** |
| **Architecture** | Amplifier | Latch | SC | Latch | RO | INV | SA | **DAC+RO** |
| **Area/bit(F$^2$)*** | 1082 | 538500 | 56623 | 9581 | 2062 | 6000 | 12000 | **1360** |
| **Energy/bit(fJ/bit)** | 91.1 | 1600 | – | 190 | 17750 | 15 | 163 | **360** |
| **95% ACF** | – | 0.0884 | – | 0.01 | 0.0283 | 0.0363 | 0.0363 | **0.0108** |
| **Throughput (Mbps)** | – | 1 | – | – | 1.6 | – | – | **100** |
| **Inter-HD** | 0.4988 | 0.5012 | 0.498** | 0.51** | 0.5007 | 0.5014 | 0.5014 | **0.4859** |
| **Intra-HD** | 0.0007 | 0.038 | 0** | 0.02683** | 0.0101 | 0.0033 | 0.0034 | **0.0906** |

* F=minimum feature; ** after post-processing

TABLE II

COMPARISON WITH STATE-OF-THE-ART TRNGs

| | [17]<br>ISSCC'14 | [18]<br>CICC'14 | [34]<br>JSSC'16 | [31]<br>ISSCC'17 | [35]<br>JSSC'17 | [19]<br>JSSC'19 | [36]<br>VLSI'18 | This<br>Work |
|---|---|---|---|---|---|---|---|---|
| **Process(nm)** | 65 | 65 | 40 | 65 | 180 | 14 | 65 | **65** |
| **Entropy Source** | Jitter accum. | Jitter accum. | Jitter accum. | Jitter accum. | Chaotic map | Meta-stability | Meta-stability | **Thermal noise** |
| **Supply(V)** | 0.9 | 0.8 | 0.9 | 1.08 | 0.6 | 0.65 | 0.53 | **1** |
| **Operating voltage(V)** | – | 0.8-1.2 | 0.6-1 | 1.08-1.44 | 0.6-0.85 | 0.55-0.75 | 0.5-1.00 | **0.9-1.2** |
| **Throughput(Mbps)** | 2.8 | 2 | 2 | 8.2 | 0.216 | 1480 | 3.2 | **100** |
| **Energy(pJ/b)** | 57 | 66 | 23 | 36 | 0.38 | 2.5 | 2.58 | **0.36** |
| **Calibration needed** | No | Yes | Yes | No | No | Yes | Yes | **No** |
| **Post-processing** | No | Yes | No | No | Yes | No | Yes | **No** |

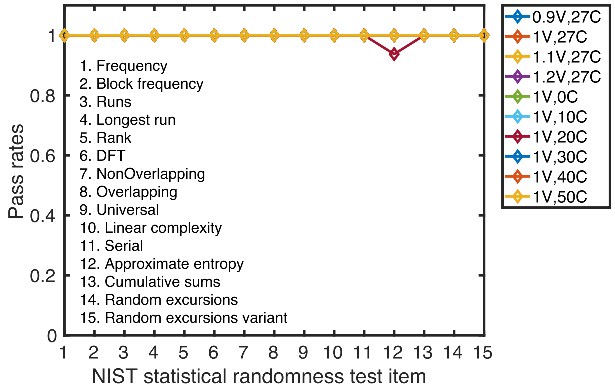


Fig. 16. NIST randomness test results for TRNG bitstreams across VT corners.

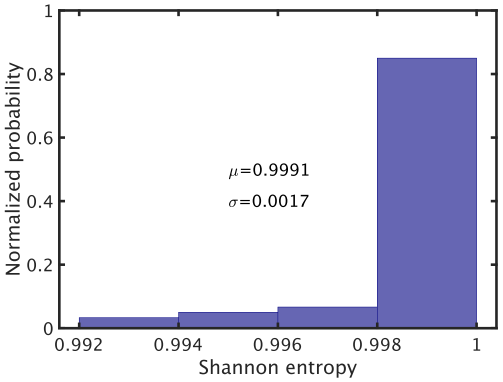


Fig. 17. Measured histogram of the Shannon entropy of raw TRNG bitstream across multiple devices and voltage and temperature corners.

