IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

True Random Number Generators Using Electrical Noise

Lishuang Gong[1], Jianguo Zhang[1], Haifang Liu[1], Luxiao Sang[1], Yuncai Wang[1,2*]

[1] Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education and Shanxi Province), College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China
[2] School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China

Corresponding author: Yuncai Wang (e-mail: wangyc@gdut.edu.cn).

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61731014, Grant No. 61671316 and Grant No.61775158, in part by the Research Project Supported by Shanxi Scholarship Council of China, and in part by the Natural Science Foundation of Shanxi Province under Grant No. 201801D121145.

ABSTRACT True random number generators (TRNGs) are a fundamental resource in information security and can guarantee the absolute security of information in principle. Entropy source is the most critical part of TRNGs, which provides the unpredictability and is the root of security for TRNGs. Electrical noise, which is inevitable and unpredictable in electronic systems, is always used as entropy source for TRNGs. This review discusses the different methods to harvest electrical noise in TRNGs, including the early amplify noise based on amplifier, phase jitter based on oscillator, the effect of electrical noise on the metastable behavior and amplify noise based on chaos circuits. Each method has its own strengths in aspect of speed, cost, complexity and portability. Finally, some post-processing technologies and TRNG evaluation methods are also discussed. With this review, we hope the current spots for TRNGs using electrical noise are summarized and some possible future directions are pointed out.

INDEX TERMS TRNGs, electrical noise, entropy source, post-processing, evaluation methods

I. INTRODUCTION

Random number generator is always important for information encryption and decryption, numerical simulations, lottery games and stochastic experiments [1]. Historically, random number generator is divided into pseudo-random number generators (PRNGs) and true random number generators (TRNGs).

PRNGs use some initial seeds and deterministic algorithms to produce pseudo-random numbers and can result in high throughput. However, once the seeds are obtained by attacker, all security will be lost. Thus, it is dangerous that using PRNGs produce secret keys. For the sake of defending against such problems, TRNGs are designed by researches, which extract random numbers from physical random processes. These are contrary to the pseudo-random numbers produced by computer program and can guarantee the absolute security of information in principle.

The randomness of TRNGs come from entropy source which is the root of security for TRNGs. Electrical noise is inevitable in electronic systems. Due to the unpredictability of white noise, it is an ideal entropy source for TRNGs. Several methods of harvesting electrical noise in TRNGs are available, such as amplify noise based on amplifier [2-4], phase jitter based on oscillator [5-8], the impact of electrical noise on the metastable behavior [9-12] and amplify noise based on chaos circuits [1, 13, 14]. Classical noise-based TRNGs use high-gain differential amplifier to amplify noise to a level and compared with a threshold in a comparator, then the noise amplified is converted to produce a digital signal [2]. However, this will consume lots of power because noise is leveled up a few orders to meet the needs of digital logic level, and designing amplifier is a complex work [10]. Hence, some researches focusing on these problems were carried out, including Si nano-devices [15], identical inverters [16], oxide breakdown [17, 18] and random telegraph noise [19].

Though these methods are valid to produce high quality true random bits, they show some great challenges when are manufactured in sub-14 nm processes. These circuits need stable supply voltage and they are sensitive to temperature and aging, which will induce device drifts. To solve these problems, generating random bits using digital circuits are studied because electrical noise also can lead to phase jitter in oscillator [20, 21]. These TRNGs extract entropy from edge-

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

jitter of oscillator and sample jitter events using phase-detector, including ring oscillators [7], coupled oscillators [2, 22, 23] and Fibonacci/Galois ring oscillators [24, 25]. Another popular digital technique harvesting noise is using the metastable behavior [9, 12, 26, 27]. Because metastability of bi-stable circuits can be influenced by thermal noise then a random bit is produced [9, 12, 26].

Due to its non-periodicity and non-reproducibility, fast TRNGs are key in information security [28-30] and large-scale parallel computation [31]. Because of lacking infinite measurement precision in chaotic circuit, it is impossible to confirm initial conditions exactly and chaotic dynamic is sensitive to initial value. Additionally, the uncertainties can be amplified by chaotic systems [32]. What's more, chaotic systems have high wideband. These make chaotic circuits convenient candidates for fast TRNGs and TRNGs using chaotic circuit have been extensive researched [33-35].

Due to intrinsic bias and correlations derived from entropy source, raw bits are usually hard to achieve good statistical properties. In this case, post-processing is need to reduce statistical flaws. And their exciting experiments are certified by randomness tests, such as NIST, Diehard, Test U01 and AIS 31. In this paper, we attempt to review the evolution of electrical noise-based TRNGs, the advantages and challenges are demonstrated and shown to the readers. TRNG model is given detailly in section II. And entropy source is introduced in section III. Subsequently, section IV reviews different methods of harvesting electrical noise in TRNGs. Section V gives a brief review on post-processing and Section Ⅵ introduces TRNG evaluation methods. In the end, conclusions are drawn in Section Ⅶ.

II. TRNG MODEL

Generally speaking, TRNGs consist of entropy source, a harvesting component and post-processing component, as shown in Figure 1. Entropy source, which is the most important component of TRNG, provides the unpredictability and is the root of security for TRNG. Harvesting component does not impede the physical of entropy source and collects entropy as much as possible. It reads data produced by entropy source and converts data to a series of bits. The output bits are called the raw data. Using harvesting component, entropy can be collected as much as possible and physical process of entropy source won't be disturbed. Though entropy source can provide true randomness, the raw bits are usually biased and not uniformly distributed for various reasons. Thus, post-processing is needed to reduce residual correlation in random sequence and make output uniformly distributed. It can cover up imperfections from entropy source or harvesting component.

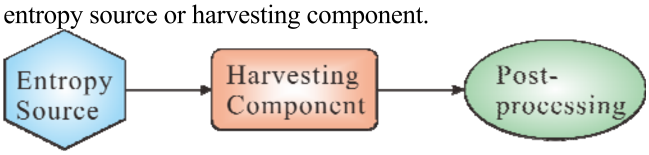

FIGURE 1. **TRNG Model.**

III. ENTROPY SOURCE

Entropy source is the root of TRNGs. To ensure the effective of TRNGs, entropy source must be unpredictable in principle. Electrical noise, which is unpredictable and inevitable in electronic systems, is an ideal entropy source. Electrical noise mainly includes shot noise, thermal noise and flicker noise. The mean square variation of external current is known as shot noise and it exists in diodes, bipolar transistors and MOS transistors. It is written as $\overline{i^2}$ and can be expressed as

$$\overline{i^2} = 2qI_D\Delta f \tag{1}$$

Where q is electronic charge and equal to 1.6×10^{-19} C, I_D is the average value of a series of random independent pulses and Δf is the bandwidth in hertz.

