Received 8 July 2023, accepted 29 July 2023, date of publication 2 August 2023, date of current version 9 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3301152

RESEARCH ARTICLE

A Method for Generating True Random Numbers With Multiple Distribution Characteristics

GANG SU[1], CHANGCHUN DING[1], SIDA LI[2], ZIJIAN LIU[1], ZHENG GAO[1], JUNFENG SONG[1,3], SHUXU GUO[1], AND MIN TAO[1,3]

[1]State Key Laboratory of Integrated Optoelectronics, College of Electronic Science and Engineering, Jilin University, Changchun 130012, China
[2]School of Astronautics, Harbin Institute of Technology (HIT), Harbin 150006, China
[3]Peng Cheng Laboratory, Shenzhen 518000, China

Corresponding author: Min Tao (taomin@jlu.edu.cn)

This research was funded by National Natural Science Foundation of China, Grant Nos. 62090054 and 61934003; the Major Scientific and Technological Program of Jilin Province, Grant Nos. 20200501007GX and 20210301014GX; Jilin Provincial Development and Reform Commission Project, Grant No. 2020C056; and the Program for JLU Science and Technology Innovative Research Team, Grant No. 2021TD-39.

ABSTRACT In this paper, a method of generating true random numbers obeying multiple distribution characteristics is proposed. First, two resistance-capacitance (RC) self-excited oscillation circuits are used to generate two jittered, periodically unstable square wave signals, and then a high-precision and high-frequency quartz crystal oscillator is used to sample and measure these two jittered signals to obtain their periods. Due to the randomness of the external environment, there is Gaussian white noise in the circuit, so the periods of these two signals are random variables subject to the Gaussian distribution. Finally, we use a field-programmable gate array (FPGA) to perform secondary processing on these two random signals, which can generate true random number sequences that conform to the distribution characteristics of Gaussian distribution, Poisson distribution, 0-1 distribution, uniform distribution, etc. The random numbers generated by the circuit can be applied to the field of intelligent control related to automatic control and machine learning. This method uses a physical entropy source to generate high-quality true random sequences, which are easy to build, low in circuit cost, and small in size. The experimental results show that the method is low-cost, highly reliable and easy to integrate, providing an effective solution for the generation of true random numbers in electronic systems.

INDEX TERMS True random number, RC self-excited oscillation, random distribution, FPGA, intelligent control.

I. INTRODUCTION

In recent years, with the advancement of science and technology, artificial intelligence (AI) technology has received more and more attention from many research institutions, enterprises, and countries. As more and more industries begin to introduce AI technology, the application of AI will become more and more widespread [1], [2], [3]. The real human thinking includes both logical thinking and non-logical thinking, and non-logical thinking has always been a source of enriching the sensual life and creativity of human society. The solution to irrational logic in the field of AI is to increase the randomness of the system. At present, the methods that can be applied to increase the randomness of the system include the credibility reasoning method, probability method, fuzzy mathematics method, grey theory method, etc. [4] and [5]. Due to the characteristics of computer systems, true random numbers have been the key to and the foundation for solving uncertainty problems in the field of AI. The generation of true random numbers has always been a difficult problem to be solved [6], [7], [8].

The history of the application of random numbers is far older than the emergence of AI. Before the advent of computers, people generally obtained random numbers by rolling the dice, drawing lots, and other methods. Later on, the methods of querying the random number table, squaring in the

The associate editor coordinating the review of this manuscript and approving it for publication was Jing Liang.

middle, reading the clock, and so on, emerged [9], [10]. With the development of computer technology, there have been some random number generators implemented by hardware and algorithms. At this time, the random number generators can be divided into pseudo-random number generators (PRNGs) and true random number generators (TRNGs). PRNGs include linear congruential generators, shift register generators, chaos generators, etc., whose systems have less than ideal encryption and randomness [11], [12], [13]. With the development of electronic systems in recent years, PRNGs are no longer able to meet the requirements of modern electronic equipment in terms of security, randomness, etc. In recent years, with the rapid development of optoelectronic semiconductor technology and integrated circuit engineering, several methods for generating true random number generators have emerged one after another, such as quantum random number generators, thermal noise generators, discrete chaos generators, oscillator sampling generators, or methods based on the above methods combined with integrated circuits, etc. [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], and [27].

Among them, the quantum random number generator is to obtain a large number of random number sequences according to the quantum effects of electrons or photons, which is the most promising research direction at present, such as using the dark pulse of avalanche diode in Geiger mode, the physical chaos in semiconductor lasers, the splitting of single photon beam in the decay process of radioactive atomic nuclei, the Polarimetry of single photons, the arrival time of photons, the spatial distribution of laser speckle, etc. [18], [19], [20], and [21] They can be used as appropriate random sources. There are many kinds of random sources. Generally speaking, their sequence generation speed is extremely fast, ranging from several Mbps to dozens of Gbps [18], [21]. However, random number generators designed based on this aspect often need to build optical paths, supporting high gain amplifiers and sampling circuits, and the implementation cost is high. The thermal noise method uses the noise generated by the electronic Brownian motion of the resistor itself when it is energized as the noise source. Due to the small amplitude of the thermal noise, it is also necessary to use devices such as high-gain amplifiers and transimpedance amplifiers to amplify the noise signal and finally convert the noise into a pure digital signal by devices such as voltage comparators. This type of generator is the most widely used, but because the noise is too small, it requires a more complex circuit structure for amplification and signal conversion, and is limited by the performance of the amplifier and other devices, so this scheme is more expensive and its robustness is poor [14]. The discrete chaos generator is based on the chaos theory of nonlinear systems, and the generator uses the uncertainty of the chaotic circuit itself as the design basis, employing a large number of XOR gate circuit structures. The system itself has a complex structure and a high cost, which is not conducive to the large-scale application of random number systems [15]. Meanwhile, with the development of electronic technology in recent years, the field-programmable gate array (FPGA), as a semi-custom integrated circuit product, has been widely used in the electronics industry. The advent of FPGAs has solved both the shortage of custom circuits and the disadvantage of the limited number of previous programmable device gate circuits. In the application field of random number generator, the implementation of a true random number generator scheme using the FPGA has the advantages of high reliability and simple system structure [22], [23]. But the ring oscillator built by FPGA itself often has correlation, which affects the quality of the random sequence generated [24], [25], [26], [27].

