IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 11, 2020, accepted October 1, 2020, date of publication October 5, 2020, date of current version October 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3028735

Fast True Random Number Generator Based on Chaotic Oscillation in Self-Feedback Weakly Coupled Superlattices

YANFEI LIU[1], CHENG CHEN[1], DONG DONG YANG[1], QI LI[1], AND XIUJIAN LI[2]
[1]Department of Basic Courses, Rocket Forces Engineering University, Xi'an 710025, China
[2]College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, China

Corresponding author: Yanfei Liu (bbmcu@126.com)

This work was supported in part by the Key Program of the National Natural Science Foundation of China under Grant 61834004.

ABSTRACT Random numbers play a vital role in communications and cryptography. However, most existing true random number generators have difficulty in satisfying the requirements of high-speed communications due to their complexity and bulkiness, or low speed limitations due to equipment bandwidth. Then, the all-electron true random number generator was presented based on GaAs/$Al_{0.45}Ga_{0.55}As$ superlattices conducted under direct current bias at room temperature, which not only possesses the characteristics of miniaturization but also generates random numbers at rates up to the Gbit/s. However, the bit rate of random number generators based on superlattices is still much slower compared to chaotic laser random number generators. In order to generate higher-rate random numbers, we modified a DC-excited superlattice and then redirected the signal generated by the superlattice back into itself, thus introducing a self-feedback, and achieved a self-feedback superlattice true random number generator. This improvement makes the superlattice have a more detailed signal shape, a more effective signal amplitude, and with lower power consumption. Therefore, these advances made the self-feedback superlattice more suitable for generating random numbers. Moreover, we propose a new post-processing method, called the adjacent bits reversal exclusive-or. This method can reduce the sequence bias and correlation without discarding any random bit. The random number obtained by the self-feedback superlattice at a sampling rate of 10 GS/s passed the triple standard deviation test and the random number standard test (NIST SP 800-22), indicating that it possessed good statistical properties as a miniaturized random number generator.

INDEX TERMS True random number generator, superlattices, self-feedback, bits-reversal.

I. INTRODUCTION

Random numbers play a vital role in Monte Carlo simulation, cryptography, digital authentication, secure communications, and various other fields [1], [2]. In protected communications, when cryptographic technologies used such methods as symmetric passwords, public key passwords, message authentication codes, digital signatures, etc., a key is required. Generally, random numbers are used as the keys to encrypt the original information. Shannon's theory [3] proves that as long as the key is completely random, consistent with the length of the information to be encrypted, and appears only once, called the one-time pad. It is theoretically impossible to decipher, so the rapid generation of safe and reliable random numbers is pivotal to the security of communication systems. Depending on the method of generation, random numbers can be divided into true random numbers and pseudo-random numbers. Pseudo-random numbers are generated by deterministic algorithms, with periodicity and reproducibility [4], [5].

The true random number generator (TRNG) is based on the unpredictable physical random phenomenon [6], which can generate unpredictable and unreproducible true random numbers. Representative TRNGs are mainly based on physical entropy sources such as circuit thermal noise [7], [8], oscillators [9], and chaotic circuits [10], [11]. But the rate of these random number generators is mostly at the Mbit/s level, which makes it difficult to meet the demands of modern communication systems for high-speed random numbers generation. In recent years, using chaotic lasers as the source of physical entropy, rates of generation of up to 100 Gbit/s [12],

The associate editor coordinating the review of this manuscript and approving it for publication was Chao-Yang Chen.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

300 Gbit/s [2] off-line, and rates up to 14 Gbit/s [13] and 20 Gbit/s [14] in real-time have been obtained. However, chaotic lasers have high costs and are complex systems, which involve electro-optical and optical-electrical conversion, and can be easily interfered with by external factors. These factors make chaotic laser-based random number generators face many challenges in practical applications. Therefore, an all-solid-state fast physical noise source with high bandwidth, miniaturization, and low power consumption is urgently needed.

Semiconductor superlattices (SLs), first proposed by IBM's L.Esaki and R.Tsu, is an all-solid-state electronic device which is periodically grown by two semiconductor materials with proper lattice matching [15]. Yaohui Zhang's team from the Chinese Academy of Sciences was the first in the world to discover the spontaneous chaos oscillation phenomenon of the GaAs/$Al_{0.45}Ga_{0.55}As$ SL in the liquid nitrogen temperature range and room temperature conditions [16]–[18]. Many scholars over the world have confirmed that this SL was an ideal source of chaotic noise by exploring the structure of the GaAs/$Al_{0.45}Ga_{0.55}As$ SL and the spontaneous chaos oscillation phenomenon, which could be used to generate true random numbers [19]. The rate of random number generation could be up to 6.25 Gbit/s by means of a single SL chip, and the rate could be increased to 80 Gbit/s when combined with six SL chips [20].

To generate faster random numbers, the signal generated by the SL itself was re-injected into the SL through an adjustable attenuator and bias-tee to form the self-feedback SL random number generator. Contributing to this change, the performance of the superlattice TRNG has been improved a lot, such as quicker changes, larger signal amplitude, and lower power consumption. These improvements made the self-feedback SL random number generator more conducive to the random number generation. In this paper, we propose a new post-processing method, called the adjacent bits reversal exclusive-or (XOR) method, which will take full advantage of the new SL signal to generate higher-rate random numbers. The self-feedback SL random number generator generates a random number at a sampling rate of 10 GS/s. The lowest 4 bits are selected, which means a rate of 40 Gbit/s. These random numbers passed the triple standard deviation test and the random number standard test (NIST SP 800-22). It is expected to promote the further application of SLs in the field of random numbers generator.

II. SL STRUCTURE AND PRINCIPLE

The structure of the investigated sample is schematically shown in Fig. 1, and consists of a 50-period, weakly coupled GaAs/$Al_{0.45}Ga_{0.55}As$ SLs with CaAs wells and $Al_{0.45}Ga_{0.55}As$ barriers. The mole fraction of Al in the barriers was selected at 0.45 to suppress the thermal leakage current though the *X* Valley [21], [22]. The conductor SL was deposited by molecular beam epitaxy (VG V80H) on a 2-inch Si-doped GaAs substrate (Wafer Technology Ltd.) [23]. It was packaged into a dual in-line package type for

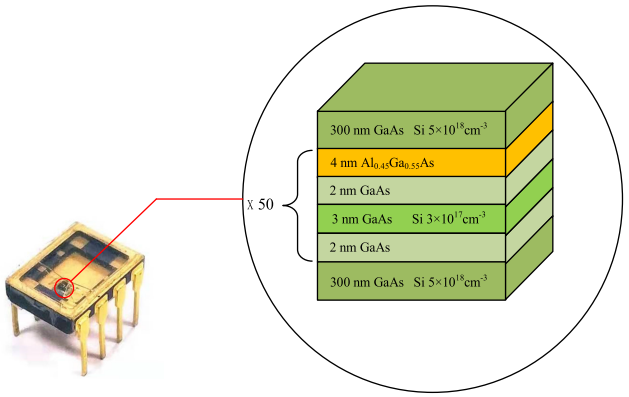


FIGURE 1. Schematic diagram of SL chip structure.

facilitating the experiment. Its core size is only 1.5 mm×1.5 mm. From a microcosmic aspect, the SL is sandwiched between two 300nm silicon-based GaAs layers, forming an n+-n-n+ diode structure. The thickness of the $Al_{0.45}Ga_{0.55}As$ barrier layer is 4nm, and the total thickness of the GaAs potential well layer is 7nm, in which there are 2nm thick undoped GaAs layers on both sides of the doped silicon-based GaAs layer to prevent the diffusion of silicon (Si) atoms to the adjacent $Al_{0.45}Ga_{0.55}As$ barrier layer [20]. Although these structures are periodic, during the growth process, their layer thickness, doping concentration, etc. inevitably introduce random fluctuations, thus constituting a random nonlinear system with a tremendous degree of freedom. The alternately grown GaAs and $Al_{0.45}Ga_{0.55}As$ materials constitute the well and barrier of the quantum well, respectively. The charge is confined to each quantum well in a weakly coupled SL, and the transport of charge is achieved by resonance tunneling between each adjacent quantum well. The sequential resonant tunneling effect of the weakly coupled SL introduces a negative differential conductance effect, which makes the behavior of electrons in the electric field non-linear, so the electrons lose their phase information, forming a particularly complicated random process.