Equation (1) demonstrates that shot noise is increased with bandwidth of measurement. The spectral density of noise-current is constant and shot noise is white noise. Equation (1) is perfectly valid into the gigahertz region. The amplitude distribution of shot noise is Gaussian and its standard variance is

$$\sigma = \sqrt{\overline{i^2}} = \sqrt{2qI_D\Delta f} \tag{2}$$

In electronic systems, random thermal motion of charge carriers will lead to thermal noise. Because electron thermal velocities in a conductor is much faster than typical electron drift velocities. Thermal noise is not affected by whether direct current present. Thermal noise is increased with absolute temperature T and it can be written as equation (3) or (4) [36]

$$\overline{v^2} = 4kTR\Delta f \tag{3}$$

Where $\overline{v^2}$ is voltage variation caused by thermal noise, k is Boltzmann constant and R is resistance.

$$\overline{i^2} = 4kT\frac{1}{R}\Delta f \tag{4}$$

Equation (3) and (4) demonstrate that the spectral density of thermal noise is also not depend on frequency and this is valid into 10^{13} Hz. Thus, thermal noise is another white noise. Because white noise is unpredictable and independent with frequency, it is an ideal entropy source for TRNGs.

Flicker noise is mainly resulted by traps connected with contamination and crystal defects. These traps random capture and release carriers and they cause a noise signal with energy concentrated at low frequencies. Flicker noise is connected with a flow of direct current and can be expressed as

$$\overline{i^2} = K_1\frac{I^a}{f^b}\Delta f \tag{5}$$

Where K_1, a and b are constant ($0.5 \le a \le 2$, $b \approx 1$), I is direct current. If b = 1, the spectral density of flicker noise depends on $1/f$ frequency. Hence flicker noise is also known as $1/f$ noise. It is valid into the megahertz range.

According to equation (5), flicker noise may cause correlation in the output of random number generations. Thus, some researchers attempt to suppress flicker noise in TRNGs

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2939027, IEEE Access

using electrical noise, [37]. Also many researches take no account the effects of flicker noise [38]. And some researches manifest flicker noise have effect on random number generation [39, 40], while these researches are insufficient to make an interpretation confidently.

With respect to the methods of harvesting electrical noise, TRNGs can be divided into four main groups: amplify noise-based TRNGs, oscillator-based TRNGs, metastability-based TRNGs and chaotic TRNGs.

IV. TRNGS BASED ON DIFFERENT METHODS OF HARVESTING ELECTRICAL NOISE

A. TRNGS BASED ON AMPLIFY NOISE

Noise is inevitable in electronic systems. Because of its natural randomness, noise is one of the preferred entropy sources for TRNGs [41]. Early noise-based TRNGs utilize analog circuitries to directly amplify noise. After amplified, noise is sampled and quantized in circuit devices [2, 42]. As shown in Figure 2, classical noise-based TRNGs employ an amplifier to deal with small voltage fluctuate caused by electrical noise from a resistor or semiconductor diode as initial randomness source. Then the amplified noise is compared with a threshold using comparator to produce digital signal. Subsequently, this digital signal is sampled and processed to generate random bit sequence.

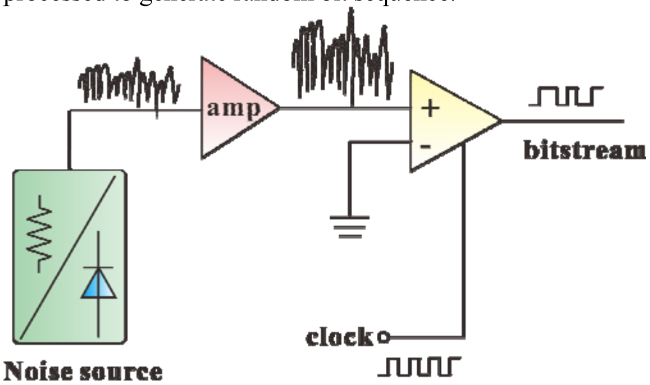

FIGURE 2. Amplify noise-based TRNGs.

For this kind of noise-based TRNGs, noise must be amplified to a level that the threshold is no bias compared by a comparator, which needs lots of power to bring the noise level up a few orders of magnitude to digital logic level, and designing amplifier is a complex work [10]. These also make it difficult balance between circuit area and quality of random numbers. To solve these problems, S. Fujita proposed using Si nanodevices to produce high-amplitude device noise, which reduced the size of TRNGs and produced high quality random numbers [15]. Later, increasing noise magnitude with inserting a SiN layer rich in high-density electron traps was proposed [43]. The experimental results showed the area of this TRNG was reduced much and the throughput was increased than TRNG previously reported [2]. However, using this method required additional photo mask, which increased the expense. Then, other TRNGs were proposed. Because the electrical properties of metal-oxide semiconductor (MOS) after soft breakdown (SBD) shows large fluctuation [17, 18]. In 2004, a novel RNG using MOS capacitors after SBD as a random source was presented [17]. In 2010, Christophe De Roover and Michiel Steyaert amplified noise using identical inverters and produced a series of random bits consuming only 0.65nw [16]. Subsequently, TRNG using random telegraph noise (RTN) was proposed due to its unpredictability and some basic guidelines for designing RNT-based TRNG also was provided [19].

For noise-based TRNG, the threshold needs to be adjusted to a proper value so that the probabilities of “0” and “1” are equal. However, owing to environment variations and temperature perturbations, it is difficult to adjusting to a precise and proper value in practice. Thus, the raw digitized bits are usually correlated or biased and post-processing is needed. What’s worse, it needs extra device to reduce the influence of electromagnetic interference. In addition, this kind of TRNGs can be easily impacted by flicker noise, which will produce correlation sequences.

B. TRNGS BASED ON OSCILLATOR

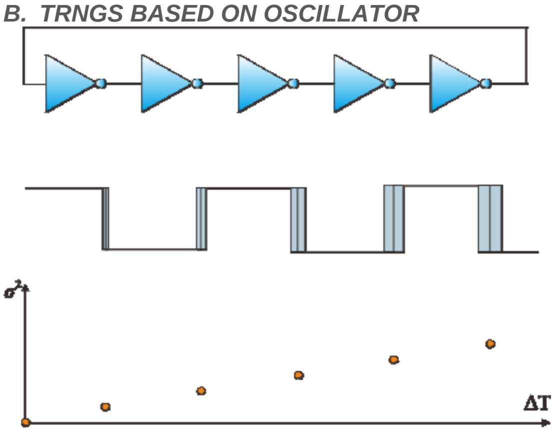

FIGURE 3. Jitter increasing with the number of inverters.

Electrical noise also can lead to phase jitter in oscillator [20, 44, 45]. The research on phase noise and jitter in oscillator was introduced and developed until 1990s [46, 47]. In 2006, a simple and straightforward model for phase noise and jitter was published by Abidi [48]. Rencently, due to its simple structure and produce random bits effectively, TRNGs using phase jitter have been extensively researched [5, 39, 49]. In theory, the simplest oscillator can contain only one inverter. However, in digital circuit, phase jitter using an inverter is very small. To increase jitter, odd inverters is chained then a simple oscillator is built. Its open loop structure is shown in Figure 3. It is perfect when the output of oscillator is a periodic square wave. But the transition spacing is variable actually on account of electrical noise. Arbitrary uncertainty in a previous transition influences all the subsequent transitions, and this influence persists indefinitely, this uncertainty will be increased with the number of inverters added.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2939027, IEEE Access

In this paper, for simplicity, the model of ring oscillator is simplified as a single inverter, a delay τ and a feedback loop and the ring oscillator following Barkhausen criterion [50]. In 1996, it was modeled that a low-frequency ring oscillator sampled a high-frequency ring oscillator using a D flip-flop for generate unpredictable bits [51], as shown in Figure 4. Generally, this configuration is called coupled oscillators. TRNGs based on coupled oscillator can be designed purely digital and without amplifier. Subsequently, some researches realized it and provided some methods to enhance its performance [23, 37, 52]. However, precisely matching the period of coupled oscillators is quite hard and two signals of frequency oscillators may drift relative to one another. These don't make for very robust TRNG designs. Some researchers used additional circuitry to adjust waveforms to make the transitions matched. While it decreases the randomness of jitter and brings in some biases.

