(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 March 2004 (04.03.2004)

PCT

(10) International Publication Number
WO 2004/019203 A2

(51) International Patent Classification[7]: G06F 7/00

(21) International Application Number:
PCT/IB2003/003659

(22) International Filing Date: 15 August 2003 (15.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/224,992 21 August 2002 (21.08.2002) US

(71) Applicant: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for AE only)*: **U.S. PHILIPS CORPORATION** [US/US]; 1251 Avenue of the Americas, New York, NY 10020 (US).

(72) Inventor: **LASZLO, Hars**; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(74) Common Representative: **KONINKLIJKE PHILIPS ELECTRONICS N.V.**; c/o Goodman, Edward, W., P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

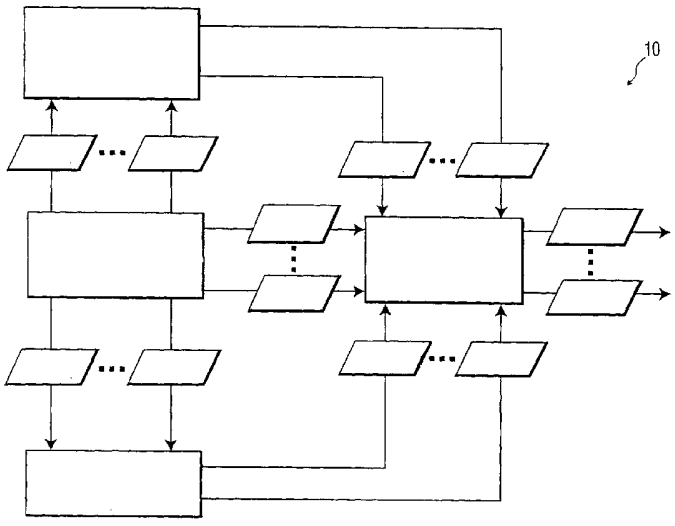
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ENTROPY ESTIMATION AND DECIMATION FOR IMPROVING THE RANDOMNESS OF TRUE RANDOM NUMBER GENERATION



(57) Abstract: A random number generating system operates to generate an output number bit sequence based on an entropy estimation of a true random number bit sequence, the randomness of the output number bit being an improvement of the randomness of the true random number bit sequence. A physical random number generator (20) communicates the true random number bit sequence to an entropy estimator (40), which generates an estimation signal indicative of the randomness of the true random number bit sequence. The estimation signal is communicated to a decimator (50) whereby, in accordance with estimation signal, the decimator (50) generates the output number bit as a representation of a decimation of a mixing of the true random number bit sequence and the pseudo random number bit sequence, or as a representation of a decimation of the psuedo random number bit sequence when the pseudo random number bit sequence is generated as a function of the true random number bit sequence.

WO 2004/019203 A2

ENTROPY ESTIMATION AND DECIMATION FOR IMPROVING THE RANDOMNESS OF TRUE RANDOM NUMBER GENERATION

TECHNICAL FIELD

[0001] The present invention generally relates to physical random number generators (i.e., a device that generates a bit or bits representative of a number by operating one or more components of the device in an undeterminable manner) and pseudo random number generators (i.e., a device that inputs a random number bit or bits to generate pseudo random number bit sequence(s) based upon an algorithm). The present invention specifically relates to an employment of one or more physical random number generators and one or more pseudo random number generators in yielding an unbiased sequence of random number bits.

BACKGROUND AND SUMMARY OF THE INVENTION

[0002] Physical random number generators as known in the art generate a random number bit or bits by operating one or more components of the device in an undeterminable manner. Conceptually, the undeterminable operation of the component(s) yields an unbiased random generation of the random number bit(s). In practice, the undeterminable operation of the component(s) typically yields a biased random generation of the random number bit(s) due to various tolerances related to the operation of the component(s). Pseudo random number generators as known in the art are employed to rectify the biased random generation of the random number bit(s) to an acceptable degree.

