A Compact Low-Voltage True Random Number Generator Based on Inkjet Printing Technology

Erozan, Ahmet Turan; Wang, Guan Ying; Bishnoi, Rajendra; Aghassi-Hagmann, Jasmin; Tahoori, Mehdi B.

DOI
10.1109/TVLSI.2020.2975876

Publication date
2020

Document Version
Final published version

Published in
IEEE Transactions on Very Large Scale Integration (VLSI) Systems

A Compact Low-Voltage True Random Number Generator Based on Inkjet Printing Technology

Ahmet Turan Erozan, Guan Ying Wang, Rajendra Bishnoi, Jasmin Aghassi-Hagmann, and Mehdi B. Tahoori, *Senior Member, IEEE*

***Abstract*— Printed electronics (PE) is a fast-growing field with promising applications in wearables, smart sensors, and smart cards, since it provides mechanical flexibility, and low-cost, on-demand, and customizable fabrication. To secure the operation of these applications, true random number generators (TRNGs) are required to generate unpredictable bits for cryptographic functions and padding. However, since the additive fabrication process of the PE circuits results in high intrinsic variations due to the random dispersion of the printed inks on the substrate, constructing a printed TRNG is challenging. In this article, we exploit the additive customizable fabrication feature of inkjet printing to design a TRNG based on electrolyte-gated field-effect transistors (EGFETs). We also propose a printed resistor tuning flow for the TRNG circuit to mitigate the overall process variation of the TRNG so that the generated bits are mostly based on the random noise in the circuit, providing a true random behavior. The simulation results show that the overall process variation of the TRNGs is mitigated by 110 times, and the generated bitstream of the tuned TRNGs passes the National Institute of Standards and Technology – Statistical Test Suite. For the proof of concept, the proposed TRNG circuit was fabricated and tuned. The characterization results of the tuned TRNGs prove that the TRNGs generate random bitstreams at the supply voltage of down to 0.5 V. Hence, the proposed TRNG design is suitable to secure low-power applications in this domain.**

***Index Terms*— Additive manufacturing, additive tuning, electrolyte-gated transistors (EGT), emerging technologies for computing, fabrication, inkjet-printing, Internet of Things (IoT), low-power, printed electronics (PE), process variation, security, true random number generator (TRNG).**

Manuscript received June 21, 2019; revised October 9, 2019, December 23, 2019, and January 29, 2020; accepted February 17, 2020. Date of publication March 16, 2020; date of current version June 1, 2020. This work was supported in part by the Ministry of Science, Research and Arts of the State of Baden-Württemberg through the MERAGEM Doctoral Program. *(Corresponding author: Ahmet Turan Erozan.)*

Ahmet Turan Erozan is with the Chair of Dependable Nano Computing, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany, and also with the Institute of Nanotechnology, Karlsruhe Institute of Technology, 76344 Eggenstein-Leopoldshafen, Germany (e-mail: ahmet.erozan@kit.edu).

Guan Ying Wang is with the Institute of Nanotechnology, Karlsruhe Institute of Technology, 76344 Eggenstein-Leopoldshafen, Germany, and also with the Department of Nanotechnology Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: jane.wang@edu.uwaterloo.ca).

Rajendra Bishnoi is with the Computer Engineering Lab, Delft University of Technology, 2600 AA Delft, The Netherlands (e-mail: r.k.bishnoi@tudelft.nl).

Jasmin Aghassi-Hagmann is with the Institute of Nanotechnology, Karlsruhe Institute of Technology, 76344 Eggenstein-Leopoldshafen, Germany, and also with the Electrical Engineering Department, Offenburg University of Applied Sciences, 77652 Offenburg, Germany (e-mail: jasmin.aghassi@kit.edu).

Mehdi B. Tahoori is with the Chair of Dependable Nano Computing, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany (e-mail: mehdi.tahoori@kit.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.2020.2975876

I. Introduction

PRINTED electronics (PE) has recently received a lot of interests, since it provides the advantages of mechanical flexibility, and low-cost, on-demand, and customizable fabrication [5]–[7], which result in the use of PE in various applications such as Internet of Things (IoT) [8], wearables [13], radio-frequency-identification tags [14], smart cards [15], smart labels [16], and smart sensors [4]. Several organic and inorganic printed transistors have been demonstrated to construct functional PE circuits that are fabricated using additive processes [19], [25]. Inorganic electrolyte-gated field-effect transistors (EGFETs), which enable low-voltage PE circuits, have recently been used in the circuits, demonstrating that they enable the circuits operating below 1 V [11], [12], [25], [26].

The growth in PE gives rise to security concerns, specifically authentication and cryptography, since the projected application areas are mostly interconnected and contain sensitive data [12], [44]. To that end, true random number generators (TRNGs) are employed to generate unpredictable keys, the initial vector of pseudorandom number generators (PRNGs), padding values, and random challenge sequences [3].

TRNGs digitize an unpredictable natural phenomenon (entropy source) such as thermal noise to random bits, as shown in Fig. 1, while PRNGs use short initial random bits generated by a TRNG and generate random-looking longer bitstreams [33]. The entropy source of the TRNG design is the most crucial component, since it provides the unpredictability, and the TRNG circuit should harvest the entropy without introducing bias. The bias caused by the entropy source, the process variation of the circuit, or the environmental changes can be masked using a postprocessor, although it is not needed in all designs [30], [33].

Additive printing processes including inkjet printing have high intrinsic process variation, resulting in the dispersion of the ink printed in multiple steps, where each step varies on its own [2], [28], [31]. Since the high process variation can significantly introduce bias to the generated bits of TRNGs, designing an inkjet-printed TRNG, in other word mitigating the high variation, is very challenging. Nevertheless, inkjet printing enables the customization of each circuit individually, which can be exploited to mitigate the high process variation of the fabricated circuits in the postfabrication phase [1], [31].

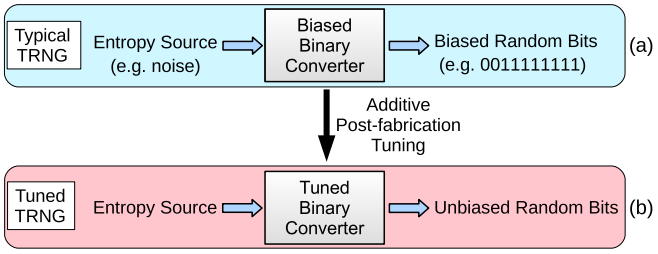


Fig. 1. Illustration of the proposed TRNG approach. (a) Typical TRNG generating biased bits because of process variation. (b) Tuned TRNG, which uses additive manufacturing to mitigate process variation.

A preliminary version of this article was published in [9], in which an inkjet-printed TRNG, which uses the customizable fabrication feature of this technology to compensate the high intrinsic process variation, is presented. A printed resistor that can be tuned by printing additional layers is presented and used in the proposed circuit to mitigate the overall process variation, so that the power-up behavior of the circuit is highly based on the noise. A resistor tuning flow is proposed to determine the point where the overall process variation of the circuit is mitigated, and the generated bits are random. In addition, we optimize the resistor tuning flow to reduce the measurement and tuning efforts. The results show that the mean of the overall process variation of the TRNG instances is reduced by 110 times using the resistor tuning flow, and the optimized tuning flow decreases the tuning time by ten times. The proposed TRNG passes the National Institute of Standards and Technology – Statistical Test Suite (NIST-STS), showing that the proposed TRNG design can provide highly random bitstreams that pass the required tests.

In this article, we extend our work in [9] with fabrication and characterization results. We fabricated and tuned TRNG circuits to validate the functionality of the proposed TRNG. The experimental results show that the proposed tuning flow mitigates the process variation of the fabricated printed TRNGs, and they generate random bitstreams with nearly 50% probability of ones. To the best of our knowledge, this is the first printed TRNG in the literature.

The summary of the contributions of the overall work is as follows.

1) We present the first inkjet-printed TRNG using an EGFET.
2) We propose a method that exploits the additive manufacturing feature of PE using the presented printed resistor to mitigate efficiently the overall process variation of the proposed TRNG circuit.
3) We validate the randomness of the tuned TRNGs using the NIST-STS.
4) We fabricate the proposed TRNG and apply the resistor tuning flow to compensate the overall process variation. We characterize the tuned TRNGs to validate their operation at below 1 V.

The rest of this article is organized as follows. The details of the PE and EGFET technologies are given in Section II. Section III explains resistor tuning using additive printing based on fabrication data. In Section IV, we present the proposed inkjet-printed TRNG design. In Section V, the proposed resistor tuning flow is elaborated. Sections VI and VII present and discuss the simulation and fabrication results, respectively. Finally, Section VII concludes this article.