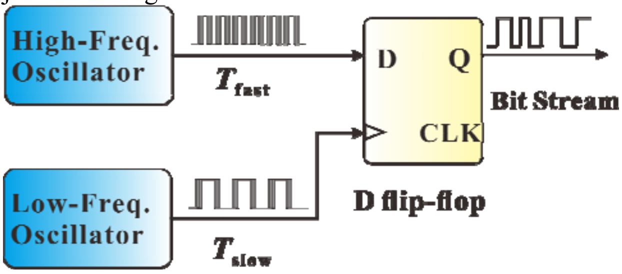

FIGURE 4. The schematic diagram of couple oscillator-based TRNG.

To alleviate these problems, Sunar *et. al.* put forward a classical TRNG combining and sampling some equal length ring oscillators [5], as illustrated in Figure 5 (a). The outputs of oscillators were XORed and sampled using D-type flip flop to generate random bits. Also, its security was proved by Sunar in [5]. Although, many resources were needed using this method, it was very popular due to its production of high entropy of random bits and easy implementation after post-processing. Ülkühan Güler and Günhan Dündar realized the first integrated circuit implementation using Sunar's method and generated high-quality random bits using the simple Von Neuman corrector instead of Sunar's post-processor [53, 54]. And to maximize randomness of CMOS ring oscillator-based TRNGs, Ülkühan Güler derived randomness equations and defined randomness parameter [39]. Later, an improved version of Sunar's method was put forward by Knut Wold and Chik How Tan [55], as shown in Figure 5 (b). With an flip-flop added after each oscillator before the XOR tree, modified TRNG could pass randomness tests without post-processing and the number of oscillators was decreased. Subsequently, Knut Wold and Slobodan Petrovi´c optimized the parameters of modified TRNG by spectral analysis and achieved 300 Mbit/s throughput [56]. However, Ring oscillator-based TRNGs using Word's method need constant oscillation of many ROs to accumulate enough jitter to produce high quality random bits, which still lead to large power consumption [57]. Also, Word's method may introduce pseudo randomness and this pseudo randomness is impossible to be eliminated [58], thus the TRNG may be attacked.

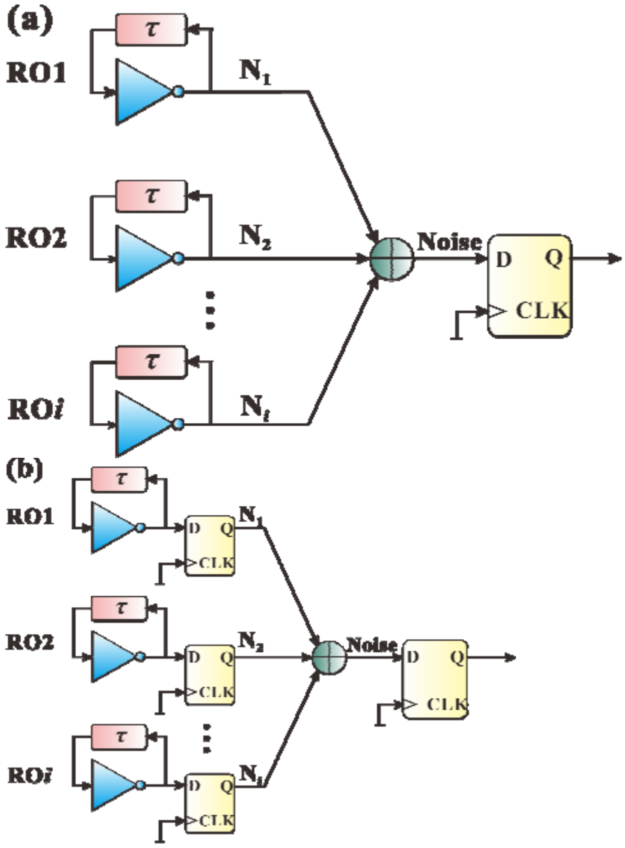

FIGURE 5. The basic schematic diagram of Sunar's method and its modification.

Fibonacci ring oscillators (FIRO) and Galois ring oscillators (GARO) are two new forms of ring oscillators. These designs refer to linear feedback shift registers (LFSR) and use inverters instead of shift registers. Schematic diagrams of FIRO and GARO are shown in Figure 6. Their feedback connections need to be chosen appropriately to avoid dynamic collapse into the fixed points. When the number of inverters reduce to only one, both FIRO and GARO become classical ring oscillator. Bothe even or odd are allowed for the number of inverters in FIRO, but not equal to 2. And the output of FIRO can be come from arbitrary inverter. While the number of inverters in GARO should be odd and the output of GARO is come from the last inverter. In 2006, FIRO and GARO for TRNG were proposed and analyzed in [24]. Subsequently, a novel sampling method nearly doubling the entropy was put forward by Jovan Golić [25]. In 2010, Ülkühan *et al.* designed the first ASIC implementation of TRNG combining FIRO with GARO and this design provided a throughput of 125Mbps [59]. Inspired by [24] and [25], Lijuan Li and Shuguo Li proposed a digital TRNG using cross feedback ring oscillator [60]. Compared with FIRO and GARO, it saved more than half of the time to accumulate very high entropy and generated one unpredictable bit.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2939027, IEEE Access

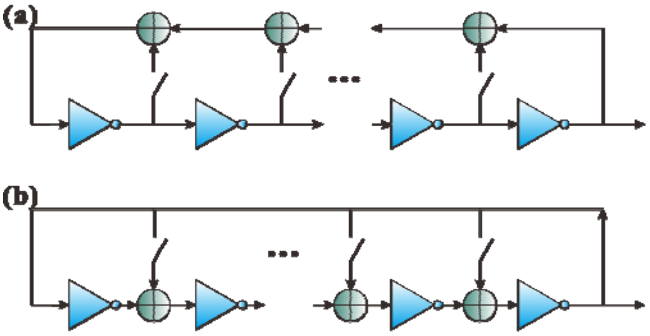

FIGURE 6. **Fibonacci ring oscillators (a) and Galois ring oscillators (b).**

By restarting FIRO and GARO under the same initial conditions and calculating time evolution of standard deviation of output, their randomness was evaluated and analyzed [25, 61]. It was demonstrated that a higher and more robust entropy rate could be achieved using FIRO and GARO. Compared to other oscillators, the number of inverters using FIRO and GARO is reduced and FIRO and GARO are more sensitive to jitter [24, 25]. Thus, jitter is quickly propagated and transformed through feedback. Thus, FIRO and GARO are more suitable entropy source.

