PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 3 :
H03K 3/84

A1

(11) International Publication Number: WO 82/ 01969

(43) International Publication Date: 10 June 1982 (10.06.82)

(21) International Application Number: PCT/US81/01519

(22) International Filing Date: 16 November 1981 (16.11.81)

(31) Priority Application Number: 210,989

(32) Priority Date: 28 November 1980 (28.11.80)

(33) Priority Country: US

(71) Applicant: NCR CORPORATION [US/US]; World Headquarters, Dayton, OH 45479 (US).

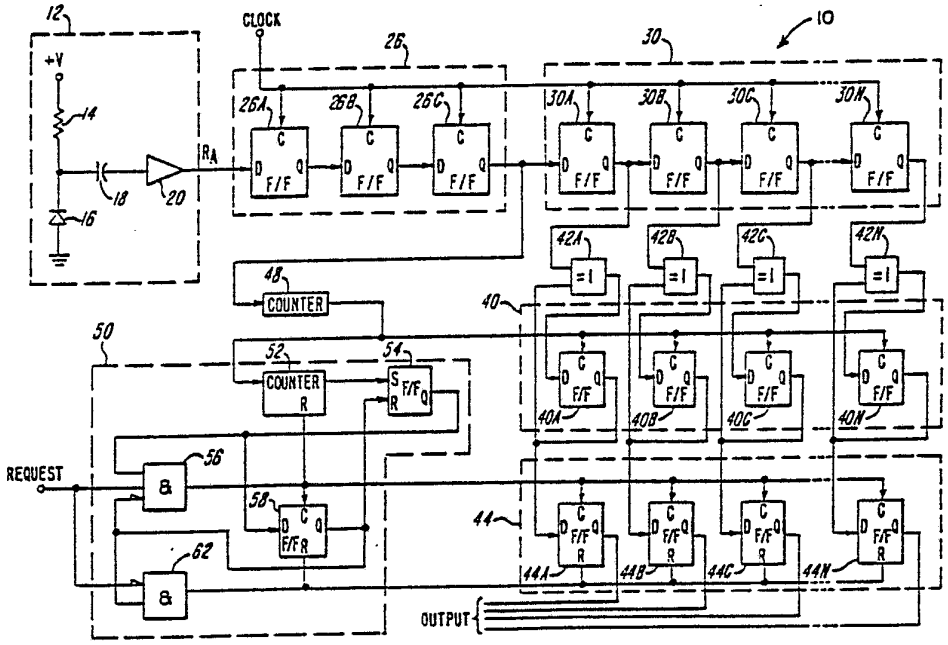
(72) Inventor: PORTER, Sigmund, Norman ; 614 Santa Alicia, Solana Beach, CA 92075 (US).

(74) Agents: DUGAS, Edward et al.; Patent Division, NCR Corporation, World Headquarters, Dayton, OH 45479 (US).

(81) Designated States: CH (European patent), DE (European patent), FR (European patent), GB (European patent), JP.

Published
With international search report.

(54) Title: RANDOM NUMBER GENERATOR



(57) Abstract

A random number generator (10) provides randomly varying bits wherein the problems of biasing and auto-correlation are reduced in a circuit (30, 40, 42, 48) coupled to a noise generator and sampling circuit (12, 26). To reduce auto-correlation, the randomly varying bits are stored in a first shift register (30), the bits in the shift register being coupled to a second shift register (40). Second shift register (40) is clocked by a counter (48) responsive to the bits supplied to the first shift register so that clocking of the second shift register only takes place after a number of bits have been discarded by the first shift register. To reduce bias, the shift registers are coupled by EXCLUSIVE OR gates (42A-42N) and the outputs of the second shift register are coupled to inputs of the EXCLUSIVE OR gates.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**KP**	Democratic People's Republic of Korea
AU	Australia	**LI**	Liechtenstein
BR	Brazil	**LU**	Luxembourg
CF	Central African Republic	**MC**	Monaco
CG	Congo	**MG**	Madagascar
CH	Switzerland	**MW**	Malawi
CM	Cameroon	**NL**	Netherlands
DE	Germany, Federal Republic of	**NO**	Norway
DK	Denmark	**RO**	Romania
FI	Finland	**SE**	Sweden
FR	France	**SN**	Senegal
GA	Gabon	**SU**	Soviet Union
GB	United Kingdom	**TD**	Chad
HU	Hungary	**TG**	Togo
JP	Japan	**US**	United States of America

RANDOM NUMBER GENERATOR

Technical Field

The present invention relates to a random number generator.