III. EXPERIMENT DESIGN

The Schematic diagram SL random number generator is shown in Fig. 2, improved from the SL random number generator under the DC bias voltage. The system can be divided into two sections: the SL physical entropy source and the random number extraction. The physical entropy source section was obtained by injecting the signal of the SL back to the SL with a DC bias voltage appended to the SL. The random number extraction section digitizes the physical entropy source signal and finally generates detectable random bits after post-processing. In this paper, we use a digital source meter (DSM, Keithley-2400) to provide the voltage regulation to the SL device and measure the corresponding current and voltage and output a linear sweep voltage to measure the I-V characteristics. The voltage sweep of the Keithley 2400 digital source meter was used to measure and

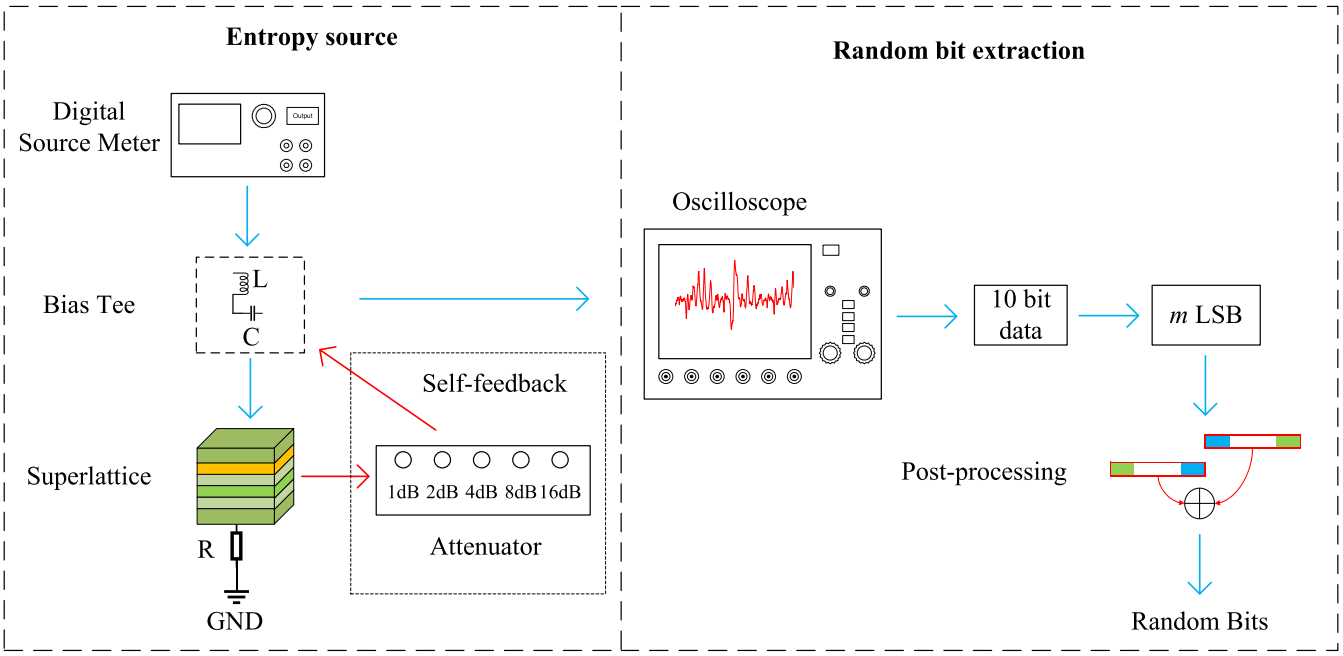


FIGURE 2. Schematic diagram of self-feedback SL random number generation.

plot the I-V characteristics. We set the voltage type to linear, from 0 V to 6 V, and set the step size to 1 mV, and the source table upper limit current was set to within 20 mA to ensure the protection of the SL device.

The DSM connected a bias-tee (Mini-Circuits ZFBT-6G+, 50 Ω, 10 to 6000 MHz) before connecting the SL, in order to avoid the influence of parasitic capacitance on high-frequency signals. The bias-tee consists of an ultra-bandwidth, near-ideal inductor L and capacitor C. The inductance prevents high-frequency signals from leaking into the DC power supply system, and the capacitor prevents the DC voltage from leaking into the high-frequency circuits and measurement instruments [24]. The connections between each device of the physical entropy source are the Small A Type (SMA) interface high-frequency coaxial cables with a bandwidth of 6 GHz. The SL was connected to the bias-tee through SMA coaxial cables to obtain a DC power supply and then grounded after a 50 Ω SMA copper-nickel coaxial load for resistance matching. The signal between the negative electrode of the SL and the load resistance was sent to the capacitor of the bias-tee through a coaxial cable to form a self-feedback. A variable attenuator is added to the path to investigate the process of the feedback signal from small to large. The attenuator has six settings: 16 dB, 8 dB, 4 dB, 2 dB, 1 dB, and 0 dB (when no button is pressed), and it will produce the corresponding attenuation when the button is pressed. The signal generated from the SL was observed and measured by the oscilloscope (OSC, Lecroy, HDO 9404-MS, 40 GS/s). Sampling and quantization were carried out in 10-bit mode, and the 4 least significant bits (LSBs) were selected for adjacent bits reversal XOR (ABRX) processing, and finally, a random sequence was obtained for detection.

IV. ANALYSIS OF SL SIGNAL

According to previous research results [19], [20], the signals output from the GaAs/$Al_{0.45}Ga_{0.55}As$ SL at different bias voltages represent different characteristics, and the chaotic oscillation signal only appears in a specific voltage range. The SLs under DC can be regarded as the amplitude of the feedback signal is infinitesimal (the attenuation coefficient is infinite). The amplitude of the feedback signal increases with the decrease of the attenuation coefficient. We continuously increased the feedback signal until no attenuation was added, and measured the I-V characteristics of the SLs with different feedback attenuation coefficients and DC bias.

When the scanning voltage of the source table is close to the chaotic oscillation region, the slope of the I-V curve increases sharply at first, then decreases, and the negative differential phenomenon appears (Fig. 3). Note that the chaotic oscillation region here does not refer to the oscillation of the I-V curve, but to the voltage range in which the SL device will produce a time-domain trace oscillation. The negative differential conductance effect is caused by the resonance tunneling effect of the electrons in the SL. The current in the semiconductor increases with the increase of voltage under normal conditions. However, the current decreases with the increase of voltage in the negative differential voltage range, which leads to the generation of the oscillation of the SL signal.

