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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 December 2014 (18.12.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/200326 A1

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

(21) International Application Number:
PCT/MY2014/000069

(22) International Filing Date:
23 April 2014 (23.04.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2013700985 11 June 2013 (11.06.2013) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(72) Inventors: **TENGKU AZIZ, Raja Mohd Fuad**; c/o MIMOS BERHAD, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **MOHAMED NOOR BEG, Ahmad Raif**; c/o MIMOS BERHAD, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(74) Agent: **CHUAH, Jern Ern**; Advanz Fidelis Sdn Bhd, Suite 609, Block D, Phileo Damansara 1, No.9, Jalan 16/11, Petaling Jaya, Selangor, 46350 (MY).

(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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

[Continued on next page]

(54) Title: DEVICE AND METHOD FOR OUTPUTTING RANDOM DATA

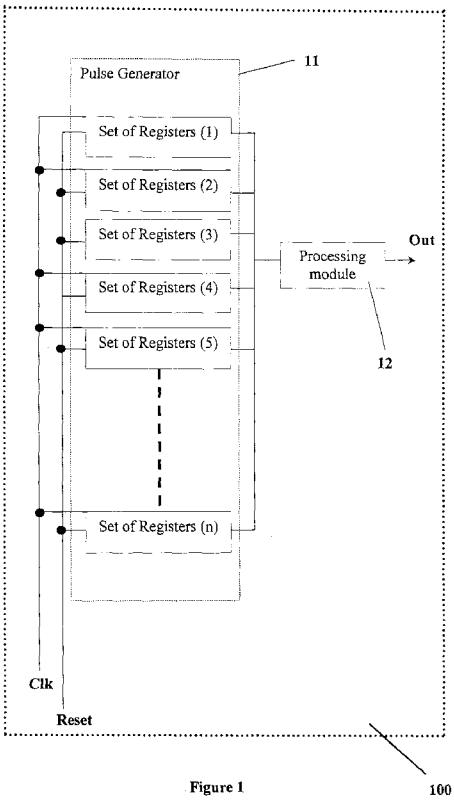


Figure 1

(57) Abstract: The present invention generally pertains to a random data generator and a method for generating and outputting random data, more particularly the present invention pertains to a random number generator comprising at least a pulse generator (11) and at least a processing module (12), and the method comprising selecting randomly a plurality of values from the pulse generator (11), determining a fixed value for the selected plurality of values, generating a pulse based on each determined fixed value, determining a time interval between each generated pulses, and comparing between each determined time interval, and generating an output from the comparison.

WO 2014/200326 A1

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

DEVICE AND METHOD FOR OUTPUTTING RANDOM DATA

FIELD OF THE INVENTION

The present invention generally pertains to a random data generator and a method for generating and outputting random data, more particularly the present invention pertains to a random number generator and a method for generating and outputting random number thereof.

BACKGROUND OF INVENTION

In various computer implemented applications these days, there is a need for generating random data with a sense of high unpredictability, high generation speed and reproducibility as in the most relevant cryptographic applications, security means, simulations or procedural generations. Such technology has ever since flourished into greater aspects of random data generation and has increased demands for greater degree of unpredictability without compromising speed and efficiency of generation.

Several prior arts divulged methods for generating random data. International patent publication no. WO2010005281 discloses a method for generating pseudo-random data whereby said method is accomplished with an additional circuit. The main embodiments of the method are the act of randomly tapping values from the output based on a plurality of registers which are connected in a linear feedback shift mode and thus providing said values for generating a single final output.

EP patent no. 171905 discloses a random number generator using the output of a true random generator to alter the behavior of a pseudorandom number generator by a mixing logic that builds a random seed for the pseudo-random number generator and comprises a generator of an alteration signal (TC1) the generation of which exploits the random instant of arrival of the bits outgoing from the true random generator.

US patent no. 6954770 discloses a random number generator comprising an oscillator with an output signal dependent upon a random source, a sampling device to sample the output

signal from the oscillator, and a fixed frequency clock driven linear feedback shift register (LFSR) to receive the sampled oscillator output, and to provide a random number at an output of the LFSR. The random number generator may comprise an optional mixing function communicatively coupled to the LFSR to read and to insert the random number into an algorithm to obtain a robust random number.

