A 82-nW Chaotic Map True Random Number Generator Based on a Sub-Ranging SAR ADC

Minseo Kim, *Student Member, IEEE*, Unsoo Ha, *Student Member, IEEE*, Kyuho Jason Lee, *Student Member, IEEE*, Yongsu Lee, *Member, IEEE*, and Hoi-Jun Yoo, *Fellow, IEEE*

***Abstract*— An ultra-low power true random number generator (TRNG) based on a sub-ranging SAR analog-to-digital converter (ADC) is proposed. The proposed TRNG is composed of a coarse-SAR ADC with a low-power adaptive-reset comparator and a low-power dynamic amplifier. The coarse-ADC part is shared with a sub-ranging SAR ADC for area reduction. The shared coarse-ADC not only plays the role of discrete-time chaotic circuit but also reduces the overall SAR ADC energy consumption by selectively activating the fine-SAR ADC. Also, the proposed dynamic residue amplifier consumes only 48 nW and the adaptive-reset comparator generates a chaotic map with only 6-nW consumption. The proposed TRNG core occupies 0.0045 mm^2 in 0.18-μm CMOS technology and consumes 82 nW at 270-kbps throughput with 0.6-V supply. It successfully passes all of National Institute of Standards and Technology (NIST) tests, and it achieves the state-of-the-art figure-of-merit of 0.3 pJ/bit.**

***Index Terms*— Adaptive-reset comparator, analog to digital conversion, chaotic map, cryptography, encryption, radio-frequency identification (RFID), security, true random number generators (TRNGs).**

I. Introduction

In RECENT years, true random number generators (TRNGs) have been used as the key building block of many applications such as cryptosystems, wireless networks, and radio-frequency identification (RFID) systems. In particular, with the extensive use of the RFID systems [1], information security becomes crucial in wireless RFID applications such as human identification and medical monitoring. Random numbers can play a crucial role to enable cryptographic algorithms and circuits to generate encryption keys which are extremely resilient to external attacks. Most of these algorithms need high entropy random numbers as the seeds for robust encoding and decoding.

A typical RFID sensor system consists of a sensor front end, a transmitter, a receiver, and a random number generator for data encryption. In this case, if an appropriate communication protocol is set and the encryption source uses true random numbers, a physical attack can be prevented efficiently [2], [3]. However, in previous wireless sensor networks for RFID wearable and implantable systems [4], [5], where low-power and small area implementation is essential, a pseudo-random number generator (PRNG) was typically used instead of a TRNG, because of its simple architecture (Fig. 1). PRNGs produce random-looking patterns using a deterministic algorithm which is determined by an initial seed value, and this seed value is typically pseudo-random in nature, which makes this approach vulnerable to manipulations by malicious attackers, and results in reduced security [6]. Furthermore, the knowledge of the internal state of the PRNG structure along with its periodicity makes the PRNG output vulnerable to cryptanalysis. Moreover, previous RFID works [4], [5] were not able to optimize the analog-to-digital converter (ADCs) due to the limited area and power available, which resulted in limited effective number of bits and conversion efficiency. To solve these problems, several TRNG designs have been reported for general applications [10]–[23] as well as for RFID systems [7]–[9]. The solutions tailored to RFID systems [7]–[9] showed, however, poor efficiency in terms of area, power, and randomness quality compared to TRNG presented for other applications [10]–[23].

TRNGs [10]–[23] can broadly be divided into two categories according to the noise harvesting mechanism, as described in Fig. 2: 1) classical approaches and 2) chaotic map-based approaches. Fig. 2(a) shows three different types of classical TRNG architectures, each of which consists of an entropy source and a harvester [10]–[14]. A direct amplification of noise was presented in [10]; however, it consumed too much power ($>$3 mW) because it required a high-gain and wide-bandwidth amplifier to magnify the small noise voltages. A noisy SIN MOSFET was introduced as source of large thermal noise in [11], but it required an additional photo mask process resulting in higher manufacturing cost. Moreover, it showed weak randomness due to the lack of appropriate shielding of the noise source from the power supply, substrate signals, and 1/f noise. A high-frequency clock was combined with a low-frequency jittery clock to generate a random sequence in [12]. This is a more robust sampling technique for deterministic noise compared to direct noise amplification, but it requires power-hungry clock generators for both frequencies to produce statistical randomness due to the insufficient oscillator jitter. Meta-stable structures were introduced [13], [14] to generate a random sequence with a low-power latch but they required additional calibration circuitry to tolerate CMOS process variations and compensate for entropy source mismatch. All of the above methods had a

Manuscript received November 30, 2016; revised February 2, 2017 and April 11, 2017; accepted April 11, 2017. Date of publication April 12, 2017; date of current version June 22, 2017. This paper was approved by Guest Editor Eugenio Cantatore. *(Corresponding author: Minseo Kim.)*

The authors are with the Department of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 305-701, South Korea (e-mail: minseokim@kaist.ac.kr).

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

Digital Object Identifier 10.1109/JSSC.2017.2694833

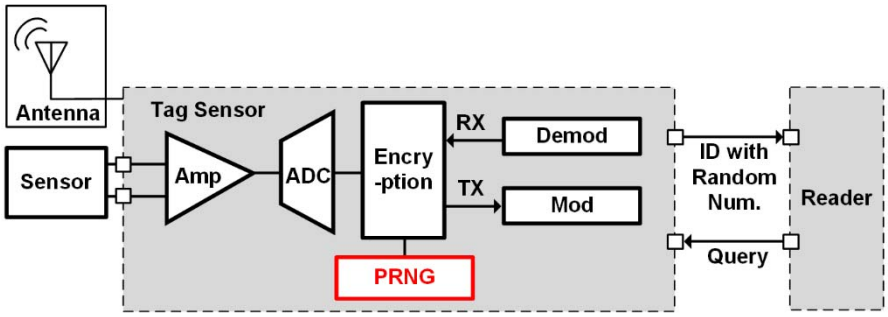


Fig. 1. Typical architecture of a wireless RFID sensor network.

critical disadvantage; they assumed statistical entropy sources like Gaussian distribution, but in reality, they experienced unknown statistical distributions because of the limited dynamic range of the entropy sources or due to external factors like supply variations [21].

To overcome this issue, chaotic map-based TRNGs were proposed [15]–[23]. The chaotic map-based TRNG architecture is schematically shown in Fig. 2(b). It provides high-quality randomness because the chaotic system depends only on its initial condition rather than the statistics of the entropy source, hence resulting in a long-term unpredictability. That is, it is insensitive to the presence of deterministic noise and its randomness is obtained from robust signal dynamic properties. However, previous chaotic map TRNG implementations also had critical drawbacks like large area ($\sim$mm^2) and large power consumption ($\sim$mW) [15]–[23].

In this paper, based on [24] we propose a chaotic map-based TRNG for an RFID system that achieves not only low-power operation but also small area. It deploys: 1) a chaotic map based on an SAR ADC architecture; 2) a sub-ranging SAR ADC of which the coarse-ADC is used both for the discrete-time chaotic system of the TRNG and for efficient power-switching the fine-SAR ADC to reduce power consumption; 3) a dynamic residue amplifier to enable power-efficient amplification; and 4) an adaptive-reset comparator for low-power comparison in the SAR ADC. Section II provides an overview of chaotic TRNGs. Section III introduces the proposed TRNG based on a sub-ranging SAR ADC architecture, and implementation details are described in Section IV. Section V shows the measurements results, a performance summary, and provides some benchmarking. Finally, conclusion will be made in Section VI.

II. Chaotic Map-Based TRNG

Chaos is a non-periodic and long-term non-predictive behavior that can be generated by a nonlinear dynamic system. A TRNG can be obtained by Chaos-based random number generators because of the following reasons. First, since the chaotic circuit is an analog machine, it is necessary to introduce a quantization of the state to generate random bits. Therefore, the internal state of the system cannot be retrieved by the sole knowledge of the quantized values because the quantization is a non-reversible operation. Second, like any other analog electronic circuits, a chaotic circuit is influenced by noise. The noise not only sets the initial system condition at the system startup but also modifies the internal states continuously during operation. From this point of view, a chaos-based random number generator is similar to a generator based on the direct observation of noise-like phenomena [25], [26]. Therefore, it can be considered as a process of amplifying initial white noise or thermal noise, in a similar way to what is done in classical TRNGs.