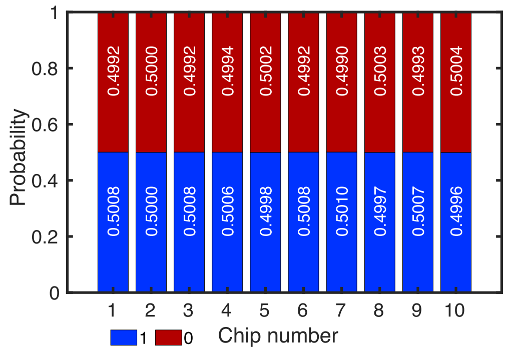


Fig. 18. Measured bias of TRNG bitstream for ten chips.

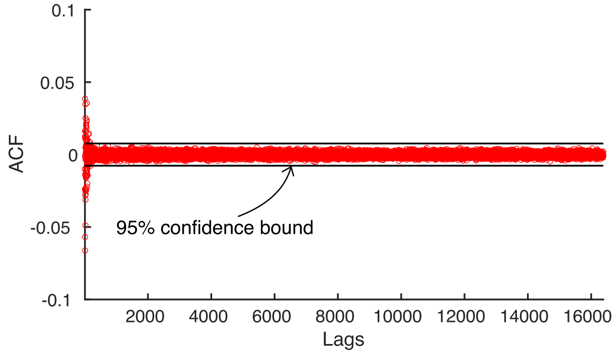
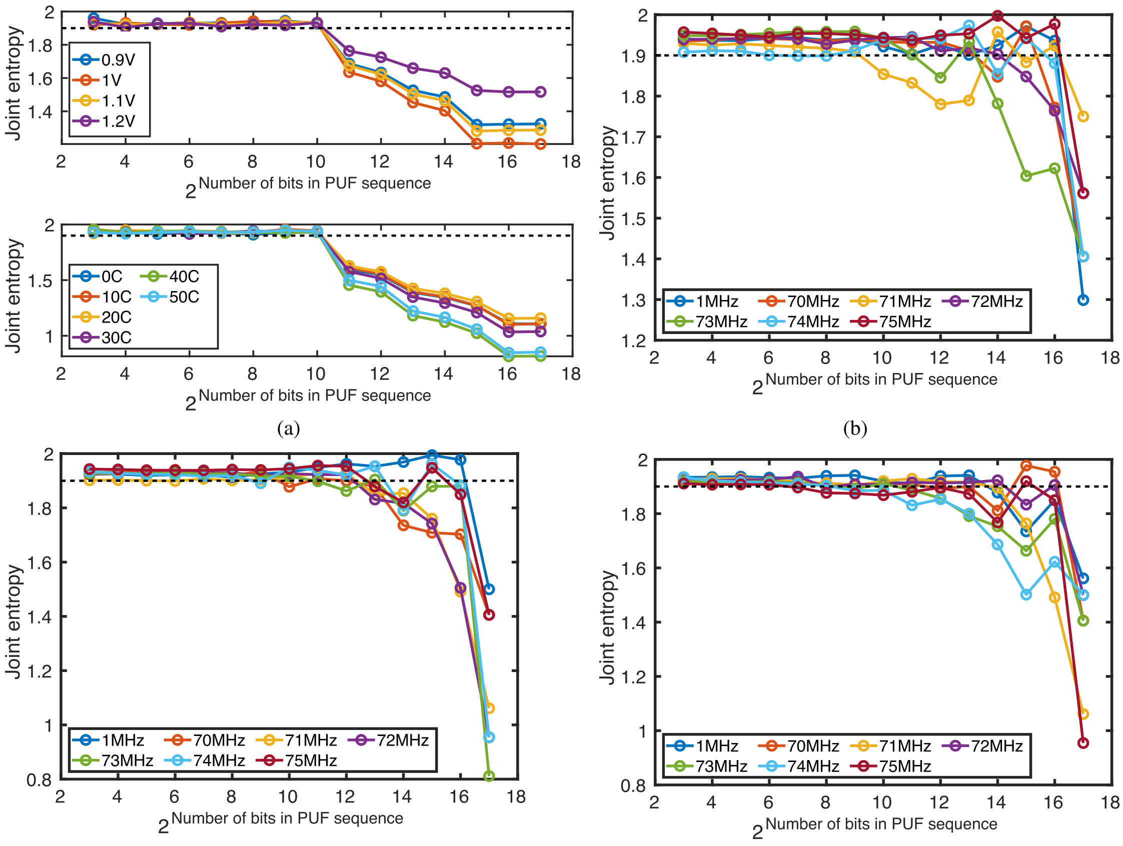