II. Preliminaries

A. Printed Electronics Technology

Printed electronics (PE) is a fast-growing market, and it enables several current and envisioned applications such as health-care diagnosis devices, energy harvesters, smart clothing, dynamic newspapers, smart labels, and smart cards, where mechanical flexibility and large-area, low-cost, lightweight, and/or on-demand fabrication are of special interest [8].

Instead of using complex, expensive, and environmentally hazardous photolithographic subtractive processes, PE circuits are fabricated using several additive processes, such as offset, screen, flexography, gravure, and inkjet printing, resulting in low-cost and on-demand fabrication [8]. The PE circuits are fabricated by printing several materials on a flexible or rigid substrate additively using one or multiple printing processes depending on the application requirements. Some of these processes, such as inkjet printing, have made possible the customizable fabrication, which is a highly beneficial feature for Industry 4.0 [1]. The customizable fabrication allows postfabrication tuning to make custom changes in the fabricated circuits.

Various printed transistors such as p-type organic-based thin-film transistors (OTFTs) [17], organic field-effect transistors (OFETs) [18], and n-type organic transistors [19], [20] are presented to form functional PE circuits. However, these transistors mostly suffer from high supply voltage and low field-effect mobility, making them unsuitable for low-power applications [5].

On the other hand, inorganic semiconductor-based transistors combined with an electrolyte gate, called electrolyte-gated field-effect transistors (EGFETs), provide high field-effect mobility and require low supply voltage ($\leq$1 V), since EGFETs have high gate capacitance [12], [21]–[27]. These advantages make the EGFET a promising candidate for low-power PE applications.

B. True Random Number Generators

Cryptographic algorithms and keys are the crucial points for securing systems. A random seed must be used to generate keys to be used in encryption/decryption, data padding, masking against differential power analysis (DPA), and one-time password (OTP) [33], [34].

TRNGs have been proposed to generate the random seed, which then can also be used for the initial vector of the pseudorandom number generators (PRNGs) to generate longer keys [33]–[35]. Metastability-based [37], [38] and RO-based [39], [40] TRNGs are commonly used to convert a physical entropy source such as thermal noise and optical noise into binary numbers. The physical entropy source should be unpredictable so that the generated numbers satisfy the randomness tests. On the other hand, the TRNG circuit should

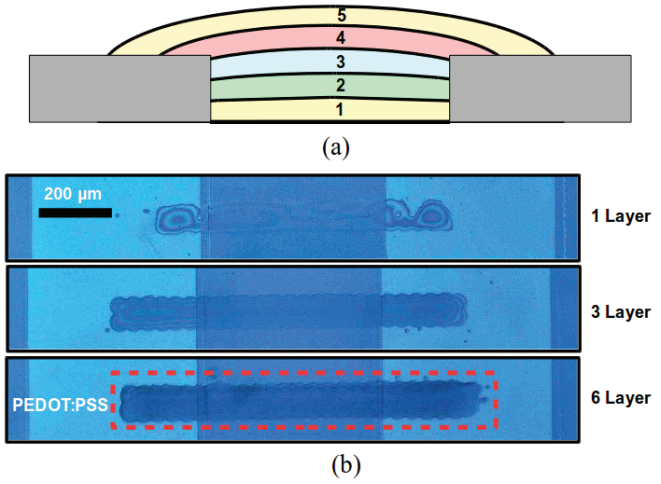


Fig. 2. (a) Illustration of additively printed layers. (b) Top-view photographs of the fabricated printed resistors.

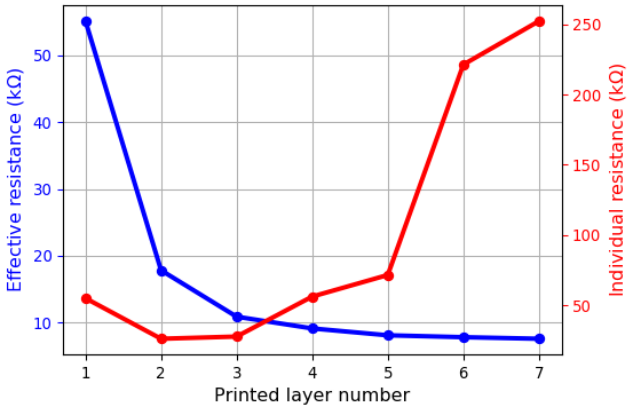


Fig. 3. Effective and individual resistance of the printed resistors with different layers.

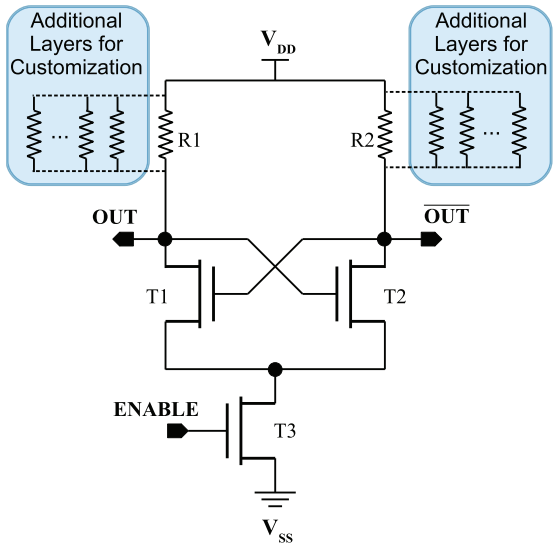


Fig. 4. Proposed TRNG circuit with customizable resistors. Overall process variation of the circuit is mitigated using additional layers for the customization of the printed resistors.

harvest the entropy without bias. The bias resulted from the entropy source, and the process and runtime variations of the circuit, or the environmental changes can be determined using online tests. Furthermore, the bias can be masked using postprocessors to increase the entropy of the TRNG output while reducing the throughput [33], [35].

C. Additive Printing of Resistors

Additive printing processes have several advantages over subtractive processes where sophisticated and/or expensive equipment and infrastructure are required. The advantages are low-cost, on-demand, and customizable fabrication. The customizable fabrication can be used to modify/tune the circuits with very little effort, after manufacturing.

We have examined an inkjet-printed resistor, exploiting the customizable fabrication [10]. The resistance of the printed resistor that uses PEDOT:PSS as a material can be modified by printing more layers on the top of the existing layers. Each layer can be represented as a resistor, and printing a layer on the top of the other layers adds another resistor in parallel, as shown in Fig. 2.

The printed resistors containing various number of layers with the width of 50 μm are fabricated and characterized at room temperature. The measured effective resistance and the extracted individual resistance of the layers are shown in Fig. 3. Since the path of each successively printed layer is longer than the previous layers, as shown in Fig. 2(a), the resistance of each layer is larger than the previous layer.

The measurements show that the effective resistance decreases while the total number of layers is increasing, and the individual resistance of the layers increases while the number of printed layers is increasing, except the first layer, since it does not form a continuous line on the substrate, as shown in Fig. 2(b). Furthermore, to reduce the effective resistance even faster, additional layers can be printed next to other layers, which adds less resistance in parallel compared with the layer printed on the top of the other layers. Therefore, this feature of resistor tuning can be used to compensate the process variation of the proposed TRNG circuit, as discussed in the next sections.

III. Proposed Inkjet-Printed TRNG Design

The proposed TRNG circuit should have a few number of circuit elements to satisfy the low-cost requirement, since most of the PE applications are expected to be at low cost. On the other hand, inkjet printing of the EGFETs causes high process variation, which results from the random dispersion of the inks on the substrate [12]. The high process variation leads to the high degree of bias on the generated bits from the TRNG, reducing the entropy. The process variation of the TRNG must be low to provide high entropy. In the existing TRNGs based on conventional technologies, the bias of the TRNG is mitigated using an additional calibration circuitry, which probes the generated bits, and examines and calibrates the core TRNG circuit [42]. However, the calibration circuitry adds an overhead to the TRNG core. Thus,

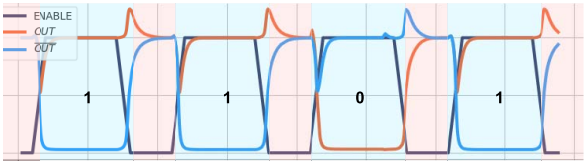


Fig. 5. Example simulated timing diagram of the output of an inkjet-printed TRNG circuit.

we have proposed a compact circuit, which uses few elements, and instead of the calibration circuitry, we have proposed a resistor tuning flow, which takes advantage of the additive manufacturing feature of inkjet printing, to mitigate the high process variation without area overhead. The proposed TRNG circuit and the proposed resistor tuning flow are elaborated in Sections III-A and III-B.