However, some drawbacks can hinder the usage oscillator-based TRNGs, such as aging, frequency locking, technology dependence and highly power consumption [62, 63]. What's worse, oscillator-based TRNGs suffer from frequency attacking easily [64], which can lead to entropy loss. Rahman *et al*. presented adding self-compensation mechanism or extra power supply noise for oscillator-based TRNG to avoid frequency attacks [65]. And Böhl *et al*. presented the on-line testable solution to ensure randomness [66].

Realizing in an all-digital design makes oscillator-based TRNGs easier to integrate into applications. Not only quality of the TRNGs are essential, but also its speed for practical applications. Additionally, the rapid development of quantum key distribution (QKD) systems will cause even more enormous challenges to the throughput of TRNGs in the next few years. Because ring oscillator-based TRNGs usually need a mass of logic gates to generate high speed random number, this method usually combine with other methods.

C. TRNGS BASED ON METASTABILITY

Metastable-based TRNG is another method can be realized using digital technique. It has been known that the final state between two equal desirable outputs can be determined by random processes. Hence, the final state of bi-stable circuit in metastable point is determined by circuit noise [9]. The classical metastable-based TRNG was developed by *Philips* in [67], which used metastable cross-coupled inverters to handle thermal noise, as shown in Figure 7. It is composed of a cross-coupled inverter pair. By pre-charging inverter diffusion nodes, the inverter pair can be driven into unstable state to identical logic values. Ultimately, either stable state (a=1, b=0) or (a=0, b=1) is decided by the differential noise at 'a' and 'b' during the metastable period.

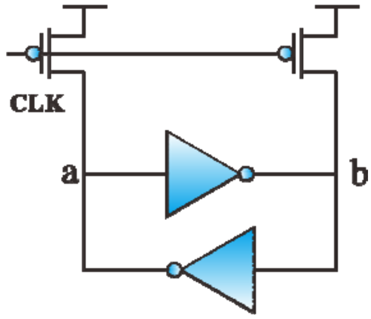

FIGURE 7. **Cross-coupled inverter pair.**

Due to its easy integration and energy-efficient in circuits [57], metastability is a perfect solution for TRNGs. However, metastability events are very sensitive to manufacturing process and voltage and temperature (PVT) changes. Hence, it is hard to keeping a bi-stable circuit in an unstable state [68, 69]. What's worse, these inaccuracies affecting the symmetry of the metastability will cause bias and decrease the entropy rate of the outputs bits of metastable circuit [70]. Hence, some researches focusing on the symmetry of metastable circuit were carried out. In 2011, a metastability-based TRNG with adaptive control was proposed by Majzoobi *et al*. [69]. The experimental results showed using programmable delay lines could precisely equalize the signal arrival times to obtain metastability and produced throughput of 2 Mbit/s. Later, Hata and Ichikawa came up with a solution using almost identical RS latch to guarantee the quality of randomness and achieved throughput of 12.5Mbps [71]. Meanwhile, a self-calibrating 2-step tuning mechanism was used for metastability-based TRNG by Intel and it provided tolerance to 20% PVT variation [10]. Subsequently, Intel improved this TRNG using in-line decorrelators and a lightweight BIW extractor. It demonstrated that this TRNG could provide a throughput of 162.5 Mbps at 1.3 GHz operation, with 1.5 mW total power consumption and a 90 μW leakage component [11].

Metastability also exists in RS latches [72] and D-type flip-flops [67]. For its all-digital design and simple structure, TRNGs using metastable circuits is increasingly popular [11, 57, 71, 73]. Meanwhile, many other solutions were proposed to keep a bi-stable circuit in a metastable state. In 2008, Tokunaga *et al*. presented the solution controlling the metastability proximity to produce random bit, which formed the bi-stable by adjusting the initial input inverters [12]. In 2010, Varchola and Drutarovsky put forward a new bi-stable structure which is known as transition effect ring oscillator for TRNG [74]. This TRNG extracted randomness from oscillatory metastability and the sensitivity of the global perturbations was lower than ring oscillator. However, the initial condition of TERO could not be adjusted. Later, Piotr Zbigniew Wieczorek proposed dual-metastability time-competitive TRNG [75, 76], which generated random number by comparing the unpredictable resolve time of two similar metastable D-latches (or flip-flops) to generate random number and this method could be carried out with

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2939027, IEEE Access

various logic programmable circuits. In 2016, Piotr Zbigniew Wieczorek proposed a novel TRNG, which adjusted the initial condition in pre-autonomous mode and extract randomness from parameters of two bi-stable transient response [63]. Due to the symmetry of the presented solution, its robustness and tolerating temperature and supply voltage variations was increased. Subsequently, Piotr Zbigniew Wieczorek combined chaotic circuit with metastability. Not only were the parameters of the circuit insensitive to PVT conditions using this method, but also this method had better performance of anti-attack of active injection side-channel attack [77]. Recently, Sha Tao and Elena Dubrova harvested entropy from latches comparators in their detectable metastable states and harnessed several ternary valued latches to address the bias caused by conditions [78]. And, Barangi *et al*. used metastable state in straintronics magnetic tunneling junction generated unpredictable random number at a high rate with low-energy overhead.

For one-time-pad, it needs abundant random bits. For this, speed is important because taking much time to produce random number is not permitted. To this end, TRNGs based on chaos are proposed and realized in recent years.

D. TRNGS BASED ON CHAOS

Due to its high bandwidth, unpredictability and insensitive to various disturbance and tolerances of components, chaos is a perfect entropy source for fast TRNGs [14, 79, 80]. In 2013, David P. Rosin *et al*. put forward a TRNG using autonomous logic gates, and this TRNG was claimed to reach the throughput of 12.8 Gbps. This do not rely on a clock and is promising candidates for TRNG because it is easily integrated [81]. Wen Li *et al*. proposed an all-electronic TRNG based on high amplitude chaotic oscillations [82]. This TRNG presented random bit throughput of 80 Gbps and its robustness and fully electronic implementation implies scalability and minimal post-processing compared with existing optical TRNG.

Physical randomness is derived from electrical noise and amplified by deterministic chaos [83]. The statistical properties can also be made more desirable by chaotic dynamics [84]. Figure 8 illustrates chaos-based TRNGs. The entropy source of the chaos-based TRNGs is a non-linear dynamical system operating in chaotic regime. Then entropy is harvested by a sampler and imperfection of entropy source is masked by post-processing.

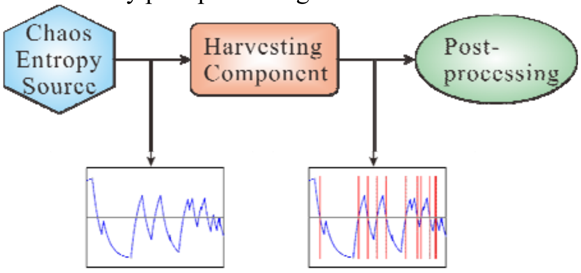

FIGURE 8. The schematic diagram of chaos-based TRNGs.