The oscillation range was about 3 V, when the amplitude of the feedback signal was very small (and the attenuation coefficient was large). While the chaotic oscillation region moves into the region of about 1V, when the feedback signal continued to increase (and the attenuation coefficient became smaller). These voltage ranges are described in detail

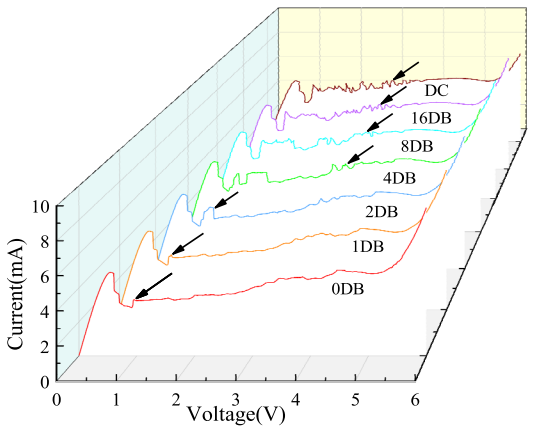


FIGURE 3. I-V characteristic curves of self feedback SLs, from back to front, the I-V curves of DC, 16dB, 8dB, 4dB, 2dB, 1dB, 0dB attenuation coefficient. The region indicated by the arrow is the voltage range where the SL oscillates.

in Table 1. When the feedback attenuation coefficient was between infinity to 4 dB, the maximum power of the SL was 14.39 mW. But the maximum power was only 3.53 mW when the attenuation coefficient was 2 to 0 dB, which was less than 1/4 of the former's power. So, from the point of view of power consumption, it was better to select a feedback coefficient of between 2 and 0 dB.

TABLE 1. Voltage range and maximum power.

feedback factor(dB)	voltage range(V)	maximum power(mW)
Infinite (DC)	[2.90-2.93V]	14.32
16	[2.95-2.97V]	14.22
8	[2.99-3.02V]	14.39
4	[3.01-3.03V]	13.98
2	[0.90-0.93V]	3.53
1	[0.91-0.93V]	3.19
0	[0.95-0.98V]	3.22

The I-V characteristics, waveform shape, and amplitude of the SL with 16-4 dB feedback coefficient are very similar to those under DC. When the feedback signal continued to increase (2–0 dB), the SL waveform changed significantly, and the waveform amplitude increased along with the increase of the feedback signal. Therefore, the self-feedback SL without attenuation (0 dB) was a better option for the entropy source of the random numbers, both in terms of power consumption and waveform amplitude.

The three most representative traces of the SL are shown in Fig. 4. The three signals are DC period, DC chaotic oscillation, and 0 dB self-feedback chaotic oscillation. It is easy to find the periodicity of the signal by observing the signal trace produced by the SL in Fig. 4 (a), and a waveform with the same shape repeatedly appears, similar to a pulse. In the frequency domain, the signal also has the characteristic of a discrete periodic signal, and the peak appears at the integral multiple of the basic frequency. So this signal can not be used for random numbers due to periodicity. The latter two are chaotic oscillation signals, quite different from the previous periodic signals. The chaotic oscillation signal in Fig. 4 (b) is similar to a time-varying pulse. The width of the peak is 3 ns, and the interspike interval (ISI) is about 7 ns, with the amplitude of the peak exceeding 90 mV. The noise amplitude between the peaks is at least one order of magnitude lower than the amplitude of the peak. These noises may come from the background noise of the test equipment and the thermal noise or scattering noise inside the SL [25]. The voltage between each peak is very low, equivalent to a "blank area". In order to avoid continuous acquisition in this area, the sampling interval has to be increased, which limits the sample rate leading to the rate of random number generation lower than expected. The power spectrum of the chaotic signal under DC is not as discrete as the previous DC periodic signal. As shown in Fig. 4 (e), it is continuous and has a bandwidth of hundreds of MHz. Fig. 4 (c) displays the 100 ns trace of the self-feedback SL signal. The "blank area" between two peaks under DC bias disappears, meaning that the self-feedback signal contains more information, and higher sampling frequency can be adopted for a higher rate of random numbers. More importantly, the amplitude and shape of the signal change more dramatically under self-feedback than under DC chaotic.

Fig. 5(a) presents the calculated probability density function (PDF) for the amplitude of the waveform generated by superlattices. Although the PDF resembles a Gaussian distribution, the PDF is clearly identified by comparing it with the fitted Gaussian (blue curve in Fig. 5(a)), which means that keeping all the 10-bit of data cannot pass the statistical tests of randomness. Therefore, to extract random bits from the entropy, post-processing should be employed. The autocorrelation trace for the SL signal is shown in Fig. 5(b). The correlation coefficient after zero-graduation decays to 0 rapidly, indicating that the signal has almost no autocorrelation.

Fig.6 shows the chaotic attractors [26] of the superlattice signal. The existence of chaotic attractors means that the proposed entropy source is chaotic and can be used to generate true random numbers.

V. POST PROCESSING

Generally, the random number quantized by direct sampling does not meet the requirements of statistical characteristics. In order to make up for the non-uniformity of quantitative data distribution and further eliminate the autocorrelation, various post-processing is needed.

A. SELECT THE LEAST SIGNIFICANT BITS

Shannon entropy [27] and minimum entropy [28] are effective tools to depict the statistical characteristics of random numbers. Shannon entropy can quantitatively evaluate the effective information in a random sequence, and the independence and uncertainty of each bit. The larger the value, the more information it contains. The minimum entropy means that the system with the minimum entropy is in a reliable state, which represents the difficulty of predicting random numbers. Shannon entropy and minimum entropy are