The prior arts however are unable to reach a solution to provide greater degree of unpredictability with increased generation speed and with reduced device complexity.

SUMMARY OF INVENTION

The main objective of the present invention is to provide a device and a method for generating random data with greater degree of data unpredictability at an increased processing speed in an environment where complexity of the hardware is not compromised. The hardware construction as implemented in the present invention provides multiple set of registers to generate the random numbers at an increased output speed.

It is an object of the present invention to provide a device for generating random data comprising at least a pulse generator, and at least a processing module, wherein the pulse generator is constructed using linear feedback shift registers, responsible for sampling data, and the processing module is responsible for determining and comparing time intervals of the successive pulses and outputting random data.

It is another object the present invention to provide a method for generating random data comprising the steps of selecting randomly a plurality of values, determining a fixed value, generating a pulse based on each determined fixed value, determining a time interval between each generated pulses and comparing between each determined time interval, and generating an output from the comparison.

The device and method for outputting random data in the present invention therefore generates and outputs random data with a greater degree of unpredictability and at an increased generation speed without compromising with the construction of the device.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 illustrates the system architecture provided by the device in accordance to the present invention.

Figure 2 illustrates the construction of the linear feedback shift register in accordance to the present invention.

Figure 3 illustrates the comparison table, the representation of the output from the pulse generator varying with time, and the representation of the output from the processing varying with time in accordance with the present invention.

Figure 4 illustrates the process flow of the method in accordance with the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Described below are preferred embodiments of the present invention with reference to the accompanying drawings. Each of the following preferred embodiments describes an example not limiting in any aspect.

Referring to Figure 1, the figure illustrates the system architecture provided in the device of the present invention, wherein the device is for generating random data, more particularly the random data is preferably but not limited to pseudo random number generated by a linear feedback shift register pseudo-random number generator (LFSR PRNG).

As the random data generators, random number generators in particular, are well known in the art, further description and elaboration on the random data generators such as the random number generators, true random generators and pseudo random number generators will not be discussed.

The device (100) as claimed in the present invention is for outputting random data and comprising at least a pulse generator (11) for generating a plurality of values, and at least a

processing module (12) for receiving the plurality of values from the pulse generator (11) and for outputting a random data thereof.

The pulse generator (11) as a preferred embodiment in the present invention is configured by a plurality set of registers, each set of registers is configured to generate a plurality of values corresponding to a seed value inputted into the pulse generator (11) and the plurality of values is fed into the processing module (12) for comparing time intervals and mapping time intervals via the plurality set of registers that is capable of generating and outputting random data thereof at greater speed and greater unpredictability.

The set of registers is preferably but not limited to linear feedback registers. It is given in the present invention in that with the construction of multiple set of registers defining the pulse generator (11), the output unpredictability and output speed, increased, hence providing greater performance.

The generation speed is increased as the plurality of values are selected and computed on a multiple set of registers, hence providing greater ability for the multiple registers to generate the random data.

In other words, by providing multiple sets of registers, more combination values can be realized. When a comparison is performed via multiple of these registers with multiple chosen values, the speed to which a match is achieved is greater, hence increasing the generation speed. Not only the speed is increased but also the unpredictability is also enhanced by the usage of multiple registers because more combinations are being used and also the match to multiple chosen values which makes guessing of probable combination as being highly impractical.

The pulse generator (11) in the present invention is responsible for selecting randomly a plurality of values that is generated from an input seed value into the linear feedback shift register, then the pulse generator (11) samples the selected plurality of values by determining a fixed value for the plurality of values. Output pulses are generated from the pulse generator (11) based on comparison between the plurality set of registers and multiple predetermined values.

The processing module (12) is responsible for determining the time interval between the generated output pulses from the pulse generator (11) by way of measuring the successive time between the pulses, and the processing module (12) compares the time intervals for mapping a binary value to the compared output, and thereby generating a random data output, preferably a random number.