In general, according to underlying dynamics, chaos-based TRNGs can be divided into continuous time and discrete time. The future state of the continuous time chaotic systems is decided by differential equations relating to the rate of change relating to the variables of current state. However, analog circuit blocks is need for continuous time chaos-based TRNGs, such as operational amplifier (OPAMP) [85, 86], which make continuous time chaos-based TRNGs have large area and high consumption. Compared with continuous time chaotic system, discrete time chaos-based TRNGs is able to be built by less components. Future state of the discrete time chaotic systems is decided by differential equations which merely relates to the current state [87]. Generally, the operation of the discrete time chaos-based TRNGs require an external clock to drive chaotic dynamics. Thus, it depends on the clock frequency that the speed of generation and development for forming the chaotic dynamic. For discrete time chaos-based TRNGs, clock frequency can be adjusted dynamically at runtime. This makes it lower consumption and high throughput without any topological modifications. What's more, discrete time chaos-based TRNG can be implemented by digital circuit. Thus, it is simple to implement digital integrated circuit and its circuit only incorporates a few typical electronic devices. These make it desirable candidates for applying to lightweight and hardware efficient TRNGs [85].

However, digital chaotic implementations involve finite computational precision, which may lead to pseudo-random output [88]. Thus, it will be very helpful that identifying a continuous random variable which can be used in digital circuits. This variable can have complementary advantages of analog chaotic signal and digital circuit. Thus, a TRNG combined chaotic circuit and metastability was proposed [77]. Where chaotic behavior results from switchable ring oscillators and metastability result from a flip-flop. This method provided high quality random bits without additional post-processing. What's more, it is immune to active injection side-channel attacks.

D. COMPARISONS and CHALLENGES

The methods of harvesting electrical noise is summarized briefly in Table I. The table gives a few representative references, the order of the typical bit rates for every kind TRNG, their advantages and challenges.

TABLE I
Comparisons of entropy source using electrical noise and their challenges

Classification		Technology	Reference	Rate(order)	Advantages	Challenges
Amplify noise		Analog	[2]	1Mbps	Simple structure	Low power consumption; High rate
Oscillator	Couple oscillator	Digital	[37]	10Mbps	Easy integration	Frequency attack; High rate
	Ring oscillator	Digital	[5]	1Mbps	Good portability	Injection locking
	FIRO/GARO	Digital	[24]	100Mbps	More sensitive to jitter	Directly prove randomness
Metastability		Digital	[77]	1Mbps	Easy integration;	Symmetry
Chaos	Continuous time chaos	Analog	[86]	10Mbps	High rate	Low power consumption
	Discrete time chaos	Digital	[33]	100Mbps	High rate	Finite Computable precision

Ⅴ. Post-processing

Due to intrinsic bias and correlations derived from entropy source, raw bits are usually hard to achieve good statistical properties. In this case, post-processing is need to reduce statistical flaws. Generally speaking, using post-processing has two goals. One is adjusting the probability distribution of raw random bits conform to a uniform distribution. With this method, statistical defects in entropy source or harvest component are compensated. The other is increasing entropy per bit using a compression function. Usually, using post-processing can increase that the probability of bits passing the test, while their throughput will be reduced [89].

A post-processing can be as simple as a XOR corrector and von Neumann corrector [76]. It can also be as complicated as a resilient function [5] and hash function [90]. XOR and Von Neumann are the most common post-processing for TRNGs because of their easy application [91]. Von Neumann algorithm is an ideal method to reduce bias, using it, uniformly distributed 0 and 1 numbers can be obtained. In addition, regarding only consequent number pairs makes Von Neumann is the simplest post-processing method. Its disadvantage is that the throughput of TRNG will be decreased, because the (0,0) and (1,1) number pairs are abandoned.

Post-processing is not needed in all TRNGs. Because post-processing may limit the bitrate of TRNGs substantially, the low rates of post-processing for TRNGs usually are not included in ultra-fast random number generation. As far as I know, the generation of fast random number bits is limited by their obtain methods with high-speed oscilloscopes. Thus, most studies of post-processing for ultrafast TRNG are carried out offline [84]. The defects of post-processing are increased power consumption and decreased in the bit rate, respectively. And some challenges also are brought including scalability to higher rates, interfacing with computing and communication architectures [90].

Ⅵ. TRNG evaluations

To use TRNGs in cryptographic applications, we must certify the output bits are secure enough. Entropy provides a convenient way for measuring randomness. In the information theory, expressing entropy in bits is a natural formulation for information processing and communications. In different entropies, Shannon entropy is well known and interesting estimator for its a simplicity and validity. It evaluates the useful information of randomness from the perspective of probability. And it is defined as

$$H_n(X) = -\sum_x P_X(x)\log_2 P_X(x) \tag{6}$$

Where $H_n(X)$ is Shannon entropy, X is random variable, $P_X(x)$ is the probability of outcome.

Shannon entropy provides a rough estimation of randomness. Higher Shannon entropy means closer to uniform distribution and we are able to harvest more random bits from entropy source. It is ideal to produce a nearly uniform distribution under the guidance of Shannon entropy.

The other popular entropy estimator is min-entropy that recommended by NIST [92]. Min-entropy evaluates the difficulty that the output of the TRNGs are predicted. The probability that a random bit is first inferred correctly is related the distribution of min-entropy which the random bit is generated from. The min-entropy, which estimates randomness from the perspective of attacker, is strongly associated with negative logarithm of the maximum probability using the optimal guessing strategy. The min-entropy $H_\infty(X)$ can be defined as

IEEE Access Multidisciplinary | Rapid Review | Open Access Journal

$$H_{\infty}(X) = -\min_{1\le i\le k}(-\log_2 p_i) = -\log_2 \max_{1\le i\le k} p_i \quad (7)$$

Where p_i is the probability of X=x_i and X is the discrete random value from A = [x_1, x_2, … , x_k]. If H is the min-entropy, then the probability that any particular outcome X is observed will be no more than 2^{-H}. When random variable accord with a uniform probability distribution, min-entropy will attain its maximum value $\log_2 k$. As the number of uniform bits, min-entropy can be extracted from a given distribution.

Both Shannon entropy and min-entropy provides strong confidence in randomness. In practical, other entropy evaluations also can be used to give us a guideline when decide how to use a randomness extractor to make the most use of available randomness, such as Kolmogorov-Sinai entropy and T-entropy. However, entropy estimation spends lots of time to achieve highly reliable results. Recently, the most common way to evaluate randomness is represented by statistical tests. NIST SP-800.22 statistical test suite [93] and Die-hard test suite [94] and Test U01 [95] and AIS31 [96] are most common statistical test suites to evaluate their RNGs by researchers. They report test results as fail or pass scores.

Ⅶ. CONCLUSION

TRNGs are playing an increasingly important in information security and cryptography. TRNGs using electric circuits has shown wide prospect because of carried out on compact electronic chips and thus worth further investigating. Electrical noise is inevitable in electronic systems. Because white noise has a uniform power spectral density, that enables obtaining uncorrelated random numbers. Therefore, it is a preferred in random number generation. Various methods of harvesting electrical noise serving as reliable entropy sources are reviewed, such as classical noise amplifier, oscillators, metastability and chaos. Each mehod has its own strengths in terms of speed, cost, complexity and portability. At present, chaos is the most suitable technique for fast random number generator.

While some entropy sources are claimed to directly generate enough random bit sequences, most TRNGs produce imperfect random bits without post-processing. To avoid this problem, TRNGs should include a well-designed post-processing, which can reduce statistical flaws and provide prediction resistance. The random bits need to be tested to prove their reliability. Thus, TRNGs evaluation including entropy estimations and statistical tests are summarized at the end of the paper.

