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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2012 (10.05.2012)

PCT

(10) International Publication Number
WO 2012/060684 A1

(51) International Patent Classification:
G06F 7/58 (2006.01) *G07C 15/00* (2006.01)

(21) International Application Number:
PCT/MY2011/000104

(22) International Filing Date:
17 June 2011 (17.06.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2010005169 2 November 2010 (02.11.2010) MY

(71) Applicant *(for all designated States except US)*: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MEILANA, Siswanto** [ID/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **GUNAWAN, Witjaksono** [ID/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah Co. (Malaysia) Sdn Bhd., Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (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, 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, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *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))*

(54) Title: QUANTUM-BASED RANDOM NUMBER GENERATOR (QRNG) WITH MULTI OUTPUT PROCESSOR (MOP)

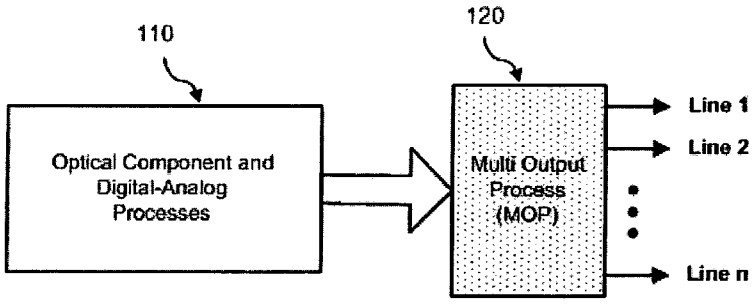

FIG. 1

(57) Abstract: A device for producing identical multiple true random numbers via quantum-based random number generator which comprises at least one optical component (110), at least one digital data processor (110) and at least one multi output processor (120); a system for producing identical multiple true random numbers via quantum based random number generator comprising at least one optical component (110), at least one digital data processor (110) for digital data processing and at least one multi output processor (120); a method for producing identical multiple true random numbers via quantum-based random number generator comprising steps of generating analog signals from at least one optical component in quantum-based random number generator, processing generated analog signals, converting analog signals to sequence of digital signals, forwarding sequence of digital signals to multi output processor in quantum-based random number generator and generating sequence of true random numbers.

WO 2012/060684 A1

QUANTUM-BASED RANDOM NUMBER GENERATOR (QRNG) WITH MULTI OUTPUT PROCESSOR (MOP)

FIELD OF INVENTION

The present invention relates to data security of information that is transmitted and stored in an electronic form utilizing quantum-based random number generator (QRNG) with multi output processor (MOP).

BACKGROUND ART

Cryptographic systems are used to encrypt information to guarantee its security and confidentiality. Encryption is the process of encoding information/data based on a specific algorithm to make it unreadable to unauthorized people unless the user is in possession of a specific key. To retrieve the information, the encrypted form must be decrypted.

Encryption systems have been developed for maintaining the privacy of information transmitted across a communications channel. Typically, a symmetric encryption system is used for this purpose. Symmetric encryption systems that use electronic keys are analogous to a physical security system where a box has a single locking mechanism with a single key hole. One key holder uses his or her key to open the box, places a message in the box, and relocks the box. Only a second holder of the identical copy of the key can unlock the box and retrieve the message. The term symmetric reflects the fact that both users must have identical copies of the key.

One of the most popular cryptographic systems is the RSA system. RSA is an acronym for the last names of the computer scientists Rivest, Shamir, and Adleman who first publicly described the algorithm used for public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

Rivest, Shamir, and Adleman as co-inventors were granted U.S. Patent No. 4,405,829 (hereinafter referred to as the '829 patent) that discloses a "Cryptographic communications system and method" using the RSA algorithm. The '829 patent describes a communications channel coupled to at least one terminal having an encoding device and decoding device. Specifically, when a message is transferred, the message is enciphered where the text is coded by encoding the message as a number M in a predetermined set using an algorithm. The resulting number is then raised to a first predetermined power (associated with the intended receiver) and finally computed. The remainder or residue, C, is computed when the exponentiated number is divided by the product of two, predetermined prime numbers (associated with the intended receiver). This is repeated again using the residue C and a second predetermined power to compute the residue M' where residue M' corresponds to the original encoded message M.