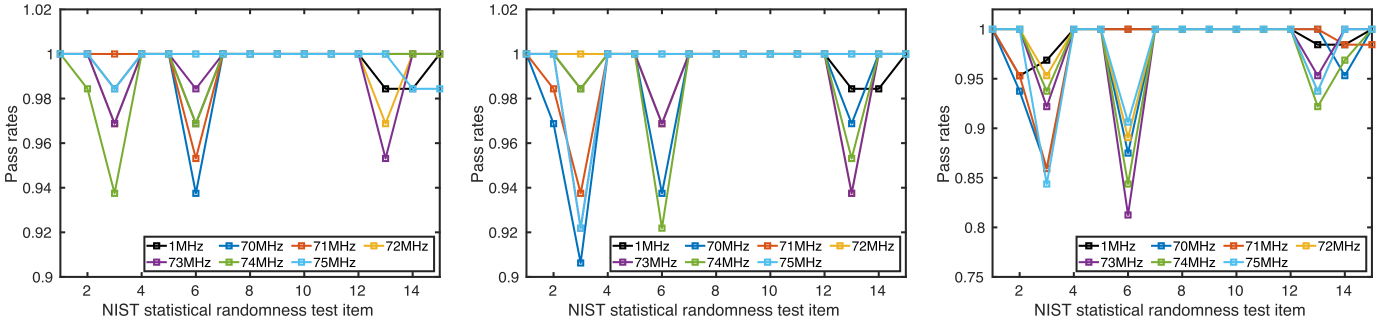
Fig. 19. Measured ACF for TRNG output.

Fig. 19 shows the measured ACF for raw TRNG output. The TRNG ACF is bounded within 95% confidence limits of 0.0077. Table II compares our TRNG with state-of-the-art TRNGs. The proposed TRNG has the lowest energy consumption of 0.36 pJ/bit. The proposed TRNG has 100× lower



(a) (b) (c) (d)

Fig. 20. Measured joint entropy averaged over four PUFs for (a) different VT conditions; and supply injection with sine-wave inputs with amplitudes of (b) 20, (c) 100, and (d) 200 mV.



(a) (b) (c)

Fig. 21. Supply injection attack results with sine-wave inputs with amplitude. (a) 20, (b) 100, and (c) 200 mV.

energy than [17] and [31] that also do not require either calibration or postprocessing.

### C. Robustness Against Fault and Injection Attacks

Fault and injection attacks can be used to reduce the entropy of both PUF and TRNG [32], [33]. For our PUF, fault attacks can be used to increase temporal correlation in the PUF output that will reduce the useful sequence length, while, for TRNG, fault attacks can be used to reduce the entropy of the TRNG bitstream. Fault attacks can be launched by a variety of techniques, such as varying supply voltage and temperature, as well as using optical attacks on decapsulated chips, such as using a laser pulse to introduce faults. In this work, we will only focus on fault attacks by varying the environmental conditions—supply voltage and temperature. Fig. 20 shows the measured joint entropy versus sequence length across VT corners as well for different sinusoidal signals injected into the power supply. The joint entropy values are averaged over four PUFs. The measured joint entropy remains above 1.9 for sequence lengths ≤128 bits, which shows that our PUF is robust against environmental fault attacks induced through a change in voltage and temperature, as well as injection of sine-wave signals into the supply voltage.

