Generation of Physical Random Numbers with a Variable-Capacitor Parametron

Yoshiaki Saitoh,1 Junichi Hori,1 Hiroshi Nishimura,2* and Tohru Kiryu2

1Department of Biocybernetics, Niigata University, Niigata, 950-2181 Japan
2Graduate School of Niigata University, Niigata, 950-2181 Japan

SUMMARY

In the present study, a random number generator which physically produces nonperiodic uniform random number was developed using the parametron principle. The parametron is an oscillation circuit at one-half of the excited frequency. The phase of the parametron cannot be predicted because it depends on the noise in the parametron circuit. The random number was generated by detecting the unpredictable phase. The randomness of the data generated by the present method was confirmed by the spatial distribution and by statistical random tests. © 2002 Wiley Periodicals, Inc. Electron Comm Jpn Pt 3, 86(2): 24–32, 2003; Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/ecjc.10040

Key words: physical random number; parametron; random number generator; random test.

1. Introduction

Random numbers that are completely disorderly and whose appearance frequency is uniform are widely used in numerical simulations of social or physical phenomena. In addition, random numbers play an important role in cryptography, and are extensively used in the field of information protection. Though various random number generation methods have been developed, most of them generate pseudorandom numbers by software algorithms such as the mean-square method or linear congruence method [1–3]. Such random number generation based on algorithms has been widely used by virtue of their reliability and high-speed generation. However, it has been confirmed that pseudorandom numbers generated by a computer have periodicity, because the computer represents only a limited number of states. Therefore, it may happen that correct solutions and satisfactory security are not provided, and a generation method that provides more disordered random numbers has been sought.

In recent years physical methods of random number generation have been developed because of the improvement of processing speed and reliability of hardware. The random number generation method using gamma rays proposed by Ishida [4] and Miyatake and colleagues [5] has the problems that its generation speed is slow and it requires large-scale equipment. The “Random Master” random number generator utilizing the internal thermal noise of a semiconductor was produced by Toshiba Corporation, but it required new hardware and facilities. Physical random number generation with the noise of diodes has also been developed [6–8].

The principle of the parametric oscillator (parametron) was proposed by Goto in 1955 [9]. This is the phenomenon in which a resonance circuit with conductor and coil oscillates with a frequency of \( f/2 \) when the capacitance or inductance changes periodically with a frequency of \( f \). The parametron has two conditions, zero-phase oscill-
lation and pi-phase oscillation, and the condition depends on the phase of tiny oscillations within the resonant circuit [9–11]. Although Goto predicted that random numbers could be generated by utilizing this property, such equipment has not been realized until now [12]. In our research, a real random number generator using a variable-capacitor parametron was developed by considering that the condition of the parametron cannot be predicted, because the oscillation phase is controlled by noise when there is no oscillation in a resonant circuit. The parametron can be realized not only in the RF band but also in the millimeter and optical frequency bands. Actually, an optical parametric oscillation technique has already been developed [13]. It is expected that the optical parametric oscillation method will solve the problem of speed in physical random number generation.

In the present paper, the basic principle of random number generation with a parametron and its application in RF-band random number generation equipment that we developed are described. The efficiency of the proposed method is confirmed by statistical evaluation of the generated random numbers.