A. TRNG Circuit

The proposed TRNG circuit is a memory-based circuit that contains two cross-coupled inverters and an enable transistor enabling/disabling the circuit. The inverters are composed of an n-type EGFET and a resistor. This is done for two reasons. First, the use of resistors in the pull-up network allows realizing additive tuning. Second, the p-type inorganic channel materials usually have very poor characteristics; hence, effective p-type transistors are still under investigation. The circuit schematic of the TRNG is shown in Fig. 4.

The OUT and $\overline{\text{OUT}}$ nodes are equal to V_{DD} when the circuit is not enabled meaning that the ENABLE input is zeros. Since the symmetrical inverters lead to a metastable state, the feedback amplifies the random noise (thermal noise, shot noise, and so on) and drives the OUT and $\overline{\text{OUT}}$ nodes to the stable states, either ones or zeros depending on the noise, while the ENABLE input is switching to ones. Therefore, the noise is digitized to generate true random bits. Fig. 5 shows the waveform of the circuit generating the random bits based on the noise.

However, since the fabrication of the circuit is based on inkjet printing, it has high intrinsic process variation being derived from the random dispersion of the ink on the substrate. In addition, contrary to the silicon technology where the process variations are divided into local and global variations, which result in low variation between two close devices, all devices are printed individually by multiple additive steps in inkjet printing, which cause higher variation, even for the two cross-coupled inverters in this circuit.

The process variation causes a skew that forces the circuit to one side, which results in the bias at the generated bits. A skewed circuit whose behavior is shown in Fig. 6(a) is biased to ones because of process variation (Δ_{PV}), while the nonskewed circuit whose behavior is shown in Fig. 6(b) is not biased and generates bits based on the random noise, which is essential for a TRNG. Therefore, to construct an inkjet-printed TRNG, its high process variation should be mitigated. For this reason, we propose a resistor tuning flow explained in Section III-B.

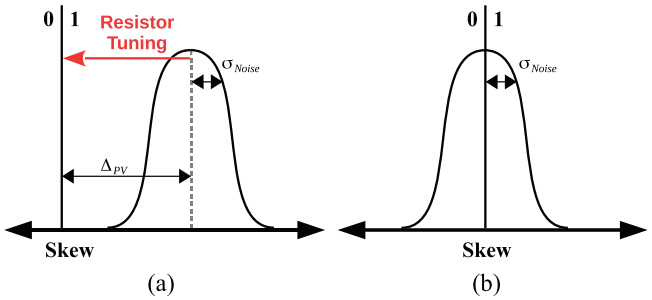


Fig. 6. Illustration of the behavior of (a) skewed and (b) nonskewed circuits (Δ_{PV}: skew because of process variation; σ_{Noise}: standard deviation of noise) [3].

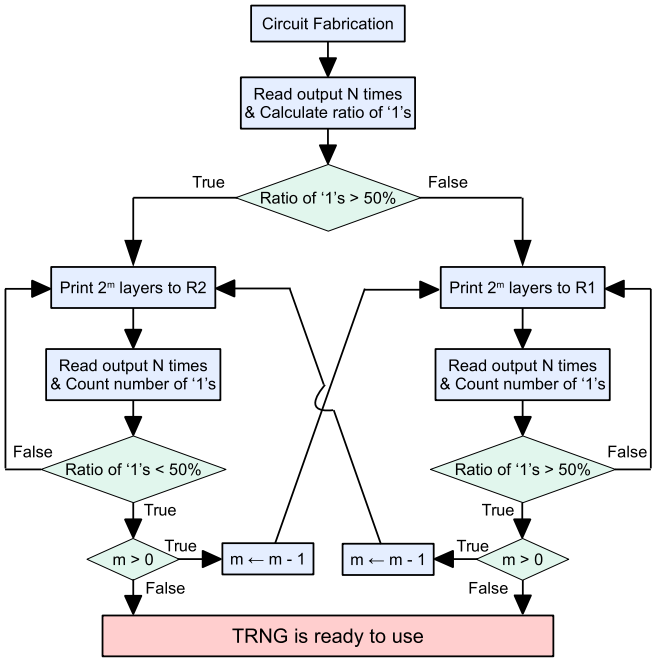


Fig. 7. Optimized resistor tuning flow to mitigate process variation of the proposed TRNG design. Resistors are additively tuned to converge the ratio of ones to 50%. m and N are flow parameters.

B. Resistor Tuning Flow

It is vital to compensate the skew of the proposed TRNG circuit, which results from the overall process variation. The proposed resistor tuning flow, as shown in Fig. 7, uses the additively printed resistor, as presented in Section III, to compensate the overall skew shown in Fig. 6. The printed resistor tuning flow is as follows. After fabricating the circuit, the output has to be read N times, and the number of ones in N read is counted. If the number of ones is greater than $N/2$ (50%), which means that the tuned circuit is skewed to ones, printing one layer to the $R2$ shifts the skew toward the neutral axis. If the number of ones is less than $N/2$, printing one layer to the $R1$ shifts the skew from zeros toward neutral axis. Printing additional layers to the $R1$ or $R2$ is repeated until the number of ones reaches to $N/2$.

Fig. 8(a) shows the ratio of ones in the generated bitstream of an inkjet-printed TRNG with respect to the number of additional layers. The simulation flow to obtain the generated

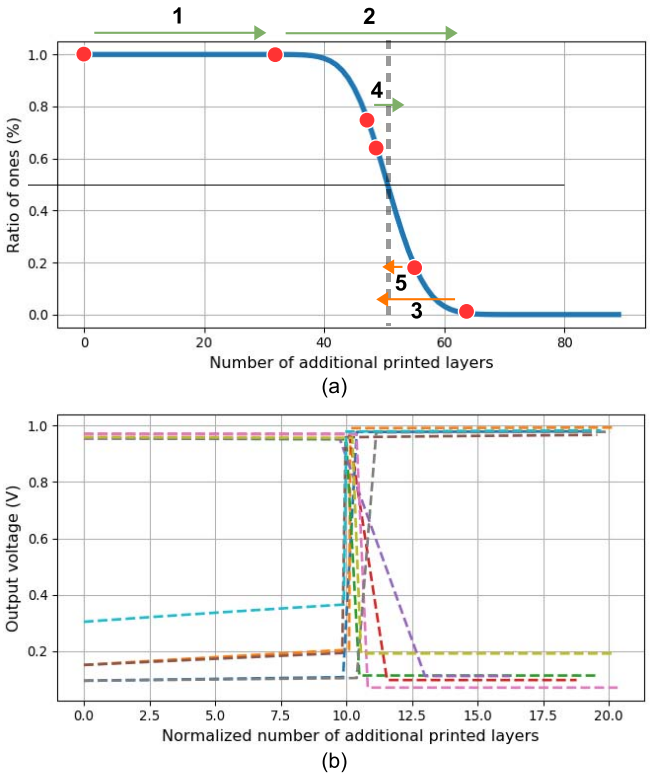


Fig. 8. (a) Ratio of ones with respect to number of additionally printed layers of a TRNG instance under noise ($\mu = 0$ V, $\sigma = 3$ mV). Red dots indicate the TRNG state, and the orange and green arrows represent the change in the TRNG state by printing additional layers to $R1$ and $R2$, respectively, based on the tuning flow shown in Fig. 7. (b) Output voltage level versus normalized number of additionally printed layers of ten TRNG instances (layer numbers where output is flipped are normalized to 10).

TABLE I

DESIGN PARAMETERS OF TRANSISTORS AND RESISTORS USED IN SIMULATION OF TRNG DESIGN. RESISTANCE OF RESISTORS IS THE INITIAL VALUE BEFORE RESISTOR TUNING

	T1	T2	T3			R1	R2
Width	200 μm		400 μm		Resistance	60 $k\Omega$	
Length	40 μm						

bitstream is based on the Monte Carlo simulation of a TRNG instance, which uses the parameters given in Table I and $\pm 10\%$ variation for the resistors and the variation model presented in [2]. In addition, a normal distributed random noise source that has the mean (μ) and sigma (σ) of 0 V and 3 mV is used in simulation. Since the range near to 50% ratio of ones (nonskewed point) is too short, the additional layers of the resistor are printed one by one to not miss the nonskewed point. However, this leads to very long tuning time (including the number of iterative measurements and printing steps), since, in each step, the circuit output has to be read N times. For this reason, we optimize the resistor tuning flow to reduce the tuning time. In the improved flow, as shown in Fig. 7, if the ratio of ones is greater (smaller) than 50%, 2^m layers are printed on the top of $R2$ ($R1$) in each step, and then, the measurements are done, until the ratio of ones is less (greater) than 50%. When it is less (greater) than 50%, 2^{m-1} layers are printed on the top of the resistor of the opposite branch, in this case $R1$ ($R2$) and vice versa, and it continues until the number of printed layers reaches one. Therefore, the overall tuning time is significantly reduced.