The TRNG has already been demonstrated to pass NIST tests across VT corners. To test the robustness of the TRNG against frequency-injection attacks, we injected sine-waves with varying amplitudes into the power supply. We injected a low-frequency 1-MHz sine-wave and at frequencies in the range of 70–75 MHz, which is close to the RO center frequency. Fig. 21(a)–(c) shows results of NIST tests at nominal conditions for input amplitudes of 20, 100, and 200 mV, respectively. The NIST tests are performed in the same sequence, as shown in Fig. 16. At 20-mV amplitude, the NIST pass rate remains above 0.98 for 1-MHz input and 0.938 for the high-frequency inputs. The injected sine waves change the bias of TRNG, which leads to a drop in pass rates for runs test, DFT test, and cumulative sums tests. However, the drop in pass rate is small, which shows that the cascode PMOS current source shields the ROs from power-supply fluctuation. The pass rate drops more for high-frequency inputs as the cascode impedance reduces at high frequency. For 100-mV sine-wave amplitude, the NIST pass rate does not change for 1-MHz input. However, the pass rates drop to near 0.9 for the high-frequency inputs. For 200-mV sine-wave amplitude, the NIST pass rate is still above 0.95 for 1-MHz input but drops significantly for the high-frequency inputs. The measurement results show that the TRNG is relatively robust to low-frequency power-supply injection attacks till 200-mV amplitude but is susceptible to power-supply injection attacks with high-frequency inputs. Robustness against supply injection attacks with high-frequency inputs can be increased by adding a low-pass filter to the power supply, as shown in [17].

## IV. Conclusion

This work presents a unified PUF+TRNG architecture based on cascode DAC and ring VCO. A mismatch between current sources in the DAC is quantized by a ring VCO and MSB of the quantized output forms PUF sequence. Thermal noise in the DAC and VCO as well as clock jitter enables LSB of the quantizer output to act as TRNG. In contrast to conventional PUFs that require $M$ unit elements to generate an $M$-bit response, the proposed architecture uses a single PUF element to generate a temporal $M$ bit sequence by sampling the VCO quantized output over $M$ periods. A 65-nm test chip is fabricated and characterized to validate the performance of the PUF and TRNG. The proposed architecture compares favorably with state-of-the-art PUF and TRNG designs in terms of energy/bit while having a small area.

## References

[1] 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*, Jun. 2004, pp. 176–179.

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

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

[4] 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 22nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 278–279.

[5] 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, Jan. 2008.

[6] 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.

[7] 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 130nm CMOS," in *Proc. Symp. VLSI Circuits*, Jun. 2017, pp. C268–C269.

[8] B. Park, M. Tehranipoor, D. Forte, and N. Maghari, "A metal-via resistance based physically unclonable function with 1.18% native instability," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2019, pp. 1–4.

[9] A. Herkle, J. Becker, and M. Ortmanns, "Exploiting weak PUFs from data converter nonlinearity—E.g., A multibit CT $\Delta\Sigma$ modulator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 7, pp. 994–1004, Jul. 2016.

[10] Q. Tang, W. H. Choi, L. Everson, K. K. Parhi, and C. H. Kim, "A physical unclonable function based on capacitor mismatch in a charge-redistribution SAR-ADC," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2018, pp. 1–5.

[11] A. Duncan, L. Jiang, and M. Swany, "Repurposing SoC analog circuitry for additional COTS hardware security," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Apr. 2018, pp. 201–204.

[12] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 5, pp. 615–621, May 2000.

[13] N. C. Laurenciu and S. D. Cotofana, "Low cost and energy, thermal noise driven, probability modulated random number generator," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 2724–2727.

[14] S. K. Mathew *et al.*, "$\mu$RNG: A 300–950 mV, 323 Gbps/W all-digital full-entropy true random number generator in 14 nm FinFET CMOS," *IEEE J. Solid-State Circuits*, vol. 51, no. 7, pp. 1695–1704, Jul. 2016.

[15] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 78–85, Jan. 2008.

[16] S. Satpathy *et al.*, "An all-digital unified static/dynamic entropy generator featuring self-calibrating hierarchical von Neumann extraction for secure privacy-preserving mutual authentication in IoT mote platforms," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2018, pp. 169–170.