In a RSA algorithm, two large, prime numbers are selected randomly to generate the secret and public keys. One of the keys is sent to the receiver by a public channel and the other key is sent to private channel. The security of the RSA-encrypted information largely depends on the size of the encryption key. The larger the key size indicates how secure the encryption/decryption is. However, it is just a matter of time before a high-speed computer will break the security of this system.

Securing the key is the main factor in information security, especially for an encryption system. Most of the conventional encryption systems are using keys based on a pseudorandom. The pseudorandom system itself has been designed on a mathematic algorithm, which does not have a truly random output since its output has a pattern with repetitive occurrences. These limitations reduce the security of the key because attackers can crack the encryption system.

The approach and methodology in the present invention is to design the best secured encryption system. This requires a true random number generator (TRNG) to produce keys that increases the complexity of the system. The ultimate true random number generator is a quantum-based random number generator (QRNG), which has unpredictable outputs of random numbers.

The state of the present art only discloses encryption systems having a single output. However, a problem will arise when implementing the QRNG for the encryption system where two parties need two identical keys. This is because the key generated by QRNG is totally independent and not the same. Therefore, QRNG with multiple identical outputs is required to serve as encryption and decryption keys.

The present invention provides for securing encryption-decryption processes by using the identical key for encryption in a transmitter side, and sending the other identical key to a receiver at the same time, which facilitates a receiver to decrypt secret messages that are sent by a transmitter. In short, receivers can receive the same secure messages together from a transmitter without transmitting different keys in the present invention.

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practice.

SUMMARY OF INVENTION

The present invention provides a device (100) for producing identical multiple true random numbers via a quantum-based random number generator. The device comprising at least one optical component (110), at least one digital data processor (110) and at least one multi output processor (120). The multi output processor (120) further comprises a plurality of m-to-n converters (230) having m-input connected to the output of the processor to convert incoming digital signals into multi parallel inputs for producing multiple identical outputs.

Another aspect of the present invention is a system for producing identical multiple true random numbers via a quantum based random number generator (100) having a multi output processor (MOP) (120). The system comprising at least one optical component and at least one digital data processor (110) for digital data processing (110) and at least one multi output processor (MOP) (120). The multi output processor (MOP) (120) further comprises a plurality of m-to-n converters (230) having m-input connected to the output of the processor to convert incoming digital signals into multi parallel inputs for producing multiple identical outputs. The multiple identical outputs are multiple identical of true random keys which secures encryption-decryption processes.

A further aspect of the present invention is a method for producing identical multiple true random numbers via a quantum-based random number generator (QRNG). The method comprising the steps of generating analog signals from at least one optical component in the quantum-based random number generator, processing the generated analog signals, converting analog signals to sequence of digital signals, forwarding sequence of digital signals to multi output processor in the quantum-based random number generator and generating sequence of true random numbers.

Preferably, the method of generating sequence of true random numbers further comprises the steps of asserting TxD_start signal, receiving m-bits data wherein m-bits data is TxD_data which is received from the optical component and digital data processor and processing the m-bits data. Further, processing the m-bits data comprises the steps of serializing the m-bits data using the m-to-n converters (530), starting a state

machine when the TxD_start signal is asserted (560), sending a busy signal when a transmission occurs (575) and ignoring the TxD_start signal when a transmission occurs, selecting a baud rate and advancing when a BaudTick signal is asserted and generating a TxD output to identical multiple outputs (240) from serial output through the m-to-n converters (590).

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

FIG. 1 illustrates a Quantum-based Random Number Generator (QRNG) device having multi identical outputs.

FIG. 2 illustrates a Multi Output Processor (MOP) with multi m-to-n converters.

FIG. 3 illustrates a communication system using a QRNG system as a producer of random key that has multiple outputs.

FIG. 4 is diagram of an asynchronous transmitter with multi m-to-n converters.

FIG. 5 is a flowchart illustrating the process of Quantum-based Random Number Generator (QRNG) with Multi Output Processor.

FIG. 6 is a flowchart illustrating a method for producing identical multiple true random numbers via quantum-based random number generator.

FIG. 7 is a flowchart illustrating a method for generating sequence of true random numbers.