[0003] The present invention additionally employs an entropy estimator and a decimator to further improve upon the randomness of a true random number bit sequence. Various aspects of the present invention are novel, non-obvious, and provide various advantages. While the actual nature of the present invention covered herein can only be determined with reference to the claims appended hereto, certain features, which are characteristic of the embodiments disclosed herein, are described briefly as follows.

[0004] The present invention is a random number generation system comprising a physical random number generator a pseudo random number generator, an entropy estimator, and a decimator. The physical random number generator operates to generate one or more true random number bit sequences. The pseudo random number generator operates to generate one or more pseudo random number bit sequences. The entropy estimator operates to generate one or more estimation signals as an indication of a randomness of the true random number bit sequence(s). In one form, the decimator operates to generate one or more output number bit sequences representative of a decimation of a mixing of the one or more true random number bit sequences and the one or more pseudo number bits in accordance with the one or more estimation signal(s). In a second form, the pseudo random number bit sequence(s) are generated as a function of the true random number bit sequence(s) and the output number bit sequences(s) are a representation of a decimation of the pseudo random number bit sequence(s) in accordance with the estimation signal(s).

[0005] The foregoing forms as well as other forms, features and advantages of the present invention will become further apparent from the following detailed description of the presently preferred embodiments, read in conjunction with the accompanying drawings. The detailed description and drawings are merely illustrative of the present invention rather than limiting, the scope of the present invention being defined by the appended claims and equivalents thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 illustrates a block diagram of a basic embodiment of a random number generation system in accordance with the present invention;

[0007] FIG. 2 illustrates a block diagram of a first embodiment of the FIG. 1 random number generation system in accordance with the present invention;

[0008] FIG. 3 illustrates a block diagram of a second embodiment of the FIG. 1 random number generation system in accordance with the present invention; and

[0009] FIG. 4 illustrates a block diagram of a third embodiment of the FIG. 1 random number generation system in accordance with the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

[0010] FIG. 1 illustrates a random number generation system 10 (hereinafter "system 10") comprising a physical random number generator 20 (hereinafter "PHNG 20"), a pseudo random number generator 30 (hereinafter "PSNG 30"), an entropy estimator 40, and a decimator 50. The PHNG 20 is in communication with the entropy estimator 40 to thereby provide one or more true random number bit sequences $TRNB_1$-$TRNB_X$ to the entropy estimator 40. The PHNG 20 can also be in communication with the decimator 50 to thereby provide the true random number bit sequences $TRNB_1$-$TRNB_X$ to the decimator 50. The entropy estimator 40 is in communication with the decimator 50 to thereby provide one or more estimation signals ES_1-ES_Y to the decimator 50. The PSNG 30 is in communication with the decimator 50 to thereby provide one or more pseudo random number bit sequences $PRNB_1$-$PRNB_Z$ to the decimator 50. The PSNG 30 can be in communication with the PHNG 20 as illustrated whereby one or more of the pseudo random number bit sequences $PRNB_1$-$PRNB_Z$ are generated as a function of one or more of the true random number bit sequences $TRNB_1$-$TRNB_X$. In accordance with the estimation signal(s) ES_1-ES_Y, the decimator 50 generates one or more output number bit sequences ONB_1-ONB_A representative of a decimation of a mixing of the true random number bit sequence(s) $TRNB_1$-$TRNB_X$ and the pseudo random number bit sequence(s) $PRNB_1$-$PRNB_Z$ or representative of a decimation of the pseudo random number bit sequence(s) $PRNB_1$-$PRNB_Z$.

[0011] The number of configurations of the PHNG 20, the PSNG 30, the entropy estimator 40, and the decimator 50 is without limit. Additionally, the aforementioned communications among the PHNG 20, the PSNG 30, the entropy estimator 40, and the decimator 50 can be achieved in numerous ways (e.g., electrically, optically, acoustically, and/or magnetically). The number of embodiments of the system 10 is therefore essentially limitless. FIGS. 2-4 illustrate exemplary embodiments of the system 10.

