



(51) International Patent Classification:
G06F 7/58 (2006.01) **G06F 9/06** (2006.01)

Putra World Trade Centre, 45, Jalan Tun Ismail 50480
Kuala Lumpur (MY).

(21) International Application Number:
PCT/MY2009/000172

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date:
20 October 2009 (20.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20084170 20 October 2008 (20.10.2008) MY

(71) Applicant (for all designated States except US): **MIMOS BERHAD** [MY/MY]; Technology Park of Malaysia, Bukit Jalil, 5700 Kuala Lumpur (MY).

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **NORASHIKIN, Binti, M., Thamrin** [MY/MY]; Mimos Berhad, Product Development, Information Securiy, Technology Park of Malaysia, Bukit Jalil 5700 Kuala Lumpur (MY). **GU-NAWAN, Witjakson** [MY/MY]; Mimos Berhad, Product Development, Information Securiy, Technology Park of Malaysia, Bukit Jalil 5700 Kuala Lumpur (MY).

Published:

(74) Agent: **MOHAN, K.**; Adastra Intellectual Property Sdn Bhd, P.O. Box 43, Suite 2B, Level 7, Menara Dato'Onn,

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: AUTOCORRELATION CIRCUIT FOR RANDOM NUMBER GENERATOR

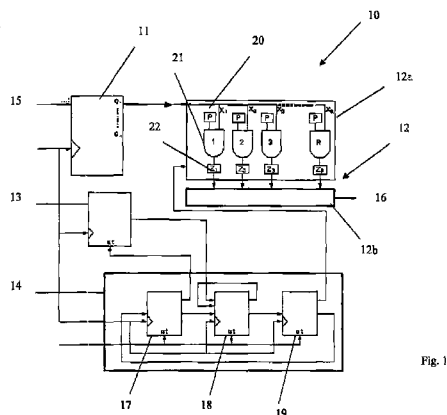


Fig. 1

(57) Abstract: A system (10) for eliminating autocorrelation bits in random number comprising a random number generator for generating a series of random bits (15), a shift register (11) having a predetermined bit length for serially receiving the randomly varying bits (15) and produce a parallel output, a counter (13) having its maximum value determined by the shift register (11) and clocked by a clocking signal, CLK which is same with the shift register (11) to count the shifted bits, and an eliminator module (12) which is activated by the counter (13) when the shifted bits have reached the maximum value, wherein the eliminator module (12) will then identify the contiguous zero and one bits and discard the unwanted bits to produce an uncorrelated random number (16).



Autocorrelation Circuit for Random Number Generator**Field of Invention**

5 The present invention relates generally to the field of random number generator and more particularly to a system and method for eliminating autocorrelation in random numbers.

Background of the Invention

10

Random numbers are essential in various fields, such as scientific computation fields, games, mathematical statistics, data protection, technological processes, communication security for example it is used to generate keys for
15 encrypting data transmitted over a transmission line to avoid unauthorized tapping of the transmission line. Random number generators (RNG) are divided into two basic types. RNGs that base their output on a physical source of randomness which generate numbers from a non-deterministic source, are known as
20 True Random Number Generators (TRNGs). RNGs that are given an initial random seed and thereafter generate random-seeming numbers in a deterministic way are known as Pseudo Random Number Generators (PRNGs).

25 The drawback of the random number generator is that it is difficult to obtain a sequence of true random numbers. This is

because, the numbers generated at the output of a random number generator are either biased or autocorrelated. In the situation where the numbers are biased, it is meant that there is greater than a fifty per cent chance that each bit will be
5 only one of the two binary values.

An autocorrelation is a phenomenon where signals tend to be periodic, cyclical or there is a predictable relationship between parts of the same signal. In random number generator,
10 especially when a hardware random number generator is used, the occurrence of autocorrelation can cause the random signal to have a periodic pattern in certain time, by producing a contiguous bit 1's and 0's and this is extremely intolerable. If this happen, the random bits is predicted and the security
15 of the generated number can be compromised. Furthermore, the presence of autocorrelation can significantly contribute to the failure of available and standard statistical tests in testing the randomness of the generated random bits. Figure 1 shows an example of bad random sequence that contains the
20 repetitive pattern caused by autocorrelation.

The present invention has overcome the drawbacks of the existing methods by providing a hardware random number generator, a shift register, eliminator module, counter and a
25 controller module to provide the uncorrelated random number.

An objective of the present invention is to provide a circuit that can reduce or eliminate autocorrelation problem in a random binary strings produced by a true random number generator.