FIG. 8 is a flowchart illustrating a method for processing m-bits data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention relates to Quantum-based Random Number Generator (QRNG) with Multi Output Processor (MOP). Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Reference is first being made to FIG. 1 and FIG. 2 respectively. FIG. 1 illustrates Quantum-based Random Number Generator (QRNG) device having multi identical outputs. Fig. 2 illustrates a Multi Output Processor (MOP) with multi m-to-n converters. As illustrated in FIG. 1, Quantum Random Number Generator (QRNG) consists of at least one optical component (110) which generates analog signals (pulses). Thereafter, analog signals are forwarded to at least one digital data processor (110). The analog and digital processes (110) will produce sequence of digital signal outputs. Subsequently, sequence of digital signal outputs will be forwarded to at least one Multi Output Processor (MOP) (120). Thereafter, the Multi Output Processor (MOP) (120) generates n parallel output of identical random numbers. The amount of parallel output depends on the number of m-to-n converters used. The number of m-to-n converters can be reconfigured as needed.

Reference is now being made to FIG. 2. FIG. 2 illustrates Multi Output Processor (MOP) with multi m-to-n converters. The Multi Output Processor (MOP) comprises a processor (250) to process input (210) from the at least one optical component and at least one digital data processor (110). The Multi Output Processor (MOP) (120) comprises a plurality of m-to-n converters (230) having m-input connected to output of the processor to convert digital signals into multi parallel inputs for producing multiple identical outputs. Multiple identical outputs of the device are multiple identical of true random keys.

The plurality of multiple identical outputs (240) in the device secures encryption-decryption processes. The order of the input (210) and m-to-n converters (220) of the

Multi Output Processor with the same structure to produce random numbers with the same speed and pattern eliminates the occurrence of noise.

Reference is now being made to FIG. 3. FIG. 3 is a communication system (300) using Quantum-based Random Number Generator (QRNG) as a producer of random key that have multiple outputs. FIG. 3 illustrates a transmitter system (330) having Quantum-based Random Number Generator (QRNG) (340) for encryption and a receiver system (370) for decryption (380) and key management (390) of encrypted keys. The communication system (300) transmits signals from a transmitter system (330) having the Quantum-based Random Number Generator (QRNG) system (340).

The Multi Output Processor (MOP) of the Quantum-based Random Number Generator (QRNG) system produces identical true random keys for securing encryption and decryption processes. The transmitter system (330) generates identical key and sends the corresponding identical key to a receiver system (370). The keys may travel via a secure channel (310) or insecure or public channel (320) as illustrated in FIG. 3. Further, both the transmitter system (330) and receiver system (370) provides key management functions (360 and 390, respectively) for holding identical random keys. By using the identical random keys for encryption on transmitter side (330), receiver side (370) decrypts secret messages sent by transmitter.

Reference is now being made to FIG. 4. FIG. 4 illustrates asynchronous transmitter (402) with multi m-to-n converter. Multi Output Processor (MOP) (120) is a computer hardware which functions as serializer, such as, an asynchronous transmitter (402) having multi output (1 to n). Multi Output Processor (MOP) comprises m-to-n converters such as multiplexer where m and n represents its input and output consecutively. As illustrated in FIG. 4, the asynchronous transmitter (400) has four inputs, *i.e.* TxD_data, TxD_start, Clock (clk), and Reset (rst), and two outputs, *i.e.*, busy and multi TxD as data outputs (TxD_1 to TxD_n). The multi outputs (TxD_1 to TxD_n) will have identical data output due to the same source in the system.

Reference is now being made to FIGs. 4, 5 and 6 respectively. FIG. 5 is a flowchart illustrating the process of Quantum-based Random Number Generator (QRNG) with Multi Output Processor. FIG. 6 is a flowchart illustrating a method for producing identical

multiple true random numbers via quantum-based random number generator while FIG. 7 is a flowchart illustrating a method for generating sequence of true random numbers and FIG. 8 is a flowchart illustrating a method for processing m-bits data. The at least one optical Component generates analog signals (502, 602) and forwards the pulses to analog process for processing generated analog signals (504, 604). Thereafter, analog signals are converted to sequence of digital signals (606) through digital process (506). The sequences of digital signals are forwarded to Multi Output Processor (MOP) in Quantum-based Random Number Generator (QRNG) (608) to generate sequence of true random numbers (610).

The method for generating sequence of true random numbers comprises asserting TxD_start signal (508,702). The Multi Output Processor (MOP) will receive m-bits data wherein m-bits data is TxD_data which is received from the at least one optical component and the at least one digital data processor (510, 704) upon asserting TxD_start signal (508, 702). Thereafter, m-bits data will be processed (512, 706).