The existing oscillation sampling generator has a single function, a complex design as an oscillation circuit for error generation, and insufficient randomness. For example, it is used in multistage feedback ring oscillators [28] to generate truly random numbers, with complex circuits and single performance. Using application specific integrated circuit (ASIC) to design a true random number generator has high cost and poor universality [29], [30]. In this paper, according to the above problems, two resistance-capacitance (RC) oscillators are designed as oscillation sources, and the signals generated by the two RC oscillators are controlled and processed by FPGA to achieve data acquisition. This method mainly uses the error generated by the phase jitter of the oscillator itself as the physical entropy source to generate random variables. Its circuit structure is simple, using only one FPGA and several resistors and capacitors. The oscillation source design is flexible and cost-effective. In addition, this method directly measures the randomness generated by physical phenomena, and the measurement error is very small. The generated true random number sequence has high quality, making it very suitable for large-scale applications of true random number generators. The generator uses the oscillator composed of non-gates (logic inverter) as the entropy source, and then uses the FPGA for data processing, which can realize the Gaussian distribution, Poisson distribution, 0-1 distribution, uniform distribution, and other functions. These random distribution functions are widely used in radar ranging, aerospace, machine learning, and other fields [31], [32], [33].

II. PRINCIPLE AND SYSTEM DESIGN

The basic idea of generating a true random number is to use the jitter error generated by the low-frequency clock signal itself as the noise source, and to use the high-frequency reference clock signal to count and sample the measured clock. Since the jitter error range of the low-frequency oscillator is far greater than the measurement period of the high-frequency reference clock signal, and the jitter is caused by the Gaussian white noise of the electronic system, the jitter presents a Gaussian distribution. In the actual system application, the jitter range of the measured clock signal needs to be large enough to ensure the accurate measurement of the reference clock signal. Generally, the variance of the jitter range is more than 10 times the period of the reference clock signal. The data sampled from the counting signal generated by the reference clock will be fed into the random number generation module. Due to the jitter error characteristic of the low-frequency clock signal, the original random signal generated by direct count sampling shows a Gaussian distribution.

A. DESIGN OF RC SELF-EXCITED OSCILLATION CIRCUIT

The system consists of a high-frequency clock signal, a low-frequency clock signal, a counting and sampling module, and a random number generation module. The high-frequency signal uses a temperature-compensated crystal oscillator with high-frequency stability as the signal source. The crystal oscillator frequency in the experiment is 50MHz, and the frequency error is 0.1 PPM (parts per million); the low-frequency clock generation module is realized using an RC self-excited oscillation circuit composed of non-gate, resistor, and capacitor. All other circuits are implemented in the FPGA.

The schematic diagram and signal sequence diagram of the RC self-excited oscillation circuit are shown in Figure 1, where U1, U2, and U3 are the non-gates, R1 is the compensation resistance, and the value of R1 is generally about 10 times that of R2. R2 and C1 constitute the RC self-excited oscillation circuit. If U2 outputs a high level, since the voltage at both ends of capacitor C1 cannot change abruptly, U1 input is also high level, and U1 output is low level. At this time, we ensure that the U2 output pulse is high level. With the charging of C1, the input voltage of the non-gate U1 drops. When the voltage drops to the off voltage of the non-gate, U1 outputs a high level and U2 outputs a low level. We then reverse charge C1, and when the voltage rises to make U1 output a high level, U2 outputs a low level. This process will continue to cycle, thus generating a square wave. The non-gate U3 plays a buffering role in the circuit, enhancing the circuit's driving load capacity, and improving the driving clock signal for the back-end circuit.

The charge-discharge time constant of capacitor C1 and resistor R2 is:

$$\tau = R_2C_1 \tag{1}$$

The first transient stable state time of the capacitor C1 charging is:

$$T_1 = \tau \ln \frac{V_{CC}}{V_{CC} - V_{TH}} = \tau \ln 2 \approx 0.7\tau \tag{2}$$

In equation (2), V_{CC} is the power supply of the gate circuit, and V_{TH} is the threshold voltage for the level inversion of the gate circuit. Typically, the V_{TH} is half the supply voltage V_{CC}.

The second transient stable state time of the capacitor C1 discharging is:

$$T_2 = \tau \ln \frac{V_{CC}}{V_{TH}} = \tau \ln 2 \approx 0.7\tau \tag{3}$$

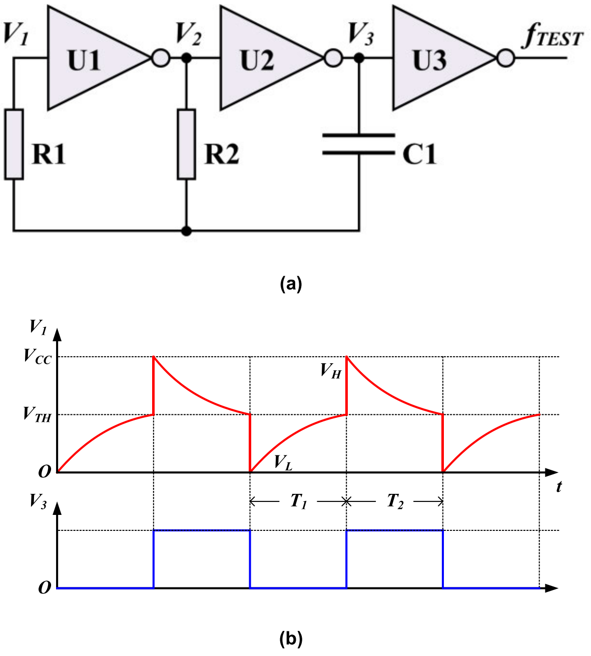


FIGURE 1. Low-frequency clock signal generation circuit. (a) Schematic circuit diagram. (b) Signal sequence diagram.