Background Art

Random number generators are useful in data processing equipment in a number of different ways. For example, a random number generator can be used to generate keys for encrypting data transmitted over a transmission line, so that unauthorized tapping of the transmission line will not yield an understandable message.

One problem encountered in the past with random number generators is that it is very difficult to obtain a sequence of true (or nearly true) random numbers. That is, the numbers generated at the output of a random number generator are frequently either (1) biased or (2) auto-correlated. By "biased", it is meant that there is greater than a fifty per cent chance that each bit will be only one of the two binary values. By "auto-correlated", it is meant that the generated numbers tend to be periodic or cyclical.

Number generators generating numbers that appear random but that are actually periodic are sometimes referred to as pseudo-random number generators and, in many circumstances, are acceptable. However, in many other circumstances, such as in the generation of keys for data encryption, a non-periodic or "true" random sequence would be preferable.

U.S. Patent No. 4,095,192 recognizes the problem of biasing associated with random number generators and discloses a reverse biased diode for generating random noise signals coupled to isolating and filtering circuits which are effective to filter a portion of the power spectrum of the diode which has a

more gaussian distribution, thereby providing a more nearly random output. However, such circuits represent only an approximate method of dealing with the problem of biasing and do not deal at all with the problem of auto-correlation.

Disclosure of the Invention

It is an object of the invention to provide a random number generator wherein the problem of auto-correlation is alleviated.

The present invention provides a random number generator comprising means for providing successive and randomly varying bits, characterized by means for receiving the randomly varying bits for reducing auto-correlation in the randomly varying bits, including means for discarding certain ones of the randomly varying bits so that random numbers provided at the output of said random number generator do not depend on the discarded bits.

By discarding certain ones of the randomly varying bits, auto-correlation can be eliminated or reduced, as will become clear later.

It is another object of the invention to provide a random number generator wherein the problems of biasing are dealt with in a more effective manner than in the known arrangement described above.

There is thus provided a random number generator characterized by a circuit for receiving randomly varying bits of a random number and reducing the bias of the randomly varying bits, the circuit comprising a plurality of EXCLUSIVE OR gates, each of the EXCLUSIVE OR gates having an input for receiving one of the bits, and a register for storing the randomly varying bits and having a plurality of stages, each stage associated with one of the EXCLUSIVE OR gates and having an input connected to the output of its associated EXCLUSIVE OR gate and an output connected to the second input of its

associated EXCLUSIVE OR gate, so that the randomly varying bits are logically combined at the EXCLUSIVE OR gates with previous randomly varying bits stored in said register.

By providing logic gate means coupled to a register, the problem of biasing can be eliminated or at least reduced, as will become clear later.

Brief Description of the Drawing

The Figure in the drawings is a block diagram showing a random number generator in accordance with the present invention.

Best Mode for Carrying Out the Invention

Referring now to the drawings, there is shown a random number generator 10 in accordance with the present invention. The random number generator 10 generates random bits at its output in response to a randomly varying noise signal R_A produced by a noise generator 12.

The noise generator 12 is constructed in a conventional fashion and includes a resistor 14, a diode 16, a capacitor 18, and an amplifier 20. A reverse voltage +V is applied across the resistor 14 and diode 16, causing the diode 16 to operate in its avalanche region and produce current having a randomly varying component or signal. The randomly varying component of the current from the diode 16 is passed through capacitor 18 and amplified by the amplifier 20 to provide the signal R_A.

The randomly varying signal R_A at the output of the noise generator 12 is periodically sampled by a sampling register 26 that includes three flip-flops 26A, 26B and 26C. The flip-flops 26A, 26B and 26C are clocked by a clocking signal CLOCK, which determines the frequency with which the random signal R_A is sampled. A suitable frequency for the signal CLOCK is ten microseconds, which will provide random bits at the output of the

random number generator 10 at a frequency appropriate for data encryption. The output of the sampling register 26 is successive or serial randomly varying binary bits, each bit at either a logic level "0" or a logic level "1".