The m-bits data is processed by serializing m-bits data using m-to-n converters (802) by starting state machine when TxD_start signal is asserted (804). The "busy" signal is asserted (518) while transmission occurs and TxD_start signal is ignored when transmission occurs (806). Multi Output Processor (MOP) generates start bit, data bits and stop bits ("busy" signal) by using a state machine in the Multi Output Processor (MOP).

Assuming that there is a "BaudTick" signal available, the baud rate is 115200 bits a second. The state machine starts right when TxD_start is asserted, but only advances when the "BaudTick" is asserted (808). Thereafter, TxD output is generated as serial output through m-to-n converters (810). Since multi m-to-n converters tap the same source of TxD_data, Multi Output Processor (MOP) generates multiple identical outputs, TxD_1 to TxD_n (520).

Therefore, the present invention produces identical multiple true random numbers via Quantum-based Random Number Generator (QRNG) which provides for securing encryption-decryption processes in a transmitter side, and sending the other identical

key to a receiver at the same time, which facilitates a receiver to decrypt secret messages that are sent by a transmitter.

The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A device (100) for producing identical multiple true random numbers via quantum-based random number generator comprising:
   at least one optical component (110);
   at least one digital data processor (110); and
   at least one multi output processor (120).

2. A device according to Claim 1, wherein the at least one multi output processor (120) further comprises a plurality of m-to-n converters (230) having m-input connected to the output of the processor to convert incoming digital signals into multi parallel inputs for producing multiple identical outputs.

3. A device according to Claim 2, wherein multiple identical outputs (240) are multiple identical of true random keys.

4. A device according to Claim 2 and 3, wherein multiple identical outputs (240) secures encryption-decryption processes.

5. A system for producing identical multiple true random numbers via quantum based random number generator (100) comprising:
   at least one optical component and at least one digital data processor (110) for digital data processing (110); and
   at least one multi output processor (MOP) (120).

6. A system according to Claim 5, wherein the at least one multi output processor (MOP) (120) further comprises a plurality of m-to-n converters (230) having m-input connected to the output of the processor to convert incoming digital signals into multi parallel inputs for producing multiple identical outputs.

7. A system according to Claim 6, wherein multiple identical outputs are multiple identical of true random keys.

8. A system according to Claim 6, wherein multiple identical outputs (240) secures encryption-decryption processes.

9. A method (600)for producing identical multiple true random numbers via quantum-based random number generator comprising steps of:
   generating analog signals from at least one optical component in quantum-based random number generator (602);
   processing generated analog signals (604);
   converting analog signals to sequence of digital signals (606);
   forwarding sequence of digital signals to multi output processor in quantum-based random number generator (608); and
   generating sequence of true random numbers (610).

10. A method (700) according to Claim 10 wherein generating sequence of true random numbers further comprises steps of:
    asserting TxD_start signal (702);
    receiving m-bits data wherein m-bits data is TxD_data which is received from the optical component and digital data processor (704); and
    processing m-bits data (706).

11. A method (800) according to Claim 11 wherein processing m-bits data further comprises the steps of:
    serializing m-bits data using m-to-n converters (802);
    starting state machine when TxD_start signal is asserted (804);
    sending busy signal when transmission occurs and ignoring TxD_start signal when transmission occurs (806);
    selecting baud rate and advancing when BaudTick signal is asserted (808); and
    generating TxD output to identical multiple outputs (240) from serial output through m-to-n converters (810).