[17] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 280–281.

[18] Q. Tang, B. Kim, Y. Lao, K. K. Parhi, and C. H. Kim, "True random number generator circuits based on single- and multi-phase beat frequency detection," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2014, pp. 1–4.

[19] S. K. Satpathy *et al.*, "An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical von Neumann extraction in 14-nm tri-gate CMOS," *IEEE J. Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, Apr. 2019.

[20] K. Lee, Y. Yoon, and N. Sun, "A scaling-friendly low-power small-area $\Delta\Sigma$ ADC with VCO-based integrator and intrinsic mismatch shaping capability," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 5, no. 4, pp. 561–573, Dec. 2015.

[21] E. Gutierrez, L. Hernandez, F. Cardes, and P. Rombouts, "A pulse frequency modulation interpretation of VCOs enabling VCO-ADC architectures with extended noise shaping," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 2, pp. 444–457, Feb. 2018.

[22] M. Pehl, A. R. Punnakkal, M. Hiller, and H. Graeb, "Advanced performance metrics for physical unclonable functions," in *Proc. Int. Symp. Integr. Circuits (ISIC)*, Dec. 2014, pp. 136–139.

[23] N. Thanh, K. Kim, S. Hong, and T. Lam, "Entropy correlation and its impacts on data aggregation in a wireless sensor network," *Sensors*, vol. 18, no. 9, p. 3118, Sep. 2018.

[24] M. M. Mukaka, "A guide to appropriate use of correlation coefficient in medical research," *Malawi Med. J.*, vol. 24, no. 3, pp. 69–71, 2012.

[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, Oct. 2018.

[26] 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 *IEEE ISSCC Dig. Tech. Papers*, Feb. 2017, pp. 146–147.

[27] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Tech. Rep. 800-22 Rev 1a, 2010.

[28] M. Danesh, A. B. Venkatasubramaniyan, G. Kapoor, and A. Sanyal, "A 0.36 pJ/bit analog PUF based on current steering DAC and VCO," in *Proc. IEEE 62nd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2019, pp. 578–581.

[29] M. Wan, Z. He, S. Han, K. Dai, and X. Zou, "An invasive-attack-resistant PUF based on switched-capacitor circuit," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 8, pp. 2024–2034, Aug. 2015.

[30] 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 40nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2015, pp. 1–3.

[31] E. Kim, M. Lee, and J.-J. Kim, "8Mb/s 28Mb/mJ robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2017, pp. 144–145.

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

[33] S. Tajik, H. Lohrke, F. Ganji, J.-P. Seifert, and C. Boit, "Laser fault attack on physically unclonable functions," in *Proc. Workshop Fault Diagnosis Tolerance Cryptography (FDTC)*, Sep. 2015, pp. 85–96.

[34] K. Yang, D. Blaauw, and D. Sylvester, "An all-digital edge racing true random number generator robust against PVT variations," *IEEE J. Solid-State Circuits*, vol. 51, no. 4, pp. 1022–1031, Apr. 2016.

[35] M. Kim, U. Ha, K. J. Lee, Y. Lee, and H.-J. Yoo, "A 82-nW chaotic map true random number generator based on a sub-ranging SAR ADC," *IEEE J. Solid-State Circuits*, vol. 52, no. 7, pp. 1953–1965, Jul. 2017.

[36] V. R. Pamula, X. Sun, S. Kim, F. U. Rahman, B. Zhang, and V. S. Sathe, "An all-digital true-random-number generator with integrated de-correlation and bias correction at 3.2-to-86 MB/S, 2.58 PJ/Bit in 65-NM CMOS," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2018, pp. 1–2.

**Mohammadhadi Danesh** (Graduate Student Member, IEEE) received the M.S. degree from the Iran University of Science and Technology, Tehran, Iran, in 2014, and the Ph.D. degree from University at Buffalo, Buffalo, NY, USA, in 2020.

He is an Analog/Digital Circuits and Design Verification Engineer at Cirrus Logic, Austin, TX, USA. Prior to this, he was a Research Assistant at University at Buffalo working on VCO-based modulators and higher order MASH ADCs in such biomedical and hardware security applications as skin cancer detection and PUFs. Also, he was an intern as a Mixed-Signal Design Verification Engineer at IDEX America Inc., Rochester, NY, USA, in 2018. Before starting his Ph.D. program, he was a Research Assistant at the Iran University of Science and Technology, working on analog computational blocks for biomedical applications.

Dr. Danesh is a recipient of the 2019 IEEE MWSCAS Best Student Paper Award.

**Aishwarya Bahudhanam Venkatasubramaniyan** received the B.E. degree in electrical and electronics engineering from Anna University, Chennai, India, in 2016, and the M.S. degree in electrical engineering from University at Buffalo, Buffalo, NY, USA, in 2018.

She is currently a Product Development Engineer with Intel Corporation, Folsom, CA, USA, working in the Nonvolatile Memory Section Group. Her research interests include nonvolatile memory, security with physically unclonable functions, and machine learning.

**Gaurav Kapoor** received the B.E. degree from PES University, Bengaluru, India, in 2016, and the M.S. degree in electrical engineering from University at Buffalo, NY, USA, in 2019.

In 2018 summer, he was an intern with the Analog/Mixed Signal Design Group, Macom Technology Solutions, Santa Clara, CA, USA, designing clock buffers to drive high-speed SERDES. He is currently a Device Engineer with the Technology Development Group, Intel Corporation, Hillsboro, OR, USA. His research interests include analog circuit design, mixed-signal security circuits, and data converters.

**Naveen Ramesh** received the B.E. degree from Anna University, Chennai, India, in 2018, and the M.S. degree in electrical engineering at University at Buffalo, Buffalo, NY, USA.

In spring 2020, he interned with Esensors Inc., Buffalo, where he is involved in an embedded system design team for developing electrical sensors. He is currently with Qualcomm, San Jose, CA, USA. His research interest includes mixed-signal machine learning circuits for biomedical applications.

**Sudarsan Sadasivuni** graduated from the University of Houston, Houston, TX, USA, in 2017. He is currently working toward the Ph.D. degree at the Department of Electrical Engineering, University at Buffalo, Buffalo, NY, USA.

His research interests include mixed signal machine learning circuits' designing, data analysis, and developing deep learning network models for medical applications.

**Sanjeev Tannirkulam Chandrasekaran** (Graduate Student Member, IEEE) received the B.Tech. degree in electronics and instrumentation from SASTRA University, Thanjavur, India, in 2016. He is currently working toward the Ph.D. degree in electrical engineering at University at Buffalo, Buffalo, NY, USA.

He has held internship positions at Mythic-AI, Austin, TX, USA, and GE Global Research, Niskayuna, NY, USA, where he was involved in mixed-signal IC design. His research interest is geared toward developing scalable energy-efficient circuits for IoT applications with a focus on data converters and edge-AI.

Dr. Chandrasekaran is a recipient of the 2019 MWSCAS Student Participation Grant and the 2019 CICC Student Travel Grant Award. He currently serves as a reviewer for the IEEE Transactions on Circuits and Systems—I: Regular Papers and IEEE Solid-State Circuit Letters.

**Arindam Sanyal** (Member, IEEE) received the B.E. degree from Jadavpur University, Kolkata, India, in 2007, the M.Tech. degree from IIT Kharagpur, Kharagpur, India, in 2009, and the Ph.D. degree from The University of Texas at Austin, Austin, TX, USA, in 2016.

He is currently an Assistant Professor with the Electrical Engineering Department, The State University of New York at Buffalo, Buffalo, NY, USA. Prior to this, he was a Design Engineer working on low-jitter PLLs at Silicon Laboratories, Austin. His research interests include analog/mixed signal design, biomedical sensor design, analog security, and on-chip artificial neural networks.

Dr. Sanyal is a recipient of the 2020 NSF CISE Research Initiation Initiative (CRII) Award, the Intel/Texas Instruments/Catalyst Foundation CICC Student Scholarship Award in 2014, and the Mamraj Agarwal Award in 2001.