In the actual practice of the present invention, any number of flip-flops can be used to provide the sampling register 26. While in many circumstances only a single flip-flop would be necessary, the provision of plural flip-flops, such as the three illustrated flip-flops 26A, 26B and 26C, minimizes the possibility of undefined states appearing at the output of the sampling register 26. That is, as the randomly varying signal R_A varies between its minimum and maximum values, it may occasionally be sampled at a value which falls between the voltage ranges which represent the two binary values, so that the output of flip-flop 26A goes to an undefined state. The signal at the output of flip-flop 26A is successively sampled by flip-flops 26B and 26C in order to reduce the likelihood that the signal at the output of the sampling register will remain in this undefined state.

As those skilled in the art will appreciate, the signal R_A generated by the noise generator 12 and, consequently, the bits at the output of the sampling register 26, will normally have some degree of both biasing and auto-correlation.

In accordance with the present invention, and as will be more fully described later, the output of the sampling register 26 is provided to circuitry that discards certain ones of the randomly varying bits in order to minimize auto-correlation. In the random number generator 10, the circuitry for discarding the bits includes a first shift register 30 and a second register 40. The register 30 has a plurality of stages or flip-flops 30A through 30N, each paired with or connected to an associated one of a plurality of stages or flip-flops 40A through 40N in register 40.

In addition, the random number generator 10 has circuitry for minimizing biasing of the randomly varying bits, such circuitry including a plurality of EXCLUSIVE OR gates 42A through 42N that are associated with and connected between the associated pairs of flip-flops in the registers 30 and 40.

The number of stages in the registers 30 and 40 and the number of EXCLUSIVE OR gates 42A through 42N are the same and are equal to the number of bits provided in parallel at the output of the random number generator 10. For example, if a 32-bit random number is provided at the output, then there would be thirty-two stages in registers 30 and 40 and thirty-two EXCLUSIVE OR gates connected therebetween.

The registers 30 and 40 are clocked so that a random portion of the bits that are serially received by the register 30 are discarded and are not transferred from the register 30 to the register 40. This is accomplished, in accordance with one aspect of the present invention, by clocking the flip-flops 30A through 30N with the same signal CLOCK that is used to clock the flip-flops 26A through 26C in sampling register 26. The flip-flops 40A through 40N in register 40, however, are clocked by a circuit in the form of a counter 48 which is incremented by the output of the sampling register 26. Counter 48 will provide an enabling clock signal to the registers 40A through 40N only when it receives a predetermined number of logic level "1" bits from the output of sampling register 26.

In the preferred embodiment illustrated in the drawings, the counter 48 is a 5-bit counter, with the counter 48 only providing an enabling clock signal when it receives thirty-two logic level "1" from the sampling register 26. Since there will be a fairly even distribution of "1's" and "0's" at the output of sampling register 26, even with some inherent biasing, the register 40 is normally clocked only after a significant

number of bits in excess of thirty-two have been serially received by the first stage 30A of register 30. These excess bits are discarded at the last stage 30N of register 30 and, when register 40 is clocked, only the remaining thirty-two bits in register 30 are transferred or passed in parallel to the register 40 by way of the EXCLUSIVE OR gates 42A through 42N.

It should be apparent, of course, to one skilled in the art that the manner in which the registers 30 and 40 are clocked in order to discard certain ones of the bits could be done other than as shown in the drawings. However, the use of the counter 48, connected as shown, is preferred since in any given sequence of bits provided by the sampling register 26 the number of "1's" will vary and will more effectively randomize the occurrence of the enabling clock signal provided at the output of counter 48. The more random the enabling clock signal, the less likely it is that the output of the random number generator will have any repetitive characteristics. In addition, the larger the count of the counter 48, the more complete the elimination of auto-correlation at the output of the random number generator.