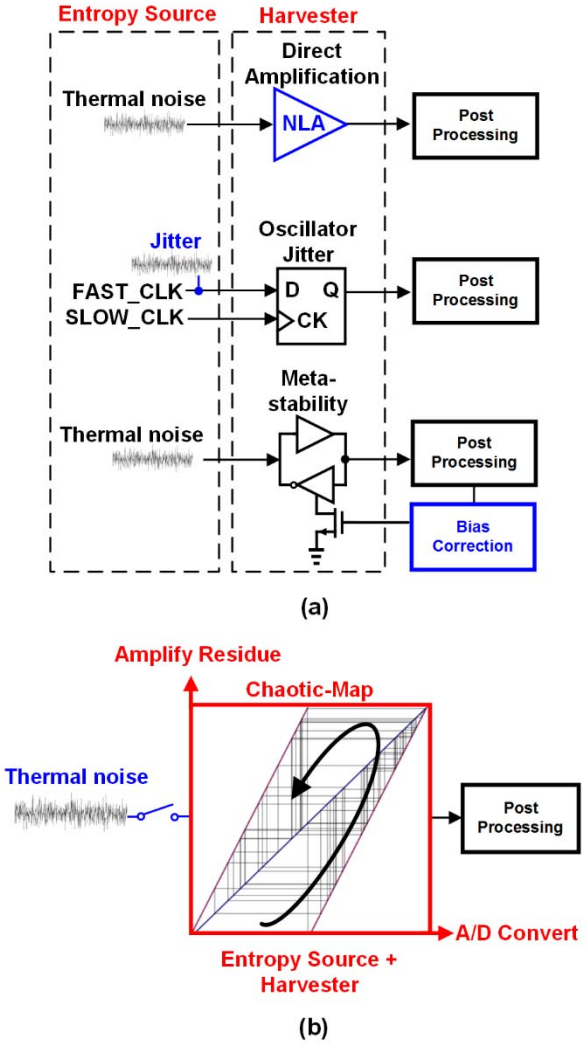


Fig. 2. Conceptual architecture of (a) conventional TRNG and (b) chaotic-map TRNG.

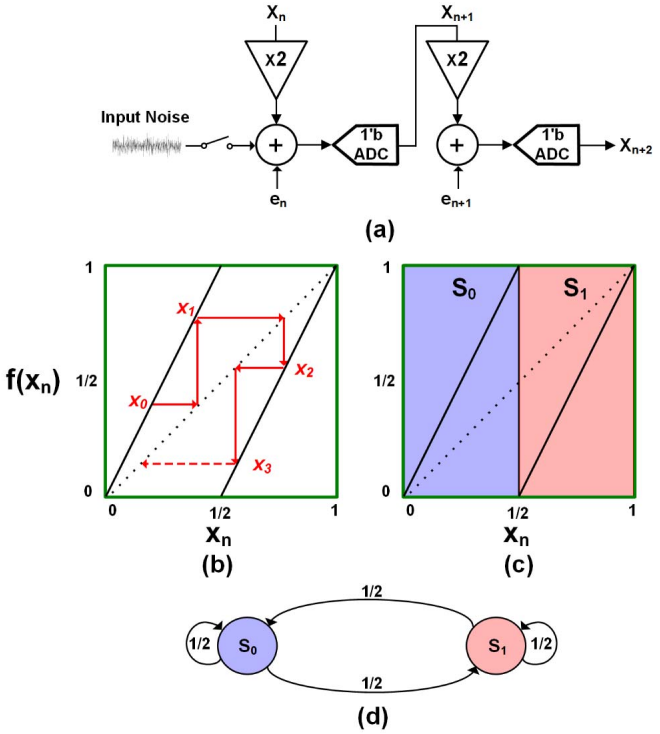


Fig. 3. Chaotic map implementation and linear Markov map. (a) Chaotic map implementation (b) corresponding linear Markov map (c) Markov evolution of the chaotic map (d) Markov chain of fair coin toss.

The characteristics of a chaotic map are summarized in [27]. First, it produces different results depending on the initial conditions over a long period. Second, the output sequence is impossible to reproduce. Third, its output range represents a full range of the chaotic map. Therefore, its output is unpredictable in the map range over a long time, which ensures its randomness. There were several approaches to implementation of the chaotic maps [15]–[23], and among those approaches, 1-D linear piecewise affine Markov (PWAM) chaotic maps are widely used in very large scale integration design due to its low implementation cost [18]. The necessary condition for realizing a 1-D linear Markov map is summarized by (1), where n is the time step, x_0 is the initial state of the system which comes from thermal or environmental noise, x_n is the state of the system at time n, and the transfer function $f(x)$ has the same domain and range ($R \rightarrow R$)

$$x_{n+1} = f(x_n) = ax_n + b, (x_n \in R). \tag{1}$$

One of the above PWAM chaotic map is the Bernoulli shift map. Its implementation example is shown in Fig. 3(a), and the corresponding map is in Fig. 3(b), which can be defined as (2) where x_n is the arbitrary input of the map

$$f(x_n) = \begin{cases} 2x_n + e_n, & 0 \le x_n < 1/2 \\ 2x_n - 1 + e_n, & 1/2 \le x_n < 1 \end{cases} = [2(x_n + e_n)] \bmod 1.0 \tag{2}$$

where e_n represents a Gaussian noise signal.

As mentioned above, the initial state is determined by thermal or environmental noise which generates an unpredictable random bit. Since the initial condition of a very small difference also produces a totally different output, it is impossible to analyze the output as long as the initial value is set by noise [27]. Even if you would know the exact value of the initial input, you get different results for the same input due to e_n. Although e_n may seem to degrade the chaotic dynamic system, e_n does not affect the sensitivity of the chaotic map because the density of the chaotic map is independent of the noise density of 1/2 LSB [33].

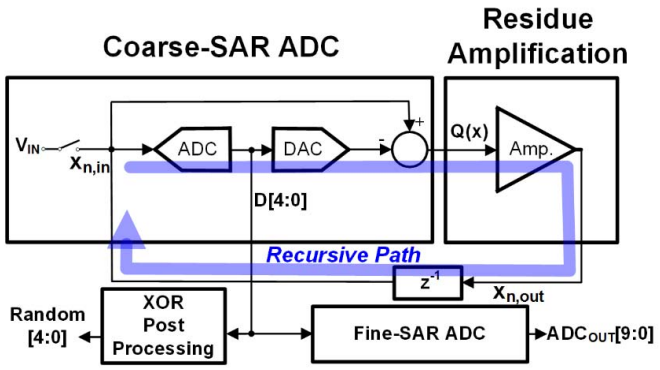


Fig. 4. Overall block diagram.

In the Bernoulli shift map-based PWAM, discrete-time chaotic maps are formed by an iteration of the output signal according to the transformation function $f(x_n) : (0, 1) \rightarrow (0, 1)$ in a feedback loop as given by $x_{n+1} = f(x_n) = f^n(x_0)$, and its Markov state chain corresponding to the Markov evolution of the chaotic map is shown in Fig. 3(c). This is the Markov chain of the fair coin toss, shown in Fig. 3(d), which corresponds to a true random system.

There were several CMOS circuit implementations of TRNG using 1-D linear Markov map such as tent map, Bernoulli map, zigzag map, and Bernoulli shift map [15]–[23]. The Bernoulli maps were generated by switched-current approaches in [15]–[19]. However, they consumed large power due to their large static current. Moreover, using Bernoulli map cannot guarantee its map region to be confined within (−R, R). If the input value becomes slightly greater than R or less than –R for any reason, the output stream gets out of the map and it never returns back to inside the region, resulting in degradation of randomness quality. To compensate for this issue, the zigzag map is presented in [22]. Utilizing zigzag map solves the confinement problem, but it also consumed large power due to its switched current architecture. Another way to resolve the confinement issue is to implement the Bernoulli shift map using an ADC, and this is the most common approach to realize 1-D linear Markov maps which do not suffer from confinement problem [20], [21]. However, these implementations used a 1.5-bit ADC to generate the Bernoulli shift map, which results in very complicated structures. Another approach, chaotic map based on SAR ADCs, has been discussed and tested in [28]–[30]. These works, however, were implemented using off-chip signal processing, resulting in large power and area consumption. Therefore, we introduce here a power-efficient chaotic map based on SAR ADC to realize a TRNG, which will be explained in detail.

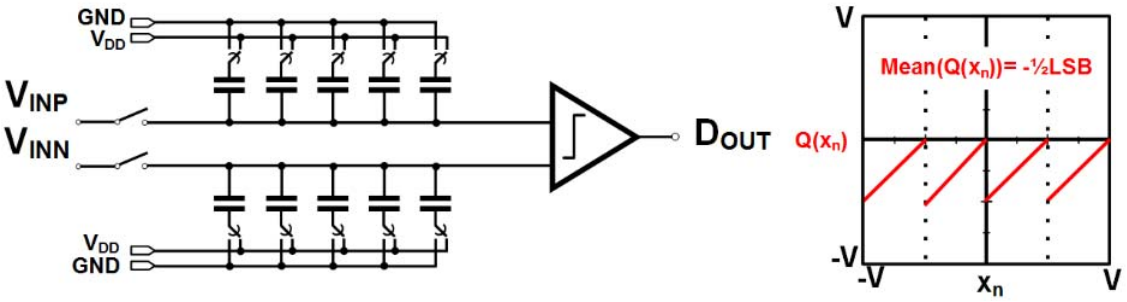


Fig. 5. Conventional residue function in SAR ADC and corresponding circuit architecture.

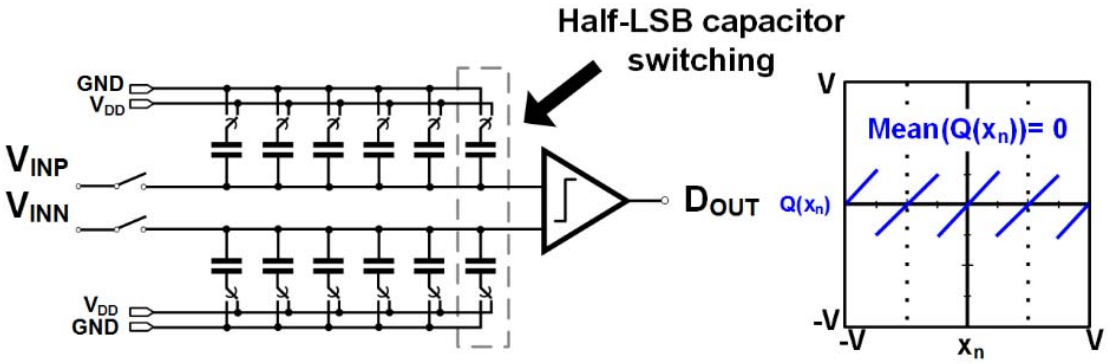


Fig. 6. Proposed residue function in SAR ADC and corresponding circuit architecture.