5

Yet another objective of the present invention is to provide a random number generator that is simple in design and inexpensive to manufacture.

10 These and other advantages will become apparent to those skilled in this art upon reading the following detailed description in conjunction with the accompanying drawings.

Summary of the Invention

15

In the present invention, a system for eliminating autocorrelation bits in random number comprising a random number generator for generating a series of random bits, a shift register having a predetermined bit length, coupled to
20 the random number generator for serially receiving the randomly varying bits and produce a parallel output, a counter connected to the shift register, the counter having its maximum value determined by the shift register and clocked by a clocking signal, CLK which is same with the shift register
25 to count the shifted bits;, and an eliminator module which is activated by the counter when the shifted bits have reached

the maximum value, wherein the eliminator module will then identify the contiguous zero and one bits and discard the unwanted bits.

- 5 In accordance to the invention, the eliminator module includes an identifier unit and a removal unit. The identifier unit comprises a plurality of AND gates with a predefined N integer of average number of contiguous bits of zero and one.
- 10 In accordance to the invention, the system further comprising a control unit which controls all the signals flow in the system.

A method for eliminating autocorrelation bits in random number
15 generated by a random number generator, the method comprising the steps of generating a series of random bits, shifting the random bits and producing a parallel output, counting the shifted bits to determine whether the bits have reached its maximum value, and eliminating autocorrelation in the random
20 bits by identifying the contiguous zero and one bits and discarding the excessive bits.

Brief Description of the Drawings

- 25 Other objects, features, and advantages of the invention will be apparent from the following description when read with

reference to the accompanying drawings. In the drawings, wherein like reference numerals denote corresponding parts throughout the several views:

5 Fig. 1 shows a block diagram illustrating the configuration of a system for eliminating autocorrelation effect in random numbers of the present invention; and

Fig. 2 is a flowchart of the control unit of the system.

10

Detailed Description of the Preferred Embodiments

In the following detailed description, numerous specific details are set forth in order to provide a thorough
15 understanding of the invention. However, it will be understood by those of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known methods, procedures and/or components have not been described in detail so as not to obscure the
20 invention. Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

Fig. 1 is a block diagram illustrating the configuration of a
25 system (10) capable of eliminating autocorrelation effect in random strings produced by a random number generator (RNG)

according to an exemplary embodiment of the present invention. The random number generator system (10) incorporates a shift register (11), an eliminator module (12), a counter (13) and a control unit (14). The random number generator (RNG) is operable to output a series of random numbers. Random number means any sequence of binary signals, a Gaussian or any other distribution of signals, a sequence of signals representing a number between zero and one, a sequence of signals representing a decimal number, or any other form that includes the desired randomness.

A string of serial input (15) generated from the random number generator unit (not shown) is input to the system (10) to produce an uncorrelated random number (16). This serial input (15) is fed into the shift register (11) for serially receiving the randomly varying bits and produce a parallel output for easier elimination process later. The eliminator module (12) is divided into two units namely an identifier unit (12a) which consists of chain of AND gates (12a) and a removal unit (12b) as shown in Fig. 1. The serial input (15) passes through an n-bit shift register (11) which determines the number of AND gates (12a) going to be used later.

The counter (13) is connected to the shift register (11). When the n-bit shift register (11) receives the input (15) from the random number generator, the n-bit counter (13) is activated.

The shift register (11) is clocked by a clocking signal, CLK and the CLK for the shift register (11) is the same CLK for the counter (13). The counter (13) increases the counting steps whenever it detects the rising edge of the CLK as the data is shifted in the shift register (11). This counter (13) is used to count the number of inputs received by the shift register (11) and if the maximum value is achieved, it starts the eliminator module (12) to eliminate autocorrelation in the random number.

The control unit (14) operates as the main control processing unit in the system (10). The control unit (14) receives counter value from the counter (13) and invokes the 'start' signal to start the elimination process. There are three stages of registers in the control unit (14), which are first register, REG1 (Start) (17), second register, REG2 (Wait) (18) and third register, REG3 (Execute) (19). Whenever the system (10) is powered up or idles, the current state is always at first register, REG1 (17) as shown in Fig. 2. Once the system (10) starts, the state moves to second register, REG2 (18) where it receives counter value from the counter (13). If the value reaches its maximum value which means that the shift register (11) is full and the elimination process can be started. Third register, REG3 (19) will then invokes 'start' signal to the eliminator module (12).