2. Basic Principles of Random Number Generation

2.1. Parametric oscillator (parametron)

Periodically changing the inductance of a coil $L$ or the capacitance of a capacitor $C$ in an L-C resonant circuit causes frequency oscillation at half the excitation frequency. A variable-capacitor diode whose capacitance changes as a function of the bias voltage was used for a parametron circuit in the present study. Figure 1 shows the fundamental circuit of the parametron. The fundamental circuit consists of a coil ($L$), a resistor ($R$), a variable-capacitor diode ($C_v$), and an RF power supply ($E$). The variable-capacitor diode is the element whose capacitance changes according to the electric excitation power. In this circuit, the capacitance of the variable-capacitor diode changes with frequency $f$ when the circuit is driven by an RF power supply of frequency $f$. As a result of the parametron principle, the circuit oscillates with a frequency of one-half ($f/2$) the excitation frequency $f$. The parametron takes the status of either zero-phase or pi-phase oscillation. When RF power is applied to the unexcited parametric circuit, the phase of the parametron, that is, zero-phase oscillation or pi-phase oscillation, depends on the phase of the small signal of frequency $f/2$ in the resonant circuit. In a parametric digital circuit, which is one of the applications of the parametron, the phase is controlled using the above principle [9–11]. On the contrary, if this small signal does not flow into a circuit, the phase of the parametron depends on the noise existing in the circuit. Since physical noise is statistically random, the phase of the parametron cannot be forecast. In the present paper, random numbers are generated by detecting the unpredictable phase of the parametron.

2.2. The parametron circuit

Since the output of the fundamental circuit of the parametron described in Fig. 1 has the RF excitation signal superimposed on it, it is difficult to determine the phase of oscillation. In order to remove the RF excitation signal and to detect only the parametron signal, the fundamental circuit is modified as in Fig. 2. The modified circuit consists of a differential amplifier with OP amplifier and two parametron devices, which are symmetrical with respect to the power supply. In Fig. 2, the RF excitation signal flows through the inner loop ($E \rightarrow C_{v1} (C_{v2}) \rightarrow A \rightarrow B \rightarrow L \rightarrow E$), and the parametron signal flows through the outer loop ($L \rightarrow A \rightarrow C_{v1} \rightarrow C_{v2} \rightarrow B \rightarrow L$). Since at points A and B in Fig. 2, the RF excitation signals are in phase with respect to the inner loop, they are rejected by differential amplifi-

![Fig. 1. Fundamental circuit of a parametron.](image1)

![Fig. 2. Parametron circuit.](image2)
cation between A and B. As a result only the parametron signal, which is in differential mode, can be detected.

2.3. Random number generator with parametron

The proposed method generates random numbers using the phase information of the parametron. However, it is impossible to obtain phase information because the phase reference is unknown in the parametron circuit alone as described in Fig. 2. Thus, two parametron circuits with an in-phase exciting RF signal are prepared, one parametron circuit is always in the condition of oscillation and the other is in the condition of on/off oscillation with an electrical switch. The phase information is detected by watching the phase between the two parametron circuits. Figure 3 depicts the composition of the whole random number generation system. This system consists of a two-output RF power supply whose phase is controllable (NF Corporation, Wave Factory 1946), two parametron circuits as shown in Fig. 2 \((L = 21.5 \mu H, C_v: SV101)\), a differential amplifier (LM741), a low-pass filter, an electrical relay, control equipment, and a personal computer (NEC Corporation, PC-9801NS/E). The RF excitation signal injected into parametron B is controlled by an electronic relay. The on/off state of the electronic relay is controlled by a clock signal from the control system. Phase information is detected by taking the differential of the two parametron outputs.

That is, if the two parametron outputs are in phase, the output is almost zero, and if they are out of phase, the output is a signal having a magnitude twice that of one parametron output. The signal is input into a personal computer through a fifth-order Chebyshev low-pass filter with a 45-Hz cutoff frequency in order to detect the magnitude component. The present system provides binary random numbers 0 and 1 when the output is zero-phase and pi-phase oscillation, respectively. The personal computer acquires and records the detected signal as synchronized to the on/off state of the switch in the clock signal of the control system. It also controls the parameters of the RF power supply as described in Section 3, providing automatic control. An RS-232C/GP-IB converter (Keithley, Model 500-Serial) is used for converting the RS-232C signal forwarded by the personal computer into a GP-IB signal, which can be controlled by the RF power supply.