Referring to Figure 2, the figure illustrates the construction of the linear feedback shift register in accordance to the present invention, wherein linear feedback shift registers are constructed using D-type flip flops. It will be appreciated by a person skilled in the art that the linear feedback shift register or the like is not limited to the construction of D-type flip flops, whereby other types of flip flops and in various logic gates connections are possible, for example T-type flip flops, JK flip flops, and etcetera.

Referring to Figure 1 and 3, Figure 3 illustrates the output comparison table in accordance to the present invention, and by way of an example to describe the preferred embodiment of the present invention, the figure further illustrates an exemplary representation of the output from the pulse generator (11) of Figure 1 varying with time, and the representation of the output from the processing module (12) of Figure 1 varying with time. The output of the processing module (12) is dependent on the output of the pulse generator (11).

The output comparison table in the Figure 3 indicates a column with time value comparison, and another column indicates the corresponding mapping value. As shown in the table, "t1" refers to the time interval between the first successive pulses and "t2" refers to the time interval between the second successive pulses. From the representation of pulses from the output of the pulse generator (11), it is shown that the "t2" is greater than "t1", and therefore by referring to the comparison table, the shown output of the pulse generator (11) will be mapped to a value of "0". The result of the output from the pulse generator (11) after mapping according to the comparison table, is shown regenerated in the output of the processing module (12).

Referring to Figure 1 and Figure 4, Figure 4 illustrates the process flow of the method for generating random data in accordance with the present invention and the method for generating random data is executed by the device (100) of Figure 1.

The method for generating random data executed by the device (100) of Figure 1, comprising the steps of initially selecting randomly a plurality of values from the pulse generator (11), determining a fixed value for the selected plurality of values, generating a pulse based on each determined fixed value, determining a time interval between each generated pulses, and comparing between each determined time interval, and generating an output from the comparison.

The method for generating random data is preferably but not limited to pseudo random number generated by a linear feedback shift register pseudo-random number generator (LFSR PRNG). As the random data generators, random number generators in particular, are well known in the art, further description and elaboration on the random data generators such as the random number generators, true random generators and pseudo random number generators will not be discussed.

In the present invention, the step of initially selecting randomly a plurality of values from the pulse generator (11) is executed by first inputting a seed value into the pulse generator (11), whereby the linear feedback shift registers constructed in the pulse generator (11) generates a plurality of values. The generated plurality of values is then sampled by determining a fixed value for the plurality of values. Then, the plurality of values is compared against with a plurality of predetermined values for generating corresponding output pulses based on each determined fixed value.

The method for generating random data then continues with measuring successive time between the generated output pulses from the pulse generator (11) and determining time intervals between each generated pulses. The determined time intervals are compared with a time interval comparison table, and the output of the pulse generator (11) is mapped to the values determined in the comparison table.

The mapped output pulses provide a final output from the processing module (12), which is the generated random data, preferably the pseudo random number.

The pulse generator (11) is configured by a plurality set of registers, each set of registers is configured to generate a plurality of values corresponding to a seed value inputted into the

pulse generator (11) and the plurality of values is fed into a post processing module (12), and the time intervals are compared and mapped via the plurality set of registers for generating and outputting random data thereof at greater speed and greater unpredictability.

The step of selecting randomly a plurality of values, determining fixed value and generating of pulse are provided by a pulse generator (11), and the steps of determining the time interval between pulses, comparing the time interval and generating an output are provided by a processing module (12).

The pulse generator (11) is defined by a polynomial representing the design of the linear feedback shift registers, whereby different polynomial according to the construction of the pulse generator (11) and different processes implemented within the circuit, generates varying stream of pulses.

The method for generating the random data is performed in a digital circuit with the incorporation of the pulse generator (11) and the processing module (12), and the generated random data is preferably a string of bits and then passed to an interface device for further processing and data retrieval.

As the present invention can be implemented in small area footprint, the present invention can be implemented in a field-programmable gate array (FPGA) or in an application-specific integrated circuit (ASIC).