The identifier unit (12a) of the eliminator module (12) comprises a plurality of AND gates (21) to identify the contiguous bits 1's and 0's before discard them through the removal unit (12b). The number of AND gates, (R) can be
 5 determined by dividing the total n-bits in the shift register (11) with N number of bits'1 and 0's to be eliminated by means of equation (1) below:

$$R = n \text{ DIV } N \quad (1)$$

10 For a better implementation, the remainder from the division should be 0. If the total number of AND gates (21), R is known, the AND gates (21) are cascaded. The P value (20) as shown in Fig. 2 is the number of desired N number of contiguous bits 1's and 0's to be discarded. It is hard-coded
 15 in a storage means (22) which is a buffer and can be called by multiple of AND gates (21). The $X_1, X_2, X_3 \dots X_R$ is a part of the n-bits of shifted input. It can be determined as:

$$X_1 = Q_0 \rightarrow Q_{N1}$$

20

$$X_2 = Q_{N1-1} \rightarrow Q_{N2}$$

$$X_3 = Q_{N2-1} \rightarrow Q_{N3}$$

;

$$X_R = Q_{NR-2} \rightarrow Q_R$$

25

Where,

$$N_1 = N$$

$$N_2 = N_1 + N$$

$$N_3 = N_1 + 2N$$

5

;

$$N_R = N_1 + (R-1)N$$

The results of AND process is stored in buffers (22) for further process. The produce bits in these buffers (22) are in
10 N size for each, $Z_1, Z_2, Z_3 \dots Z_R$.

In the removal unit (12b), it discards any Z_i value that contains all 1's and concatenates the accepted sequence. The condition of removal unit (12b) is as below: -

15

For i = 0 to R

If $Z_i = "111..1_N"$ or $Z_i = "000..0_N"$ then

Null;

Else

20

$Y = Y || Z_i;$

Next i

This system (10) is necessary in producing a string of random bits that is not correlated to itself after certain of time.
25 As a result, the produced random number can be made more random and autocorrelation defect can be removed.

As will be readily apparent to those skilled in the art, the present invention may easily be produced in other specific forms without departing from its essential characteristics. The present embodiments is, therefore, to be considered as
5 merely illustrative and not restrictive, the scope of the invention being indicated by the claims rather than the foregoing description, and all changes which come within therefore intended to be embraced therein.

Claims

1. A system (10) for eliminating autocorrelation bits in random number comprising:

- 5 a random number generator for generating a series of random bits (15);
- a shift register (11) having a predetermined bit length, coupled to said random number generator for serially receiving said randomly varying bits (15) and produce a parallel output;
- 10 a counter (13) connected to said shift register (11), said counter (13) having its maximum value determined by said shift register (11) and clocked by a clocking signal, CLK which is same with said shift register (11) to count the shifted bits; and
- 15 an eliminator module (12) which is activated by said counter (13) when said shifted bits have reached said maximum value, wherein said eliminator module (12) will then identify the contiguous zero and one bits and discard the unwanted bits to produce an uncorrelated random number (16).

20

2. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 1, wherein said eliminator module (12) includes an identifier unit (12a) and a removal unit (12b).

25

3. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 2, wherein said identifier unit (12a) comprises a plurality of AND gates (21) with a predefined N integer of average number of contiguous bits of zero and one.

4. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 3, wherein said N integer is the number of contiguous bits of zero and one to be eliminated and gathered from the results of AND gates (21) process.

5. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 4, wherein said contiguous bits of zero and one to be eliminated is stored in storage means (22).

6. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 5, wherein said storage means (22) is buffer.

7. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 5, wherein said unwanted contiguous bits stored in storage means is removed by said removal unit (12b).

8. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 1, wherein said system (10) further comprising a control unit (14) which controls all the signals flow in said system (10).

5

9. The system (10) for eliminating autocorrelation bits in random number as claimed in claim 8, wherein said control unit (14) comprising:

a first register REG1 (17) as initial stage of operation;

10 a second register REG2 (18) connected to said first register (17) and said counter (13) to receive signals flow from said first register (17) when said system (10) starts and to receive counter value from said counter (13); and

a third register REG3 (19) connected to said second register
15 (18) and eliminator module (12) to receive invoke signal from said second register (18) when said maximum value of said counter (13) is reached and to activate said eliminator module (12).

20 10. A method for eliminating autocorrelation bits in random number generated by a random number generator, the method comprising the steps of:

generating a series of random bits;

shifting said random bits and producing a parallel output;

25 counting the shifted bits to determine whether said bits have reached its maximum value; and

eliminating autocorrelation in said random bits by identifying the contiguous zero and one bits and discarding the excessive bits.

- 5 11. The method for eliminating autocorrelation bits in random number as claimed in claim 10, wherein said method further comprising the step of invoking for eliminating process by a control unit (14) from said step of counting.