12. A method as claimed in Claim 11, wherein identical multiple outputs (240) secures encryption-decryption processes.

100

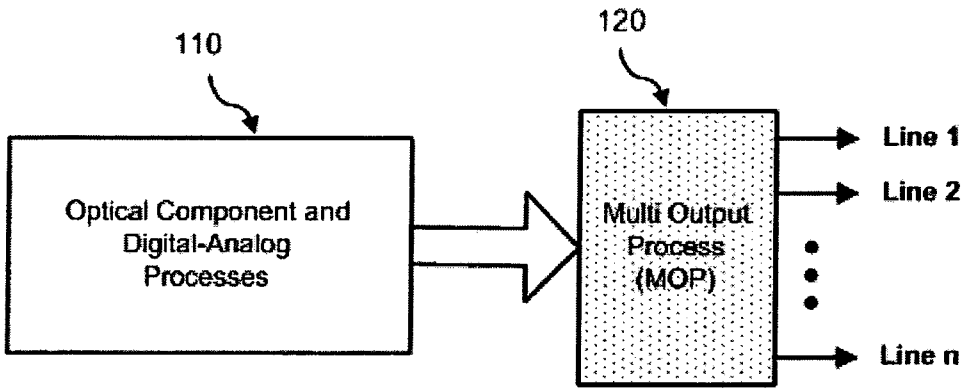
110
120
Optical Component and Digital-Analog Processes
Multi Output Process (MOP)
Line 1
Line 2
Line n

FIG. 1

200

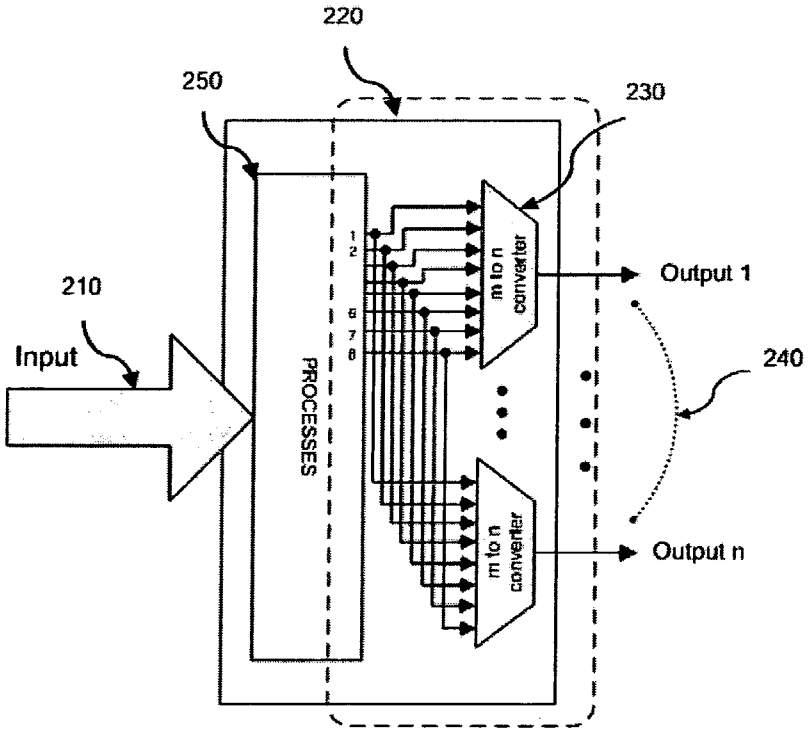
220
250
230
210
Input
PROCESSES
1
2
6
7
8
m to n converter
m to n converter
Output 1
Output n
240

FIG. 2

300

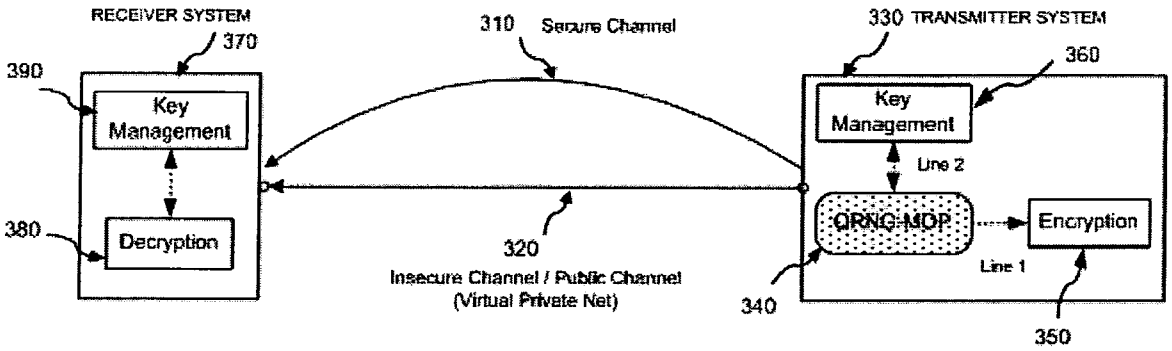
RECEIVER SYSTEM
370
390
Key Management
380
Decryption
310 Secure Channel
320
Insecure Channel / Public Channel
(Virtual Private Net)
330 TRANSMITTER SYSTEM
360
Key Management
Line 2
QRNG-MOP
Encryption
Line 1
340
350