With this review, we hope the current spots for TRNGs using electrical noise are summarized and some possible future directions are pointed out.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61731014, Grant No. 61671316 and Grant No.61775158, in part by the Research Project Supported by Shanxi Scholarship Council of China, and in part by the Natural Science Foundation of Shanxi Province under Grant No. 201801D121145. Additionally, the authors sincerely thank the anonymous reviewers for their valuable comments. Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] 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 Transactions on Circuits and Systems I: Regular Papers., vol. 53, no. 2, pp. 326-337, Feb. 2006.

[2] C. S. Petrie, and A. Connelly, “A noise-based IC random number generator for applications in cryptography,” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications., vol. 47, no. 5, pp. 615-621, May. 2000.

[3] M. Huang, A. B. Wang, P. Li, H. Xu, and Y. C. Wang, “Real-time 3 Gbit/s true random bit generator based on a super-luminescent diode,” Optics Communications., vol. 325, pp. 165-169, Aug. 2014.

[4] N. C. Gov, M. K. Mihcak, and S. Ergun, “True Random Number Generation Via Sampling From Flat Band-Limited Gaussian Processes,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 58, no. 5, pp. 1044-1051, May. 2011.

[5] B. Sunar, W. J. Martin, and D. R. Stinson, “A provably secure true random number generator with built-in tolerance to active attacks,” IEEE Transactions on Computers., vol. 56, no. 1, pp. 109-119, Jan. 2007.

[6] K. Wold, and C. H. Tan, "Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings." International Journal of Reconfigurable Computing., vol. 2009, no. 1, pp. 385-390.

[7] K. Yang, D. Fick, M. B. Henry, and Y. Lee, "16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS." in 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers, San Francisco, CA, USA, 2014, pp. 280-281.

[8] K. Yang, D. Blaauw, and D. Sylvester, "A robust −40 to 120°C all-digital true random number generator in 40nm CMOS." in 2015 Symposium on VLSI Circuits, Kyoto, Japan, 2015, pp. C248-C249.

[9] D. J. Kinniment, and E. G. Chester, "Design of an on-chip random number generator using metastability." in Proceedings of the 28th European Solid-State Circuits Conference, Florence, Italy, 2002, pp. 595-598.

[10] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, “2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors,” IEEE Journal of Solid-State Circuits., vol. 47, no. 11, pp. 2807-2821, Nov. 2012.

[11] S. K. Mathew, D. Johnston, S. Satpathy, and V. Suresh, P. Newman, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen and R. K. Krishnamurthy,“ RNG: A 300–950 mV, 323 Gbps/W All-Digital Full-Entropy True Random Number Generator in 14 nm FinFET CMOS,” IEEE Journal of Solid-State Circuits., vol. 51, no. 7, pp. 1695-1704, July. 2016.

[12] C. Tokunaga, D. Blaauw, and T. Mudge, “True random number generator with a metastability-based quality control,” IEEE Journal of Solid-State Circuits., vol. 43, no. 1, pp. 78-85, Jan. 2008.

[13] S. Ergun, U. Guler, and K. Asada, “A High Speed IC Truly Random Number Generator Based on Chaotic Sampling of Regular Waveform,” Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences., vol. E94-A, no. 1, pp. 180-190, Jan. 2011.

[14] T. Stoianovski, and L. Kocarev, “Chaos-based random number generators—partI: analysis,” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications., vol. 48, no. 3, pp. 281-288, Mar. 2001.

[15] S. Fujita, K. Uchida, S. Yasuda, R. Ohba, H. Nozaki, and T. Tanamoto, "Si nanodevices for random number generating circuits

for cryptographic security." in 2004 IEEE International Solid-State Circuits Conference, San Francisco, CA, USA, 2004, pp. 294-295.

[16] C. D. Roover, and M. Steyaert, "A 500 mV 650 pW Random Number Generator in 130 nm CMOS for a UWB Localization System," in 2010 Proceedings of ESSCIRC, Seville, Spain, 2010, pp. 278-281.

[17] S. Yasuda, H. Satake, T. Tanamoto, and R. Ohba, "Physical random number generator based on MOS structure after soft breakdown," IEEE Journal of Solid-State Circuits., vol. 39, no. 8, pp. 1375-1377, Aug. 2004.

[18] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw, "A true random number generator using time-dependent dielectric breakdown." in 2011 Symposium on VLSI Circuits-Digest of Technical Papers, Honolulu, HI, USA, 2011, pp. 216 - 217.

[19] X. Chen, L. Wang, B. Li, Y. Wang, X. Li, Y. Liu, and H. Yang, "Modeling Random Telegraph Noise as a Randomness Source and its Application in True Random Number Generation," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems., vol. 35, no. 9, pp. 1435-1448, Sept. 2016.

[20] A. Hajimiri, S. Limotyrakis, and T. H. Lee, "Jitter and phase noise in ring oscillators," IEEE Journal of Solid-State Circuits., vol. 34, no. 6, pp. 790-804, Jun. 2002.

[21] A. Demir, "Computing timing jitter from phase noise spectra for oscillators and phase-locked loops with white and 1/f noise," IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 53, no. 9, pp. 1869-1884, Sept. 2006.

[22] Q. Tang, B. Kim, Y. Lao, and K. K. Parhi, "True Random Number Generator circuits based on single- and multi-phase beat frequency detection." in Proceedings of the IEEE 2014 Custom Integrated Circuits Conference, San Jose, CA, USA, 2014, pp. 1-4.

[23] M. Bucci, and R. Luzzi, "Fully Digital Random Bit Generators for Cryptographic Applications," IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 55, no. 3, pp. 861-875, April. 2008.

[24] J. D. J. Golic, "New Methods for Digital Generation and Postprocessing of Random Data," IEEE Transactions on Computers., vol. 55, no. 10, pp. 1217-1229, Oct. 2006.

[25] M. Dichtl, and J. D. Golić, "High-Speed True Random Number Generation with Logic Gates Only." in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 2007, pp. 45-62.

[26] J. Holleman, S. Bridges, B. P. Otis, and C. Diorio, "A 3 W CMOS True Random Number Generator With Adaptive Floating-Gate Offset Cancellation," IEEE Journal of Solid-State Circuits., vol. 43, no. 5, pp. 1324-1336, May. 2008.

[27] S. Srinivasan, S. Mathew, V. Erraguntla, R. Krishnamurthy, and I. C. Soc, "A 4Gbps 0.57pJ/bit Process-Voltage-Temperature Variation Tolerant All-Digital True Random Number Generator in 45nm CMOS," in 22nd International Conference on VlSI Design, New Delhi, India, 2009, pp. 301-306.

[28] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," Physical Review Letters., vol. 108, no. 7, pp. 070602, Feb. 2012.

[29] H. Koizumi, S. Morikatsu, H. Aida, T. Nozawa, I. Kakesu, A. Uchida, K. Yoshimura, J. Muramatsu, and P. Davis, "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," Optics Express., vol. 21, no. 15, pp. 17869-17893, July. 2013.

[30] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers," Optics Express., vol. 17, no. 11, pp. 9053-9061, May. 2009.