1/2

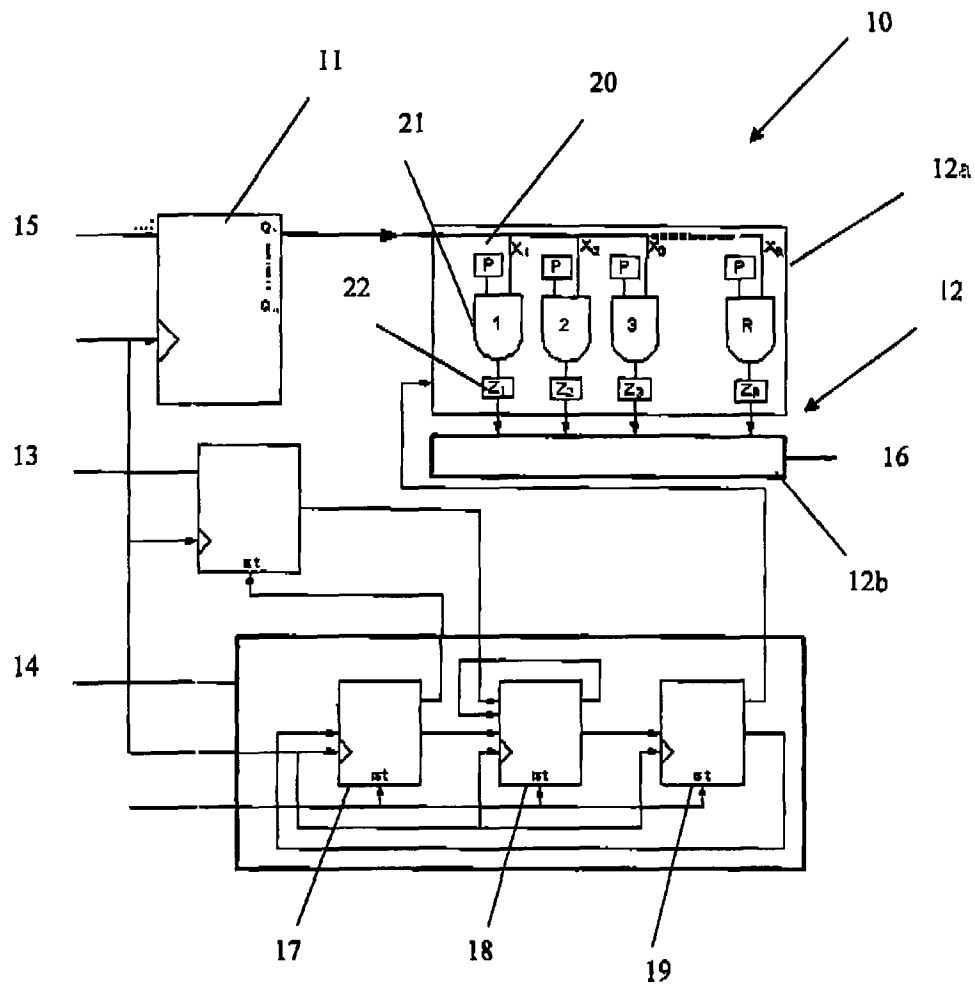


Fig. 1

2/2

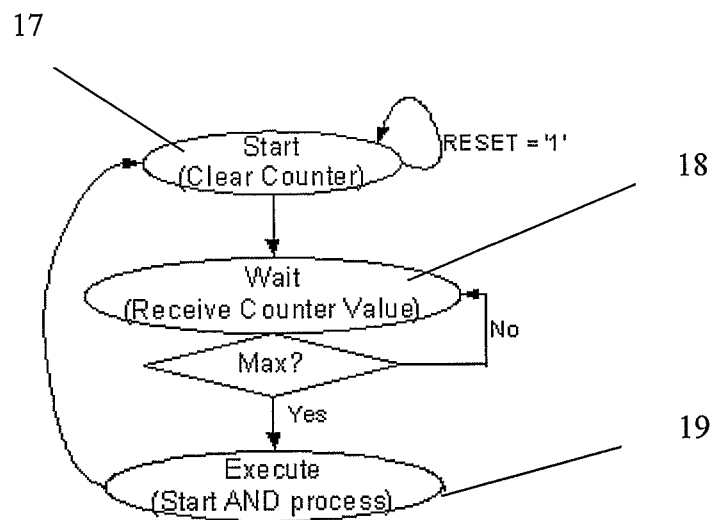


Fig. 2