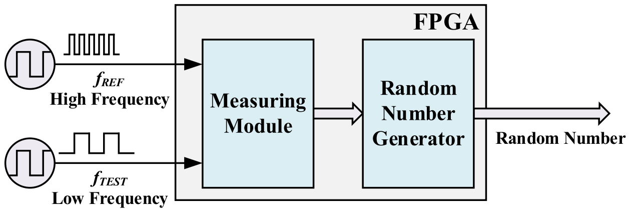


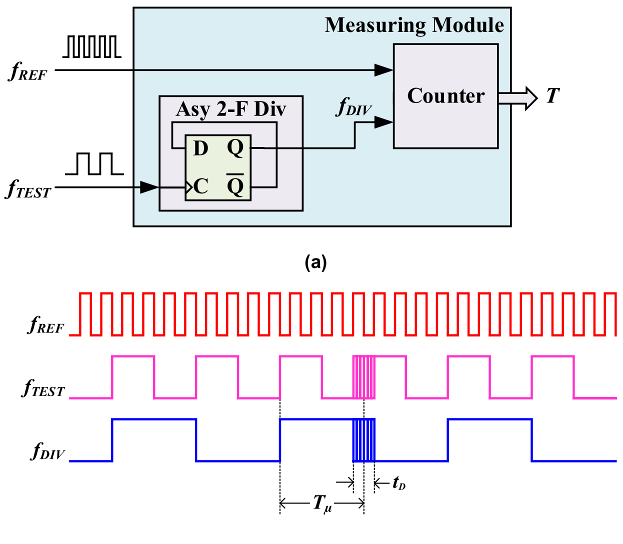
FIGURE 2. System block diagram of the true random number generator.

Finally, the capacitor charging and discharging cycle can be obtained as follows:

$$T = T_1 + T_2 = 1.4\tau \tag{4}$$

B. PRINCIPLE OF TRUE RANDOM NUMBER GENERATION

The functional block diagram of the true random number generation system is shown in Figure 2. A high-frequency oscillation source and a low-frequency oscillation source, which are mutually independent, are connected to the FPGA, and then the measurement module is used for sampling and counting. The high-frequency clock f_{REF} is used as the counting clock to sample the cycle of the low-frequency clock f_{TEST} for measurement. The instability of f_{TEST} causes the measured cycle T_{TEST} value to show the characteristics of random numbers. Since the noise source of the low-frequency clock jitter comes from the external white noise, the values of T_{TEST} show a Gaussian distribution, that is, this system can directly obtain the true random numbers with the characteristics of Gaussian distribution. The random number generation module is used to process the original data output by the



(a)

(b)

FIGURE 3. Measurement module. (a) Functional block diagram. (b) Measurement sequence diagram.

measurement module, and finally, output true random number sequences for other electronic systems.

The functional circuit block diagram and the signal sequence diagram of the measurement module are shown in Figure 3. The circuit consists of an asynchronous 2-frequency division (Asy 2-F Div) module and a counter module. Among them, we used the asynchronous 2-frequency divider module to divide the measured low-frequency signal f_{TEST} into two frequencies to obtain the two-frequency division signal f_{DIV}. The counter measured the pulse width of f_{DIV} to obtain the cycle of the signal f_{TEST}. In Figure 3(b), T_{TEST} is the cycle of the measured low-frequency clock signal, and t_D is the jitter range of the measured low-frequency clock signal. When the rising edge of the two-frequency division signal f_{DIV} comes, the counter module starts counting, and stops counting when the falling edge of f_{DIV} comes. The cycle range of the measured low-frequency clock signal is:

$$T_\mu - \frac{t_D}{2} \leq T \leq T_\mu + \frac{t_D}{2} \tag{5}$$

where T_μ is the expected value of the f_{TEST} signal cycle. In practical applications, the random number generator needs to generate different types of random numbers according to the different requirements of the system.

The system in Figure 2 can only generate true random numbers subject to the Gaussian distribution. In order to be applicable to electronic systems with different requirements, it is also necessary to obtain true random number generators subject to other distribution characteristics. Therefore, a low-frequency clock generator is added on the basis of Figure 2 to realize a true random number generator subject to the Gaussian distribution, uniform distribution, 0-1 distribution, and binomial distribution.

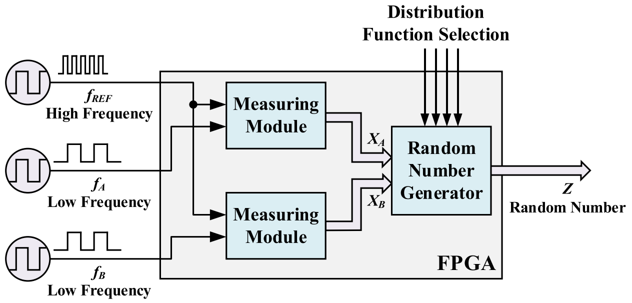


FIGURE 4. Principle block diagram of the true random number generator subject to multiple distribution characteristics.

C. REALIZATION OF TRUE RANDOM NUMBERS BASED ON MULTIPLE RANDOM DISTRIBUTIONS

As shown in Figure 4, in order to realize a random number generator with multiple distribution characteristics, we needed to add an RC multivibrator circuit to the random number generator we designed. The two low-frequency signals f_A and f_B are measured by two counting and sampling modules at the same time to obtain two sets of independent random number sequences X_A and X_B. These two random numbers are simultaneously fed into the random number generator module for processing operation, and finally, the random sequence Z with specific distribution characteristics is output.

The two random number sequences X_A and X_B obtained by the measurement module obey the Gaussian distribution, and the random number sequences Z_{GA} and Z_{GB} with the expectation of 0 and the standard deviation of 1 are obtained through the standardization transformation in the random number generator of the FPGA. The transformation formula is obtained according to equation (6).

$$\begin{cases} Z_{GA} = (X_A - \mu_A)/\sigma_A \\ Z_{GB} = (X_B - \mu_B)/\sigma_B \end{cases} \tag{6}$$

where μ_A and μ_B are the mathematical expectations of X_A and X_B, respectively, and σ_A and σ_B are the standard deviations of X_A and X_B, respectively. The expectation and standard deviation are calculated in the random number generator by equation (7).

$$\begin{cases} \mu = \frac{1}{N} \sum\limits_{j=0}^{N-1} X(j) \\ \sigma = \sqrt{\frac{1}{N} \sum\limits_{j=0}^{N-1} [X(j) - \mu]^2} \end{cases} \tag{7}$$

We can choose Z_{GA} and Z_{GB} as standard Gaussian distribution data sequences to be output as random numbers.