III. Chaotic Map Implementation in an SAR ADC

Fig. 4 shows the block diagram of the proposed TRNG. It consists of 5-bit coarse-SAR ADC, a dynamic residue amplifier, a 10-bit fine-SAR ADC, and an XOR post-processing block. The quantization error of the coarse-SAR ADC is amplified and recursively fed back into the input to implement the chaotic system. The ADC implicitly implements a discrete-time chaotic map whenever the quantization error is generated. In addition, the coarse-SAR ADC is used to enable fine-SAR ADC's switching power reduction by adopting detecting and skip (DAS) switching [31]. The detailed architecture and operation principle of the proposed TRNG will be discussed.

A. Residue Function of the SAR ADC

Generally, the quantization error Q (residue voltage) is defined

$$D_{\mathrm{OUT}} = V_{\mathrm{IN}} + Q. \tag{3}$$

D_{OUT} is the digital representation generated by the ADC and V_{IN} is the analog input voltage of the ADC. In a single SAR ADC, the residue voltage generated by the N-bit SAR ADC at the end of the conversion is the difference between input voltage and D_{OUT} of (N − 1)th decision. Therefore, in this design, we utilize the differential digital-to-analog converter (DAC) architecture to compute (3). The differential SAR ADC architecture and its residue function are shown in Fig. 5. Naturally, there exists an offset between input and output range of the chaotic map because the mean value of the residue is not zero, and this would degrade the entropy that can be delivered by the chaotic map. In order to resolve the offset of map range, we apply an additional capacitor switching to shift the average value to zero. The modified architecture and its residue function are shown in Fig. 6.

B. Implementation of PWAM Chaotic Map in the SAR ADC

As described in the above section, the ADC implicitly implements a PWAM function whenever a conversion error (residue) is generated. Let x be the input voltage of ADC and $D(x)$ be the quantization function of ADC, then the residue function of ADC is $Q(x) = x - D(x)$. If we choose the residue function from the proposed SAR ADC architecture, the corresponding model of chaotic map is defined as (4) with the interval $R = [-V/2, V/2]$

$$x_{n+1} = f(x_n) = A * Q(x_n) + B,\ f : R \rightarrow R. \tag{4}$$

The transition probabilities become uniform if the coefficients A and B are chosen to match input and output ranges of the PWAM chaotic map. For that, the coefficient A becomes 2^{k-1} for a k-bit ADC the map improves the deliverable entropy rate of the chaotic dynamic system [32]. Then, the value that sets the quantized value to the center of the chaotic map becomes the optimial value of coefficient B. Fig. 7 shows the chaotic map of a 2-bit SAR ADC which is built as a particular case of the more general discussed in [29]. For a 2-bit ADC, $Q(x)$ has four consequent unitary-slope ramp characteristics with a 1-bit interval. In this case, the coefficients become A $= 2^{2-1} = 2$ and B $= 0$. After conversion of the given input of the SAR ADC, $Q(x)$ remains as sampled value at the top node of the capacitor DAC (CDAC). Thanks to the differential architecture of the SAR ADC and half LSB switching, the quantization noise is centered at 0. Even if offset error occurs, an offset up to $V/4$ does not affect the sensitivity of the chaotic map because the density of the chaotic map is

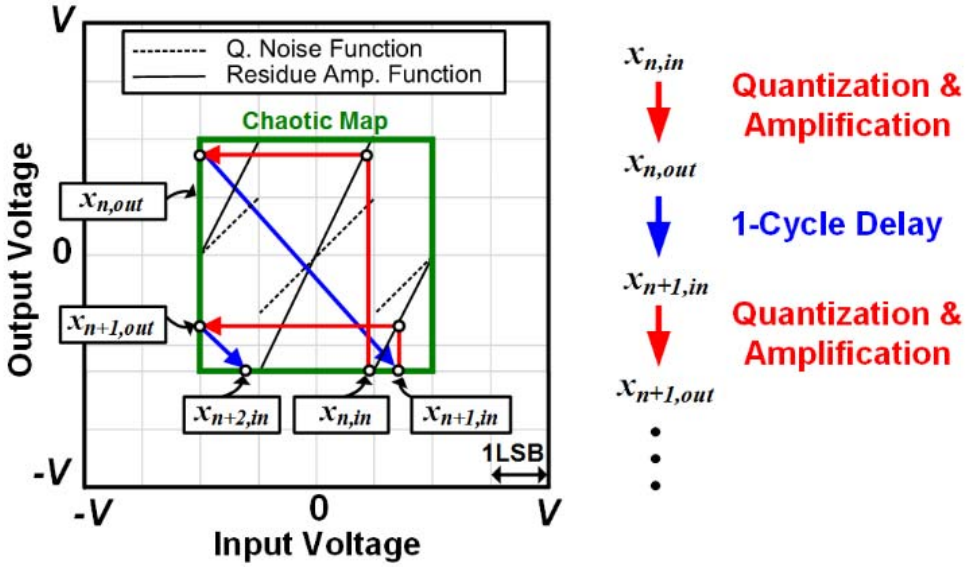


Fig. 7. Markov-map of the proposed SAR ADC and its operation.

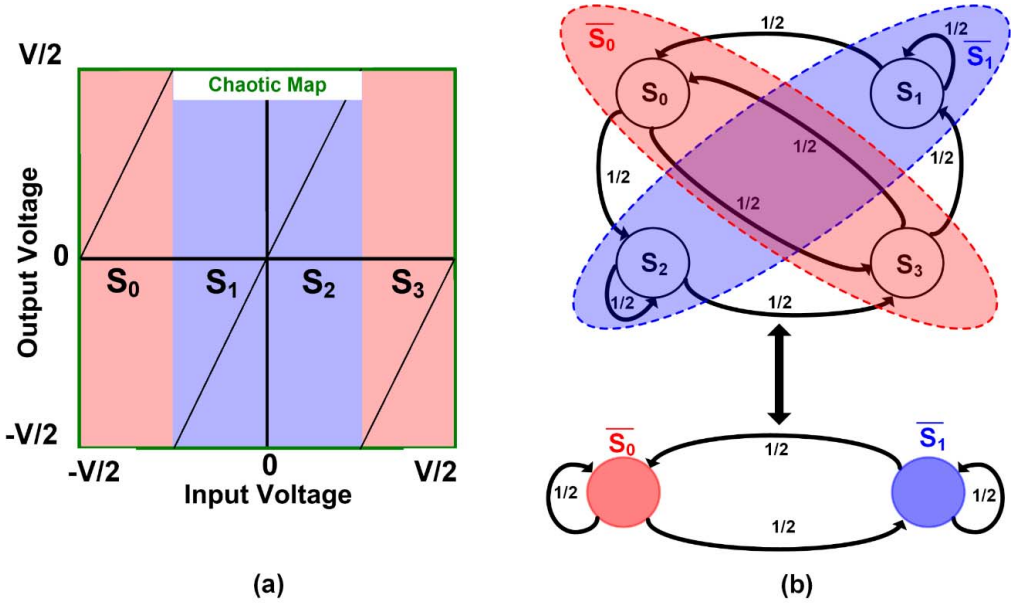


Fig. 8. Markov-chain of the proposed SAR ADC. (a) Markov Map and (b) Markov-chain of the proposed SAR ADC.

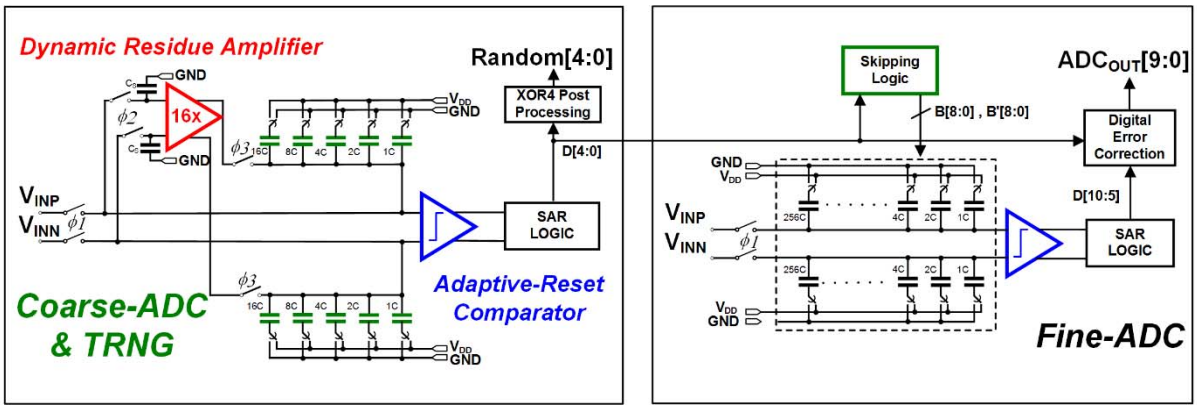


Fig. 9. Detailed overall architecture.