In as much as the present invention is subject to many variations, modifications and changes in detail, it is intended that all matter contained in the foregoing description or shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

CLAIMS

1. A device (100) for outputting random data comprising:

at least a pulse generator (11) for generating a plurality of values; and

at least a processing module (12) for receiving the plurality of values from the pulse generator (11) and for outputting a random data thereof;

characterized in that the pulse generator (11) is configured by a plurality set of registers, each set of registers is configured to generate the plurality of values corresponding to a seed value inputted into the pulse generator (11) and the plurality of values is fed into the processing module (12) for comparing time intervals and mapping time intervals via the plurality set of registers that is capable of generating and outputting random data thereof at greater speed and greater unpredictability.

2. A device (100) for outputting random data according to claim 1, wherein the plurality set of registers increases the random number generation speed.

3. A method for outputting random data via the device (100) of claim 1, the method characterized by the steps of:

inputting at least a seed value into at least a pulse generator (11);

selecting randomly a plurality of values from the pulse generator (11);

determining a fixed value for the selected plurality of values;

generating a pulse based on each determined fixed value;

determining time intervals between each generated pulses, comparing the time intervals with a predetermined rule, and mapping each determined time intervals to a corresponding value; and

generating an output from the mapped values;

wherein, the pulse generator (11) is configured by a plurality set of registers, each set of registers is configured to generate a plurality of values corresponding to a seed value inputted into the pulse generator (11) and the plurality of values is fed into at least a processing module (12), and the time intervals are compared and mapped via the plurality set of registers for generating and outputting random data thereof at greater speed and greater unpredictability.

4. A method for outputting random data according to claim 3, wherein the pulse generator (11) is constructed using linear feedback shift registers.

5. A method for outputting random data according to claim 3, wherein the pulse generator (11) is defined by a polynomial.

6. A method for outputting random data according to claim 5, wherein different polynomial and different processes involved generates different stream of pulses.

7. A method for outputting random data according to claim 3, wherein the steps of selecting randomly a plurality of values, determining fixed value and generating the pulse are provided by the pulse generator (11).

8. A method for outputting random data according to claim 3, wherein the steps of determining the time intervals between pulses, comparing the time intervals, mapping each determined time intervals and generating an output are provided by the processing module (12).

9. A method for outputting random data according to claim 3, wherein the output generated upon completion of the comparison step is a string of bits.

10. A method for outputting random data according to claim 3, wherein the plurality set of registers increases the random number generation speed.