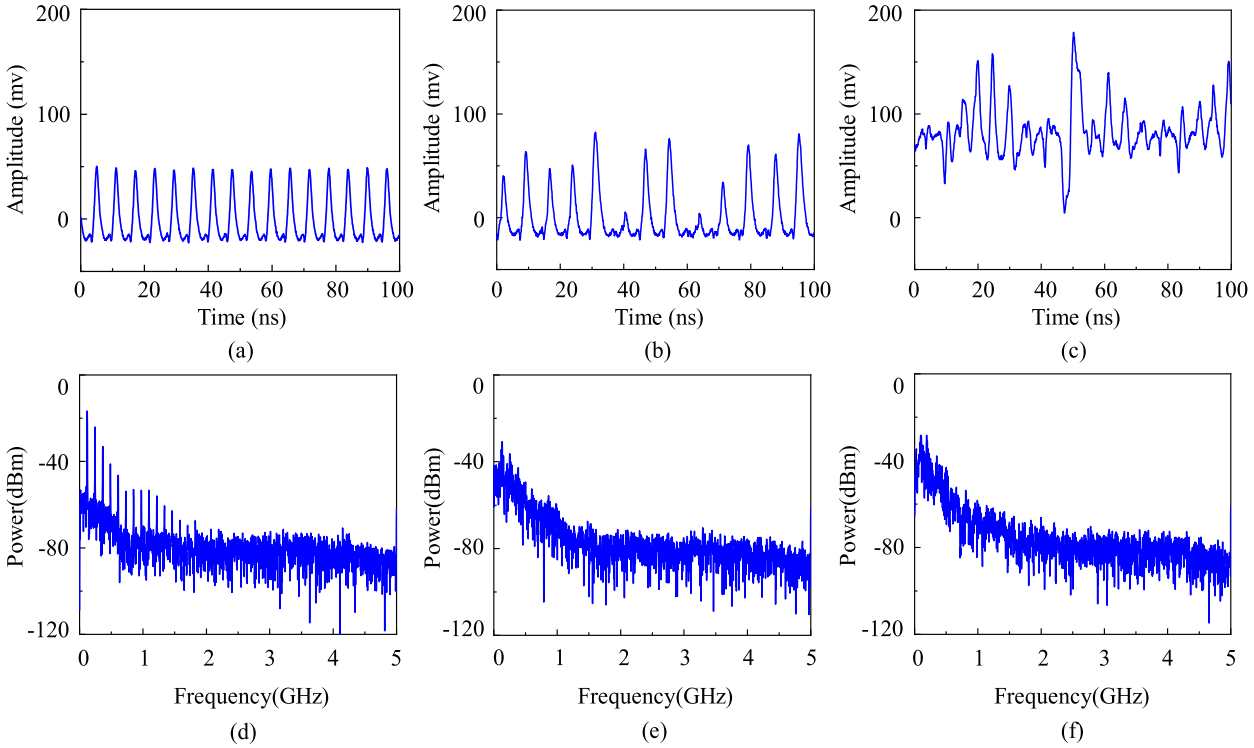


FIGURE 4. Three types 100 ns trace of SL oscillations digitized at 40 GHz.(a)DC period (b)DC chaotic(c)self-feedback chaotic. Three types power spectrum of the oscillations(d)DC-period (e)DC-chaotic(f)self-feedback- chaotic.

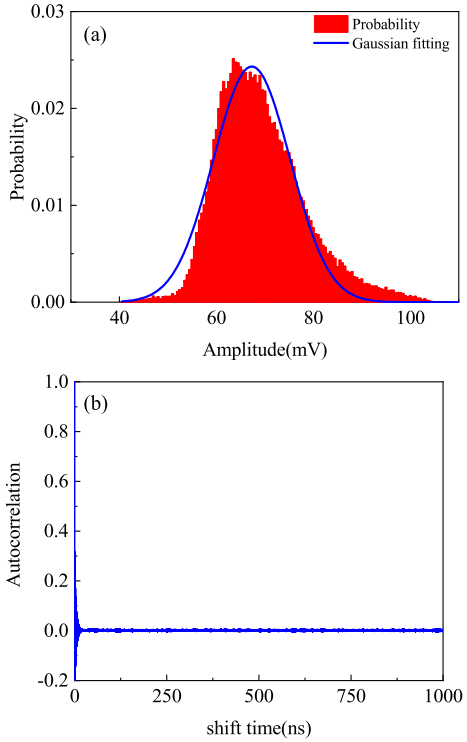


FIGURE 5. Statistical properties of SL chaos. (a) PDF and (b) autocorrelation of the SL waveforms. The blue curve in (a) denotes the fitted Gaussian.

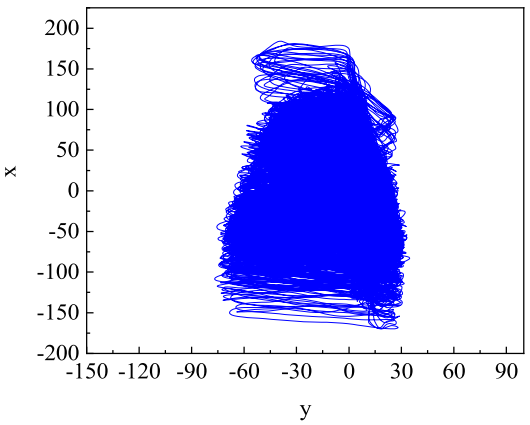


FIGURE 6. Chaotic attractors of superlattice signal. X and Y represent the voltage on the superlattice and the load, respectively.

defined:

$$H_n(X) = -\sum_{i=1}^{2^n} p_i \log_2 p_i \tag{1}$$

$$H_{\min}(X) = -\log_2 \max\{p_i\} \tag{2}$$

where H_n is the Shannon entropy, and H_{min} is the minimum entropy, and X is a discrete random variable in the range $R = \{x_1, x_2, x_3, \ldots, x_{2^n}\}$, and p_i is the probability of value when $X = x_i$. It can be obtained by calculation that when the random number sequence corresponds to a uniform distribution, $p_i = 1/2^n$, the Shannon entropy value of the sequence reaches the maximum value $H_n(X) = n$, and at the same time makes $H_{min}(X)$ have a minimum value $= n$. The Shannon entropy value reaches the maximum value so that the random number sequence has the maximum information entropy. Meanwhile, it has the maximum stability with minimum entropy. Shannon

entropy and minimum entropy both indicate that the random number sequence should conform to a uniform distribution.

In order to make up for the non-uniformity of quantified data distribution and further eliminate autocorrelation, selecting the m least significant bits (LSBs) is a relatively common and simple method to improve the uniformity of distribution [29]. Hirano *et al.* [30], Nguimdo *et al.* [31], and Li and Chan [32] selected the 6, 4, and 3 LSBs, respectively, and obtained uniformly distributed random bits. Oliver *et al.* [33] pointed out that it is effective to estimate the appropriate number of bits by drawing histograms of amplitude-frequency distributions of different digits, and successively lowering the value of m bit a flat frequency distribution histogram is obtained within the allowed statistical variation range. Consistent with the descriptions in references [29], [33], when more high bits are continuously discarded, and fewer LSBs are selected, the unevenness of distribution is greatly improved, gradually approaching a uniform distribution. When $m = 4$, the amplitude distribution of the quantized result and the uniform distribution are almost consistent, as shown in Fig. 7. The quantized output bits of the multi-bit ADC determine the speed of random number generation. The more digits are reserved, the higher the rate. Therefore, when extracting m LSBs as a random number output, it is necessary to make the value of m as large as possible under the premise of satisfying the quantized amplitude distribution of the balance, at the same time taking into account the rate of random number generation.

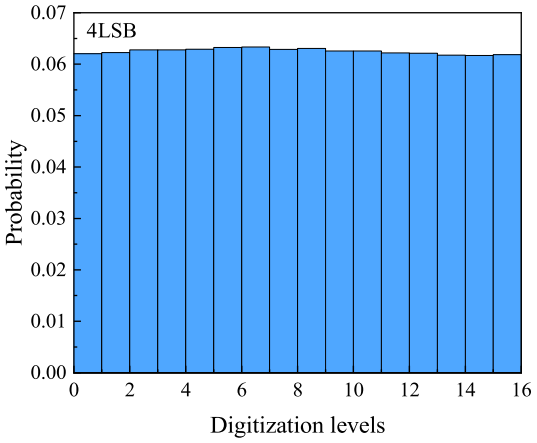


FIGURE 7. Probability distribution histogram of different 4 LSBs.

B. ADJACENT BITS REVERSAL XOR

The random bits processed by the LSBs method do not mean that they can pass all the statistical tests of randomness because there are still obvious deviations or correlations in the generated random bits. So it is still necessary to combine with other post-processing steps to ensure that the random numbers meet the requirements for good randomness. Ido Kanter [2] adopts an 8-bit ADC to sample and quantize the signal converted from chaotic lasers to voltage at a rate of 40 GS/s, then performed multi-order differentials, and selected m LSBs to ensure passing the random number test. The schematic diagram of the device Ido Kanter operated is quoted in Fig. 8(a). Additionally, Sze Chun Chan directly performs XOR on the 3 LSBs of adjacent signals after obtaining ADC quantization as quoted in Fig. 8(b).

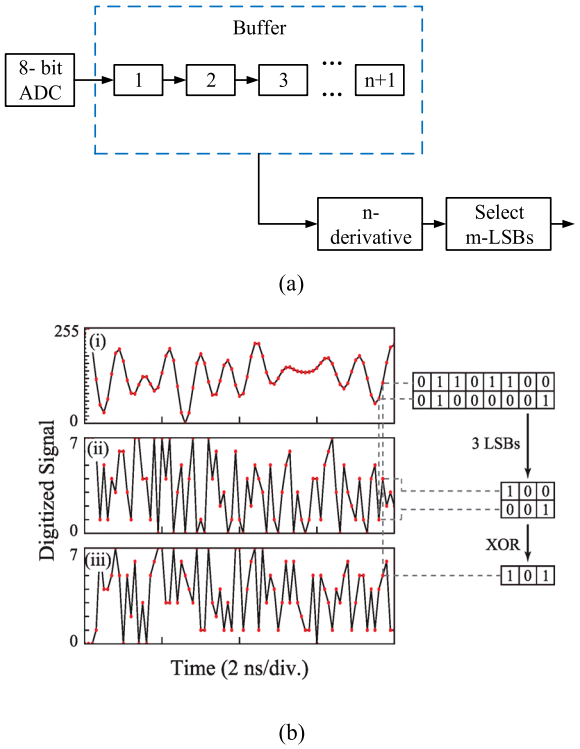


FIGURE 8. (a)Post-processing methods of Ido Kanter, reproduced from ref [2]. (b) Post-processing methods of ISze-Chun Chan, reproduced from ref [28].

The method proposed by Ido Kanter is very effective and achieves a breakthrough 300 Gbit /s random generator under the laboratory conditions, which is a historic breakthrough in the rate of random numbers generation. However, due to the large number of calculations and the need for a large amount of cache, it is difficult to realize such a rate in reality. Conversely, Sze Chun Chan's method has almost no computation, and only selects LSBs and conducts XOR, without any multi-step differential calculation. But half of the random bits are discarded during the XOR operation.

Therefore, we need post-processing which can meet the following three conditions. Firstly, it can reduce the bias and correlation of random sequences to ensure that it can pass the random number test. Secondly, it only needs a few calculations to facilitate real-time processing. Thirdly, it does not need to discard the random bits to improve the random number generation rate.

As XOR is considered to be a very important method to process random numbers, we will analyze it here. Suppose that the values of two random variables X and Y are 0 or 1, and their mathematical expectation values are μ and ν

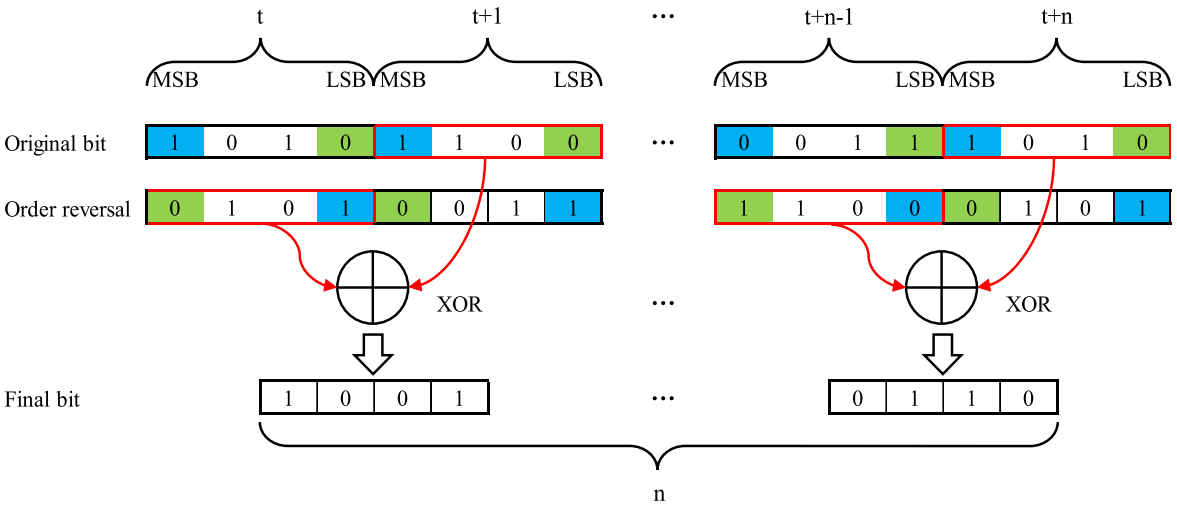


FIGURE 9. Schematic diagram of adjacent bits reversal XOR operation.

respectively. We carry out an XOR operation between X and Y to obtain a new random variable Z, and so its mathematical expectation value is as follows [34]:

$$E(Z) = \frac{1}{2} - 2\left(\mu - \frac{1}{2}\right)\left(v - \frac{1}{2}\right) - 2\rho\sqrt{\mu(1-\mu)v(1-v)} \quad (3)$$

where ρ is the cross-correlation coefficient of X and Y, representing the degree of correlation between them. When the correlation degree of random variables X and Y is very small so that ρ can be ignored. Because X and Y are random variables, μ and v are very close to 0.5, and (μ-10.5)×(v-0.5) is much less than either of (μ-10.5) or (v-0.5). So when X and Y are independent, the error of the sequence after XOR will be less than any of the original sequence. If we find a way to make the two adjacent random numbers lose correlation, then we would treat random numbers by direct XOR.

The Hamming distance [35] between different binary sequences can reflect the independence between them. If the hamming distance is closer to 0.5, their independence is stronger. Table 2 shows the hamming distance between the different bits(1 Gbit data at 10GS/s).

TABLE 2. Hamming distance of bits.

Hamming distance	bit 2	bit 3	bit 4
bit 1	0.49885706	0.49961956	0.49994618
bit 2	×	0.49980831	0.50009043
bit 3	×	×	0.50044093

Therefore, we propose a new method, called adjacent bits reversal XOR, which is illustrated in Fig. 9. And there is no correlation between the first bit and the last bit of the data collected by ADC [36]. Firstly, the original data is processed with m LSB and the least 4 bit data is selected to improve its uniformity. Secondly, reverse the original 4-bit bits at time t, and then XOR them directly with the four bits sampled from t+1 the following time, then output the result. According to this method, input 4 (n + 1) bit data, and finally obtain 4 n bit data. When n is very large, it can be considered that there is no need to discard random bits during the adjacent bits reversal XOR process, and the random bit generation rate will not decrease. But the deviation and correlation of random bits is reduced greatly. Compared with the previous method, the adjacent bits reversal XOR is quite different because the former needs to discard half of the random numbers. However, our method only needs to reverse the data for XOR (change the byte high-order and low-order read order), without introducing complex calculations such as multi-level difference and other resource-consuming calculations. This post-processing, as presented is easy, and is also easy to conduct in the Embedded hardware. In summary, the adjacent bits reversal XOR can greatly reduce the random sequence deviation and autocorrelation coefficient without losing random numbers and greatly reduces the number of post-processing calculations.

VI. RANDOMNESS TEST

A. TRIPLE STANDARD RANDOM TEST

Triple standard deviation test (3σ criterion) [37] based on the feature of ideal random bits is a common method to validate random numbers. A model that generates random numbers by tossing a coin under ideal conditions is set up for 3σ criterion. The probability of either side of the coin landing face up is equal, and in the equation the positive side represents 1 and the negative side represents 0.

Under the same initial conditions, n repeated coin tossing experiments are carried out to obtain a random sequence X of length n. As the number of coin flips n increases, the probability of the event gradually approaches the Gaussian distribution from the binomial distribution. The variance ($D(x)$) of

the sequence X is:

$$D(x) = E\left(x^2\right) - E^2(x) = \frac{1}{4n} \tag{4}$$

where $E(x)$ is the mathematical expectation. According to the central limit theorem: when $n \to \infty$.

$$p[e(n)] = N\left(0, \frac{1}{2\sqrt{n}}\right) = \frac{1}{\sqrt{2\pi}\sigma_e} e^{-\frac{e(n)^2}{2\sigma_e^2}} \tag{5}$$

where $p[e(N)]$ is possibility of $e(N)$, with $\sigma_e = 1/2\sqrt{n}$, $e(N) = E(X)$-0.5.

To calculate the first-order autocorrelation coefficient $(a_1(n))$ of sequence X:

$$a_1(n) = \left. \frac{\sum_{i=1}^{n} [x_i - E(x)]\,[x_{i+1} - E(x)]}{\sum_{i=1}^{n} [x_i - E(x)]^2} \right|_{x_i=\{1,0\}} \tag{6}$$

Because of $x_i = 0, 1, x^2 = x, E(x^2) = E(x)$, the numerator of the formula can be simplified according to the values of x_i and x_{i+1} shown in Table 3.

$$\begin{aligned} a_1(n) &= \frac{\left. \sum_{i=1}^{n} y_i \right|_{y_i=\left\{\left(\frac{1}{2}+e\right)^2, \left(\frac{1}{2}-e\right)^2, -\frac{1}{4}+e^2\right\}}}{n\left(\frac{1}{4}+e^2\right)} \\ &\approx \frac{\left. 4\sum_{i=i}^{n} y_i \right|_{y_1=\left\{-\frac{1}{4}, \frac{1}{4}\right\}}}{n} = \frac{\left. \sum_{i=1}^{n} y_i \right|_{y_i=\{-1,1\}}}{n} \end{aligned} \tag{7}$$

where x and y is a random sequence. With the help of the coin toss model, it is simple to calculate $a_1(n)$, but the difference is that the positive side represents 1 and the negative side represents -1. So the distribution of the first-order autocorrelation coefficient a_1 is:

$$p\left[a_1(n)\right] = N\left(0, \frac{1}{\sqrt{n}}\right) = \frac{1}{\sqrt{2\pi}\sigma_a} e^{-\frac{a_1(n)^2}{2\sigma_a^2}} \tag{8}$$

According to the principle of hypothesis testing, within the range $[-3\sigma, 3\sigma]$, the area enclosed by the probability function and the x-axis is 99.7%. This means that the probability that the offset of a true random sequence of length n falls within the range $[-1.5/\sqrt{n}, 1.5/\sqrt{n}]$ is 99.7%. Similarly, the first-order autocorrelation coefficient of the random sequence should also fall within the range $[-3/\sqrt{n}, 3/\sqrt{n}]$. By comparing the deviation and autocorrelation coefficient of the random sequence to be detected with the sequence deviation and autocorrelation coefficient of the coin-tossing model, it is very easy to determine whether the random sequence meets the triple standard error test.

1 Gbit data from SL, with and without the adjacent bits reversal XOR method, was examined at a sampling rate of 10 GS/s to validate the method proposed in this paper. This 1 Gbit data was obtained by selecting only 4 LSBs. We recorded the deviation of data $|e(N)|$disposed by adjacent bits reversal XOR and $|\bar{e}(N)|$ without using this process

TABLE 3. simplified formula.

x_i	x_{i+1}	P	Simplified formula
0	0	1/4	$(1/2+e)^2$
0	1	1/2	-1/4+ e^2
1	0		
1	1	1/4	$(1/2-e)^2$

in Fig. 10(a). The first-order autocorrelation coefficient a_1 of this 1 Gbit data, recorded respectively $|a_1(N)|$and $|\bar{a}_1(N)|$. The curve of $|e(N)|$ was always below the $3\sigma_e$, but the $|e(N)|$ exceeded the ideal random curve, so it did not pass the 3σ criterion. Like the former, $|a_1(N)|$was always below $3\sigma_{a_1}$, but $|\bar{a}_1(N)|$ exceeded the $3\sigma_{a_1}$as shown in Fig. 10(b).

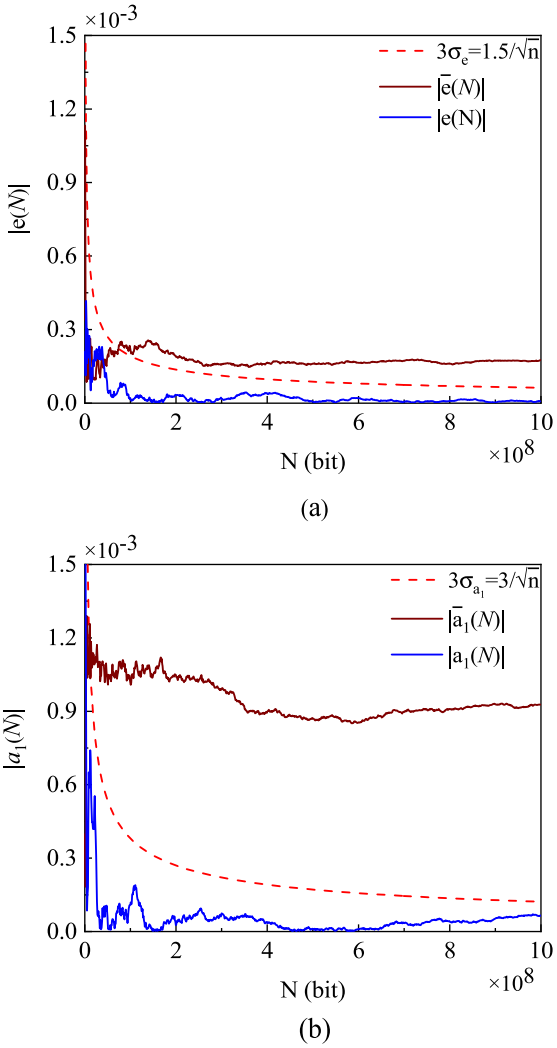


FIGURE 10. 3σ **criterion of 1 G bit random sequences.(a) Sequence bias** $|e(N)|$ **(b) first-order autocorrelation coefficient of the sequence** $|a_1(N)|$.

B. NIST STATISTICAL TESTSUITE

The statistical test suite 800-22 from the National Institute of Standards and Technology(NIST) [38] is a recognized standard for testing random numbers. So we used it for further testing and verification of the quality of the random bits of the final output. The random bit sequence passed the NIST statistical test using 1000 bitstreams of 1 Mbit length. Test items

TABLE 4. Results of NIST statistical test.

Statistical test	2.5 GS/s		5 GS/s		10 GS/s		Result
	P-Value	Proportion	*P*-Value	Proportion	*P*-Value	Proportion	
Frequency	0.706149	0.989	0.595549	0.995	0.350485	0.988	Success
BlockFrequency	0.834308	0.991	0.334538	0.987	0.029713	0.987	Success
CumulativeSums	0.804337	0.987	0.383827	0.993	0.236810	0.996	Success
Runs	0.534146	0.994	0.319084	0.986	0.117047	0.999	Success
LongestRun	0.232760	0.985	0.867692	0.994	0.202268	0.991	Success
Rank	0.671779	0.983	0.419021	0.983	0.437274	0.994	Success
FFT	0.253551	0.993	0.554420	0.993	0.213309	0.997	Success
NonOverlappingTemplate	0.148094	0.987	0.366918	0.983	0.145326	0.989	Success
OverlappingTemplate	0.407091	0.982	0.401199	0.986	0.474986	0.994	Success
Universal	0.387702	0.988	0.266512	0.990	0.118983	0.994	Success
ApproximateEntropy	0.110952	0.997	0.437274	0.994	0.350485	0.981	Success
RandomExcursions	0.212894	0.988	0.162606	0.995	0.275709	0.988	Success
RandomExcursionsVariant	0.474645	0.986	0.275709	0.987	0.025193	0.987	Success
Serial	0.671779	0.981	0.474986	0.993	0.574903	0.996	Success
LinearComplexity	0.324180	0.991	0.071177	0.986	0.534146	0.993	Success

TABLE 5. The performances of different trng.

Year	System	Post-processing	Bits	Sampling rate (GS s–1)	Bit rate (Gb s–1)
2010	LD+OF	8-bit + nth derivative + LSB	15	20	300
2013	LD+OF	8-bit + LSB	4	40	160
2013	SL+dc biased	8-bit + nth derivative + LSB	5	1.25	6.25
2016	VF+PBS	16-bit + LFSR	8	0.06	0.48
2020	SL+self-feelback	10-bit + bit reversal	4	10	40

LD, laser diode; OF, optical feedback VF,vacuum fluctuations,BPS, polarizing beam splitter, LFSR,linear feedback shift register

and outcomes, pass rate, and p-values are shown in Table 4. It lists the *P*-values of all 15 sub-test items and corresponding pass rates at the sampling rates of 2.5 Gs/s, 5 Gs/s, and 10 Gs/s in turn. We extracted the 4LSBs from each 10-bit sample, and converted sampling rates to the rates of random bits, which were respectively 10 Gbit/s, 20 Gbit/s and 40 Gbit/s. And as the sampling rate continued to increase, the NIST test failed. An all-electronic physical random number generator at rates up to 40 Gbit/s is realized by a single SL chip. Usually the significant level $\alpha = 0.01$, when the *P*-Value $> \alpha$, can it be considered to have passed the test. The possibility of *P*-Value > 0.01 should fall in the range of [0.9805,0.9995] [39]. All of the tests succeeded, and it showed that the random number from self-feedback SL has good statistical randomness. In summary, a single SL chip generates random numbers with a rate of up to 40 Gbit/s and can pass 3σ deviation and NIST tests.

Table 5 includes the TRNG system, post-processing, speed of random bits, etc., to compare the different performances of advanced TRNG in recent years. Although The superlattice TRNG has been greatly improved, there is still a gap between superlattice TRNG and laser TRNG in speed.

VII. CONCLUSION

Random numbers are crucial for communications and cryptography. And superlattice TRNG is a new generator in recent years. In order to generate higher-rate random numbers, we presented a self-feedback superlattice TRNG, which can generate random bits at rates up to 40 Gbit/s with adjacent bits reversal exclusive-or method for post-processing. It is expected to play a vital role in the field of random numbers with its ultra-low power consumption, small size and high speed.

ACKNOWLEDGMENT

The authors would like to thank Prof. Y. Zhang from Suzhou Nanometer Institute of Chinese Academy of Sciences for SLs devices and useful discussions.

REFERENCES

[1] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol. 2, no. 12, pp. 728–732, Dec. 2008.

[2] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photon.*, vol. 4, no. 1, pp. 58–61, Jan. 2010.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

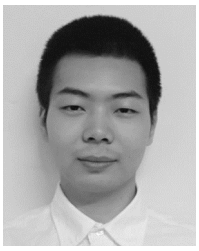
[4] F. Yu, Q. Wan, J. Jin, L. Li, B. He, L. Liu, S. Qian, Y. Huang, S. Cai, Y. Song, and Q. Tang, "Design and FPGA implementation of a pseudo-random number generator based on a four-wing memristive hyperchaotic system and Bernoulli map," *IEEE Access*, vol. 7, pp. 181884–181898, 2019.

[5] S. Zhu, C. Zhu, H. Cui, and W. Wang, "A class of quadratic polynomial chaotic maps and its application in cryptography," *IEEE Access*, vol. 7, pp. 34141–34152, 2019.

[6] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, Apr. 2010.
[7] Y. Yamanashi and N. Yoshikawa, "Superconductive random number generator using thermal noises in SFQ circuits," *IEEE Trans. Appl. Supercond.*, vol. 19, no. 3, pp. 630–633, Jun. 2009.
[8] L. Gong, J. Zhang, H. Liu, L. Sang, and Y. Wang, "True random number generators using electrical noise," *IEEE Access*, vol. 7, pp. 125796–125805, 2019.
[9] Y. Lu, H. Liang, L. Yao, X. Wang, H. Qi, M. Yi, C. Jiang, and Z. Huang, "Jitter-quantizing-based TRNG robust against PVT variations," *IEEE Access*, vol. 8, pp. 108482–108490, 2020.
[10] F. Pareschi, G. Setti, and R. Rovatti, "A fast chaos-based true random number generator for cryptographic applications," presented at the 32nd Eur. Solid-State Circuits Conf., 2006.
[11] N. Nguyen, L. Pham-Nguyen, M. B. Nguyen, and G. Kaddoum, "A low power circuit design for chaos-key based data encryption," *IEEE Access*, vol. 8, pp. 104432–104444, 2020.
[12] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," *Opt. Express*, vol. 22, no. 14, pp. 17271–17280, Jul. 2014.
[13] L. S. Wang, T. Zhao, D.-M. Wang, D.-Y. Wu, L. Zhou, J. Wu, X.-Y. Liu, and A.-B. Wang, "14-Gb/s physical random numbers generated in real time by using multi-bit quantization of chaotic laser," *Acta Phys. Sinica*, vol. 66, no. 23, 2017, Art. no. 234205.
[14] Y.-Y. Sun, P. Li, Y.-Q. Guo, X.-M. Guo, X.-L. Liu, J.-G. Zhang, L.-X. Sang, and Y.-C. Wang, "Chaotic laser-based ultrafast multi-bit physical random number generation without post-process," *Acta Phys. Sinica*, vol. 66, no. 3, 2017, Art. no. 030503.
[15] R. Tsu and L. Esaki, "Tunneling in a finite superlattice," *Appl. Phys. Lett.*, vol. 22, no. 11, pp. 562–564, Jun. 1973.
[16] Y. Zhang, J. Kastrup, R. Klann, K. H. Ploog, and H. T. Grahn, "Synchronization and chaos induced by resonant tunneling in GaAs/AlAs superlattices," *Phys. Rev. Lett.*, vol. 77, no. 14, pp. 3001–3004, Sep. 1996.
[17] Y. Zhang, R. Klann, H. T. Grahn, and K. H. Ploog, "Transition between synchronization and chaos in doped GaAs/AlAs superlattices," *Superlattices Microstruct.*, vol. 21, no. 4, pp. 565–568, Jun. 1997.
[18] Y. Huang, W. Li, W. Ma, H. Qin, and Y. Zhang, "Experimental observation of spontaneous chaotic current oscillations in GaAs/$Al_{0.45}Ga_{0.55}As$ superlattices at room temperature," *Chin. Sci. Bull.*, vol. 57, no. 17, pp. 2070–2072, Jun. 2012.
[19] Y. Huang, W. Li, W. Ma, H. Qin, H. T. Grahn, and Y. Zhang, "Spontaneous quasi-periodic current self-oscillations in a weakly coupled GaAs/(Al,Ga)As superlattice at room temperature," *Appl. Phys. Lett.*, vol. 102, no. 24, Jun. 2013, Art. no. 242107.
[20] 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," *Phys. Rev. Lett.*, vol. 111, no. 4, Jul. 2013, Art. no. 044102.
[21] M.-H. Meynadier, R. E. Nahory, J. M. Worlock, M. C. Tamargo, J. L. de Miguel, and M. D. Sturge, "Indirect-direct anticrossing in GaAs-AlAs superlattices induced by an electric field: Evidence of Γ-χ mixing," *Phys. Rev. Lett.*, vol. 60, no. 13, pp. 1338–1341, Mar. 1988.
[22] Y. Zhang, X. Yang, W. Liu, P. Zhang, and D. Jiang, "New formation mechanism of electric field domain due to $\Gamma-\chi$ sequential tunneling in GaAs/AlAs superlattices," *Appl. Phys. Lett.*, vol. 65, no. 9, pp. 1148–1150, Aug. 1994.
[23] W. Li, Y. Aviad, I. Reidler, H. Song, Y. Huang, K. Biermann, M. Rosenbluh, Y. Zhang, H. T. Grahn, and I. Kanter, "Chaos synchronization in networks of semiconductor superlattices," *Europhys. Lett.*, vol. 112, no. 3, p. 30007, Nov. 2015.
[24] C. Gettings and C. C. Speake, "A method for reducing the adverse effects of stray-capacitance on capacitive sensor circuits," *Rev. Sci. Instrum.*, vol. 90, no. 2, Feb. 2019, Art. no. 025004.
[25] Y. Bomze, R. Hey, H. T. Grahn, and S. W. Teitsworth, "Noise-induced current switching in semiconductor superlattices: Observation of nonexponential kinetics in a high-dimensional system," *Phys. Rev. Lett.*, vol. 109, no. 2, Jul. 2012, Art. no. 026801.
[26] *Detecting Strange Attractors in Turbulence*, FlorisTakens, Groningen, The Netherlands, 1981, no. 1, pp. 366–381.
[27] A. Bulinski and D. Dimitrov, "Statistical estimation of the Shannon entropy," *Acta Mathematica Sinica, English Ser.*, vol. 35, no. 1, pp. 17–46, Jan. 2019.
[28] F. Cicalese, L. Gargano, and U. Vaccaro, "Minimum-entropy couplings and their applications," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3436–3451, Jun. 2019.
[29] N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," *Opt Express*, vol. 22, no. 6, pp. 6634–6646, Mar. 2014.
[30] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," *Opt Exp.*, vol. 18, no. 6, pp. 5512–5524, Mar. 2010.
[31] R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, "Fast random bits generation based on a single chaotic semiconductor ring laser," *Opt Express*, vol. 20, no. 27, pp. 28603–28613, Dec. 2012.
[32] X. Z. Li and S. C. Chan, "Random bit generation using an optically injected semiconductor laser in chaos with oversampling," *Opt. Lett.*, vol. 37, no. 11, pp. 2163–2165, Jun. 2012.
[33] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Fast random bit generation using a chaotic laser: Approaching the information theoretic limit," *IEEE J. Quantum Electron.*, vol. 49, no. 11, pp. 910–918, Nov. 2013.
[34] R. Davies. (Feb. 28, 2002). *Exclusive OR (XOR) and Hardware Random Number Generators*. [Online]. Available: http://www.robertnz.net/pdf/xor2.pdf
[35] K. A. S. Abdel-Ghaffar, "Sets of binary sequences with small total Hamming distances," *Inf. Process. Lett.*, vol. 142, pp. 27–29, Feb. 2019.
[36] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8×50 Gb/s," *IEEE Photon. Technol. Lett.*, vol. 24, no. 12, pp. 1042–1044, Jun. 2012.
[37] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 81, no. 5, May 2010.
[38] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dary, and S. Vo. *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html
[39] Y. Liu, M.-Y. Zhu, B. Luo, J.-W. Zhang, and H. Guo, "Implementation of 1.6 tb S–1 truly random number generation based on a superluminescent emitting diode," *Laser Phys. Lett.*, vol. 10, no. 4, Apr. 2013, Art. no. 045001.

YANFEI LIU was born in Xianyang, Shanxi, China, in 1975. He received the B.S. degree from the National University of Defense Technology, in 1997, the M.S. degree from the Nanjing University of Aeronautics and Astronautics, in 2005, and the Ph.D. degree from Rocket Forces Engineering University, Xi'an, China, in 2015.

He has hosted and participated in important national science foundation many times and has been invited to serve as a Judge of the National Electronic Design Competition. He is currently a Professor with Rocket Forces Engineering University. He is the author of nine books, more than 40 articles, and more than seven patents. His research interests include superlattice, integrated circuit design, embedded systems, and optimal control.



CHENG CHEN was born in Yongzhou, Hunan, China, in 1996. He received the B.S. degree from Rocket Forces Engineering University, Xi'an, China, in 2014, where he is currently pursuing the M.S. degree with the Department of Computer Science and Technology.

His research interests include the superlattice random number generator and security of embedded systems.

DONG DONG YANG was born in Shijiazhuang, Hebei, China, in 1985. He received the B.S. and M.S. degrees from Rocket Forces Engineering University, Xi'an, China, and the Ph.D. degree from Rocket Forces Engineering University, in 2015.

He is currently a Lecturer with Rocket Forces Engineering University. His research interests include superlattice, nonlinear signal processing, and analog electronics technique.

QI LI was born in Hanzhong, Shanxi, China, in 1974. She received the B.S. degree from Northwestern Polytechnical University, Xi'an, in 1997, and the M.S. degree from Rocket Forces Engineering University, in 2004.

She was a Graduate Student with Rocket Forces Engineering University, in 2016. She is currently an Associate Professor with Rocket Forces Engineering University. Her research interests include integrated circuit design and application of digital electronic technology.

XIUJIAN LI was born in Pingguo, Guangxi, China, in 1974. He received the B.S., M.S., and Ph.D. degrees from the National University of Defense Technology, Changsha, China, in 1997, 2002, and 2007, respectively.

He is currently a Professor of physics with the National University of Defense Technology. His research interests include superlattice, photonics, and optical information processing.