As mentioned above, the EXCLUSIVE OR gates 42A through 42N minimize the inherent bias that exists in the randomly varying bits that are provided at the output of the sampling register 26 and that are passed by the register 30 to the register 40. The EXCLUSIVE OR gates 42A through 42N each have one input connected to its associated stage in the register 30 and its output connected to the input of its associated stage in the register 40. The output of its associated stage in the register 40 is connected back to the second input of the EXCLUSIVE OR gate. In addition, the output of each stage in the register 40 is connected to an associated one of a plurality of stages 44A through 44N of an output register 44. The outputs of the stages in the

register 44 provide, in parallel, the output of the random number generator 10.

The output register 44 is clocked by a clocking circuit, designated 50, that provides an enabling clocking signal when the random number generator 10 is requested to provide a random number at its output. In order to further randomize the bits in the number generated by the random number generator 10 and, in particular, to more completely reduce the bias of the bits at the output of the random number generator 10, a second counter 52 is provided in the clocking circuit 50.

In the preferred embodiment, the counter 52 is, for example, a 4-bit counter. The counter 52 counts the enabling clock signals at the output of the counter 48 so that bits from the register 30 are repeatedly EXCLUSIVE ORed at the EXCLUSIVE OR gates 42A through 42N and stored in the register 40, before being passed to the output register 44. The output of the counter 52 is connected to the SET input of an SR flip-flop 54 that is in turn connected at its output to one input of AND gate 56 and to the data input of a flip-flop 58. A second input of the AND gate 56 is connected for receiving a signal REQUEST, which is received from an external source and is at a "1" when a random number is desired from the output of the random number generator 10. The output of the flip-flop 58 is normally at a "0" and is connected to the third input of the AND gate 56.

When the counter 52 reaches its full count, the flip-flop 54 is set and goes to a "1". When the signal REQUEST goes to a "1", the AND gate 56 provides an enabling clock signal to the flip-flops 44A through 44N in register 44 in order to provide the bits of a random number to the output of the random number generator 10. In addition, the output of AND gate 56 resets counter 52 and, at the same time, clocks the flip-flop 58 so that, momentarily later, the "1" at the output of SR flip-flop 54 is stored in flip-flop 58. The "1" in

flip-flop 58 is provided back to AND gate 56, to end the clock signal at its output.

The output of the flip-flop 58 is also connected to one input of an AND gate 62, whose output is connected to the reset input of the flip-flops 44A through 44N in the register 44. The second input of the AND gate 62 is connected for receiving the REQUEST signal, so that when the request ends and REQUEST goes to a "0", the output of AND gate 62 goes to a "1" in order to reset the flip-flops in the register 44.

It should be apparent from the foregoing that the random number generator 10 provides bits at its output that are neither biased nor periodic. As described above, by clocking the registers 30 and 40 so that bits in excess of the predetermined number needed for the output are shifted into register 30, and so that the excess bits are discarded before being passed to register 40, the inherent repetitiveness or auto-correlation of the randomly varying bits provided by the sampling register 26 is minimized. In addition, by causing the bits being passed from register 30 to register 40 to also be EXCLUSIVE ORed with bits previously stored in register 40, and by also clocking the register 44 so that the EXCLUSIVE ORing is repeated, the inherent biasing of the randomly varying bits is minimized.

Although the presently preferred embodiment of this invention has been described, it will be understood that within the purview of this invention various changes may be made within the scope of the appended claims.

CLAIMS:

1. A random number generator (10) comprising means (12, 26) for providing successive and randomly varying bits, characterized by means for receiving the randomly varying bits for reducing auto-correlation in the randomly varying bits, including means (30, 40, 48) for discarding certain ones of the randomly varying bits so that random numbers provided at the output of said random number generator do not depend on the discarded bits.

2. A random number generator according to claim 1, characterized in that said means for discarding comprises a first shift register (30) for serially receiving the randomly varying bits, and for providing an output comprising in parallel only a portion of the bits received by the register, a second shift register (40) connected for receiving in parallel bits whose values are dependent on the output of the first shift register, and the second shift register providing an output comprising the bits received by the second shift register.