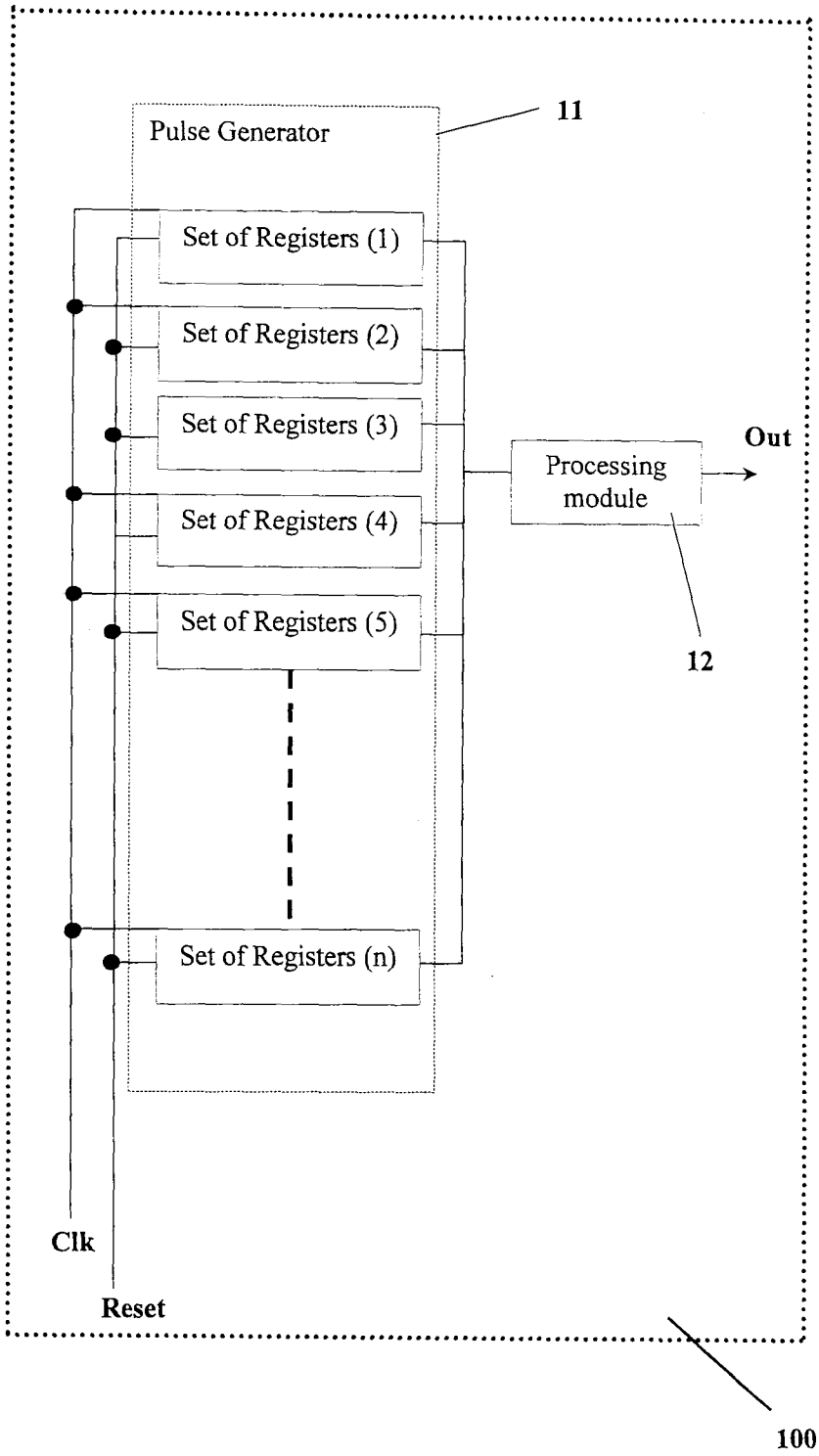
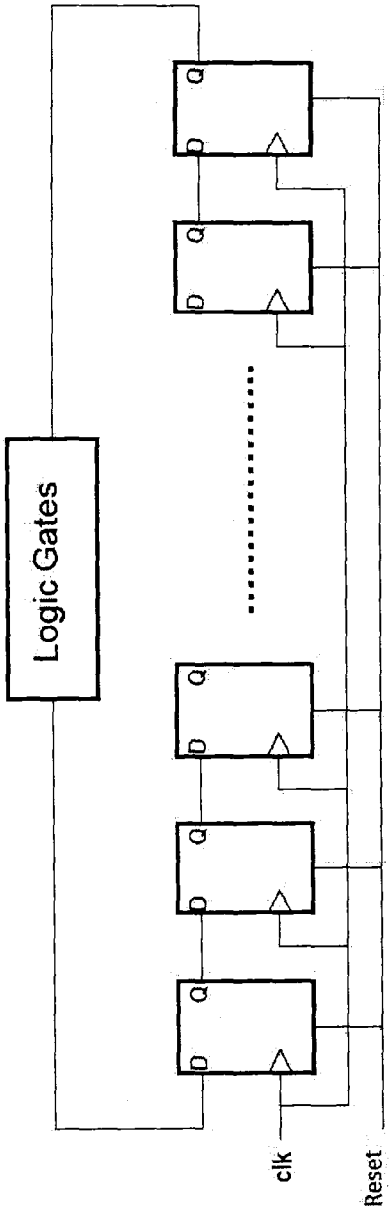

Pulse Generator
11
Set of Registers (1)
Set of Registers (2)
Set of Registers (3)
Set of Registers (4)
Set of Registers (5)
Set of Registers (n)
Processing module
Out
12
Clk
Reset
100