independent of the noise density [33]. Moreover we utilized a large unit-capacitor size of 45 fF for the 5-bit ADC. Therefore, a more accurate offset control is possible. Next, x_n is recursively quantized and amplified to make x_{n+1}. Fig. 8 shows the resulting Markov chain for the proposed chaotic map. Assuming the partition intervals $S = \{S_0, S_1, S_2, S_3\} =$

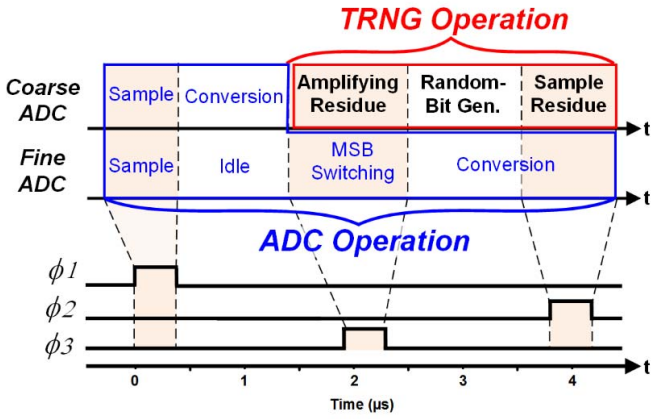


Fig. 10. Detailed operation flow.

$\{[-V/2, -V/4), [-V/4, 0), [0, V/4), [V/4, V/2)\}$ as shown in Fig. 8(a), the evolution of the system is described by the four-state Markov chain as depicted in top diagram of Fig. 8(b). In that case, assuming $\overline{S0} = \{S_0, S_3\}$ and $\overline{S1} = \{S_2, S_4\}$, the resulting state diagram can be simplified to the bottom diagram of Fig. 8(b), which is identical to the fair coin toss probability.

C. Hardware-Reusing Technique in Sub-Ranging SAR ADC and Its Operation Flow

The detailed overall architecture of the proposed TRNG based on the sub-ranging SAR ADC is shown in Fig. 9. The coarse-ADC uses a 5-bit CDAC and additional half unit capacitors for half LSB switching. The half LSB switching adjusts the mean value of quantization noise from half LSB to zero for chaotic map generation. The fine-SAR ADC uses a 10-bit CDAC including redundancy capacitors, of which the 5-MSB capacitors are switched by B[8:0] and B′[8:0] decoded from the coarse-ADC bits, to reduce switching power by adopting a DAS switching scheme [31]. Furthermore, a digital error correction block compensates the CDAC gain and comparator offset mismatches by using the redundant capacitors. In each ADC, an adaptive-reset comparator (described in Section IV) reduces the ADC's operation power. Fig. 10 shows the detailed operation flow of the TRNG based on sub-ranging SAR ADC. The frequency of the main clock signal is 13 times the sampling clock frequency (216 kHz). In phase $\phi 1$, the input is sampled in both of the coarse-SAR ADC and the fine-SAR ADC during one clock period. After the sampling phase, the coarse-ADC converts the sampled input while fine-SAR ADC is in the idle state during five clock periods. After the coarse-ADC conversion is completed in phase $\phi 3$, its DAC is reset and the amplification of the sampled residue input at Cs of the previous TRNG operation begins, while the fine-SAR ADC switches its MSB capacitor using coarse-SAR ADC's bit during the next seven clock periods. After amplifying the residue, both ADCs start conversion. When the $\phi 2$ signal is triggered, the conversion bits of the coarse-SAR ADC go through a simple XOR post-processing and the residue value is sampled in C_S, while the fine-SAR conversion is still executed. The sampling caps increase the unit capacitors of the entire coarse-DAC, but their switching power is still negligible. The entire operation is recursively repeated to generate a chaotic map. In this chaotic map architecture, the most power-hungry operation are quantization and amplification. Therefore, in the 5-bit ADC, an adaptive-reset comparator and a dynamic residue amplifier are required in this paper for low-power operation. In addition, accurate sampling is required because leakage should not occur at the input. When the ADC sampling rate is adjusted to a lower rate, leakage affects more the sampling voltage. Then, the data rate of TRNG can be adjusted according to duty of $\phi 1$, 2, 3 and ADC sampling rate. Therefore, the switch design of $\phi 1$, 2, 3 should be considered carefully. The most important circuit blocks are discussed in detail in the following section.

IV. Circuit Implementation

A. Dynamic Residue Amplifier

The residue amplification is the most crucial process in the proposed ADC-based chaotic map TRNG architecture. The key limitation of conventional residue amplifiers is their considerable power consumption because of their large dc bias current. Fig. 11 shows a conventional dynamic residue amplifier and its operation. During the amplification phase, a differential pair discharges the two output nodes from V_{DD} at different rates until the sampling phase is finished. Assuming that I_D is biasing the input pair during the evaluation phase, calling g_m its transconductance and C_{LOAD} the load capacitor, the output voltages at a time t in the evaluation phase can be written as

$$V_{\mathrm{OUTN,P}} = V_{\mathrm{DD}} - \frac{I_D \pm \frac{g_m}{2}\Delta V_{\mathrm{IN}}}{C_{\mathrm{LOAD}}} t. \tag{5}$$

Let $V_{\mathrm{CM}} = V_{\mathrm{DD}}/2$ be the common voltage output voltage in the instant t_{end} when the evaluation phase ends, then

$$t_{\mathrm{end}} = \frac{V_{\mathrm{DD}} C_{\mathrm{LOAD}}}{2 I_D}. \tag{6}$$

From (5) and (6), the residue amplifier gain can be calculated as in (7), where V_{GT} is the gate overdrive voltage of the input transistors

$$A_V = \frac{g_m V_{\mathrm{DD}}}{2 I_D} = \frac{V_{\mathrm{DD}}}{V_{\mathrm{GT}}}. \tag{7}$$

This circuit suffers from poor gain, due to the limited value of V_{DD}. Fig. 12 shows the proposed dynamic gain amplifier, which overcomes this limitation. During the reset phase, $V_{P,N}$ and $\mathrm{OUT}_{P,N}$ nodes are charged to V_{DD}, as shown in Fig. 13. When CK goes high, the nodes V_P and V_N discharge with different rates according to the input signals V_{INN} and V_{INP} at M3, 4. When $V_{P,N}$ are pulled one threshold voltage of the cascaded nMOS pair M5, 6 below V_{DD}, the nodes $\mathrm{OUT}_{\mathrm{P,N}}$ begin to discharge. In this way, the overall gain of the integrator is increased due to the increased time interval between discharging $V_{P,N}$ and $\mathrm{OUT}_{P,N}$. In this case, the gain can be expressed

$$A_V = \frac{g_m V_{\mathrm{DD}}}{2 I_D}\left(1 + \frac{C2}{C1}\right). \tag{8}$$

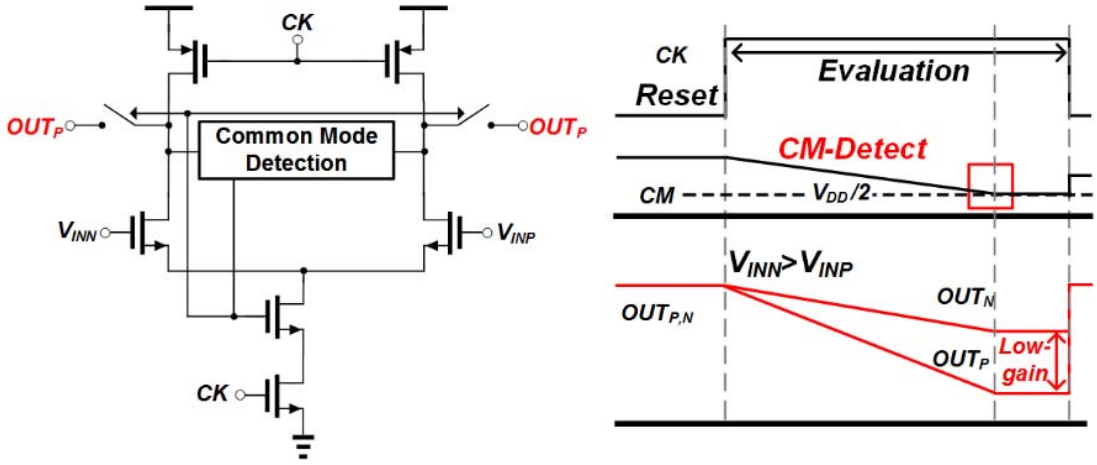


Fig. 11. Conventional dynamic amplifier with its waveforms.

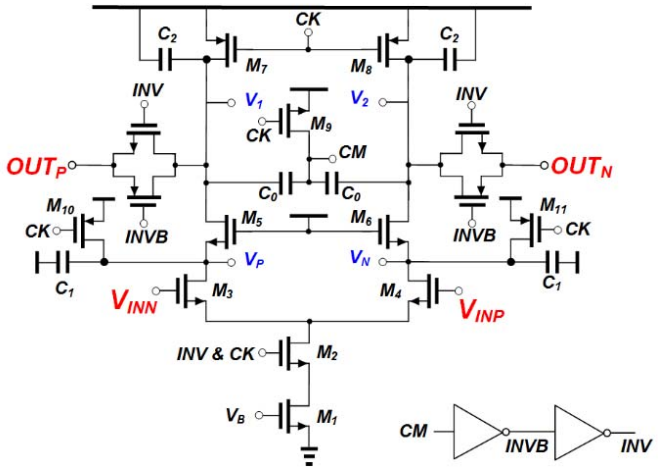


Fig. 12. Proposed dynamic residue amplifier.