The uniformly distributed random number sequence can be obtained by processing two mutually independent Gaussian distributed random number sequences. According to the Box-Muller transformation, the relationship between uniform dis-

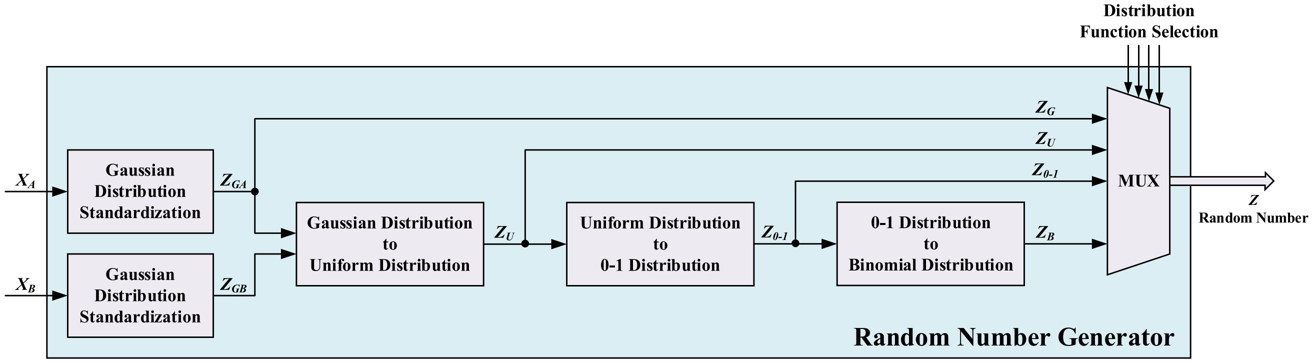

Distribution
Function Selection
X_A
Gaussian Distribution Standardization
Z_{GA}
X_B
Gaussian Distribution Standardization
Z_{GB}
Gaussian Distribution to Uniform Distribution
Z_U
Uniform Distribution to 0-1 Distribution
Z_{0-1}
0-1 Distribution to Binomial Distribution
Z_B
Z_G
Z_U
Z_{0-1}
MUX
Z
Random Number
Random Number Generator

FIGURE 5. The internal structure of the random number generator module.

tribution and Gaussian distribution is given by [34] and [35]:

$$\begin{cases} Z_{GA} = \cos(2\pi Z_{UA})\sqrt{-2\ln Z_{UB}} \\ Z_{GB} = \sin(2\pi Z_{UA})\sqrt{-2\ln Z_{UB}} \end{cases} \tag{8}$$

According to equation (8), the relationship between uniform distribution and Gaussian distribution can be obtained:

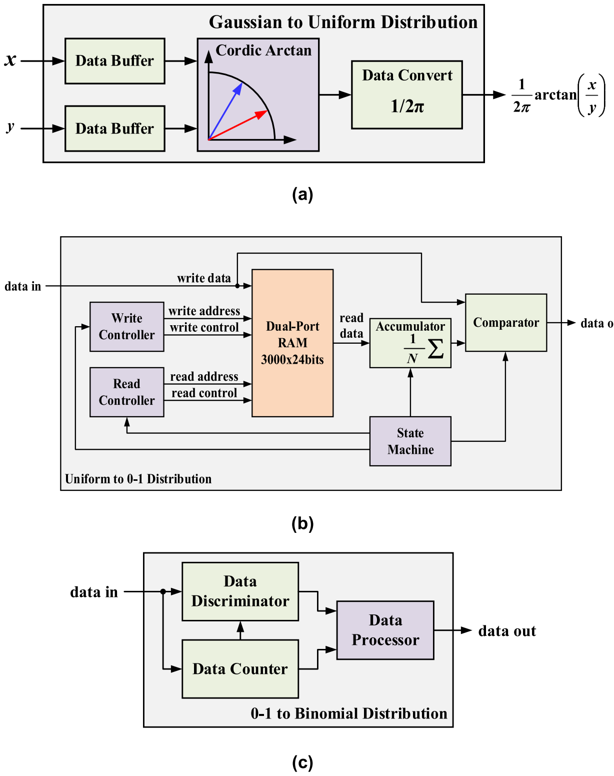
$$Z_U = \frac{1}{2\pi}\arctan\left(\frac{Z_{GB}}{Z_{GA}}\right) \tag{9}$$

That is, by measuring two random number sequences that obey the Gaussian distribution, we can calculate the required uniformly distributed random number sequence through equation (9). Since the trigonometric function cannot be directly calculated in the FPGA, we use the CORDIC (Coordinate Rotation Digital Computer) algorithm for trigonometric calculation. The CORDIC algorithm uses addition and subtraction shifts to convert them into vectors for iterative calculation. This algorithm has a high utilization rate of hardware resources and is easy to implement [35].

Next, we need to get a random number sequence with a 0-1 distribution, which is a special form of the binomial distribution, also known as the Bernoulli distribution. In the actual system implementation, we compare the uniformly distributed random numbers with a specific value and output the random number greater than that value as 1, and otherwise it is 0. The specific value is composed of the average of N uniformly distributed random numbers in a group. In the experiment, we took $N = 3000$. According to equation (10), the sequence of random numbers obeying the 0-1 distribution can be obtained.

$$Z_{0-1} = \begin{cases} 1, \; Z_U \geq \frac{1}{N}\sum\limits_{j=0}^{N-1} Z_U(j) \\ 0, \; Z_U < \frac{1}{N}\sum\limits_{j=0}^{N-1} Z_U(j) \end{cases} \tag{10}$$

If in the Bernoulli experiment repeated n times, the probability of the event occurrence is set as P, and X represents the number of times of occurrence probability of event A, then the distribution probability density of the random variable X is a binomial distribution. In the system design, we record the result of 0 in the 0-1 distribution as event A and calculate the probability, and finally generate the corresponding binomial distribution random numbers. The 0-1 distribution can be used to calculate the random number sequence obeying the binomial distribution.



(a)

(b)

(c)

FIGURE 6. Random distribution conversion module. (a) Gaussian to uniform distribution module. (b) Uniform to 0-1 distribution module. (c) 0-1 to binomial distribution module.

Figure 5 shows the internal structure of the random number generation module. X_A and X_B are two independent random number sequences directly sampled by the measurement module, which obey the Gaussian distribution. X_A and X_B are sent into the Gaussian distribution standardization module and converted into the standard Gaussian distribution ran-

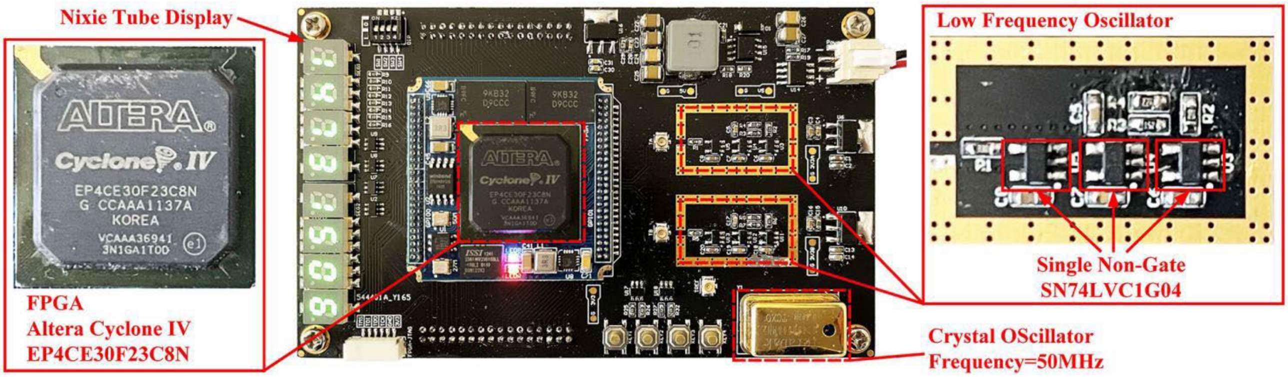


FIGURE 7. The hardware system of the true random number generator obeying multiple distribution characteristics.

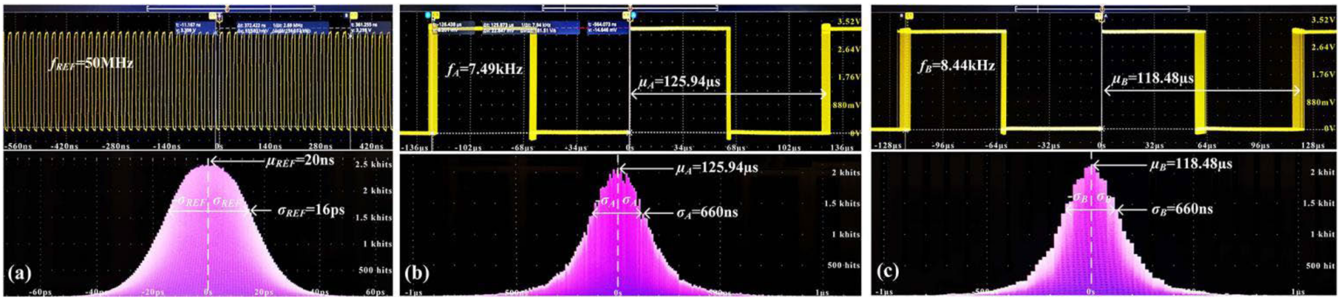


FIGURE 8. Clock signal test. (a) High-frequency reference clock signal f_{REF}. (b) Low-frequency clock signal f_A. (c) Low-frequency clock signal f_B.

dom number sequence Z_{GA} and Z_{GB} with an expectation of 0 and a standard deviation of 1. Z_{GA} and Z_{GB} are sent into the Gaussian distribution to a uniform distribution module and converted into the uniform distribution random number sequence Z_U. Then, Z_U is sent into the uniform distribution to the 0-1 distribution module to obtain the 0-1 distribution random number sequence Z_{0-1}, and Z_{0-1} is sent into the 0-1 distribution to the binomial distribution module to obtain the binomial distribution random number sequence Z_B. After the above conversion, the random number sequences with the four distribution characteristics of Z_G, Z_U, Z_{0-1}, and Z_B can be obtained. Finally, the four random number sequences are sent to the multiplexer for selection and output, and the random number sequences with different distribution characteristics can be obtained. The random number sequences with other distribution characteristics can be further realized by constructing conversion modules inside the FPGA.

Figure 6 shows the implementation methods of several random distribution con-version modules in FPGA. Figure 6(a) shows the internal structure of the Gaussian distribution to the uniform distribution module. The module is composed of a data buffer, a CORDIC arctangent module, and a data processing module. The data buffer simultaneously collects two random numbers x and y of Gaussian distribution, sends them to the CORDIC arctangent module to calculate the arctangent value of x/y, and the data conversion module outputs the arctangent value after normalization processing to obtain a random variable subject to the uniform distribution.

Figure 6 (b) shows the internal structure of the uniform distribution to the 0-1 distribution module. The dual port random access memory (RAM) has 3000 × 24bits data space, the write controller module continuously stores 3000 random variables subject to a uniform distribution in RAM. The read controller module reads out 3000 random variables in RAM in turn and sends them to the accumulator for summation. The accumulator obtains the average value of these 3000 random numbers and compares this average value with the current input data. If the current data is greater than the average value, the output of the comparator is 1, otherwise, 0, the output data of the comparator is a random variable subject to the 0-1 distribution. The state machine in the module controls the working sequence of each sub-module.

Figure 6(c) shows the internal structure of the 0-1 distribution to the binomial distribution module. The module consists of a data discriminator, a data counter, and a data processor. The data counter records the number of input data, the data discriminator judges whether the current data is 1 or 0, and the data processor records the number of 1 and accumulates the number of occurrences of 1, When the counter counts to 30, the value of 1 in the 30 data output by the data processor is the binomial distribution random number obtained by repeating 30 independent Bernoulli experiments. By changing the max-

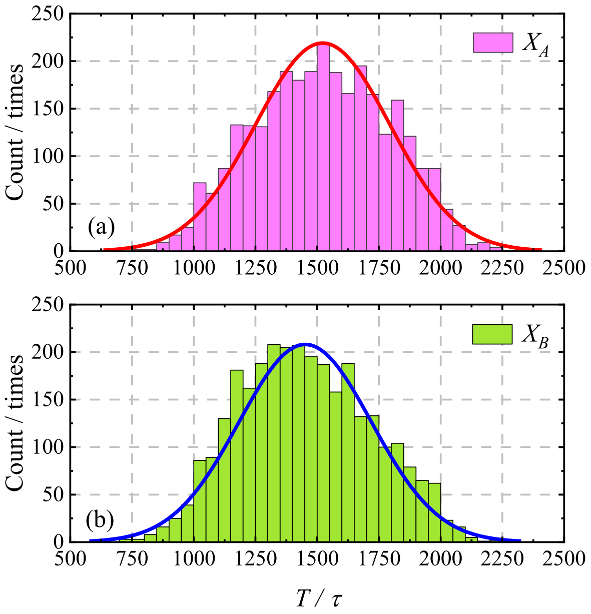


FIGURE 9. The histogram of random numbers obeying the Gaussian distribution. (a) Measurement data X_A of low-frequency clock A. (b) Measurement data X_B of low-frequency clock B.

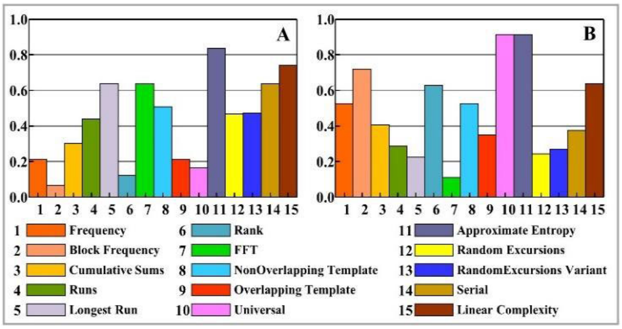


FIGURE 10. NIST SP 800-22 test of two random numbers with Gaussian distribution.

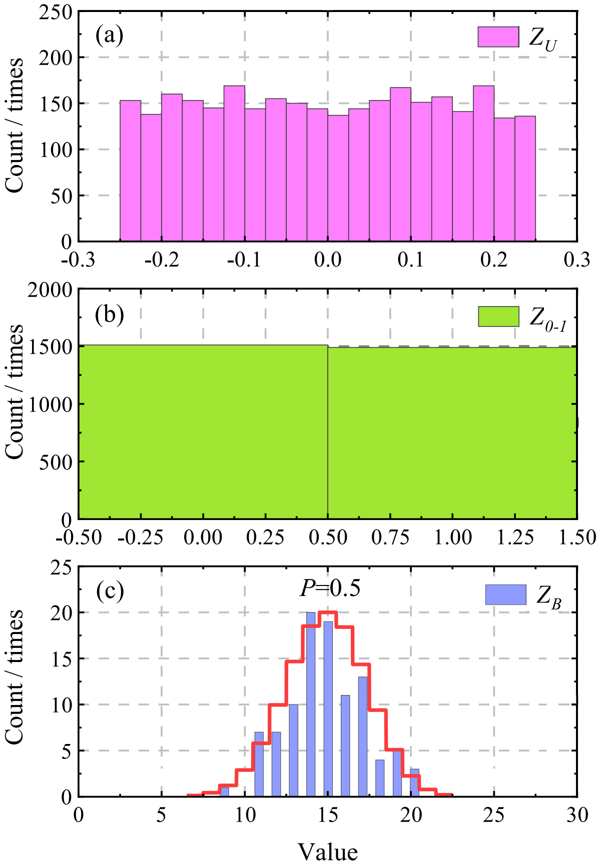


FIGURE 11. Probability distribution diagram of other random numbers. (a) Uniform distribution. (b) 0-1 distribution. (c) Binomial distribution.

imum count value of the counter, the binomial distribution random number obtained from other repeated independent Bernoulli tests can be obtained.

III. EXPERIMENT AND DATA ANALYSIS

The hardware system is the platform to verify the feasibility of our method. For this reason, we have built the hardware system required for experimental verification, as shown in Figure 7. The FPGA model used in this system is the Cyclone IV, EP4CE40F23C8 chip from Altera Corporation (now acquired by Intel Corporation). The non-gate chip used to form the low-frequency RC oscillation circuit is a single non-gate chip SN74LVC1G04 from Texas Instruments (TI). The high-frequency crystal oscillator is a temperature-compensated crystal oscillator with a frequency of 50 MHz and a jitter of 0.1 PPM. The random number sequences with different distribution characteristics can be switched through the keys on the printed circuit board (PCB) and then displayed on the nixie tube.

We can observe the waveform of the oscillator and the distribution range of signal frequency jitter through the oscilloscope. Figure 8 shows the signal waveforms of the high-frequency clock signal f_{REF}, the low-frequency clock signals f_A and f_B, and the histogram distribution of five hundred thousand of signal cycle tests. From Figure 8, we can observe that the actual frequencies of the signals f_A and f_B are 7.94 kHz and 8.44 kHz, respectively. The signal with these frequencies can reduce the flicker noise of the circuit and its interference with the system [36]. From the histogram distribution of f_A and f_B cycles, it can be seen that the standard deviation of the cycles is $\sigma = 660$ ns, and the jitter range is 3σ, which is about 2 μs. Among them, the probability of the low frequency signal value distributed in the interval range (μ - 3σ, $\mu + 3\sigma$) is 99.74%. The standard deviation of the high-frequency signal f_{REF} is 16ps, which is very stable, and the jitter range is about 50ps. The jitter ranges of the low-frequency signals are far greater than the clock cycle of the high-frequency signal, so the system meets the design requirements of measurement.

TABLE 1. Low-frequency clock signal parameters.

Signal	Frequency (/ kHz)	Samples (/ points)	Expectation (/ τ)	Standard Deviation (/ τ)
f_A	7.49	3000	1522.4	273.0
f_B	8.44	3000	1451.6	268.6

Next, we extracted the measured data and measured 3000 random numbers out-put by the oscillation circuits A and B. Figure 9 shows the random number distribution of the signals f_A and f_B. It can be seen that these two signals obey the Gaussian distribution and are completely consistent with the distribution characteristics measured in Figures 8 (b) and (c). The periods of the signals f_A and f_B are about 120 μs. The cycle of the counting clock is 20 ns, and the measured value is about 6000. With conservative processing, we subtracted 4500 to get the final data. The expectation of the final data is about 1500, and the standard deviation is about 270. Table 1 shows the expectation and standard deviation of these two groups of Gaussian distributed random numbers.

To test the performance indicators of random numbers, we use NIST SP800-22 statistical test package [28], [37] to test the random numbers generated by two RC oscillators A and B. Set the size of each group of data to be tested as 1Mbit, then select 15 test indicators for testing, set the number of groups $m = 20$, and select the confidence level $\alpha = 0.01$. The test results are shown in Figure 10, which shows the histogram of *P-value* values of all test items of NIST SP800-22. The data to be tested passed all test items of NIST SP800-22, with good random performance.

In order to further verify the random number sequence obeying other distribution characteristics, we also conducted the signal tests of uniform distribution and 0-1 distribution, and the test results are shown in Figure 11. The distribution of uniformly dis-tributed random numbers is shown in Figure 11 (a). According to the calculation method of equation (9), we converted the data measured in Figure 8 into uniformly distributed random data in the FPGA. The probability distribution of the random data is about -0.25–+0.25.

We continued to generate 0-1 distributed random data on the basis of uniform distribution, and the calculation method is according to equation (10). In this experiment, we determined the part less than or equal to 0 as 0, and the part greater than 0 as 1. The result is shown in Figure 11(b).

The binomial distribution is the Bernoulli trial repeated n times independently. In each trial, there are only two possible results, and the occurrence of the two results is opposite and independent of each other, independent of the results of other trials. The probability of the occurrence of the event remains unchanged in each independent tri-al. Then this series of trials is called the n-fold Bernoulli experiment. When the number of trials is 1, the binomial distribution follows the 0-1 distribution. We continued to use the 0-1 distribution to generate the binomial distribution. We took 30 random numbers subject to the 0-1 distribution for testing. The number of occurrences of event 1 was counted as the random number output by the binomial distribution. 3000 random numbers subject to the 0-1 distribution can be divided into 100 groups according to a group of 30, that is, 100 random numbers subject to the binomial distribution can be output. Figure 11(c) is the histogram of the distribution of 100 random numbers subject to the binomial distribution, and the envelope is the binomial distribution obtained by repeating 30 independent Bernoulli trials.

IV. CONCLUSION

In this paper, a method for generating true random numbers based on two RC oscillation circuits with FPGA design and obeying multiple distribution characteristics is proposed. The system uses the FPGA and RC oscillation circuits to realize random number sequences that can generate multiple distribution characteristics. We have carried out a series of data testing experiments with the system, and the experimental results show that the system can output random number sequences that obey Gaussian distribution, uniform distribution, 0-1 distribution, and binomial distribution. The system structure is simple, reliable, easy to implement, and low-cost, and can stably and reliably generate high-quality random number sequences. In addition, the system can provide true random number data sources for electronic systems in the field of automatic control and AI.

REFERENCES

[1] S. A. Hassan, S. Akbar, A. Rehman, T. Saba, H. Kolivand, and S. A. Bahaj, "Recent developments in detection of central serous retinopathy through imaging and artificial intelligence techniques—A review," *IEEE Access*, vol. 9, pp. 168731–168748, 2021.

[2] A. P. James, "The why, what, and how of artificial general intelligence chip development," *IEEE Trans. Cognit. Develop. Syst.*, vol. 14, no. 2, pp. 333–347, Jun. 2022.

[3] J. Liu, X. Kong, F. Xia, X. Bai, L. Wang, Q. Qing, and I. Lee, "Artificial intelligence in the 21st century," *IEEE Access*, vol. 6, pp. 34403–34421, 2018.

[4] S. J. H. Pirzada, A. Murtaza, T. Xu, and L. Jianwei, "Initialization vector generation for AES-CTR algorithm to increase cipher-text randomness," in *Proc. 2nd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE)*, Sep. 2019, pp. 138–142.

[5] K. Zhang, "Random simulation on error of grey forecasting model," in *Proc. IEEE Int. Conf. Grey Syst. Intell. Services*, Sep. 2011, pp. 228–232.

[6] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, "A contact-resistive random-access-memory-based true random number generator," *IEEE Electron Device Lett.*, vol. 33, no. 8, pp. 1108–1110, Aug. 2012.

[7] M. Saranya, M. Revathy, and A. K. Rahuman, "Harvard architecture based post processed true random number generator," *Mater. Today, Proc.*, vol. 47, pp. 135–138, Jan. 2021.

[8] Y. Kim, X. Fong, and K. Roy, "Spin-orbit-torque-based spin-dice: A true random-number generator," *IEEE Magn. Lett.*, vol. 6, pp. 1–4, 2015.

[9] P. Uday and P. D. Gawande, "A survey on implementation of random number generator in FPGA," *Int. J. Sci. Res. (IJSR)*, vol. 4, no. 3, pp. 1590–1592, 2015.

[10] 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.

[11] B. Perach and S. Kvatinsky, "An asynchronous and low-power true random number generator using STT-MTJ," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, pp. 2473–2484, 2019.

[12] V. L. Vanoli and M. P. Dieser, "PseudoRandom: A proposal of educational material for pseudorandom number generators learning," in *Proc. 12th Latin Amer. Conf. Learn. Technol. (LACLO)*, Oct. 2017, pp. 1–4.

[13] W. V. Camp and T. G. Lewis, "Implementing a pseudorandom number generator on a minicomputer," *IEEE Trans. Softw. Eng.*, vol. SE-3, no. 3, pp. 259–262, May 1977.

[14] Y. Wang, L. Niu, and H. Zhang, "Thermal noise random number generator based on SHA-2(512)," in *Proc. Int. Conf. Mach. Learn. Cybern.*, 2005.

[15] Y. Zheng, J. Pan, Y. Song, H. Cheng, and Q. Ding, "Research on the quantifications of chaotic random number generators," in *Proc. Int. Conf. Sensor Netw. Secur. Technol. Privacy Commun. Syst.*, May 2013, pp. 139–143.

[16] T. Nakura, M. Ikeda, and K. Asada, "Ring oscillator based random number generator utilizing wake-up time uncertainty," in *Proc. IEEE Asian Solid-State Circuits Conf.*, Nov. 2009, pp. 121–124.

[17] M. Coustans, C. Terrier, T. Eberhardt, S. Salgado, A. Cherkaoui, and L. Fesquet, "A subthreshold 30 pJ/bit self-timed ring based true random number generator for Internet of Everything," in *Proc. IEEE SOI-3D-Subthreshold Microelectron. Technol. Unified Conf.*, Oct. 2017, pp. 1–3.

[18] Y. Zhu, Y. Bian, J. Yang, Y. Zhang, and S. Yu, "21 Gbps source-independent quantum random number generator based on vacuum fluctuations," in *Proc. Asia Commun. Photon. Conf. (ACP)*, Nov. 2022, pp. 2140–2142.

[19] S. K. Tawfeeq, "A random number generator based on single-photon avalanche photodiode dark counts," *J. Lightw. Technol.*, vol. 27, no. 24, pp. 5665–5667, 2009.

[20] 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.

[21] J. Lee, Y. Seo, and J. Heo, "Analysis of random number generated by quantum noise source and software entropy source," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 729–732.

[22] D. B. Thomas and W. Luk, "The LUT-SR family of uniform random number generators for FPGA architectures," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 4, pp. 761–770, Apr. 2013.

[23] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadyay, "An improved DCM-based tunable true random number generator for Xilinx FPGA," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 64, no. 4, pp. 452–456, Apr. 2017.

[24] K. Wold and S. Petrovic, "Security properties of oscillator rings in true random number generators," in *Proc. IEEE 15th Int. Symp. Design Diag. Electron. Circuits Syst. (DDECS)*, Apr. 2012, pp. 145–150.

[25] R. N. Wuerdig, M. L. L. Sartori, and N. L. V. Calazans, "Asynchronous quasi-random number generator: Taking advantage of PVT variations," in *Proc. IEEE 10th Latin Amer. Symp. Circuits Syst. (LASCAS)*, Feb. 2019, pp. 137–140.

[26] R. Sato, Y. Kodera, M. A. Ali, T. Kusaka, Y. Nogami, and R. H. Morelos-Zaragoza, "Consideration for affects of an XOR in a random number generator using ring oscillators," *Entropy*, vol. 23, no. 9, p. 1168, Sep. 2021.

[27] M. Garcia-Bosque, A. Naya, G. Díez-Señorans, C. Sánchez-Azqueta, and S. Celma, "Suitability of generalized GAROs on FPGAs as PUFs or TRNGs considering spatial correlations," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 112–122, 2023.

[28] J. Cui, M. Yi, D. Cao, L. Yao, X. Wang, H. Liang, Z. Huang, H. Qi, T. Ni, and Y. Lu, "Design of true random number generator based on multi-stage feedback ring oscillator," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 3, pp. 1752–1756, Mar. 2022.

[29] S. T. Chandrasekaran, V. E. G. Karnam, and A. Sanyal, "0.36-mW, 52-Mbps true random number generator based on a stochastic delta-sigma modulator," *IEEE Solid-State Circuits Lett.*, vol. 3, pp. 190–193, 2020.

[30] J. Park, B. Kim, and J.-Y. Sim, "A PVT-tolerant oscillation-collapse-based true random number generator with an odd number of inverter stages," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 10, pp. 4058–4062, Oct. 2022.

[31] R. Frehlich, "Cramer-Rao bound for Gaussian random processes and applications to radar processing of atmospheric signals," *IEEE Trans. Geosci. Remote Sens.*, vol. 31, no. 6, pp. 1123–1131, Nov. 1993.

[32] D. J. Kong, L. Y. Chen, and S. Wang, "Research on modeling spying radar simulation system of anti-aircraft campaign based on HLA," (in Chinese), *Comput. Simul.*, vol. 28, no. 4, pp. 22–25, 2011.

[33] N. D. Truong, J. Y. Haw, S. M. Assad, P. K. Lam, and O. Kavehei, "Machine learning cryptanalysis of a quantum random number generator," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 403–414, Feb. 2019.

[34] A. Çaglan, E. Inceöz, E. Balcisoy, M. E. Özbek, and E. Çavus, "FPGA implementation of AWGN noise generator using box-muller method," in *Proc. 24th Signal Process. Commun. Appl. Conf. (SIU)*, May 2016, pp. 1813–1816.

[35] K. Puntsri, B. Bunsri, Y. Pittayang, T. Bubpawan, W. Partipralam, and W. Phakphisut, "Reconfigurable AWGN generator using box-muller method with CORDIC-based square root calculation," in *Proc. 37th Int. Tech. Conf. Circuits/Syst., Comput. Commun. (ITC-CSCC)*, Jul. 2022, pp. 1–4.

[36] J. Chang, A. A. Abidi, and C. R. Viswanathan, "Flicker noise in CMOS transistors from subthreshold to strong inversion at various temperatures," *IEEE Trans. Electron Devices*, vol. 41, no. 11, pp. 1965–1971, Nov. 1994.

[37] F. Yu, Z. Zhang, H. Shen, Y. Huang, S. Cai, and S. Du, "FPGA implementation and image encryption application of a new PRNG based on a memristive Hopfield neural network with a special activation gradient," *Chin. Phys. B*, vol. 31, no. 2, Jan. 2022, Art. no. 020505.

GANG SU received the B.S. and M.S. degrees from Jilin University, Changchun, China, in 2016 and 2022, respectively. His current research interests include laser radar circuit design, embedded system development, FPGA system design, and motor control technology.

CHANGCHUN DING received the B.S. degree from Northeast Petroleum University, Daqing, China, in 2019. He is currently pursuing the M.S. degree with the College of Electronic Science and Engineering, Jilin University. His current research interests include laser communication technology and the development of FPGA systems.

SIDA LI received the B.S. degree from the Nanjing Institute of Technology, Nanjing, China, in 2019, and the M.S. degree from Jilin University, Changchun, China, in 2022. He is currently pursuing the Ph.D. degree with the School of Astronautics, HIT, Harbin, China. His current research interests include automatic control, embedded system development, and FPGA system development.

ZIJIAN LIU received the B.S. degree from Jilin University, Changchun, China, in 2019. He is currently pursuing the M.S. degree with the College of Electronic Science and Engineering, Jilin University. His current research interests include unmanned vehicle development and FPGA system development.

ZHENG GAO received the B.S. degree from the North University of China, Taiyuan, China, in 2021. He is currently pursuing the M.S. degree with the College of Electronic Science and Engineering, Jilin University. His current research interests include photoelectric detection technology and FPGA system development.

JUNFENG SONG received the B.S. and Ph.D. degrees from Jilin University, Changchun, China, in 1993 and 2000, respectively. He was a Professor with Jilin University, in 2004, where he was a Doctoral Supervisor, in 2005. From 2006 to 2016, he was a Senior Researcher with the Singapore Microelectronics Research Institute, where he is mainly engaged in the research of silicon-based optoelectronic integrated devices. He is currently a Professor with the College of Electronic Science and Engineering, Jilin University. His current research interests include the development of optoelectronic integrated all-solid-state lidar, the design of a silicon-based optoelectronic integrated quantum communication chip, and the development of a novel silicon-based optoelectronic integrated device.

SHUXU GUO received the B.S., M.S., and Ph.D. degrees in electronic engineering from Jilin University, Changchun, China, in 1982, 1989, and 2006, respectively. Since 2000, he has been a Professor with the State Key Laboratory on Integrated Optoelectronics, College of Electronic Science and Engineering, Jilin University, where he is involved in the reliability of semiconductor devices and digital image processing and analysis.

MIN TAO received the B.S. degree from the Inner Mongolia University of Science and Technology, Baotou, China, in 2013, and the M.S. and Ph.D. degrees from Jilin University, Changchun, China, in 2017 and 2022, respectively. He has been a Lecturer with the College of Electronic Science and Engineering, Jilin University. His current research interests include driving and control technology of solid-state lidar, robot development, the development of embedded systems, and FPGA system design.