FIG. 3

400

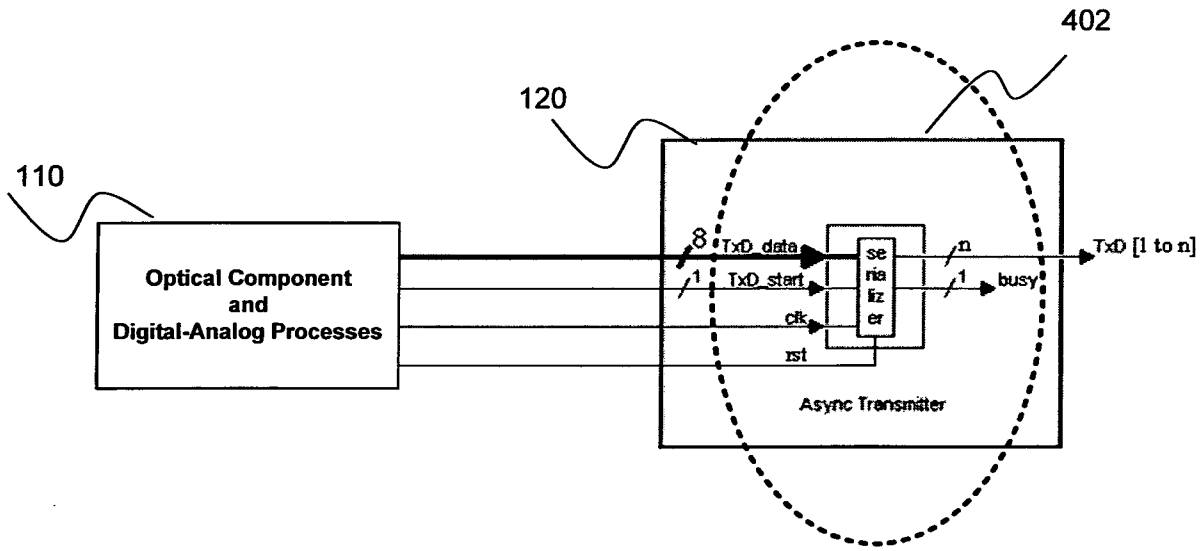
402
120
110
Optical Component
and
Digital-Analog Processes
8
TxD_data
1
TxD_start
clk
rst
se
ria
liz
er
n
1
busy
TxD [1 to n]
Async Transmitter