In addition to these improvements for the resistor tuning flow, the TRNG output voltage level can be used to improve further the tuning efforts. The change in the TRNG output voltage level with each successive printed resistor layer can give an insight about the skewness of the TRNG so that the step size can be adjusted more effectively. Fig. 8(b) shows the output voltage level of a TRNG circuit at different successive printing layers generated from the same setup described above. The more the circuit is skewed, the closer the output voltage levels to V_{DD} (or GND). As the skewness decreases, the output voltage level degrades more. This information could be used to optimize further the tuning flow. However, using such information requires more precise, costly, and sophisticated measurements at the tuning steps, unlike the fast and low-cost binary readouts used in the proposed tuning flow.

IV. SIMULATION-BASED ANALYSIS

The proposed TRNG design and the impact of the resistor tuning flow are evaluated based on the simulation results in this section. The details of the simulation setup, the results of the resistor tuning flow, and the results of the NIST-STS are explained in Sections IV-A–IV-D.

A. Simulation Setup

The design parameter details are given in Table I. We have assumed that the printed resistors are composed of 100 layers resulting in 60-kΩ effective resistance, and we extrapolated the effective resistance of each additional printed layer. In addition, the process variation of the resistors is considered as $\pm 10\%$ of resistances based on the experiments. For the EGFETs, we have employed the variation model of the EGFET presented in [2]. We have used 100 Monte Carlo instances of the printed TRNG, and a normal distributed noise source that has the mean (μ) and sigma (σ) of 0 V and 3 mV, respectively, is introduced between the inverters as an overall noise in the circuit to extract the results.

B. Resistor Tuning Flow Results

The minimum noise level to flip the output, which is called *flipping noise level* in this article, is used to quantify the overall skewness of the TRNG instances. To extract the flipping noise level of the instances, instead of a normal distributed noise, a dc voltage was swept between -100 and $+100$ mV. The number of TRNG instances based on their flipping noise levels, before and after resistor tuning, is shown in Fig. 9. The mean values of the absolute flipping noise level before and after the tuning are 35.41 and 0.32 mV, respectively, showing that the tuning flow reduces the mean variation by more than 110 times. In addition, the percentage of TRNG instances with the flipping noise level between ± 1 mV, resulting in less bias at the generated bits, increases from 1% to 96% after tuning.

As described in Section III, the resistors are tuned by printing additional layers in two ways, which we name *Baseline*

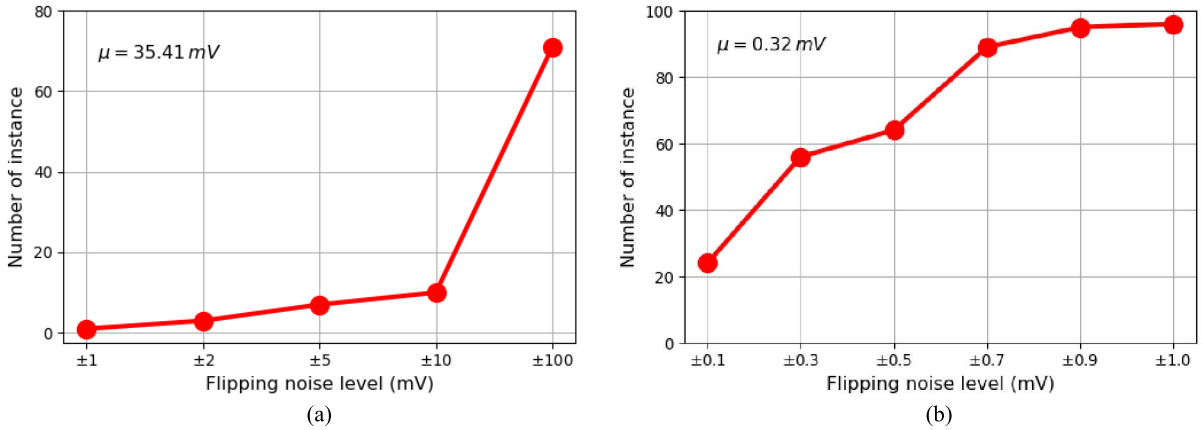


Fig. 9. Number of TRNG instances between various flipping noise levels (a) before resistor tuning and (b) after resistor tuning.

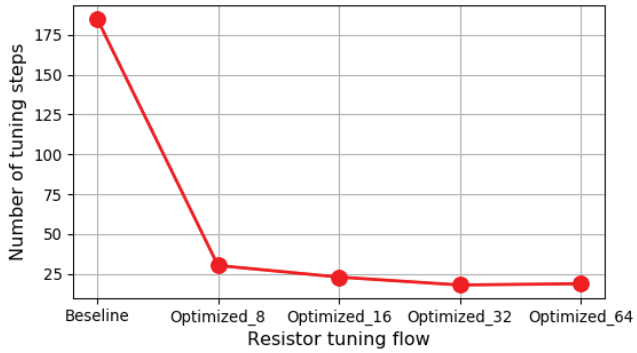


Fig. 10. Mean number of tuning steps of 100 TRNG instances for baseline (one-by-one layer printing) and optimized tuning flows (2^m layer printing). Baseline denotes one-by-one additional layer printing flow; 8, 16, 32, and 64 denote the initial 2^m value.

(one by one, printing only one resistor) and *Optimized_n*, where n is equal to 2^m and is the step size (n steps and tuning both resistors) for convenience. The average trials to tune the instances are shown in Fig. 10. The average number of tuning steps for the baseline flow is 185.15, while with the step size of 32 ($m = 5$), the average number of tuning steps is minimized to 17.98. Therefore, the number of tuning steps is reduced by more than ten times using our proposed method.

C. Analysis of Temperature Effect on Generated Bits

The generated bits of the circuits after resistor tuning are slightly biased, compared with ideal true random bits because of the remained skewness of the process variation, due to the process variation of the additional printed resistor layers as well as the discrete nature of tuning.

The effect of the remained skewness on the bits can be quantified as the sigma (σ) of the distribution of the ones ratio in the generated bits, which is 1.27%, while the mean is 49.81% at 25 °C, as shown in Fig. 11(a). To analyze the temperature effect on the randomness of the proposed TRNG, we use the EGFET model with temperature effect described in [12] and implemented a temperature constant into a printed resistor according to the ratios given in [43]. The mean and standard deviation of the number of ones are 49.78% and 1.67% at 60 °C, and 49.83% and 2.31% at −35 °C, as shown in Fig. 11(b) and (c), respectively. These results show that the effect of the temperature on the randomness of the tuned TRNGs is negligible.

TABLE II

NIST TEST RESULTS. GENERATED BITSTREAM INCLUDES 10 000 BITS FROM 100 SIMULATED TRNG INSTANCES. (A TEST REQUIRES THE P-VALUE GREATER THAN 0.001 AND THE PROPORTION GREATER THAN 96/100 TO PASS

Statistical Test	P-value	Proportion	Result
Frequency	0.202268	96/100	Pass
Block frequency	0.213309	100/100	Pass
Cumulative sums	0.428568	96/100	Pass
Runs	0.171867	99/100	Pass
Longest run of ones	0.437274	100/100	Pass
FFT	0.474986	98/100	Pass
Overlapping Template	0.055361	99/100	Pass
Serial	0.494555	100/100	Pass
Linear Complexity	0.249284	97/100	Pass

D. NIST-STS Test Results

The NIST-STS contains several tests explained in [29] to evaluate the randomness of the generated bits. We have used NIST-STS to evaluate the 10 000 bits generated from each tuned TRNG instance. A P-value greater than 0.001 and a proportion greater than 96/100 are required to pass the NIST tests. The results given in Table II show that the generated bits satisfy the requirements, and therefore, the proposed TRNG design passes the given NIST-STS tests.

V. FABRICATION-BASED ANALYSIS

We fabricated, tuned, and characterized the proposed TRNG design to validate our approach. It should be noted that the inkjet-printed EGFET technology used in the proposed TRNG is an emerging technology, and due to the lab setup that has limited yield and throughput, it requires a lot of effort to have functional circuits and to tune these circuits at this stage of the technology. The details of fabrication and characterization are explained in Sections V-A and V-B.