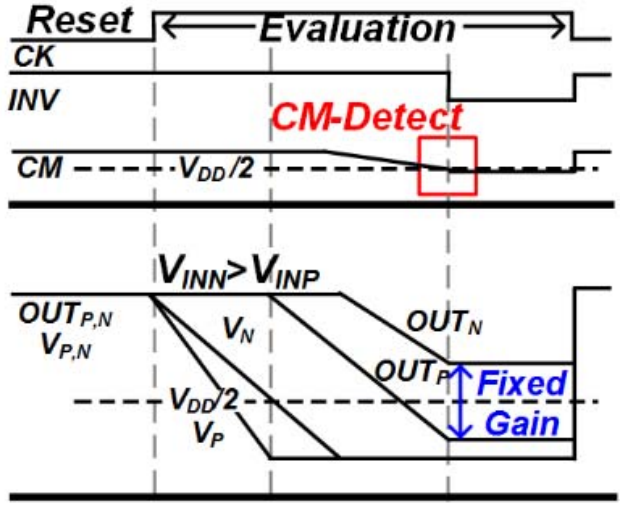


Fig. 13. Key node waveforms of the proposed dynamic amplifier.

As the output voltage decreases, the input pair MOSFET M3, 4 enters into the linear region. To avoid linearity degradation, it is necessary to sample the $\mathrm{OUT}_{P,N}$ voltages before INV falls to GND. The common-mode detection circuit is added to improve linearity. The common-mode-related voltage CM is determined by (9), where C_0 is the capacitance used to detect the output common-mode voltage and C_X is the parasitic capacitance at node CM

$$\mathrm{CM} = \frac{1}{1+C_X/2C_0}\frac{(V1+V2)}{2} + \frac{C_X}{C_X+2C_0}V_{\mathrm{DD}}. \quad (9)$$

In this case, CM approximates to the common-mode voltage of $V1$ and $V2$ as C_X is relatively small compared to C_0. When the CM of $\mathrm{OUT}_{P,N}$ reaches the switching threshold of the inverter, the tail current is cut off for power reduction and $\mathrm{OUT}_{P,N}$ is sampled on CDAC. Simulations show that the proposed CM-detection technique saves power by 45% compared to the traditional approach, with the same gain and noise performance. However, calibration is required for the proposed dynamic residue amplifier because of process, voltage, and temperature variation. For a constant gain under variation, the bias current is determined by a 5-b current DAC, whose amplitude can be programmed in the range of 80–220 nA. Because the overdrive voltage of the input pair varies according to the square root of the tail current, the gain can be calibrated by adjusting the tail current. Higher bias current is required mainly because of the decrease of threshold voltage at high temperature; the gain obtained compensating different corners and temperatures with suitable tail currents is shown in Table I.

B. Adaptive-Reset Comparator

The conventional dynamic comparator, consisting of a preamplifier and latch, is shown in Fig. 14. The two parasitic capacitors C_P are charged to V_{DD} during the pre-charge phase. During the comparison phase, C_P is discharged causing the voltages SN and SP to drop with different rates. When SP or SN passes the switching threshold voltage of the latch, the outputs of the latch reach V_{DD} and GND. In this architecture, the preamplifier allows independent optimization of the latch and smaller kick-back noise. The equivalent input noise of this preamplifier is shown in (10) and it is inversely

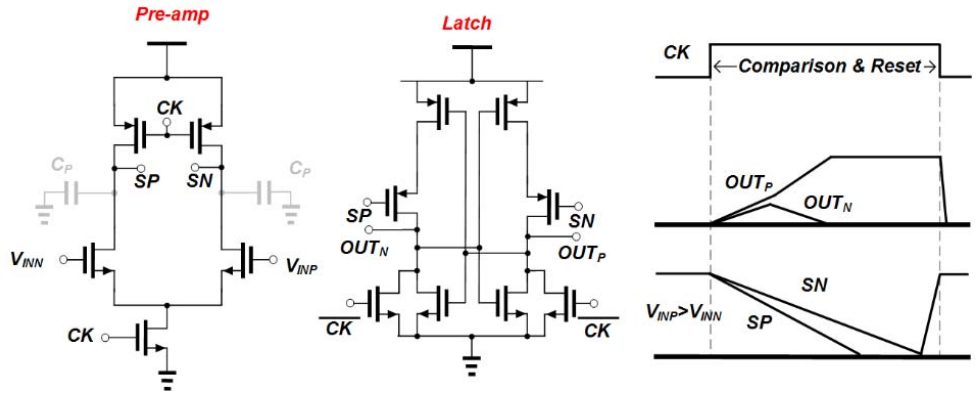


Fig. 14. Conventional comparator and its waveforms.

TABLE I
GAIN AND BIAS CURRENT RELATIONSHIP OF DYNAMIC AMP

Corner	Temp (°C)	Bias(nA)	Gain
tt	27	100	16.01
ss	-40	110	15.9
ss	120	182	16.12
sf	-40	102	15.89
sf	120	220	15.99
fs	-40	102	16.11
fs	120	152	16.1
ff	-40	80	15.95
ff	120	200	16.06

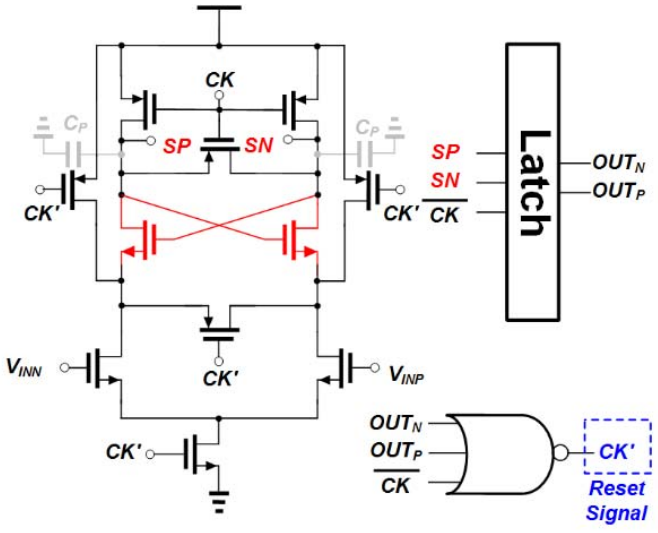


Fig. 15. Proposed adaptive-reset comparator.

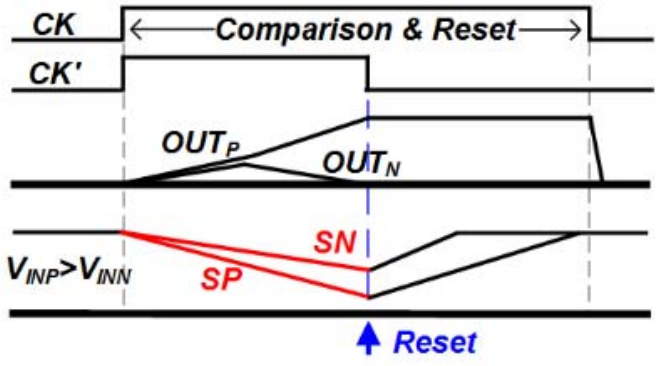


Fig. 16. Key node waveforms of the proposed comparator.

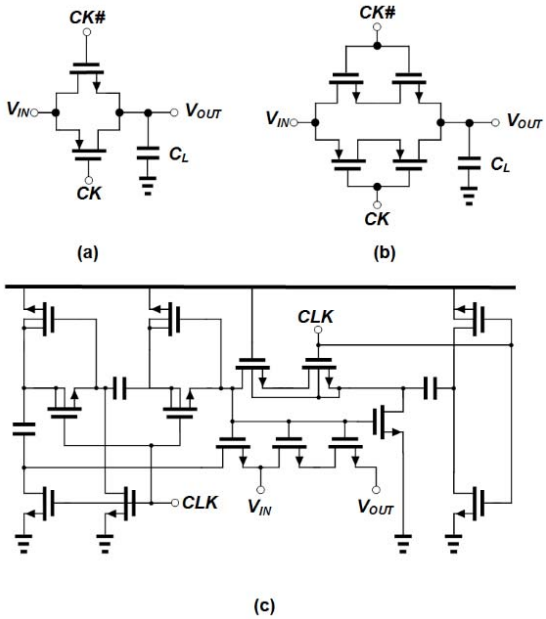


Fig. 17. Sampling circuit implementation using (a) conventional switch (b) stacked switch (c) double-bootstrapped switch.

proportional to the preamp's output capacitance C_P [34]

$$\sigma_V = \mathrm{kT}\sqrt{\frac{8}{qV_{\mathrm{th}}C_P}}. \tag{10}$$

The energy dissipated for one comparison cycle is approximately $2{\cdot}C_P \cdot V_{\mathrm{DD}}^2$. A low-power adaptive-reset comparator is proposed here to increase the power efficiency of the ADC. The proposed adaptive-reset comparator is shown in Fig. 15. The circuit includes a cross-coupled nMOS pair load and reset control circuitry. Fig. 16 depicts the operation: the

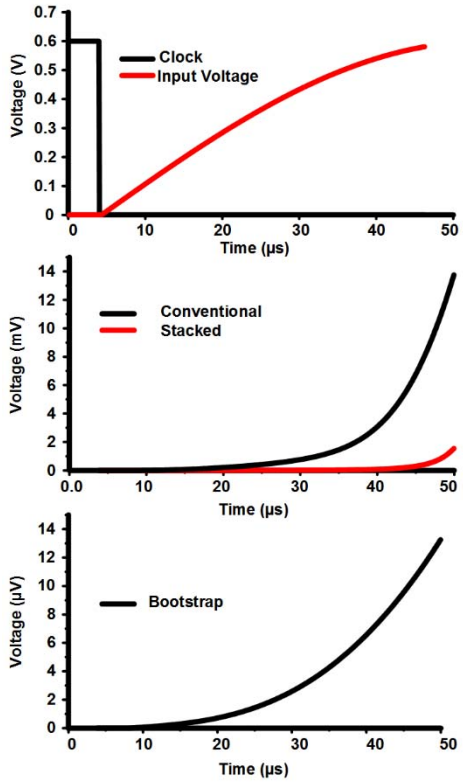


Fig. 18. FF corner simulation result of the sampling circuits.

TABLE II
NIST TEST RESULT OF RAW BIT STREAM

NIST Pub 800-22 Test (Non Post processing)	Result
Frequency	10/10 Pass
Block Frequency	8/10 Pass
Cumulative Sums	10/10 Pass
Runs	3/10 Pass
Longest Runs of 1's	10/10 Pass
Rank	10/10 Pass
FFT	3/10 Pass
Non-overlapping Template	5/10 Pass
Overlapping Template	10/10 Pass
Universal Statistical	3/10 Pass
Approximate Entropy	10/10 Pass
Random Excursions	10/10 Pass
Random Excursions Variant	10/10 Pass
Serial	5/10 Pass
Linear Complexity	10/10 Pass

two capacitors at the drains of the input pair are charged to V_{DD} during the pre-charge phase. When the comparison begins, the nodes SP and SN show different dropping rates due to the input difference. If SP and SN reach the switching threshold of the latch, the CK' signal goes to GND. At that point, the preamplifier's tail MOSFET is switched off while SP and SN are reset to V_{DD}. It can be found that energy consumed for each comparison in this circuit is only $C_P \cdot V_{DD}^2$, which is half of the previous structure: this is because, SP and SN do not need to be discharged to GND. Another advantage of this architecture comes from the increased gain provided by the cross-coupled nMOS pair load. The comparator in Fig. 14 has a simple single-stage

TABLE III
NIST TEST RESULT AFTER PROCESSING

NIST Pub 800-22 Test	P-value	Result
Frequency	0.604516	Pass
Block Frequency	0.479645	Pass
Cumulative Sums	0.670332	Pass
Runs	0.248512	Pass
Longest Runs of 1's	0.411082	Pass
Rank	0.403234	Pass
FFT	0.532412	Pass
Non-overlapping Template	100% Success	Pass
Overlapping Template	0.088015	Pass
Universal Statistical	0.171075	Pass
Approximate Entropy	0.255739	Pass
Random Excursions	0.29578	Pass
Random Excursions Variant	0.082536	Pass
Serial	0.179012	Pass
Linear Complexity	0.288754	Pass

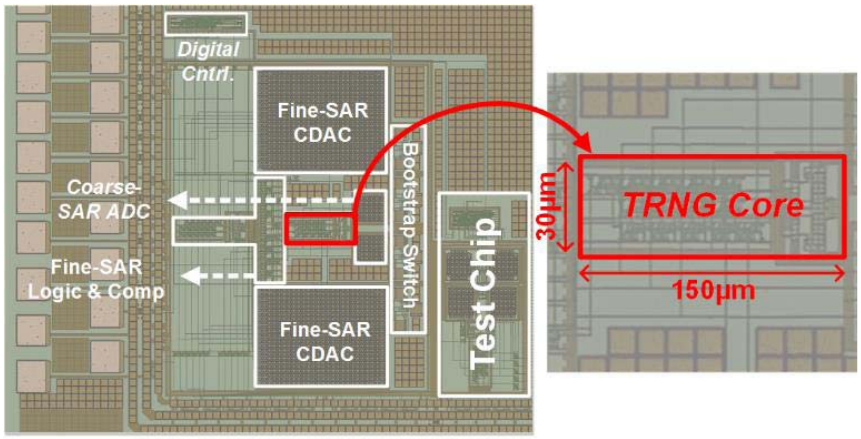
integrator as pre-amplifier, which provides low gain. For this reason, it must have a large latch gain to reduce the overall noise. In the proposed architecture, the cross-coupled nMOS boosts the gain due to its positive feedback. Therefore, the second stage can be designed for higher noise margin than in the previous circuit. From simulations, the proposed adaptive-reset comparator saves 58% power compared to [34] with achieving the same noise performance.

C. Switch Implementation

At low supply voltage, realizing sampling switches becomes challenging due to the degraded ratio of "ON" conductance to "OFF" current. Fig. 17 shows different sampling switch implementations, and Fig. 18 shows the transient simulation of the different switch in the FF corner. Fig. 17(a) depicts a conventional transmission gate, and its transient waveform at 20 kS/s rate is shown in Fig. 18. It has significant leakage of 16 mV when the drain and source voltage of the S/H circuit increase. Due to this leakage, we chose the stacked switch implementation shown in Fig. 17(b), resulting in a significant reduction of leakage to 2 mV when the voltage difference between drain and source is 600 mV. This is sufficient for the TRNG, requiring 5-bit resolution, however, further reduction of the leakage is required for the fine-SAR ADC. To further reduce the leakage current, a double-bootstrapped switch from [35] is adopted, as shown in Fig. 17(c). The gate–source voltage of the sampling transistors is fixed at double the supply voltage, which results in low on-resistance and improves the switch linearity. Fig. 18 shows that the leakage in the circuit exploiting bootstrap is reduced to 15 μV, which is sufficient for the 10-bit requirement of the fine-SAR ADC.

V. IMPLEMENTATION RESULTS

Fig. 19 shows the chip photograph and performance summary table. The proposed chaotic TRNG and 10-bit ADC are fabricated in a 180-nm CMOS process. The ultra-low-power and high-randomness chaotic TRNG and the low-power 10-bit ADC utilizing hardware-reusing technique are implemented in a single chip. The TRNG core occupies only 30 μm $\times$ 150 μm excluding the shared ADC blocks and it passes all the subtests at 270 kb/s bit rate, while the ADC core occupies 0.21 mm^2 and achieves 56.4 signal-to-noise plus distortion ratio at 216-kb/s sampling rate. Thanks to the coarse-SAR ADC block,



TRNG Performance	
Technology	180 nm Mixed CMOS
Supply	0.6V
Area	0.0045mm^2
Data Rate	Max 270kb/s
TRNG Power Breakdown	
CDAC	3nW
Digital Process	25nW
Residue Amp	48nW
Comparator	6nW

ADC Performance	
Technology	180 nm Mixed CMOS
Sampling Rate	Max 216kb/s
INL	0.64 / -0.65 LSB
DNL	0.42 / -0.49 LSB
SNDR	56.4 dB
SFDR	68.2 dB
Area	0.0045mm^2
Power	312nW

Fig. 19. Chip microphotograph and performance summary.

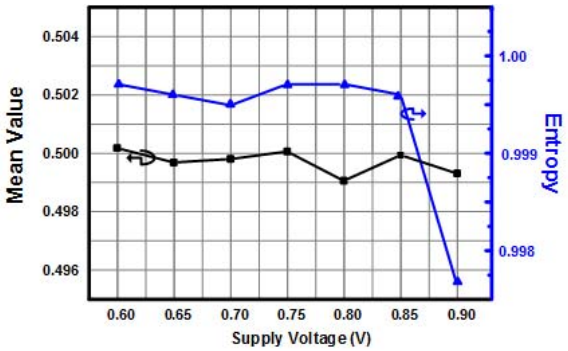


Fig. 20. Measured mean and entropy of the raw random output versus supply voltage.

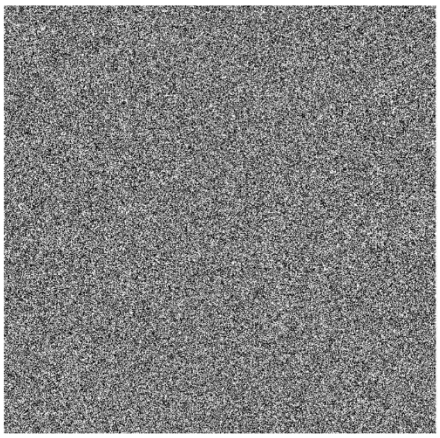


Fig. 21. 1-M TRNG output bits displayed in a 1024 × 1024 array.

which is shared with the proposed TRNG, the switching power is reduced by 82% compared to a conventional architecture. Moreover, the proposed adaptive-reset comparator reduces the power consumption by 58%. As a result, the total ADC power consumption is only 312 nW. Fig. 20 shows the measured mean and entropy of TRNG output bit with respect to the supply voltage. For a supply voltage range of 0.6–0.9 V, the output bit of TRNG sustains high entropy (∼1) and even means (∼0.5). The entropy is estimated according to (11) which is the Shannon entropy test [38]

$$h = \frac{-\sum_{i=0}^{2^k-1} v_i \log_2 v_i}{k} \tag{11}$$

where v_i is the observed frequency in the outcomes of the TRNG during a period of time and the sequence is divided into subsequent non overlapping strings of k bits. In this test, we use 4-M bit raw data stream (without post-processing) and $k = 5$. The measured supply voltage is limited to 0.9 V because the proposed TRNG operates together with the ADC that uses a double bootstrap switch. Therefore, depending on the system application, TRNG can operate at higher voltage if it is not combined with the ADC. Fig. 21 shows the measured 1-M bit steam of TRNG without perceptible patterns (0 = black dot, 1 = white dot). The total power consumption is 82 nW at 0.6-V supply voltage. The measured waveforms of the proposed ADC and TRNG are shown in Fig. 22. In each four-conversion period, the TRNG generates five random bits (MSB to LSB) while the ADC converts four sampled inputs. NIST SP-800.22 tests [38] are used to evaluate the randomness of TRNG with a threshold of

TABLE IV
PERFORMANCE COMPARISON OF THE TRNG

	ISSCC'08 [9]	ISSCC'14 [10]	JSSC'12 [11]	ASSSC'14 [12]	TCASI'10 [19]	JSSC'16 [39]	JSSC'16 [40]	This Work
Technology	250nm	28/65nm	45nm	40nm	180nm	180nm	14nm	**180nm**
Entropy Source	Sin-MOSFET	Oscillator Jitter	Metast-ability	Metast-ability	Chaotic System	Oscillator Jitter	Metast-ability	**Chaotic System**
Bit Rate (Mb/s)	2	23.16/2.8	2400	0.5	80	0.18	8.6/162.5	**0.27**
TRNG Core Area ($\mu m^2/L^2$)	19k	478k/227k	1975k	875k	3888k	223k	5142k	**138k**
Power(μW)	1900	54/159	7000	0.214	22000	3.7	27/1500	**0.082**
Efficiency (pJ/bit)	950	23/57	2.9	0.43	275	21	3/9.2	**0.30**

TABLE V
PERFORMANCE COMPARISON OF ADCS WITH TRNGS

	[4]	[5]	[36]	[37]	This Work
Process	130nm	180nm	130nm	130nm	**180nm**
ADC (bit)	8	8	10	8	**10**
RNG Type	PRNG	PRNG	PRNG	PRNG	**TRNG**
Power* (ADC+RNG)	900nW	2.36μW	4.5μW	2μW	**394nW**
Area* (ADC+RNG)	0.17mm^2	0.065mm^2	0.095mm^2	0.042mm^2	**0.21mm^2**
Sampling Rate	100	95k	36k	100k	**216k**

* Only ADC is included in other work and area is estimated

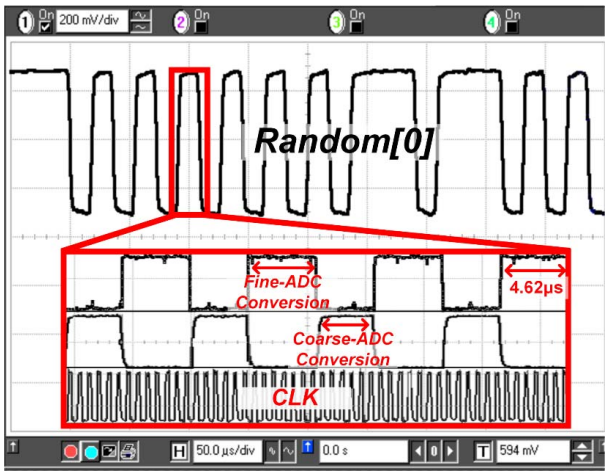


Fig. 22. Measured waveforms.

P-value $>$ 0.01(significance level). Table II shows the NIST test result of 100 $\times$ 1 M bit raw bit stream with 0.6-V supply. The TRNG is tested with ten data sets, and 10 out of 15 subtests are passed successfully while five subtests are failed due to imperfections in the implementation of the chaotic map. The imperfection in chaotic map is due to the quantization error from CDAC mismatch or comparator offset. Therefore, we performed an XOR post-processing (parity-based post-processing). As shown in Table III, when the post-processing bit width is 4, the TRNG successfully passed all of the 15 subtests for 100 $\times$ 1 M bit streams. The performance summary and comparison with recent TRNG's are described in Table IV and Fig. 23. Although the data rate is reduced to 1/4 due to the post-processing, the proposed TRNG still achieved 29.3% power reduction (82 nW) at 270 kb/s throughput, and it achieved a 0.30-pJ/bit figure-of-merit (FOM) which is the state of the art. Table V shows the comparison table with recent RFID tag system including ADC and random number generators. The proposed ADC and TRNG core represents the lowest power consumption (394 nW) even if it generates true random numbers, while previous works were only capable of generating pseudo-random numbers.

VI. CONCLUSION

In this paper, we present a chaotic map TRNG based on a sub-ranging SAR ADC for wireless RFID sensor system that not only consumes low power but also can be integrated into wireless sensor nodes with compact area. The coarse-ADC is shared for area reduction, and it is used not only

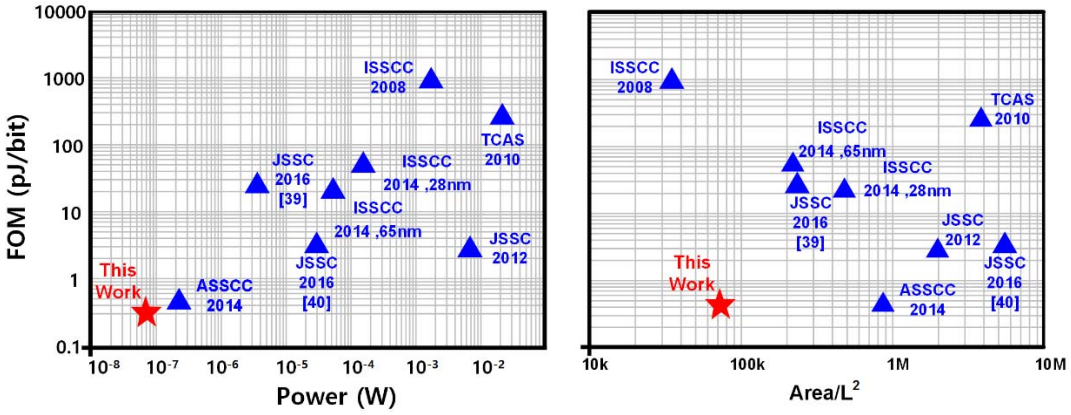


Fig. 23. FoM versus area and power.

for the discrete-time chaotic system but also for DAC switching of the fine-SAR ADC, to reduce power consumption. Moreover, a new dynamic residue amplifier and an adaptive-reset comparator are proposed to achieve 45% and 58% power saving over previous implementations. The proposed TRNG dissipated only 82-nW power and achieves the best reported FOM 0.3 pJ/bit while passing all NIST tests.

REFERENCES

[1] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[2] Z. Liu and D. Peng, "True random number generator in RFID systems against traceability," in *Proc. IEEE Consum. Netw. Conf. (CCNS)*, Jan. 2006, pp. 620–624.

[3] Y. Yao. (2011). *A Sub-0.5V Lattice-Based Public-Key Encryption Scheme for RFID Platforms in 130 nm CMOS*. [Online]. Available: http://www.cs.virginia.edu/evans/pubs/rfidsec11/rfidsec.pdf

[4] D. Yeager, F. Zhang, A. Zarrasvand, N. T. George, T. Daniel, and B. P. Otis, "A 9 μA, addressable Gen2 sensor tag for biosignal acquisition," *IEEE J. Solid-State Circuits*, vol. 45, no. 10, pp. 2198–2209, Oct. 2010.

[5] V.-H. Duong, N. X. Hieu, H.-S. Lee, and J.-W. Lee, "A battery-assisted passive EPC Gen-2 RFID sensor tag IC with efficient battery power management and RF energy harvesting," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7112–7123, Nov. 2016.

[6] M. Dichtl, "How to predict the output of a hardware random number generator," in *Proc. Workshop Cryptograph. Hardw. Embedded Syst.*, vol. 2779, 2003, pp. 181–188.

[7] G. K. Balachandran and R. E. Barnett, "A 440-nA true random number generator for passive RFID tags," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 11, pp. 3723–3732, Dec. 2008.

[8] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.

[9] J. Holleman, B. Otis, S. Bridges, A. Mitros, and C. Diorio, "A 2.92 μW hardware random number generator," in *Proc. 32nd Eur. Solid-State Circuits Conf.*, Sep. 2006, pp. 134–137.

[10] 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.

[11] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita, "1200 μm^2 physical random-number generators based on SiN MOSFET for secure smart-card application," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2008, pp. 414–415.

[12] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "16.3 A 23 Mb/s 23 pJ/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 280–283.

[13] S. K. Mathew *et al.*, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[14] T. K. Kuan, Y. H. Chiang, and S. I. Liu, "A 0.43pJ/bit true random number generator," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2014, pp. 33–36.

[15] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A feedback strategy to improve the entropy of a Chaos-based random bit generator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 2, pp. 326–337, Feb. 2006.

[16] M. Degaldo-Restituto, F. Medeiro, and A. Rodriguez-Vazquez, "Nonlinear switched-current CMOS IC for random signal generation," *Electron. Lett.*, vol. 29, no. 25, pp. 2190–2191, Dec. 1993.

[17] C.-C. Wang, J.-M. Huang, H.-C. Cheng, and R. Hu, "Switched-current 3-bit CMOS 4.0-MHz wideband random signal generator," *IEEE J. Solid-State Circuits*, vol. 40, no. 6, pp. 1360–1365, Jun. 2005.

[18] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-Part I: Analysis," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 38, no. 3, pp. 281–288, Mar. 2001.

[19] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators—Part II: Practical realization," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 38, no. 3, pp. 281–288, Mar. 2001.

[20] S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and Chaos," *IEEE Trans. Signal Process.*, vol. 48, no. 3, pp. 382–385, Aug. 2005.

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

[22] H. Nejati, A. Beirami, and W. H. Ali, "Discrete-time chaotic-map truly random number generators: Design, implementation, and variability analysis of the ZigZag map," *Analog Integr. Circuits Signal Process.*, vol. 73, no. 1, pp. 363–374, 2012.

[23] J. Bean and P. J. Langlois, "A current mode analog circuit for tent maps using piecewise linear functions," in *Proc. IEEE ISCAS*, Jun. 1994, pp. 125–128.

[24] M. Kim, U. Ha, Y. Lee, K. Lee, and H. J. Yoo, "A 82 nW chaotic-map true random number generator based on sub-ranging SAR ADC," in *Proc. IEEE ESSCIRC*, Sep. 2016, pp. 157–160.

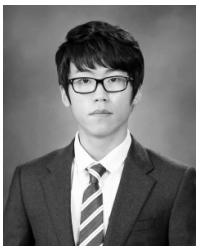
[25] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos*, 2nd ed. New York, NY, USA: Springer, 2003.

[26] L.-S. Young, "Ergodic theory of chaotic dynamical systems," in *Proc. 12th Int. Congr. Math. Phys.*, 1997, pp. 311–319.

[27] T. Inoue, "Ergodic theorems for piecewise affine Markov maps with indifferent fixed points," *Hiroshima Math. J.*, vol. 24, no. 3, pp. 447–471, Jan. 1993.

[28] M. Fabbri and S. Callegari, "Very low cost entropy source based on chaotic dynamics retrofittable on networked devices to prevent RNG attacks," in *Proc. ICECS*, 2014, pp. 175–178.

[29] S. Callegari, M. Fabbri, and A. Beirami, "Very low cost Chaos-based entropy source for the retrofit or design augmentation of networked devices," *Analog Integr. Circuits Signal Process.*, vol. 87, no. 2, pp. 155–167, 2016.
[30] S. Callegari and G. Setti, "ADCs, Chaos and TRNGs: A generalized view exploiting Markov chain lumpability properties," in *Proc. IEEE ISCAS*, 2007, pp. 213–216.
[31] H.-Y. Tai, Y.-S. Hu, H.-W. Chen, and H.-S. Chen, "A 0.85 fJ/conversion-step 10b 200 kS/s subranging SAR ADC in 40 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 196–197.
[32] G. Setti, G. Mazzini, R. Rovatti, and S. Callegari, "Statistical modeling of discrete time chaotic processes: Basic finite dimensional tools and applications," *Proc. IEEE*, vol. 90, no. 5, pp. 662–690, May 2002.
[33] F. Pareschi, G. Setti, and R. Rovatti, "Noise robustness condition for chaotic maps with piecewise constant invariant density," in *Proc. ISCAS*, 2004, pp. 681–684.
[34] M. van Elzakker, E. van Tuijl, P. Geraedts, D. Schinkel, E. Klumperink, and B. Nauta, "A 1.9 μW 4.4 fJ/conversion-step 10 b 1 MS/s charge-redistribution ADC," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2008, pp. 244–245.
[35] J.-Y. Lin and C.-C. Hsieh, "A 0.3 V 10-bit 1.17 f SAR ADC with merge and split switching in 90 nm CMOS," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 31–43, Jan. 2015.
[36] H. Reinisch *et al.*, "A multifrequency passive sensing tag with on-chip temperature sensor and off-chip sensor interface using EPC HF and UHF RFID technology," *IEEE J. Solid-State Circuits*, vol. 46, no. 12, pp. 3075–3087, Dec. 2011.
[37] D. Brenk *et al.*, "Energy-efficient wireless sensing using a generic ADC sensor interface within a passive multi-standard RFID transponder," *IEEE Sensors J.*, vol. 11, no. 11, pp. 2698–2710, Nov. 2011.
[38] W. Schindler and W. Killmann, "Evaluation criteria for true (physical) random number generators used in cryptographic applications," in *Proc. Cryptograph. Hardw. Embedded Syst.*, 2003, pp. 431–449.
[39] A. Rukhin *et al.*, "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," Nat. Inst. Standards Technol., Odisha, India, Tech. Rep. 800-22, 2010.
[40] 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.
[41] S. K. Mathew *et al.*, "μ 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.



Minseo Kim (S'14) received the B.S. degree in semiconductor system engineering from Sung Kyun Kwan University, Seoul, South Korea, in 2014, and the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2016, where he is currently pursuing the Ph.D. degree.

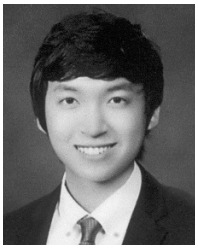
His current research interests include low-power biomedical system-on-chip for wearable healthcare system.

Unsoo Ha (S'12) received the B.S. *(summa cum laude)* degree from the School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2012, where he is currently pursuing the Ph.D. degree.

His current research interests include biomedical system-on-chip design especially with a focus on multimodal brain monitoring system and designing bio-signal sensor front end for low-power application.

Kyuho Jason Lee (S'12) received the B.S. and M.S. degrees from the School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2012 and 2014, respectively, where he is currently pursuing the Ph.D. degree.

His current research interests include the development of analog/digital mixed-mode neural network system-on-chip (SoC) design, object matching processor and its algorithm for computer vision, energy-efficient network-on-chip-based SoC design for mobile devices, and intelligent vision processor for advanced driver assistance system.



Yongsu Lee (S'13–M'16) received the B.S. and M.S. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2013 and 2015, respectively, where he is currently pursuing the Ph.D. degree.

His current research interests include low-power biomedical system-on-chip (SoC) for wearable healthcare system and human body communication SoC for low-power application.

Hoi-Jun Yoo (M'95–SM'04–F'08) received the bachelor's degree from the Electronic Department, Seoul National University, Seoul, South Korea, in 1983, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 1985 and 1988, respectively.

From 2001 to 2005, he was the Director of the Korean System Integration and IP Authoring Research Center (SIPAC) in Korea. From 2003 to 2005, he was the full time Advisor to the Minister of Korea with the Ministry of Information and Communication in Korea, and the National Project Manager for system-on-chip (SoC) and computer. In 2007, he founded the System Design Innovation and Application Research Center, KAIST. Since 1998, he has been a Faculty Member with the Department of Electrical Engineering, KAIST, where he is currently a Full Professor. He has co-authored *DRAM Design* (South Korea: Hongrung, 1996), *High Performance DRAM* (South Korea: Sigma, 1999), *Future Memory: FRAM* (South Korea: Sigma, 2000), *Networks on Chips* (Morgan Kaufmann, 2006), *Low-Power NoC for High-Performance SoC Design* (CRC Press, 2008), *Circuits at the Nanoscale* (CRC Press, 2009), *Embedded Memories for Nano-Scale VLSIs* (Springer, 2009), *Mobile 3-D Graphics SoC from Algorithm to Chip* (Wiley, 2010), *Biomedical CMOS ICs* (Springer, 2011), *Embedded Systems* (Wiley, 2012), and *Ultra-low-Power Short-Range Radios* (Springer, 2015). His current research interests include computer vision SoC, body area networks, and biomedical devices and circuits.

Dr. Yoo was a recipient of the Electronic Industrial Association of Korea Award for his contribution to DRAM technology in 1994, the Hynix Development Award in 1995, the Korea Semiconductor Industry Association Award in 2002, the Best Research of KAIST Award in 2007, the Scientist/Engineer of this month Award from the Ministry of Education, Science and Technology of Korea in 2010, the Best Scholarship Awards of KAIST in 2011, and the Order of Service Merit from the Ministry of Public Administration and Security of Korea in 2011, and a co-recipients of the ASP-DAC Design Award in 2001, the Outstanding Design Awards of 2005–2007, 2010, 2011, and 2014 A-SSCC, and the Student Design Contest Award of 2007, 2008, 2010, and 2011 DAC/ISSCC. He served as a member of the executive committee of ISSCC, Symposium on VLSI, and A-SSCC, a TPC Chair of the A-SSCC 2008 and ISWC 2010, the IEEE Distinguished Lecturer from 2010 to 2011, the Far East Chair of ISSCC from 2011 to 2012, the Technology Direction Sub-Committee Chair of ISSCC 2013, a TPC Vice Chair of ISSCC 2014, and a TPC Chair of ISSCC 2015. Since 2010, he has been serving as the General Chair of the Korean Institute of Next Generation Computing.