Figure 1



Basic LFSR Circuit

Figure 2

t1 and t2 comparison	Value
t1 > t2	1
t2 > t1	0
t1 = t2	Data not captured

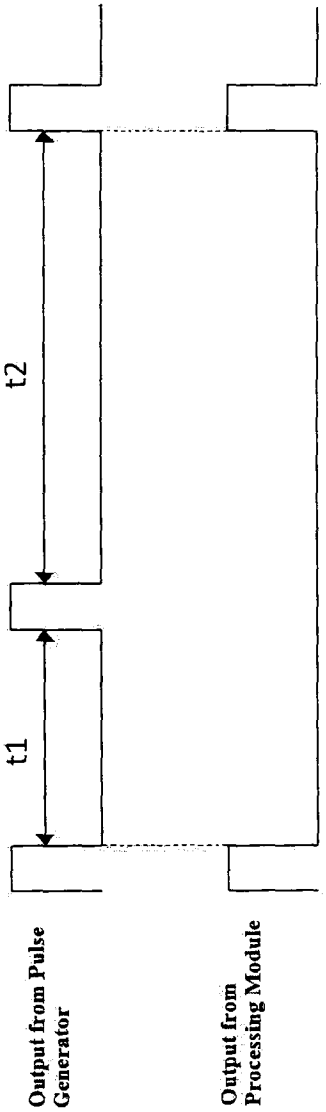


Figure 3

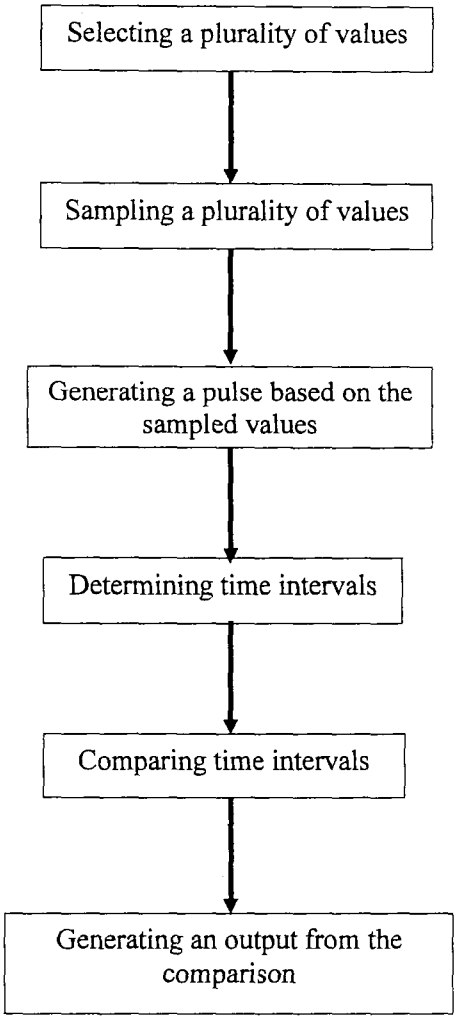

Selecting a plurality of values
Sampling a plurality of values
Generating a pulse based on the sampled values
Determining time intervals
Comparing time intervals
Generating an output from the comparison

Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2014/000069

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010/005281 A2 (MIMOS BERHAD [MY]; AHMAD RAIF BIN MOHAMED NOOR BE [MY]; RAJA MOHD FUAD) 14 January 2010 (2010-01-14) cited in the application the whole document	1-10
X	EP 1 544 726 A1 (INST ADVANCED STUDIES CO LTD [JP]; LEISURE ELECTRONICS TECHNOLOGY [JP]) 22 June 2005 (2005-06-22) paragraph [0027] - paragraph [0031]; figure 3	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

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

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published 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; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 October 2014	10/10/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Prins, Leendert

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2014/000069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010005281 A2	14-01-2010	MY 146157 A	29-06-2012
		WO 2010005281 A2	14-01-2010
EP 1544726 A1	22-06-2005	AU 2003285742 A1	03-03-2004
		EP 1544726 A1	22-06-2005
		JP 4195007 B2	10-12-2008
		US 2005198091 A1	08-09-2005
		WO 2004017191 A1	26-02-2004