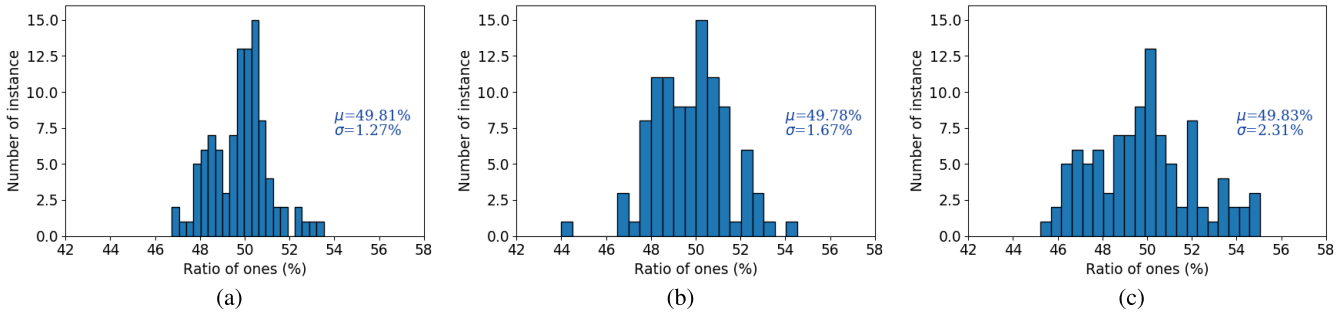
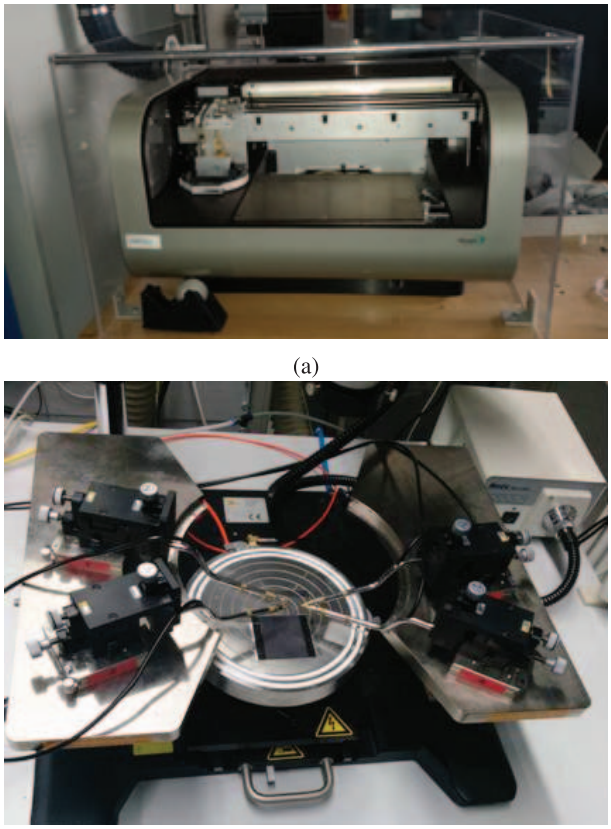


Fig. 11. Distribution of the ratio of ones out of 100 bits for tuned 100 Monte Carlo TRNG samples at (a) 25 °C, (b) 60 °C, and (c) −35 °C. Sigma values are similar in distributions, indicating that temperature effect on randomness is negligible.



(a)

(b)

Fig. 12. (a) Dimatix DMP-2831 Inkjet Printer used for fabrication and resistor tuning. (b) Süss Microtec Probe Station used for characterization.

A. Fabrication and Characterization Setup

The proposed TRNG circuit contains three transistors and two resistors. The width and length of the printed resistors are selected as 50 μm and 1 mm. The widths of T1, T2, and T3 are selected as 200, 200, and 600 μm, respectively, and the length of the transistors is selected as 60 μm.

In the fabrication process of the EGFETs, the channel material indium-oxide (In_2O_3) semiconductor is inkjet-printed using Dimatix DMP-283, which is shown in Fig. 12(a), between the drain and source electrodes, which are lithographically structured indium-tin oxide (ITO). Then, the substrates are annealed at 400 °C for 2 h. After that, the electrolyte is inkjet-printed on the top of the channel instead of a gate dielectric. Finally, poly(3,4-ethylenedioxythiophene)-polystyrenesulfonic acid (*PEDOT:PSS*) is inkjet-printed on the top of the electrolyte as a top gate [25], [41]. The detailed views, the fabrication process, and an optical image of the EGFET devices are shown in Fig. 13. For printed resistors, PEDOT:PSS is inkjet-printed with the width of 50 μm and the length of 1 mm. The wiring and test pads are structured using a conducting material, which is indium-tin oxide (ITO).

The fabricated TRNG circuits are contacted through a Süss Microtech probe station shown in Fig. 12(b). Agilent 4156C precision semiconductor parameter analyzer is used as the source for the supply voltage. The enable signal (ENABLE) is generated using a Keithley 3390 arbitrary waveform generator. The enable and output (OUT) signals are recorded using the Yokogawa DL6104 digital oscilloscope. All measurements are performed at room temperature and 50% relative humidity.

B. Results

The fabricated TRNGs are powered by 1-V supply voltage and enabled by applying a 1-Hz, 50% duty cycle pulse signal to the ENABLE input. The high level of the enable signal is set to supply voltage. After each power-up, the circuits are enabled 100 times, and their outputs are measured to observe their functionality and calculate the ratio of ones. Depending on the ratio of ones, an additional PEDOT:PSS layer is inkjet-printed on the top of either $R1$ or $R2$, as discussed in Section III-B. Fig. 14 shows the annotated images of a fabricated TRNG before and after resistor tuning. The area usage of the fabricated TRNG is 4.59 mm^2.

Fig. 15 shows the measured timing waveform of a fabricated TRNG after resistor tuning. After enabling the circuit, the output (OUT) becomes ones or zeros depending on the mismatch of the inverter pair, which results from the process variation and the noise in the circuit. Since the additive resistor tuning alleviates the mismatch stemmed from process variation, the output value relies on the random noise each time the circuit is enabled.

The change in the ratio of the ones of the fabricated TRNGs with respect to the number of additional layers is shown in Fig. 11. Fabricated TRNGs are annotated with a number (e.g., TRNG-1) for convenience. The measurements show that resistor tuning mitigates the process variation of the circuit,

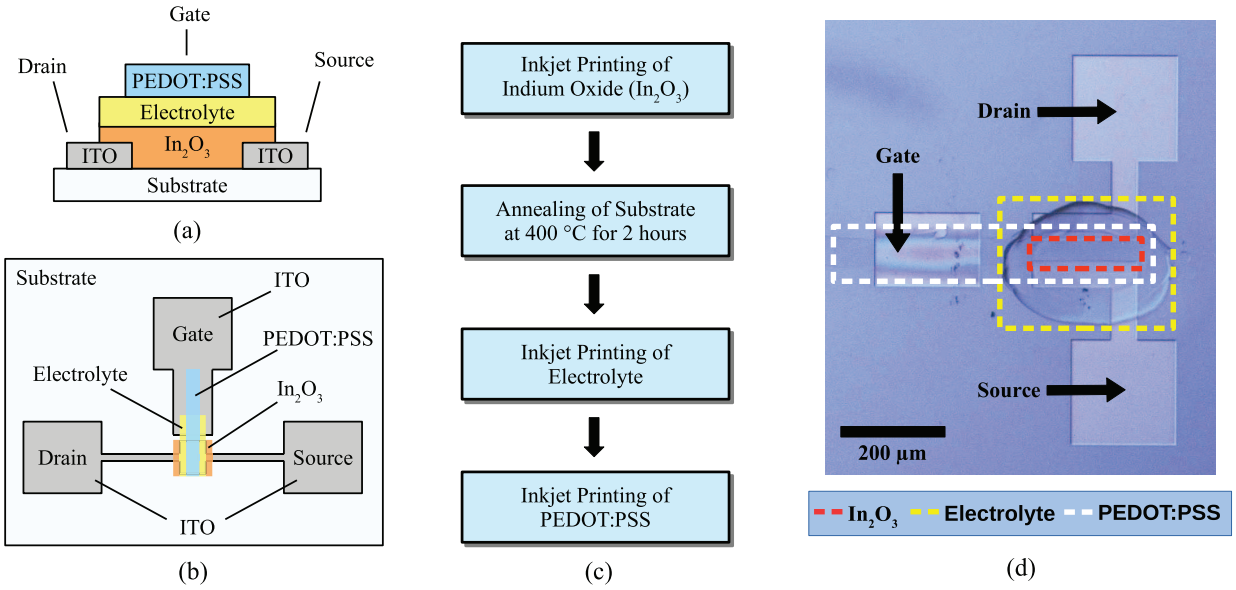


Fig. 13. Description of the EGFET technology. (a) Cross-sectional view of the EGFET on the substrate [25]. (b) Top view of the EGFET on the substrate [25]. (c) Fabrication process of the EGFET. (d) Optical image of a fabricated EGFET device.