[0012] FIG. 2 illustrates a random number generation system 11 (hereinafter "system 11") as one embodiment of system 10 (FIG. 1). The system 11 includes a physical random number generator 21 (hereinafter "PHNG 21") for generating a true random number bit sequence $TRNB_1$ (X=1), and a pseudo random number generator 24 (hereinafter "PSNG 31") for generating a pseudo random number bit sequence $PRNB_1$ (Z=1). The PHNG 21 and the PSNG 31 may be in embodied in software, hardware, or a combination of software and hardware. In one embodiment of the PHNG 21, the PHNG 21 is configured in accordance with a U.S. Patent Application Serial No. [FILL IN} entitled "Latching Electronic Circuit For Random Number Generation", the entirety of which is hereby incorporated by reference and commonly owned by the assignee. In a second embodiment of the PHNG 21, the PHNG 21 is configured in accordance with a U.S. Patent Application Serial No. [FILL IN} entitled "Switching Electronic Circuit For Random Number Generation", the entirety of which is hereby incorporated by reference and commonly owned by the assignee. In one embodiment of the PSNG 24, the PSNG 24 is configured in accordance with a U.S. Patent Application Serial No. [FILL IN} entitled "Linear Feedback Shift Register For Improving A Randomness Of A Physical Random Number Generator", the entirety of which is hereby incorporated by reference and commonly owned by the assignee. With this embodiment, the true random number bit sequence $TRNB_1$ can be

communicated to the PSNG 31 by the PHNG 21 whereby the pseudo random number bit sequence $PRNB_1$ is a function of the true random number bit sequence $TRNB_1$.

[0013] The system 11 further includes an entropy estimator 41 for generating an estimation signal ES_1 (Y=1) as a function of the true random number bit sequence $TRNB_1$. The entropy estimator 41 can be embodied in software, hardware, or a combination of software and hardware. In one embodiment, the entropy estimator 41 employs a conventional method of measuring a largest randomness error in the generation of the true random number bit sequence $TRNB_1$ as would occur to one having skill in the art. The accuracy of the estimation signal ES_1 can be enhanced with a running averaging or an exponential averaging of the measurements. When security is a high priority, the entropy estimator 41 can further employ one or more conventional randomness test algorithms and/or one or more conventional attack detectors.

[0014] The system 11 further includes a decimator 51 having a logic component in the form of an XOR gate 53 that receives the true random number bit sequence $TRNB_1$ and the pseudo random number bit $PRNB_1$. Alternatively, other logic components consisting of one or more logic circuits can be utilized in lieu of XOR gate 53. The decimator 51 further includes a counter 54. The output of the XOR gate is communicated to a data input DI of the counter 54, and the estimation signal ES_1 is communicated to a selection input SI of the counter 54. In accordance with the estimation signal ES_1, the counter 54 generates an output number bit sequence ONB_1 (A=1) as a representation of a decimation of a mixing of the true random number bit sequence $TRNB_1$ and the pseudo random number bit sequence $PRNB_1$.

[0015] Preferably, the PSNG 21, the PHNG 31, the entropy estimator 41, and the counter 54 are synchronously operated by a clock signal CS as illustrated in FIG. 2. Alternatively, one or more of the PSNG 21, the PHNG 31, the entropy estimator 41, and the counter 54 can be synchronously operated in a different manner and/or asynchronously operated.

[0016] FIG. 3 illustrates a random number generation system 12 (hereinafter "system 12") as one embodiment of system 10 (FIG. 1). The system 12 includes the PSNG 21, the PHNG 31, and the entropy estimator 41 as previously described herein in connection with FIG. 2. To enhance the mixing of the true random number bit sequence $TRNB_1$ and the pseudo random number bit sequence $PRNB_1$, the system 12 further includes a decimator 52 including the XOR gate 53, the counter 54, and a bi-stable latch in the form of a D-type flip-flop 55. The flip-flop 55 has a clock input receiving the true random number bit sequence $TRNB_1$ and an inverted output Q providing a latched random number bit LRNB to a data input D of the flip-flop 55 and an input of the XOR gate 53. Alternatively, other types of bi-stable latches may be utilized in lieu of the flip-flop 55.