3. A random number generator (10) according to claim 2, characterized in that the first shift register is arranged to store a predetermined number of the randomly varying bits and has a plurality of stages (30A-30N), including a first stage (30A) and a last stage (30N), each stage for storing one of the bits, whereby the first shift register discards the one of the bits in the last stage (30N) when one of the bits is received in the first stage (30A), and in that the second shift register is arranged to store the same predetermined number of bits, and further characterized by means for clocking (48) the second shift register to receive an input only after a number in excess of the

3. (concluded)
predetermined number of bits have been serially received in said first shift register and at least one of the bits has been discarded in said first shift register.

4. A random number generator according to claim 3, characterized in that the means for clocking the second shift register comprises a first binary counter (48) having an input connected for receiving the successive random bits, the count in the first counter being incremented by bits having one predetermined binary value, the first counter having an output connected for providing an enabling clock signal to the second register upon said count reaching a predetermined value.

5. A random number generator according to claim 2, characterized by circuit means for reducing bias in the randomly varying bits, including logic gate means (42A-42N) connected between the first register and the second register in order to logically combine said only a portion of the bits provided as an output by the first shift register with the bits provided as an output by the second shift register.

6. A random number generator according to claim 5, characterized in that said logic gate means comprises a plurality of EXCLUSIVE OR gates (42A-42N), each of the EXCLUSIVE OR gates having an input for receiving one of the bits provided as an output by the first shift register, the second shift register having a plurality of stages (40A-40N), each stage associated with one of the EXCLUSIVE OR gates and having an input connected to the output of its associated EXCLUSIVE OR gate and an output connected to a second input of its associated EXCLUSIVE OR gate, so that the randomly varying bits are logically combined at the EXCLUSIVE OR

6. (concluded)
gates with previous randomly varying bits stored in the second shift register.

7. A random number generator according to claim 1, characterized in that said means (12, 26) for providing successive and randomly varying bits, comprises means (12) for generating a randomly varying signal, and means (26) for periodically sampling said randomly varying signal and providing the sampled signals as the randomly varying binary bits.

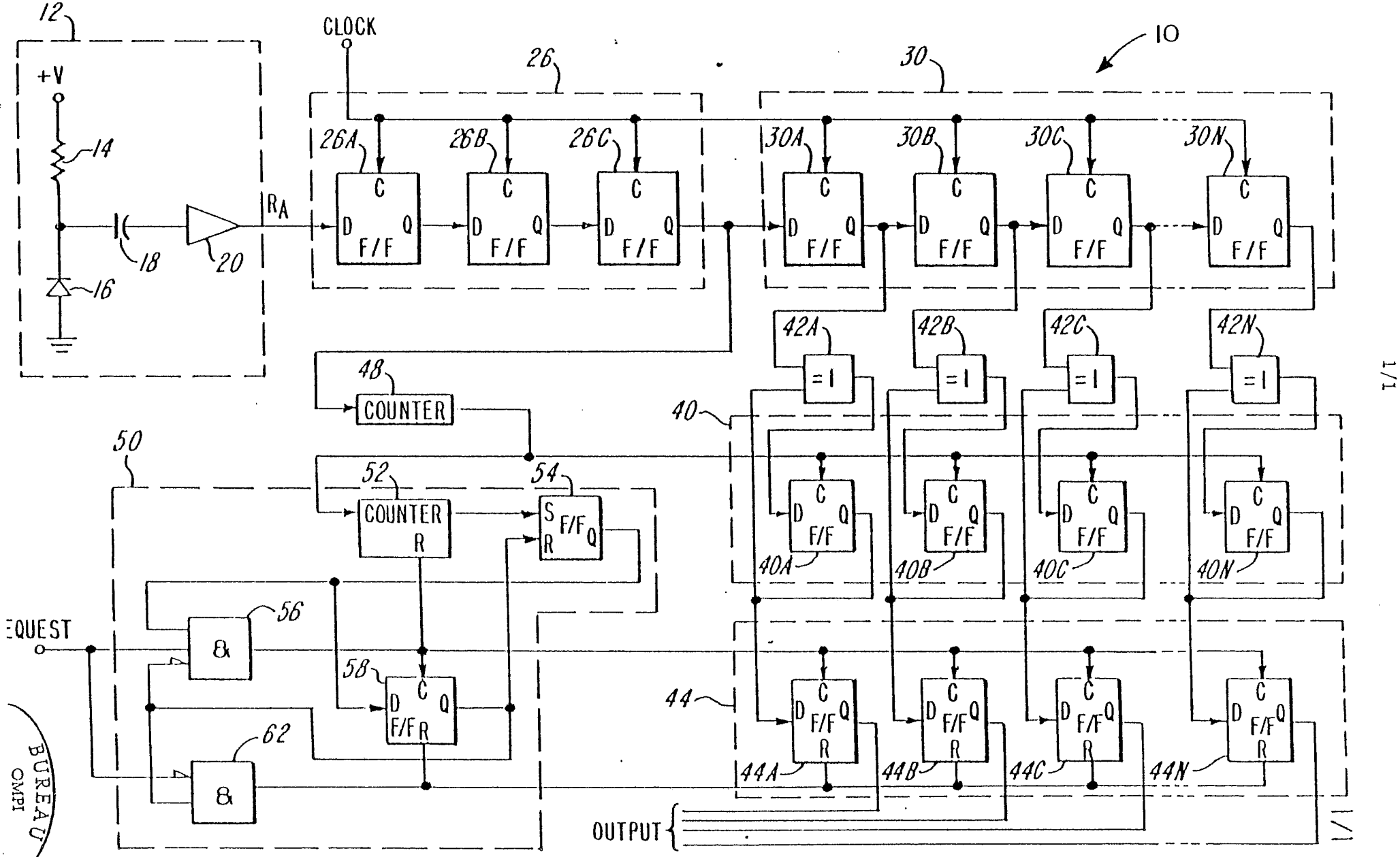
8. A random number generator according to claim 3, characterized by a third shift register (44) having a plurality of stages (44A-44N), each stage for receiving the bit stored in an associated one of the stages in said second register (40), the third shift register (44) being clocked at intervals greater than the intervals at which the second shift register is clocked.