2.4. Stabilization of equipment

The probability of random number generation should be controlled in order to achieve stable random number generation. Supposing an occurrence probability of zero, the ratio of the number of zeros to all data is \(P_0 = N_0/N\), where \(N\) is the number of all data and \(N_0\) is the number of zeros. The occurrence probability of a one \((P_1)\) is the same as \(P_0\). It is desirable that the occurrence probability of 0s and 1s be 1/2 to produce random numbers. The random number generation equipment in Fig. 3 has two parameters, the excitation frequency and the phase difference of the excitation signals. The occurrence probabilities \(P_0\) and \(P_1\) may be varied by changing these parameters. The phase difference of the excitation signals expresses the phase difference between RF signals just before injection into the two parametrons. The phase caused by a difference of cable lengths between the power supply and the two parametrons was corrected for in advance. In addition, the inductance of the coil might be changed by environmental circumferences because the coil used as an element of the parametron was handmade. It is difficult to keep generating stable random numbers for a long period because changes of inductance cause changes of the resonant frequency and as a result the occurrence probability changes with time. Thus, we plan to stabilize the equipment by controlling the excitation frequency dynamically according to the monitored occurrence probability of generated 0s and 1s. Figure 4 is a flowchart of the frequency control algorithm. Stable random numbers could be obtained by this method even if the ambient environment changes.
3. Characteristics of Random Number Generation Device

In this section we describe the characteristics of the random number generation equipment introduced in Section 2.3, verifying its output in order to obtain the optimum parameters for uniform random number generation.

Figure 5 shows one example of the output waveform of parametrons A and B in the random number generation equipment shown in Fig. 3. In parametron B either (a) zero-phase oscillation or (b) pi-phase oscillation was observed while parametron A oscillated continuously. Figure 6 shows one example of the output waveform of the low-pass filter in Fig. 3. By controlling parametron B, either zero-phase or pi-phase oscillation could be observed relative to the output of parametron A.

In order to generate uniform random numbers, we examined the occurrence probability of 0s and 1s by changing the excitation frequency and the phase difference, which were parameters of the random number generation equipment. Figure 7(a) shows the occurrence probability of 0s and 1s as the excitation frequency is changed and the phase difference remains constant. The testing was performed at room temperature (23.5 °C); the magnitude of RF was 0.2 Vp-p, the phase difference was 0°, and the clock frequency of the control equipment was 45 Hz. The occurrence probability of 0s and 1s was recorded at excitation frequencies from 10.85 to 11.30 MHz in 0.001-MHz steps. The occurrence probability was measured three times at each frequency and the average of the three measurements.
was recorded. As shown in Fig. 7(a), the occurrence probability of 0s increased when the excitation frequency became high, and became 1/2 at about 10.988 MHz. Furthermore, as the frequency increased, the occurrence probability of 0s suddenly began to decrease at 11.177 MHz and became zero by 112.030 MHz.

Next, Fig. 7(b) shows the occurrence probability as the phase difference is changed at a fixed excitation frequency. The occurrence probability of 0s and 1s was recorded for phase differences from –180° to 180° in 0.1° steps with the excitation frequency of 10.988 MHz constant. The occurrence probability of 0s suddenly began to decrease at –125° and became zero at –94°. After that, as the phase difference increased, the occurrence probability increased, and it became 1/2 at about zero.

4. Evaluation of Random Numbers

We inspected whether the data generated with the parameters noted in Section 3 were random numbers or not. First a total of $N = 4096$ numeric data ($M = 8$ bits) were obtained from 32,768 binary data generated with the random number generation equipment described in Section 2.3. For comparison, 4096 random numbers of 8-bit numeric data generated by the “rand” function of the C standard library (Borland Turbo C Ver2.0) were prepared. The algorithm is a linear congruence method. Pseudorandom numbers generated with a computer are periodic, as described in Section 1. Since the number of data generated with the random function of the C language was much smaller than the period of $2^{32}$, the data were assumed to represent uniform random numbers. The randomness of the generated numbers was evaluated in terms of the two- and three-dimensional frequency distributions and by statistical randomness testing.