FIG. 4

500

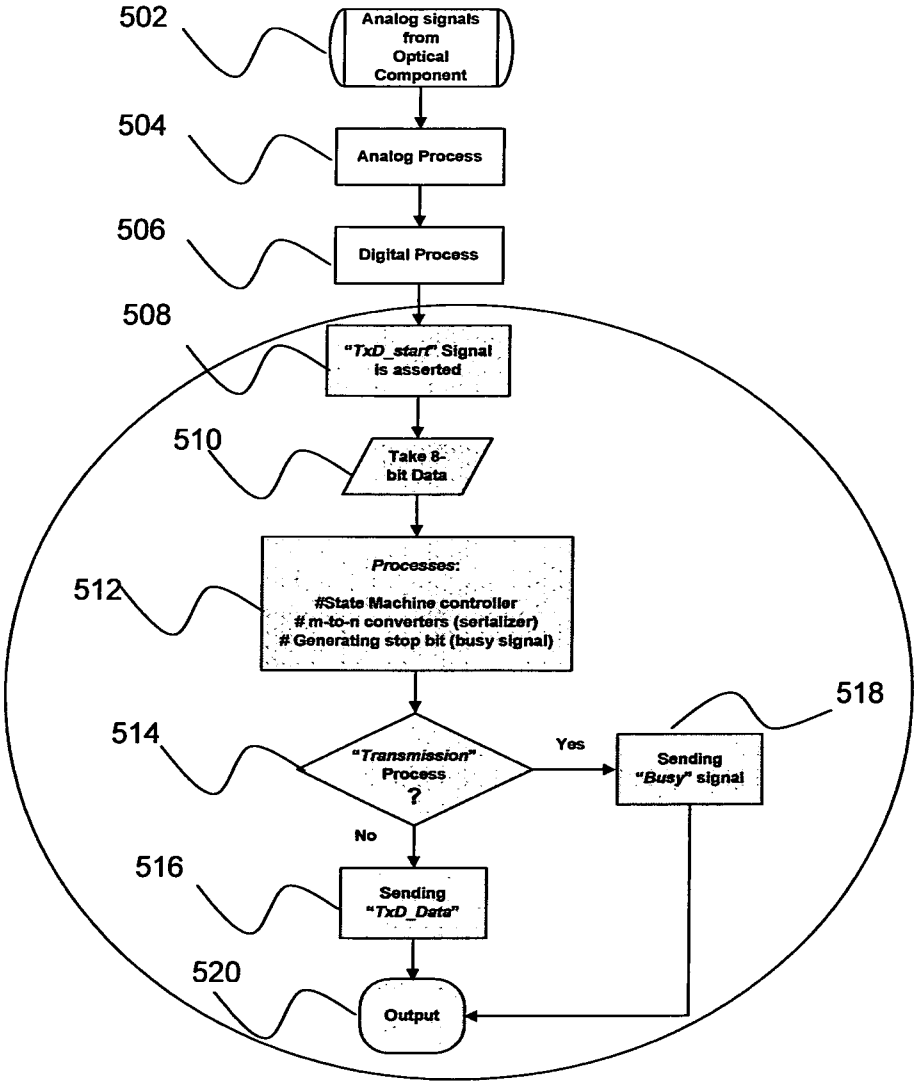
502
Analog signals from Optical Component
504
Analog Process
506
Digital Process
508
"TxD_start" Signal is asserted
510
Take 8-bit Data
512
Processes:
#State Machine controller
m-to-n converters (serializer)
Generating stop bit (busy signal)
514
"Transmission" Process ?
Yes
518
Sending "Busy" signal
No
516
Sending "TxD_Data"
520
Output