[31] H. Miyazawa, and M. Fushimi, "An Implementation of a 5-term GFSR Random Number Generator for Parallel Computations." in Proceedings of the International Symposium on Operations Research and Its Applications, Zhangjiajie, China, 2009, pp. 448–452.

[32] R. F. Fox, and J. Keizer, "Amplification of intrinsic fluctuations by chaotic dynamics in physical systems," Physical Review A., vol. 43, no. 4, pp. 1709-1720, 1991.

[33] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 12, pp. 3124-3137, Dec. 2010.

[34] I. Cicek, A. E. Pusane, and G. Dundar, "A novel design method for discrete time chaos based true random number generators," INTEGRATION, the VlSI Journal., vol. 47, no. 1, pp. 38-47, Jan. 2014.

[35] E. Farcot, S. Best, R. Edwards, I. Belgacem, X. Xu, and P. Gill, "Chaos in a ring circuit," Chaos., vol. 29, no. 4, Apr. 2019.

[36] J. B. Johnson, "Thermal Agitation of Electricity in Conductors," Physical Review., vol. 32, no. 2984, pp. 50-51, July. 1928.

[37] 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 Transactions on Computers., vol. 52, no. 4, pp. 403-409, Apr. 2003.

[38] J. D. Golic, "New methods for digital generation and postprocessing of random data," IEEE Transactions on Computers., vol. 55, no. 10, pp. 1217-1229, Oct. 2006.

[39] U. Guler, and G. Dundar, "Modeling CMOS Ring Oscillator Performance as a Randomness Source," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 61, no. 3, pp. 712-724, Mar. 2014.

[40] C. Liu, "Jitter in oscillators with 1/f noise sources and application to true RNG for cryptography," 2006.

[41] M. Herrerocollantes, and J. C. Garciaescartin, "Quantum Random Number Generators," Reviews of Modern Physics., vol. 89, no. 1, pp. 015004-1- 015004-48 Feb. 2016.

[42] V. Bagini, and M. Bucci, "A Design of Reliable True Random Number Generator for Cryptographic Applications," in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 1999, pp. 204-218.

[43] M. Matsumoto, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita, "1200μm2 Physical Random-Number Generators Based on SiN MOSFET for Secure Smart-Card Application," in IEEE International Solid-State Circuits Conference, San Francisco, CA, USA, pp. 414-624.

[44] A. Hajimiri, and T. H. Lee, "A general theory of phase noise in electrical oscillators," IEEE Journal of Solid-State Circuits., vol. 33, no. 10, pp. 2314-2314, Feb. 1998.

[45] A. Demir, "Phase noise and timing jitter in oscillators with colored-noise sources," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications., vol. 49, no. 12, pp. 1782-1791, Dec. 2002.

[46] A. A. Abidi, and R. G. Meyer, "Noise in relaxation oscillators," IEEE Journal of Solid-State Circuits., vol. 18, no. 6, pp. 794-802, Dec. 1983.

[47] J. A. McNeill, "Jitter in ring oscillators," IEEE Journal of Solid-State Circuits., vol. 32, no. 6, pp. 870-879, June. 1997.

[48] A. A. Abidi, "Phase noise and jitter in CMOS ring oscillators," IEEE Journal of Solid-state Circuits., vol. 41, no. 8, pp. 1803-1816, Aug. 2006.

[49] U. Guler, A. E. Pusane, and G. Dunder, "Investigating Flicker Noise Effect on Randomness of CMOS Ring Oscillator based True Random Number Generators, " in 2014 International Conference on Information Science, Electronics and Electrical Engineering, Sapporo, Japan, 2014, pp. 845-849.

[50] J. Xu, S. Verma, and T. Lee, "Coupled Inverter Ring I/Q Oscillator for Low Power Frequency Synthesis." in 2006 Symposium on VLSI Circuits, Honolulu, HI, USA, 2006, pp. 172-173.

[51] C. S. Petrie, and J. A. Connelly, "Modeling and simulation of oscillator-based random number generators." in 1996 IEEE International Symposium on Circuits and Systems, Atlanta, GA, USA, 1996, pp. 324-327.

[52] H. Bock, M. Bucci, and R. Luzzi, "An Offset-Compensated Oscillator-Based Random Bit Source for Security Applications," Lecture Notes in Computer Science., vol. 3156, pp. 27-83, June. 2004.

[53] Ü. Güler, and G. Dündar, "Modeling phase noise and jitter in subthreshold region and assessing the randomness performance of CMOS ring oscillators." in 2012 International Conference on

Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design, Seville, Spain, 2012, pp. 257-260.

[54] Ü. Güler, and G. Dündar, "Maximizing randomness in ring oscillators for security applications." in 20th European Conference on Circuit Theory and Design, Linkoping, Sweden, 2011, pp. 118-121.

[55] K. Wold, and C. H. Tan, “Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings,” International Journal of Reconfigurable Computing, vol. 2009, no. 1, pp. 385-390, June. 2009.

[56] K. Wold, and S. Petrovic, "Optimizing Speed of a True Random Number Generator in FPGA by Spectral Analysis." in 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, Seoul, South Korea, 2009, pp. 1105-1110.

[57] V. B. Suresh, and W. P. Burleson, “Entropy and Energy Bounds for Metastability Based TRNG with Lightweight Post-Processing,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 62, no. 7, pp. 1785-1793, Jul. 2015.

[58] N. Bochard, F. Bernard and V. Fischer, “Observing the randomness in RO-based TRNG, ” in 2009 International Conference on Reconfigurable Computing and FPGAs, Quintana Roo, Mexico, 2009, pp. 237-242.

[59] Ü. Güler, S. Ergün, and G. Dündar, "A digital IC Random Number Generator with logic gates only." in 17th IEEE International Conference on Electronics, Circuits and Systems, Athens, Greece, 2010, pp. 239-242.

[60] L. Li, and S. Li, “A Digital TRNG Based on Cross Feedback Ring Oscillators,” Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences., vol. E97A, no. 1, pp. 284-291, Jan. 2014.

[61] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, “On the Security of Oscillator-Based Random Number Generators,” Journal of Cryptology., vol. 24, no. 2, pp. 398-425, Apr. 2011.

[62] A. T. Markettos, and S. W. Moore, "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators." in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 2009, pp. 317-331.

[63] P. Z. Wieczorek, “Lightweight TRNG Based on Multiphase Timing of Bistables,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 63, no. 7, pp. 1043-1054, Jul. 2016.

[64] A. T. Markettos, and S. W. Moore, "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators." in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 2009, pp. 317-331.

[65] M. T. Rahman, K. Xiao, D. Forte, X. Zhang, J. Shi, and M. Tehranipoor, "TI-TRNG: Technology Independent True Random Number Generator." in Proceedings of the 51st Annual Design Automation Conference, San Francisco, CA, USA, 2014, pp. 1-6.

[66] E. Bohl, M. Lewis, and S. Galkin, "A true random number generator with on-line testability." in 19th IEEE European Test Symposium, Paderborn, Germany, 2014, pp. 1-6.

[67] M. Epstein, L. Hars, R. Krasinski, M. Rosner, and H. Zheng, "Design and implementation of a true random number generator based on digital circuit artifacts," in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 2003, pp. 152-165.

[68] P. Z. Wieczorek, and K. Golofit, “Dual-Metastability Time-Competitive True Random Number Generator,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 61, no. 1, pp. 134-145, Jan. 2014.