4.1. Comparison by two- and three-dimensional frequency distributions

The randomness of data generated by the fundamental composition of the random number generator in Fig. 3 was confirmed by displaying the two- and three-dimensional frequency distributions. First, the generated $N = 4096$ data ($M = 8$ bits) were divided into two and three pairs in order to get two- and three-dimensional coordinate data, respectively. Thus, 2048 and 1365 sets of data were generated in the case of two and three dimensions, respectively. Next, the pairs of data were plotted in two and three dimensions. The results of the two- and three-dimensional frequency distributions are shown in Figs. 8(a) and 8(b), respectively. It was confirmed that the generated data both with the “random” function of the C language and the proposed method were random numbers, because the results were uniformly distributed without periodicity in two- and three-dimensional spaces.

4.2. Comparison by statistical testing for randomness

Next, $N = 4096$ generated data with $M = 8$ bits were evaluated statistically for randomness by a frequency test, a run test, and a combination test.

(A) Frequency test

The occurrence probability of numeric value $k$ is $P(k) = f_k/N$ ($k = 0, 1, \ldots, K – 1$) when the value $k$ appears $f_k$ ($k = 0, 1, \ldots, K – 1$) times among $N$ generated numeric data. Because the occurrence probability for each value is the same, for a random number the theoretical occurrence probability is $P(k)^* = 1/K$. The data are assumed to be random numbers in the frequency test if the calculated value of

$$
\chi^2_{K-1} = \sum_{k=0}^{K-1} \frac{(P(k) – P(k)^*)^2}{P(k)^*}
$$

was recorded.
is smaller than the chi-squared value for \( K - 1 \) degrees of freedom at the 5 or 1% significance level [1]. In the present investigation the test is done under conditions of \( K = 2M = 256 \) and \( N = 4096 \).

(B) The run test

A “run” refers to how long the data monotonically increase or decrease when comparing numeric values in the data stream [3]. The number of data included in one monotonically increase or decrease is called the run length. In the present paper, \( \chi^2 \) was calculated by the modified run test method [1]. The data can be assumed to be random numbers in the run test if the value is smaller than the chi-square value for 4 degrees of freedom at significance levels of 5 or 1%.

(C) Combination test

Let us consider a series of \( N \) of \( M \)-bit binary numbers. The probability of occurrence of \( k \) 1’s among \( M \) column binary data is theoretically represented by

\[
P(k) = \frac{N!}{k!(M-k)!}(\frac{1}{2})^M\quad (k = 0, 1, \ldots, M - 1)
\]

for random data [1]. Here, \( MC_k \) is the number of combinations of \( k \) 1’s in \( M \) data. The data can be assumed to be random in the combination test if the value calculated by \( \chi^2_{M-1} \) is smaller than the chi-squared value for 7 degrees of freedom at a significance level of 5 or 1%. Table 1 shows the results of the three statistical randomness tests, the frequency test, the run test, and the combination test for the generated data. The results show the values of the \( \chi^2 \) distribution with the rejection threshold at a significance level of 5%. The value of the proposed data proves to be smaller than that of the “rand” function in the run test, but is larger than that of the “rand” function in the frequency test and combination test. However, it may be said that the data are random in every test because the calculated value of the proposed method is below the rejection thresholds.

5. Discussion

5.1. Characteristics of random number generation equipment

In the present paper, we considered the principle of the parametron as a method of generating uniform physical random numbers without periodicity. The parametron is a circuit which oscillates at half the excitation frequency, and it is difficult to predict the phase because it is governed by the internal noise of the circuit. We developed equipment which generated random numbers by detecting the unpredictable phase.

In the random number generation equipment using the parametron as shown in Fig. 7, the occurrence probability of random numbers varies with both the excitation frequency and the phase difference. In the case of the conductance and capacitance used for our experiment, we confirmed that the frequency associated with an occurrence probability of 1/2 was 10.988 ± 0.001 MHz, as indicated by the results in Fig. 7(a). In addition, we confirmed that the occurrence probability changed greatly when the phase difference deviated from 0°, as indicated by Fig. 7(b). The excitation frequency at which the occurrence probability is 1/2 may vary with environmental conditions such as the ambient temperature. In order to generate uniform random numbers, the excitation frequency was con-
trolled by the occurrence probability with a fixed phase difference of 0°. The generation speed of random numbers was slow, a maximum of 45 8-bit random numbers per second for the present system. The reason for the low generation speed is the time required to reach stable oscillation of the parametron in each rise and fall. It is possible to increase the speed if the excitation frequency and clock frequency are set to high. In addition, a marked speed-up can be expected if the random numbers are generated with an optical parametron, operating at optical frequencies.

5.2. Stabilization of equipment

The occurrence probability of the proposed random number generation equipment may be changed by environmental conditions as mentioned in Section 5.1. In order to stabilize the equipment so that the occurrence probability would remain constant, the excitation frequency was sequentially controlled according to the monitored occurrence probability. The proposed system controlled the excitation frequency by the actual measured value, but a further upgrade is necessary for high-speed generation of uniform random numbers. Specifically, high-reliability frequency control using PID is necessary. In addition, control methods that consider the properties of uniform random numbers other than the occurrence probability can be examined. Furthermore, the effect of the ambient environment on the proposed equipment should be examined. For example, the influence of high-frequency noise sources in nearby computers on the occurrence probability should be considered. Furthermore, we must examine speed-up of random number generation.

5.3. Simplification of equipment

In the fundamental system of random number generation equipment shown in Fig. 3, a special RF power supply with two outputs whose relative phase could be controlled is necessary. When controlling only frequency, the system can be simplified by using a power supply with one-channel output. A block diagram of the simplified system is shown in Fig. 9(a). The output of the RF power supply is divided into two outputs before the electrical relay. The same electronic relays are inserted before the two parametron circuits in order to assure a phase difference of 0°. In addition, the noise in the parametron circuits is independent because the two parametron circuits are divided by the electronic relays and each parametron oscillates with independent phase. Figure 9(b) shows the characteristics of the occurrence probability when the excitation frequency of the simplified random number generation equipment is varied. As compared with the occurrence probability characteristics of the fundamental configuration in Fig. 7(a), the occurrence probability characteristics of the simplified version suddenly changed to zero and $\pi$ phases. However, paying attention to the frequency band around 11.02 MHz in which the occurrence probability is about 1/2, as shown by the arrow in Fig. 9(b), the change of the occurrence probability with frequency was closely similar to that of the fundamental circuit of Fig. 7(a). It is inferred that the occurrence probability is controllable even with the simplified equipment.

5.4. Evaluation of random numbers

Now, consider the applications of coding that uses random numbers. Since pseudorandom numbers generated with a computer are calculated with arithmetic expressions, the same key data may be reproduced if the derivation formula and for random numbers if its parameters are known. On the other hand, the physical random generator described in the present paper provides advanced security because it is impossible to generate the same key data even if the random number is generated with the same equipment and by the same method. In addition, more precise computer simulations can be executed by using physical random numbers.

Fig. 9. Simplified random number generators. (a) Block diagram; (b) probability characteristics.
The data generated with our proposed method were evaluated using two- and three-dimensional frequency distributions and statistical testing for randomness. The data were uniformly distributed over the two- and three-dimensional frequency distribution spaces, as shown in Fig. 8. In the statistical testing for randomness, the obtained values were smaller than the theoretical values at the relevant significance levels for all tests used in the present study. The data provided by our equipment were confirmed to be random numbers in all evaluation methods used in the present study. Incidentally, in statistical testing for randomness, the results for the numbers generated by our equipment were larger than the values given by the random numbers generated by the C standard library “rand” function. This may be caused by variation of the excitation frequency that provides 0.5 occurrence probabilities of 0s and 1s during data measurements. In addition, since the number of evaluation data was smaller than the period of the “rand” function ($2^{32}$), the result of the “rand” function looks better than our data. It will be necessary to test large numbers of data with increased bit width in order to confirm this result.

### 5.5. Comparison with other random number generation methods

First, in comparing our proposed physical random number generation method with pseudorandom number generation by algorithm, the problem of periodicity cannot be avoided when many pseudorandom numbers are generated with the algorithm. On the other hand, the physical random number generation method that we proposed is superior to the algorithmic method in terms of nonperiodicity, because it is based on the randomness of a natural phenomenon. The proposed method is the same as the traditionally proposed physical random number generation method in terms of the meaning of the random number characteristics [4–8].