[0017] FIG. 4 illustrates a random number generation system 13 (hereinafter "system 13") as one embodiment of system 10 (FIG. 1). The system 13 includes the PSNG 21, the entropy estimator 41, and the counter 54 as previously described herein in connection with FIG. 2. For system 13, a PHNG 32 generates the pseudo random number bit sequence $PRNB_1$ as a function of the true random number bit sequence $TRNB_1$ and communicates the pseudo random number bit sequence $PRNB_1$ to the data input DI of the counter 54. In response thereto, the counter 54 generates the output number bit sequence ONB_1 (A=1) as a representation of a decimation of the pseudo random number bit sequence $PRNB_1$ in accordance with the estimation signal ES_1.

[0018] While the embodiments of the present invention disclosed herein are presently considered to be preferred, various changes and modifications can be made without departing from the spirit and scope of the present invention. The scope of the present invention is indicated in the appended claims, and all changes that come within the meaning and range of equivalents are intended to be embraced therein.

FOREIGN CLAIMS AND ABSTRACT:

1. A random number generating system, comprising:

a physical random number generator (20) operable to generate one or more true random number bit sequences;

a pseudo random number generator (30) operable to generate one or more pseudo random number bit sequences;

an entropy estimator (40) operable to generate one or more estimation signals indicative of a randomness of the one or more true random number bit sequences; and

a decimator (50) operable to generate one or more output number bit sequences representative of a decimation of a mixing of the one or more true random number bit sequences and the one or more pseudo random number bit sequences in accordance with the one or more estimation signal(s).

2. The random number generating system of claim 1, wherein said pseudo random number generator (30) generates the one or more pseudo random number bit sequences as a function of the one or more true random number bit sequences.

3. A random number generating system, comprising:

a physical random number generator (20) operable to generate one or more true random number bit sequences;

a pseudo random number generator (30) operable to generate one or more pseudo random number bit sequences;

an entropy estimator (40) operable to generate one or more estimation signals indicative of a randomness of the one or more true random number bit sequences; and

a decimator (50) operable to generate one or more output number bit sequences as a representation of a decimation of the one or more of the

pseudo random number bit sequences in accordance with the one or more estimation signal(s).

4. The random number generating system of claim 3, wherein said pseudo random number generator (30) generates the one or more pseudo random number bit sequences as a function of the one or more true random number bit sequences.

5. A random number generating system, comprising:

a physical random number generator (20) operable to generate a true random number bit sequence;

a pseudo random number generator (30) operable to generate a pseudo random number bit sequence;

an entropy estimator (40) operable to generate an estimation signal indicative of a randomness of the true random number bit sequence; and

a decimator (50) operable to generate an output number bit sequence as a representation of decimation of a mixing of the true random number bit sequence and the pseudo number bit sequence in accordance with the estimation signal.

6. The random number generating system of claim 5, wherein said decimator (50) includes

a logic component (53) operable to input the true random number bit sequence and the psuedo random number bit sequence.

7. The random number generating system of claim 6, wherein said decimator (50) includes a counter (54) operable to input an output of said logic component (53).

8. The random number generating system of claim 6, wherein said decimator (50) includes a counter (54) operable to input the estimation signal and an output of said logic component (53).

9. The random number generating system of claim 5, wherein said decimator (50) includes

a bi-stable latch (55) operable to input the true random number bit sequence, and

a logic component (53) operable to input the psuedo random number bit sequence and an output of said bi-stable latch (55).

10. The random number generating system of claim 9, wherein said decimator (50) includes a counter (54) operable to input an output of said logic component (53).

11. The random number generating system of claim 9, wherein said decimator (50) includes a counter (54) operable to input the estimation signal and an output of said logic component (53).

12. The random number generating system of claim 5, wherein said pseudo random number generator (30) generates the pseudo random number bit sequence as a function of the true random number bit sequence.