9. A random number generator according to claim 8, characterized by clocking circuitry (50) for providing an enabling clock signal to the third shift register (44), said clocking circuitry including a second counter (52) having its input connected to the output of said first counter (48).

10. A random number generator characterized by a circuit (30, 40, 42) for receiving randomly varying bits of a random number and reducing the bias of the randomly varying bits, the circuit comprising a plurality of EXCLUSIVE OR gates (42A-42N), each of the EXCLUSIVE OR gates having an input for receiving one of the bits, and a register (40) for storing the randomly varying bits and having a plurality of stages (40A-40N), each stage associated with one of the EXCLUSIVE OR gates

10. (concluded)

and having an input connected to the output of its associated EXCLUSIVE OR gate and an output connected to the second input of its associated EXCLUSIVE OR gate, so that the randomly varying bits are logically combined at the EXCLUSIVE OR gates with previous randomly varying bits stored in said register.


12
+V
14
16
18
20
R_A
CLOCK
10
26
30
26A
26B
26C
30A
30B
30C
30N
C
D
Q
F/F
42A
42B
42C
42N
=1
48
COUNTER
40
50
52
54
COUNTER
R
S
R
F/F
Q
40A
40B
40C
40N
EQUEST
56
&
58
D
C
Q
F/F
R
44
62
44A
44B
44C
44N
OUTPUT
BUREAU
OMPI
1/1

INTERNATIONAL SEARCH REPORT

International Application No PCT/US81/01519

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

INT . CL.[3] H03K 3/84
US. CL. 364/717

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
U.S.	364/717 331/78 178/22.15

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [5]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
X	US,A, 3,790,768 Published 05 February 1974, Chevalier et al	1-10
A	US,A, 3,691,472 Published 12 September 1972, Bohman	1-10
A	US,A, 4,115,657 Published 19 September 1978, Morgan	1-10

* Special categories of cited documents: [15]

"A" document defining the general state of the art

"E" earlier document but published on or after the international filing date

"L" document cited for special reason other than those referred to in the other categories

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but on or after the priority date claimed

"T" later document published on or after the international filing date or priority date and not in conflict with the application, but cited to understand the principle or theory underlying the invention

"X" document of particular relevance

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
01 February 1982	19 FEB 1982
International Searching Authority [1]	Signature of Authorized Officer [20]
ISA/US	D.H. Marzahn

Form PCT/ISA/210 (second sheet) (October 1977)