[69] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control." in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 2011, pp. 17-32.

[70] W. A. M. V. Noije, W. T. Liu, and S. Navarro, Jr, “Metastability behavior of mismatched CMOS flip-flops using state diagram analysis,” in Proceedings of IEEE Custom Integrated Circuits Conference-CICC'93, San Diego, CA, USA, 1993. pp. 27.7.1- 27.7.4.

[71] H. Hata, and S. Ichiawa, “FPGA Implementation of Metastability-Based True Random Number Generator,” Ieice Transactions on Information and Systems., vol. E95D, no. 2, pp. 426-436, Feb. 2012.

[72] L. Kleeman, and A. Cantoni, “Metastable Behavior in Digital Systems,” Design & Test of Computers IEEE, vol. 4, no. 6, pp. 4-19, Dec. 1987.

[73] S. Mathew, D. Johnston, P. Newman, S. Satpathy, V. Suresh, M. Anders, H. Kaul, G. Chen, A. Agarwal, and S. Hsu, "µRNG: A 300–950mV 323Gbps/W all-digital full-entropy true random number generator in 14nm FinFET CMOS." in ESSCIRC Conference 2015-41st European Solid-State Circuits Conference, Graz, Austria, 2015, pp. 1-10.

[74] M. Varchola, and M. Drutarovsky, "New High Entropy Element for FPGA Based True Random Number Generators." in International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Germany, 2010, pp. 351-365.

[75] P. Z. Wieczorek, “Dual-metastability FPGA-based true random number generator,” Electronics Letters., vol. 49, no. 12, pp. 744-745, Jun. 2013.

[76] P. Z. Wieczorek, “An FPGA Implementation of the Resolve Time-Based True Random Number Generator With Quality Control,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 61, no. 12, pp. 3450-3459, Dec. 2014.

[77] P. Z. Wieczorek, and K. Gołofit, “True Random Number Generator Based on Flip-Flop Resolve Time Instability Boosted by Random Chaotic Source,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 65, no.4, pp. 1279-1292, Apr. 2018.

[78] S. Tao, and E. Dubrova, "TVL-TRNG: Sub-Microwatt True Random Number Generator Exploiting Metastability in Ternary Valued Latches." in IEEE 47th International Symposium on Multiple-Valued Logic, Novi Sad, Serbia, 2002, pp. 130-135.

[79] A. Beirami, and H. Nejati, “A Framework for Investigating the Performance of Chaotic-Map Truly Random Number Generators,” IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 60, no. 7, pp. 446-450, Jul. 2013.

[80] M. Drutarovsky, and P. Galajda, "A Robust Chaos-Based True Random Number Generator Embedded in Reconfigurable Switched-Capacitor Hardware." in 17th International Conference Radioelektronika, Brno, Czech Republic, 2007, pp. 1-6.

[81] R. Zhang, H. L. D. d. S. Cavalcante, Z. Gao, D. J. Gauthier, J. E. S. Socolar, M. M. Adams, and D. P. Lathrop, “Boolean chaos,” Physical Review E., vol. 80, no. 4, pp. 045202, Oct. 2009.

[82] W. Li, I. Reidler, Y. Aviad, Y. Huang, H. Song, Y. Zhang, M. Rosenbluh, and I. Kanter, “Fast physical random-number generation based on room-temperature chaotic oscillations in weakly coupled superlattices,” Physical Review Letters., vol. 111, no. 4, pp. 044102, Jul. 2013.

[83] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K.-i. Arai, A. Uchida, and P. Davis, “Theory of fast nondeterministic physical random-bit generation with chaotic lasers,” Physical Review E., vol. 85, no. 4, Apr. 2012.

[84] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, “Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser,” Physical Review Letters., vol. 103, no. 2, Jul. 2009.

[85] V. Tavas, A. S. Demirkol, S. Ozoguz, A. Zeki, and A. Toker, “Integrated cross-coupled chaos oscillator applied to random number generation,” Iet Circuits Devices & Systems., vol. 3, no. 1, pp. 1-11, Feb. 2009.

[86] M. E. Yalcin, J. A. K. Suykens, and J. Vandewalle, “True random bit generation from a double-scroll attractor,” IEEE Transactions on Circuits and Systems I: Regular Papers., vol. 51, no. 7, pp. 1395-1404, Jul. 2004.

[87] J. Dvorakova, “Chaos in nonautonomous discrete dynamical systems,” Communications in Nonlinear Science and Numerical Simulation., vol. 17, no. 12, pp. 4649-4652, Dec. 2012.

[88] M. François, D. Defour, and C. Negre, “A Fast Chaos-Based Pseudo-Random Bit Generator Using Binary64 Floating-Point Arithmetic,” Informatica., vol. 38, no. 2, pp. 115--124, 2014.

[89] Y. Wang, C. Hui, C. Liu, and C. Xu, “Theory and implementation of a very high throughput true random number generator in field programmable gate array,” Review of Scientific Instruments., vol. 87, no. 4, Apr. 2016.

[90] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, “Fast nondeterministic random-bit generation using on-chip chaos lasers,” Physical Review A., vol. 83, no. 3, Mar. 2011.

[91] E. Avaroglu, T. Tuncer, A. B. Ozer, B. Ergen, and M. Turk, "A novel chaos-based post-processing for TRNG," Nonlinear Dynamics., vol. 81, no. 1-2, pp. 189-199, Jul. 2015.
[92] M. P. Pawlowski, A. Jara, and M. Ogorzalek, "Harvesting Entropy for Random Number Generation for Internet of Things Constrained Devices Using On-Board Sensors," Sensors., vol. 15, no. 10, pp. 26838-26865, Oct. 2015.
[93] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special publication 800-22, May 2001, National Institute for Standards and Technology (NIST).
[94] G. Marsaglia, "The marsaglia random number CD-ROM including the DieHard battery of test of randomness," [Online]. Available: http://stat. fsu.edu/pub/diehard/
[95] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," AMC Trans. Math. Softw., vol. 33, no. 4, Aug. 2007, Art. No. 22.
[96] W. Killmann and W. Schindler, "AIS 31: Functionality classes and evaluation methodology for true (physical) random number generators," in Bundesamt fur Sicherheit in Der Informationstechnik (BSI), Bonn, 2001, version 3.1.

Lishuang Gong is a reading doctor in Taiyuan University of Technology. Her current research is focused on physical random number generation.

Jianguo Zhang received his Ph.D. degree in circuit and system from Taiyuan University of Technology, China, in 2013. Now, he is an associate professor at Key Laboratory of Advanced Transducers and Intelligent Control System, Taiyuan University of Technology. His research interests include instrument science and measurement technology.

Haifang Liu is a reading doctor in Taiyuan University of Technology. Her current research is focused on physical random number generation.

Luxiao Sang is a reading doctor in Taiyuan University of Technology. Her current research is focused on generation and application of chaotic signal.

Yuncai Wang received Ph.D. degree in physics and optics from Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Shanxi, China, in 1997. Since 2003, he has been a Professor at Key Laboratory of Advanced Transducers and Intelligent Control System, Taiyuan University of Technology. His current research interests include nonlinear dynamics of semiconductor lasers, fibers and their applications, and generation of physical random number.