13. A random number generating system, comprising:

a physical random number generator (20) operable to generate a true random number bit sequence;

a pseudo random number generator (30) operable to generate a pseudo random number bit sequence;

an entropy estimator (40) operable to generate an estimation signal indicative of a randomness of the true random number bit sequence; and

a decimator (50) operable to generate an output number bit sequence as a representation of a decimation of the pseudo random number bit sequence in accordance with the estimation signal.

14. The random number generating system of claim 13, wherein said decimator (50) includes a counter (54) operable to input the pseudo random number bit sequence and the estimation signal.

15. The random number generating system of claim 13, wherein said psuedo random number generates the pseudo random number bit sequence as a function of the true random number bit sequence.

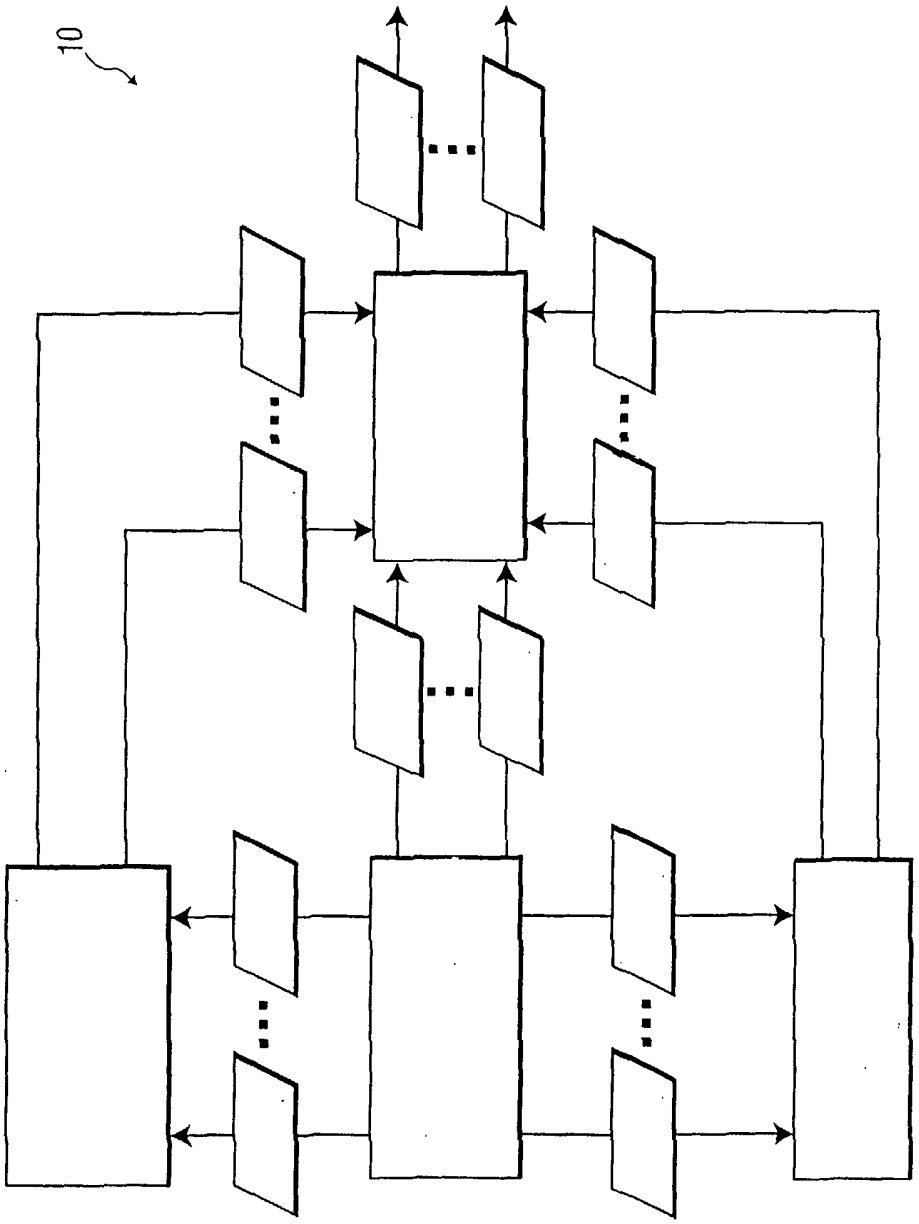


FIG. 1

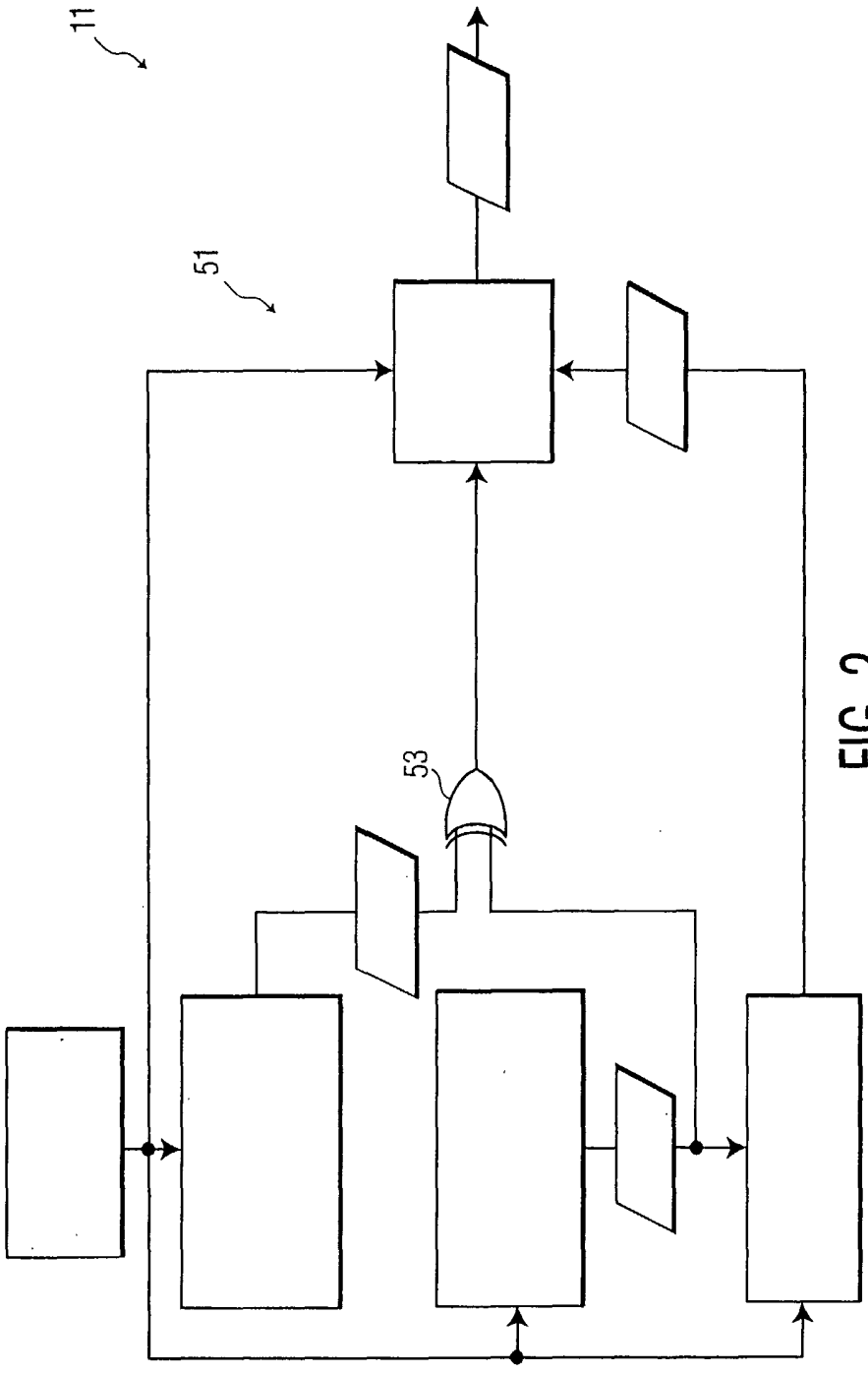


FIG. 2

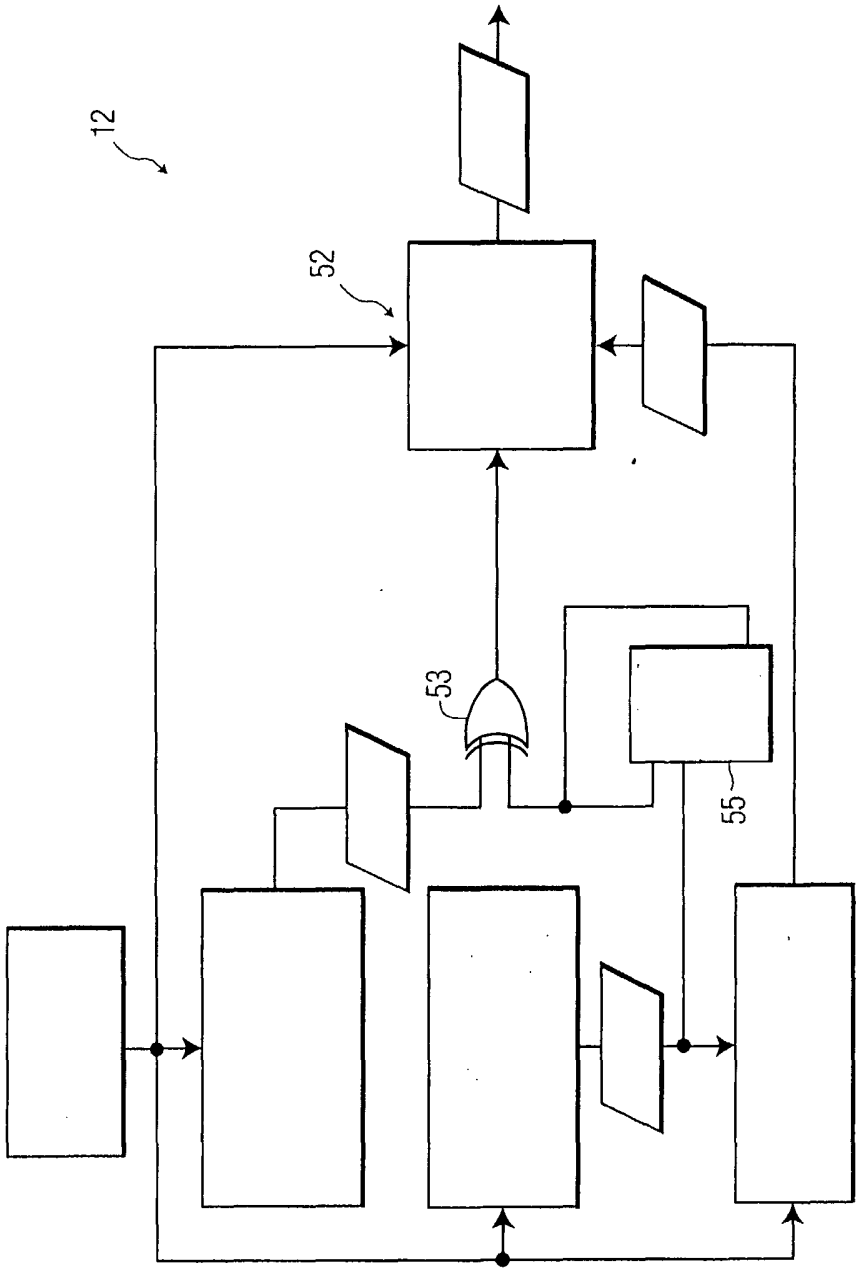


FIG. 3

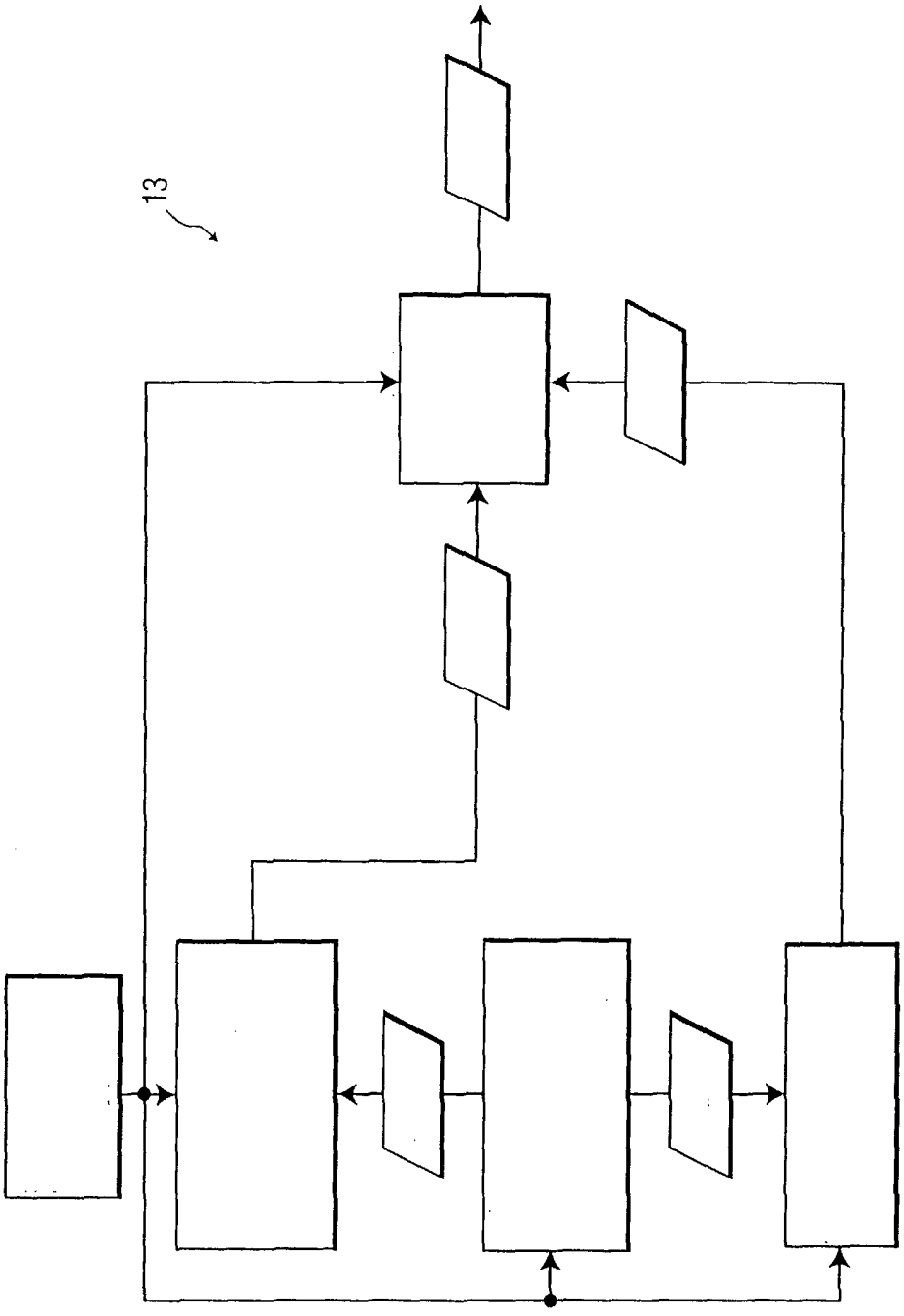


FIG. 4