Methods using radioactivity have been proposed as physical random number generation methods [4, 5]. Although they provide high-quality random numbers, they require special materials and equipment to generate and detect the radioactivity. Our proposed system, which consists of a power supply, a resistance, an electric coil, and a variable-capacitor diode, can generate high-quality random numbers without special hardware. Physical random number generators based on noise occurring in a semiconductor or a diode have been proposed [6–8]. Although these methods, not requiring any special equipment, may be installed on computers in the future, there is a limitation on the generation speed of random numbers. The generation speed of the random number generator we proposed is also limited and is about 1/100 as great as that of conventional methods, because it was examined in the RF band in the present study. However, it is expected that the generation speed of random numbers could increase greatly in the near future if the optical parametron technique is applied to random number generation. The present paper has demonstrated this possibility in principle.

### 6. Conclusions

We have developed a method of generating physical random numbers using a parametron. In order to generate uniformly distributed random numbers consistently, the occurrence probability was controlled by measuring the occurrence characteristics relative to phase difference and excitation frequency. In addition, we showed the possibility of simplifying the random number generation equipment. Confirmation that uniformly distributed random numbers could be generated by the proposed method was provided by testing of frequency distributions and by three statistical random number tests. In the near future, we will examine the miniaturization of the equipment, speed-up of random number generation, and consideration of environmental effects on the equipment. Because our system used the RF band, its random number generation speed was relatively slow. However, we believe that generation speed will be greatly improved if we apply the principle at higher frequencies such as millimeter waves or in an optical parametron.

### REFERENCES


AUTHORS (from left to right)

Yoshiaki Saitoh (member) received his B.E. degree in electrical engineering from Niigata University in 1963, and M.E. and Ph.D. degrees in electrical engineering from Hokkaido University in 1965 and 1970. In 1965 he joined the staff of the Department of Electronics, Niigata University, as an instructor, and has been a professor in the Department of Information Engineering since 1980. His recent research interests include measurements and stimulation of human organs, hyperthermia systems, and biomedical signal processing. He is a member of IEEE and the Japan Society of Medical Electronics and Biological Engineering.

Junichi Hori (member) received his B.E. and M.E. degrees in information engineering from Niigata University in 1986 and 1988, and Ph.D. degree in computer science from Tokyo Institute of Technology in 1996. In 1988 he joined the staff of the Department of Information Engineering, Niigata University, as a research associate, and is currently an associate professor in the Department of Biocybernetics. He was a visiting scholar in the Biomedical Functional Imaging and Computation Laboratory at the University of Illinois at Chicago in 1999–2000. His research interests include inverse problem of physiological systems, biomedical signal and image processing, and biomedical measurements.

Hiroshi Nishimura (member) received his B.E and M.E. degrees in information engineering from Niigata University in 1997 and 1999. He then joined Matsushita Communication Kanazawa R&D Labs., and has been working on mobile communication.

Tohru Kiryu (member) received his B.E. and M.E. degrees in electronics engineering from Niigata University in 1975 and 1977, and D.Eng. degree in computer science from Tokyo Institute of Technology in 1985. From 1977 to 1978, he was with the School of Dentistry of Niigata University, and from 1978 to 1995, the Department of Information Engineering. Since 1995, he has been with the Graduate School of Science and Technology as a professor. He was a visiting scientist at the Neuromuscular Research Center of Boston University in 1990–1991. He has been working on biomedical signal processing, especially time-varying spectral analysis, time-varying parameter estimation using nonstationary models and nonstationary stochastic process. For applications, his recent interests have been in myoelectric signal analysis during dynamic movements, muscular fatigue evaluation at a required time, and mental stress evaluation from multidimensional time series. He is a member of IEEE, the Japan Society of Medical Electronics and Biological Engineering, and the Japan Prosthodontic Society.