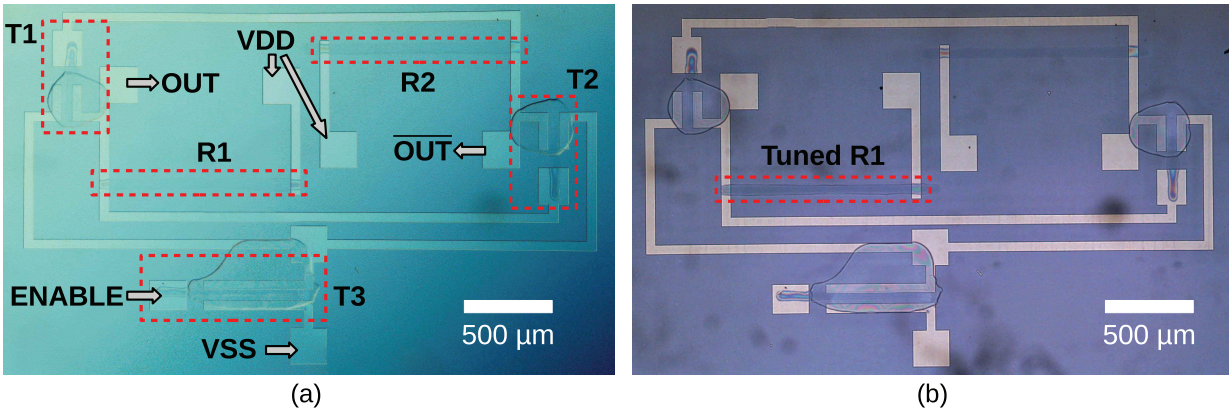


Fig. 14. Images of a fabricated TRNG. (a) Before resistor tuning. (b) After resistor tuning.

and the ratio of ones for each TRNG converges to 50%, which indicates that the output is highly dependent to random noise. Moreover, we have consistently printed additional layers on the top of the R2 of TRNG-4 to examine its behavior. As shown in Fig. 16(b), after the second and third additional layers are printed, its ratio of ones is reduced from 83% to 53% and 45%, respectively, meaning that the influence of the process variation is mostly reduced. Moreover, after the fourth and fifth printed layers, the ratio of ones is decreased to 9% and 8%, respectively, since the tuning excesses the mismatch resulting in process variation.

We swept the supply voltage of the TRNG-3 from 0.6 to 1.2 V to examine the susceptibility of its ratio of ones to supply voltage. The ratio of ones is 32%, 32%, 39%, and 36% for the supply voltage of 0.6, 0.8, 1.0, and 1.2 V, respectively, which show that the change in the supply voltage does not bias the output to one value. Moreover, the slight change in the ratio of ones for different supply voltages demonstrates that the supply voltage susceptibility of the TRNG-3 is low.

Furthermore, we constantly measure the TRNG-3 for 12 weeks to check its functionality. During 12 weeks of measurements, the ratio of ones of TRNG-3 changed from 39% to 41% and finally became 37%. This shows that the randomness of the tuned TRNG does not significantly change. In addition, after 12 weeks, the maximum delays measured at different supply voltages are observed between 69 and 76 ms, showing that it does not significantly vary at different supply voltages. Therefore, the throughput of the TRNG-3 is ~13.16 bit/s, which is sufficient for most of the PE applications.

Fig. 17 shows the current and power consumption of the tuned TRNG-3 at various supply voltages. The quiescent and active currents decrease from ~3.94 μA and ~395.22 to ~0.99 and ~16.49 μA, respectively, when the supply voltage is lowered from 2.0 down to 0.5 V. The quiescent and active power consumptions sink from ~7.88 and ~790.43 μW to ~0.50 and ~8.24 μW, respectively, when the supply voltage is reduced from 2.0 down to 0.5 V. The active power

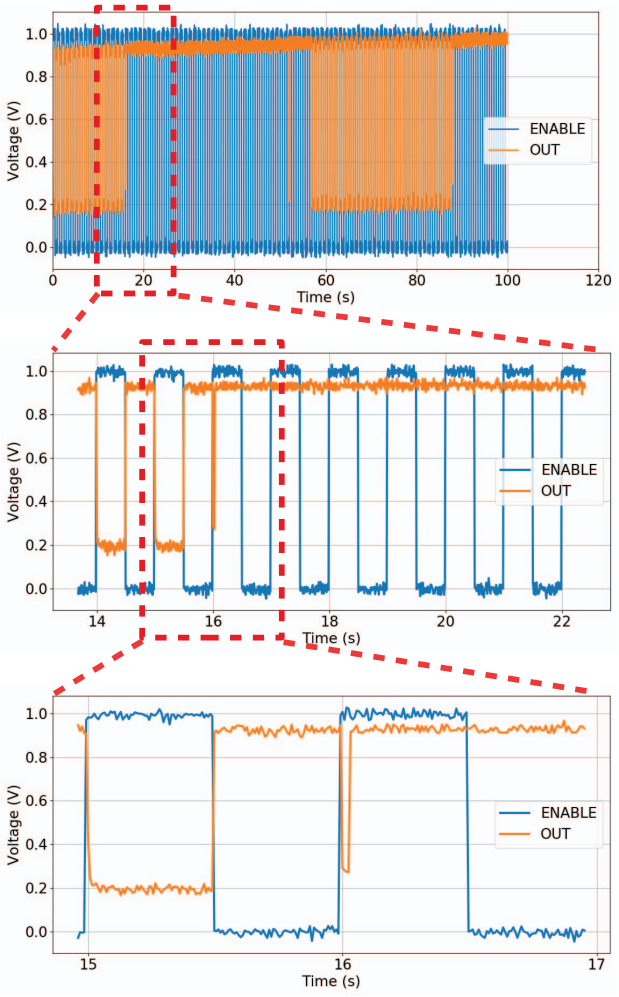


Fig. 15. Timing waveform of a fabricated TRNG operating at 1 V after resistor tuning.

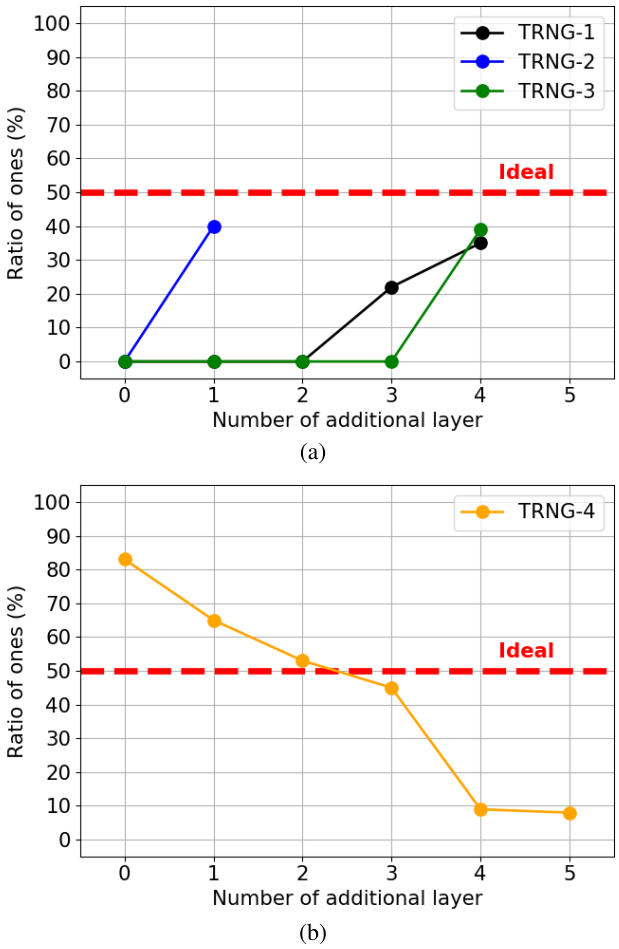


Fig. 16. Ratio of ones out of 100 bits of fabricated TRNGs. (a) Ratio of ones for three TRNGs converges to 50%. Bias due to process variation is mitigated by printing an additional layer to the corresponding printed resistor. (b) Ratio of ones for another TRNG converges to 50%. While more layers are printed to the same resistor, it converges to 0%.

consumption is always higher than the quiescent power consumption due to the enable transistor (T3) in the design.

C. Discussion on Comparison With Existing TRNGs

PE enables the applications where ultralow-cost is the vital requirement. The ultralow-cost requirement constraints the complexity of the PE circuits including security primitives such as physical unclonable functions (PUFs) and TRNGs to secure interconnected applications of PE. The silicon-based TRNGs usually contain a calibration circuitry, which result in an additional cost, to mitigate the process variation. The complexity constraint of PE makes existing TRNGs infeasible in PE applications. The proposed circuit and its additive tuning method enable to realize a compact TRNG for ultralow-cost PE applications. The power efficiency and the throughput of an existing silicon-based TRNG [42] and the proposed TRNG are incomparable, since the feature sizes of the silicon-based TRNG and the printed TRNG are 14 nm and 10 μm, respectively, and it is infeasible to extrapolate their power efficiency and throughput. However, the area usage of two designs can be compared by extrapolating their reported area usage according to their feature size. The extrapolated area usage of the

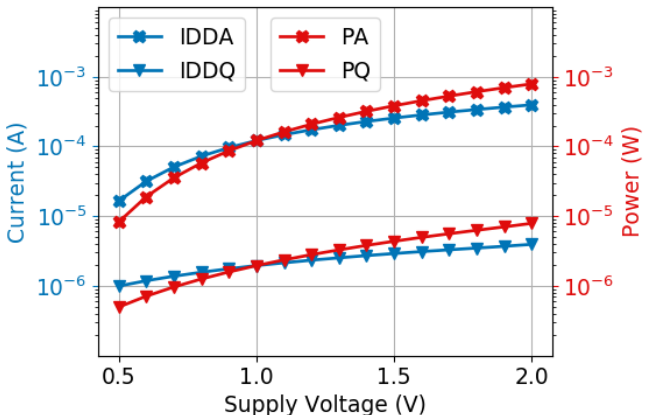


Fig. 17. Current and power measurements of tuned TRNG-3 at various supply voltages. (Left axis) Quiescent and active currents (IDDQ, IDDA). (Right axis) Quiescent and active power consumption (PQ, PA).

silicon-based TRNG is 555 mm^2 in 10-μm feature size, while the reported area usage of the proposed TRNG is 4.59 mm^2, which is less than 1% of the silicon counterpart. Therefore,

the utilization of existing TRNGs in PE stems from high area usage resulting from their additional calibration circuitry.

D. Suitability of TRNG Postprocessing Techniques

The generated bitstream can be postprocessed to compensate any bias and/or correlation. However, postprocessing techniques introduce additional area and power overhead, which harm the target low-cost and low-power applications [32]. Therefore, the postprocessing technique should be selected according to the constraints of the target application. For instance, the XOR function postprocessing technique has high overhead, and hence is inefficient for PE applications, since it calculates the odd parity of multiple TRNG instances to accumulate entropy from the TRNGs [33], [35]. On the other hand, the von Neumann corrector generates one bit from two bits, and removes consecutive ones/zeros increasing the entropy to one [36]. However, it reduces the throughput by at least 75%, which is not harmful for most of PE applications where the operation requiring random bits is infrequent [8], [13]. Therefore, the von Neumann correct is a suitable postprocessing technique, since it has low overhead while providing sufficient throughput for the target applications.

VI. Conclusion

PE was paving its way in many application domains. These applications might require random keys generated by the TRNGs to secure their operations. Since PE circuits had high intrinsic process variation, designing a proper TRNG required the mitigation of the process variation. In this article, we had presented an inkjet-printed TRNG design that exploited the customizable fabrication feature of the PE to tune the circuit to mitigate the process variation impact. The proposed resistor tuning flow reduced the effect of the overall process variation by 110 times such that the tuned TRNGs could pass the NIST randomness test. Moreover, the proposed TRNG are fabricated and tuned using resistor tuning flow to validate our approach. The experimental results showed that the fabricated TRNGs after tuning generated random bitstreams, while operable at below 1 V and consuming down to $\sim$8.24-μW active power.

Acknowledgment

This work was supported by the Ministry of Science, Research and Arts of the state of Baden-Württemberg in the form of the MERAGEM doctoral program.

References

[1] M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, "How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective," *Int. J. Mech., Ind. Sci. Eng.*, vol. 8, no. 1, pp. 37–44, 2014.

[2] F. Rasheed, M. Hefenbrock, M. Beigl, M. B. Tahoori, and J. Aghassi-Hagmann, "Variability modeling for printed inorganic electrolyte-gated transistors and circuits," *IEEE Trans. Electron Devices*, vol. 66, no. 1, pp. 146–152, Jan. 2019.

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

[4] B. S. Cook, A. Shamim, and M. M. Tentzeris, "Passive low-cost inkjet-printed smart skin sensor for structural health monitoring," *IET Microw., Antennas Propag.*, vol. 6, no. 14, pp. 1536–1541, Nov. 2012.

[5] J. S. Chang, A. F. Facchetti, and R. Reuss, "A circuits and systems perspective of organic/printed electronics: Review, challenges, and contemporary and emerging design approaches," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 1, pp. 7–26, Mar. 2017.

[6] G. A. Torres Sevilla and M. M. Hussain, "Printed organic and inorganic electronics: Devices to systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 1, pp. 147–160, Mar. 2017.

[7] R. A. Street *et al.*, "From printed transistors to printed smart systems," *Proc. IEEE*, vol. 103, no. 4, pp. 607–618, Apr. 2015.

[8] P. Rosa, A. Câmara, and C. Gouveia, "The potential of printed electronics and personal fabrication in driving the Internet of Things," *Open J. Internet Things*, vol. 1, no. 1, pp. 16–36, 2015.

[9] A. T. Erozan, R. Bishnoi, J. Aghassi-Hagmann, and M. B. Tahoori, "Inkjet-printed true random number generator based on additive resistor tuning," in *Proc. IEEE Design, Autom. Test in Europe (DATE)*, Mar. 2019, pp. 1361–1366.

[10] S. K. M. Jönsson *et al.*, "The effects of solvents on the morphology and sheet resistance in poly(3,4-ethylenedioxythiophene)-polystyrenesulfonic acid (PEDOT-PSS) films," *Synth. Met.*, vol. 139, no. 1, pp. 1–10, Aug. 2003.

[11] A. T. Erozan, M. S. Golanbari, R. Bishnoi, J. Aghassi-Hagmann, and M. B. Tahoori, "Design and evaluation of physical unclonable function for inorganic printed electronics," in *Proc. 19th Int. Symp. Qual. Electron. Design (ISQED)*, Mar. 2018, pp. 419–424.

[12] A. T. Erozan *et al.*, "Inkjet-printed EGFET-based physical unclonable function—Design, evaluation, and fabrication," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 12, pp. 2935–2946, Dec. 2018.

[13] H. F. Castro *et al.*, "Degradation of all-inkjet-printed organic thin-film transistors with TIPS-pentacene under processes applied in textile manufacturing," *Organic Electron.*, vol. 22, pp. 12–19, Jul. 2015.

[14] V. Subramanian *et al.*, "Progress toward development of all-printed RFID tags: Materials, processes, and devices," *Proc. IEEE*, vol. 93, no. 7, pp. 1330–1338, Jul. 2005.

[15] J. Marques *et al.*, "Thermoplastic packaging and embedding technology for ID-cards," in *Proc. Eur. Microelectron. Packag. Conf.*, 2013, pp. 1–5.

[16] L. Weiss Ferreira and C. Decker, "A survey on organic smart labels for the Internet-of-Things," in *Proc. 7th Int. Conf. Networked Sens. Syst. (INSS)*, Jun. 2010, pp. 161–164.

[17] C. D. Dimitrakopoulos and P. R. L. Malenfant, "Organic thin film transistors for large area electronics," *Adv. Mater.*, vol. 14, no. 2, pp. 99–117, Jan. 2002.

[18] H. Sirringhaus, "25th anniversary article: Organic field-effect transistors: The path beyond amorphous silicon," *Adv. Mater.*, vol. 26, no. 9, pp. 1319–1335, Jan. 2014.

[19] L.-L. Chua *et al.*, "General observation of n-type field-effect behaviour in organic semiconductors," *Nature*, vol. 434, no. 7030, pp. 194–199, Mar. 2005.

[20] S. Kyung, J. Kwon, Y.-H. Kim, and S. Jung, "Low-temperature, solution-processed, 3-D complementary organic FETs on flexible substrate," *IEEE Trans. Electron Devices*, vol. 64, no. 5, pp. 1955–1959, May 2017.

[21] S. K. Garlapati *et al.*, "Electrolyte-gated, high mobility inorganic oxide transistors from printed metal halides," *ACS Appl. Mater. Inter.*, vol. 5, no. 22, pp. 11498–11502, Nov. 2013.

[22] P. K. Nayak, M. N. Hedhili, D. Cha, and H. N. Alshareef, "High performance In_2O_3 thin film transistors using chemically derived aluminum oxide dielectric," *Appl. Phys. Lett.*, vol. 103, no. 3, Jul. 2013, Art. no. 033518.

[23] G. C. Marques, F. Rasheed, J. Aghassi-Hagmann, and M. B. Tahoori, "From silicon to printed electronics: A coherent modeling and design flow approach based on printed electrolyte gated FETs," in *Proc. 23rd Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2018, pp. 658–663.

[24] G. C. Marques, D. Weller, A. T. Erozan, X. Feng, M. Tahoori, J. Aghassi-Hagmann, "Progress report on 'from printed electrolyte-gated metal-oxide devices to circuits,"' *Adv. Mater.*, vol. 31, no. 26, Jun. 2019, Art. no. 1806483.

[25] G. C. Marques *et al.*, "Electrolyte-gated FETs based on oxide semiconductors: Fabrication and modeling," *IEEE Trans. Electron Devices*, vol. 64, no. 1, pp. 279–285, Jan. 2017.

[26] G. C. Marques *et al.*, "Digital power and performance analysis of inkjet printed ring oscillators based on electrolyte-gated oxide electronics," *Appl. Phys. Lett.*, vol. 111, no. 10, Sep. 2017, Art. no. 102103.

[27] D. Weller, G. C. Marques, J. Aghassi-Hagmann, and M. B. Tahoori, "An inkjet-printed low-voltage latch based on inorganic electrolyte-gated transistors," *IEEE Electron Device Lett.*, vol. 39, no. 6, pp. 831–834, Jun. 2018.
[28] F. Rasheed, M. S. Golanbari, G. C. Marques, M. B. Tahoori, and J. Aghassi-Hagmann, "A smooth EKV-based DC model for accurate simulation of printed transistors and their process variations," *IEEE Trans. Electron Devices*, vol. 65, no. 2, pp. 667–673, Feb. 2018.
[29] A. L. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-22, Apr. 2010.
[30] B. Jun and P. Kocher, "The Intel random number generator," Intel, Santa Clara, CA, USA, White Paper, Apr. 1999.
[31] M. Singh, H. M. Haverinen, P. Dhagat, and G. E. Jabbour, "Inkjet printing-process and its applications," *Adv. Mater.*, vol. 22, no. 6, pp. 673–685, Feb. 2010.
[32] V. B. Suresh and W. P. Burleson, "Entropy and energy bounds for metastability based TRNG with lightweight post-processing," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 7, pp. 1785–1793, Jul. 2015.
[33] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007.
[34] K. Lee, S.-Y. Lee, C. Seo, and K. Yim, "TRNG (True random number Generator) method using visible spectrum for secure communication on 5G network," *IEEE Access*, vol. 6, pp. 12838–12847, 2018.
[35] J. S. Liberty *et al.*, "True hardware random number generation implemented in the 32-nm SOI POWER7+ processor," *IBM J. Res. Develop.*, vol. 57, no. 6, pp. 4:1–4:7, Nov./Dec. 2013.
[36] J. von Neumann, "Various techniques used in connection with random digits," *J. Res. Nat. Stand. Appl. Math.*, vol. 3, pp. 768–770, 1963.
[37] 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.
[38] J. Holleman, S. Bridges, B. P. Otis, and C. Diorio, "A 3 μW CMOS true random number generator with adaptive floating-gate offset cancellation," *IEEE J. Solid-State Circuits*, vol. 43, no. 5, pp. 1324–1336, May 2008.
[39] 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.
[40] U. Guler and G. Dundar, "Modeling CMOS ring oscillator performance as a randomness source," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 3, p. 712–724, Mar. 2014.
[41] G. C. Marques *et al.*, "Influence of humidity on the performance of composite polymer electrolyte-gated field-effect transistors and circuits," *IEEE Trans. Electron Devices*, vol. 66, no. 5, pp. 2202–2207, May 2019.
[42] S. Mathew, S. Satpathy, V. Suresh, and R. Krishnamurthy, "Ultra-low energy circuit building blocks for security technologies," in *Proc. Design, Autom. Test Eur. Conf. Exhibit. (DATE)*, Mar. 2018, pp. 391–394.
[43] C. Ionescu, P. Svasta, A. Vasile, and D. Bonfert, "Investigations on organic printed resistors based on PEDOT:PSS," in *Proc. IEEE 18th Int. Symp. Design Technol. Electron. Packag. (SIITME)*, Oct. 2012, pp. 85–89.
[44] A. T. Erozan, M. Hefenbrock, M. Beigl, J. Aghassi-Hagmann, and M. B. Tahoori, "Reverse engineering of printed electronics circuits: From imaging to netlist extraction," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 475–486, 2020.

Ahmet Turan Erozan received the B.S. degree from Istanbul Technical University, Istanbul, Turkey, in 2013, and the M.S. degree from Ankara Yildirim Beyazit University, Turkey, in 2015. He is currently pursuing the Ph.D. degree with the Chair of Dependable Nano Computing Group, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany.

He was a Digital Design Engineer in industry for more than three years. His current research interests include resource-constrained hardware security, circuits and systems, and emerging technologies.

Guan Ying Wang, photograph and biography not available at the time of publication.

Rajendra Bishnoi received the Ph.D. degree in computer science from the Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, in 2017.

He was a Research Leader for the MRAM Group, Chair of Dependable Nano Computing, KIT, for more than two years. From 2006 to 2012, he was a Design Engineer with Freescale, Noida, India, where he was a part of the Technical Solution Group in memory and SoC flow. He is currently an Assistant Professor with the Computer Engineering Laboratory, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology (TU-Delft), Delft, The Netherlands.

Dr. Bishnoi was a recipient of the EDAA Outstanding Dissertation Award for the year 2017.

Jasmin Aghassi-Hagmann received the M.Sc. degree (Hons.) in physics from Aachen University (RWTH), Aachen, Germany, and the Ph.D. degree from the Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany.

In 2012, she joined KIT as a Group Leader and was additionally appointed as a Full Professor in electrical engineering with the Offenburg University of Applied Sciences, Offenburg, Germany, in 2013. She worked as a Research Engineer and Manager with Infineon Technologies AG and Intel Mobile Communications GmbH, Munich, Germany.

Mehdi B. Tahoori (Senior Member, IEEE) received the B.S. degree in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2000, and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, USA, in 2002 and 2003, respectively.

He is currently a Full Professor and the Chair of Dependable Nano-Computing, Department of Computer Science, Karlsruhe Institute of Technology, Karlsruhe, Germany. In 2003, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA, USA, where he became an Associate Professor in 2009. From August to December 2015, he was a Visiting Professor with the VLSI Design and Education Center (VDEC), University of Tokyo, Tokyo, Japan. From 2002 to 2003, he was a Research Scientist with Fujitsu Laboratories of America, Sunnyvale, CA, USA, in advanced computer-aided research, engaged in reliability issues in deep-submicrometer mixed-signal very large-scale integration (VLSI) designs. He has authored over 250 publications in major journals and conference proceedings on a wide range of topics, from dependable computing and emerging nanotechnologies to system biology. He holds several pending and granted U.S. and European patents. His current research interests include resilient and secure system design, emerging nonvolatile memory technologies, and printed electronics.

Dr. Tahoori has served on the Organizing and Program Committee of various conferences and symposia in the areas of VLSI testing, reliability, and emerging nanotechnologies, including ITC, VTS, DAC, ICCAD, DATE, ETS, ICCD, ASP-DAC, GLSVLSI, and VLSI Design. He is currently the Editor-in-Chief of the *Elsevier Microelectronic Reliability Journal*. He is an Associate Editor of the *IEEE Design and Test Magazine*, the Coordinating Editor for the *Springer Journal of Electronic Testing* (JETTA), and an Associate Editor of the *VLSI Integration Journal* and the *IET Computers and Digital Techniques*. He was the Associate Editor of the *ACM Journal of Emerging Technologies for Computing (JETC)*. He is the Program Chair of the 2018 IEEE VLSI Test Symposium and the General Chair of the 2019 IEEE European Test Symposium (ETS). He received a number of best paper nominations and awards at various conferences and journals, including ICCAD, TODAES, and FPL. He was a recipient of the National Science Foundation Early Faculty Development (CAREER) Award. He is the Chair of the ACM SIGDA Technical Committee on Test and Reliability.