FIG. 5

600

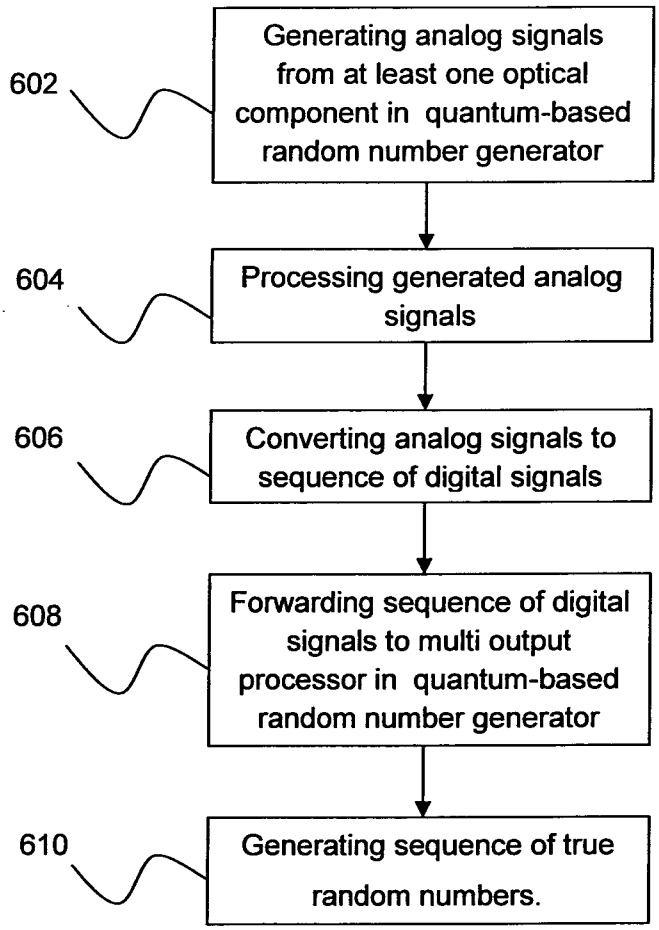

FIG. 6

700

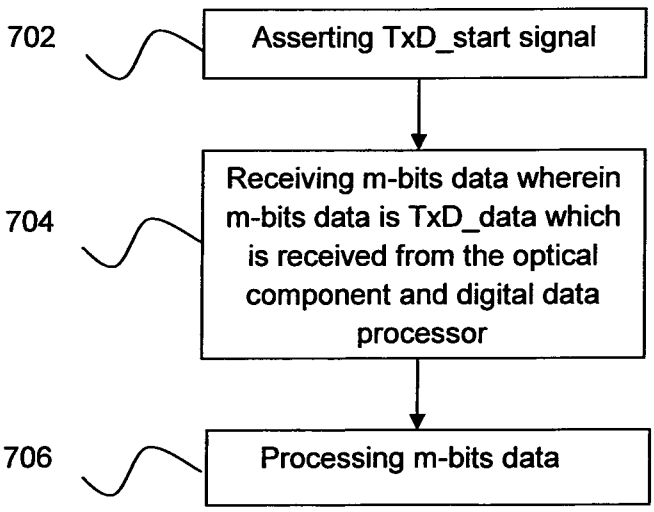

FIG. 7

800

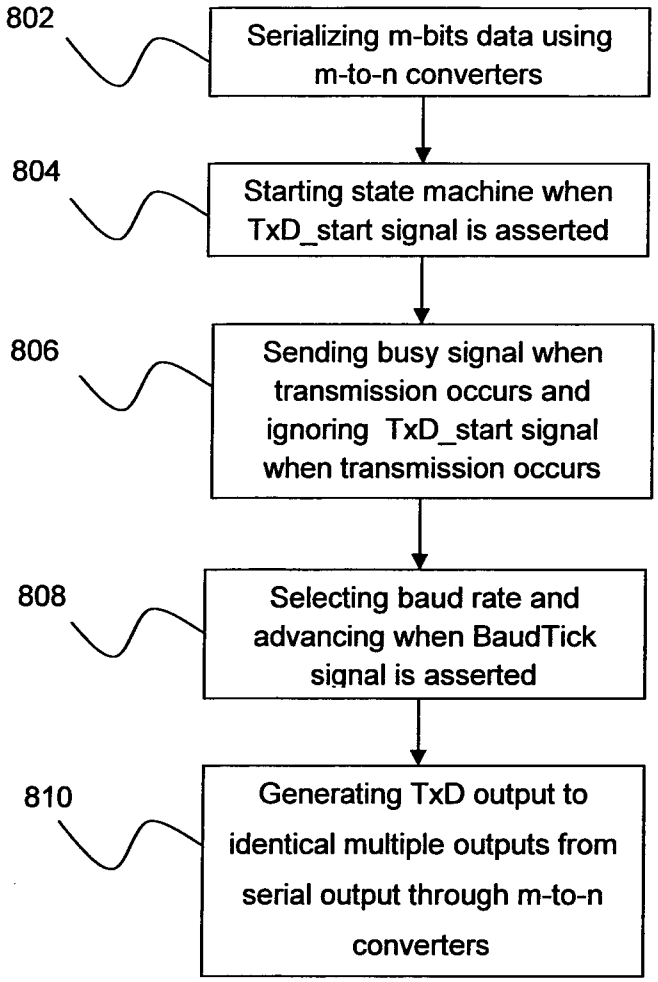
802
Serializing m-bits data using m-to-n converters
804
Starting state machine when TxD_start signal is asserted
806
Sending busy signal when transmission occurs and ignoring TxD_start signal when transmission occurs
808
Selecting baud rate and advancing when BaudTick signal is asserted
810
Generating TxD output to identical multiple outputs from serial output through m-to-n converters

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2011/000104

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 7/58 (2006.01) ***G07C 15/00*** (2006.01)

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)

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)
WPI, Google, Patent Lens, Google Patent, Patentscope, esp@cenet "random, quantum, generator, optic etc."

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0080386 A1 (DONNANGELO et al.) 1 April 2010 Paragraph 78 lines 1 to 3, paragraph 84 line 30, paragraph 103 lines 9 to 13, paragraph 110, figures 1, 6 and 21 in particular.	1,5,9
X	JENNEWEIN T. et al., "A fast and compact quantum random number generator", Review of Scientific Instruments, Volume 71, Number 4, April 2000. Pages 1675 to 1680.	1,5,9

☐ 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
20 September 2011	21/09/2011
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **P. THONG** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 2128

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2011/000104

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report	Patent Family Member
US 2010080386	NONE

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX