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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 July 2014 (31.07.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/114981 A3

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

(21) International Application Number:
PCT/IB2013/003259

(22) International Filing Date:
8 October 2013 (08.10.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/711,390	9 October 2012 (09.10.2012)	US
61/747,647	31 December 2012 (31.12.2012)	US
13/826,779	14 March 2013 (14.03.2013)	US

(71) Applicant: **KING ABDULLAH UNIVERSITY OF SCIENCE AND TECHNOLOGY** [SA/SA]; 4700 King Abdullah University of Science and Technology, Thuwal, 23955-6900 (SA).

(72) Inventors: **BARAKAT, Mohamed, L.**; King Abdullah University Of Science And Technology, 4700 King Abdullah University of Science and Technology, Thuwal, 23955-6900 (SA). **MANSINGKA, Abhinav, S.**; King Abdullah University Of Science And Technology, 4700 King Abdullah University of Science and Technology, Thuwal, 23955-6900 (SA). **RADWAN, Ahmed Gomaa, Ahmed**; King Abdullah University Of Science And Technology, 4700 King Abdullah University of Science and Technology, Thuwal, 23955-6900 (SA). **SALAMA, Khaled, Nabil**; King Abdullah University Of Science And Technology, 4700 King Abdullah University of Science and Technology, Thuwal, 23955-6900 (SA).

(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, 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).

Published:

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

(88) Date of publication of the international search report:
30 October 2014

(54) Title: CHAOS-BASED PSEUDO-RANDOM NUMBER GENERATION

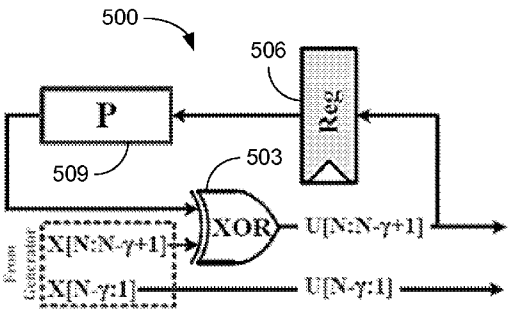


FIG. 5

(57) Abstract: Various methods and systems related to chaos-based pseudo-random number generation are presented. In one example, among others, a system includes a pseudo¬ random number generator (PRNG) to generate a series of digital outputs and a nonlinear post processing circuit to perform an exclusive OR (XOR) operation on a first portion of a current digital output of the PRNG and a permutated version of a corresponding first portion of a previous post processed output to generate a corresponding first portion of a current post processed output. In another example, a method includes receiving at least a first portion of a current output from a PRNG and performing an XOR operation on the first portion of the current PRNG output with a permutated version of a corresponding first portion of a previous post processed output to generate a corresponding first portion of a current post processed output.

WO 2014/114981 A3

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/003259

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.
A	AFFAN ZIDAN M ET AL: "Random number generation based on digital differential chaos", CIRCUITS AND SYSTEMS (MWSCAS), 2011 IEEE 54TH INTERNATIONAL MIDWEST SYMPOSIUM ON, IEEE, 7 August 2011 (2011-08-07), pages 1-4, XP031941211, DOI: 10.1109/MWSCAS.2011.6026266 ISBN: 978-1-61284-856-3 section III ----- -/--	1-14

[X] Further documents are listed in the continuation of Box C.

[X] 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
23 July 2014	31/07/2014

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/003259

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YASUHIRO AKIZAWA ET AL: "Fast Random Number Generation With Bandwidth-Enhanced Chaotic Semiconductor Lasers at 8 $\,\times\,$ 50 Gb/s", IEEE PHOTONICS TECHNOLOGY LETTERS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 24, no. 12, 1 June 2012 (2012-06-01), pages 1042-1044, XP011443996, ISSN: 1041-1135, DOI: 10.1109/LPT.2012.2193388 section A -----	1-14
A	US 4 355 366 A (PORTER SIGMUND N) 19 October 1982 (1982-10-19) abstract figure 1 -----	1-14
A	WO 2009/074889 A1 (NDS LTD [GB]; KALUZHNY URI [IL]) 18 June 2009 (2009-06-18) figure 5 -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2013/003259

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4355366 A	19-10-1982	EP 0067842 A1	29-12-1982
		US 4355366 A	19-10-1982
		WO 8201969 A1	10-06-1982
WO 2009074889 A1	18-06-2009	AT 484791 T	15-10-2010
		EP 2100219 A1	16-09-2009
		ES 2354136 T3	10-03-2011
		IL 188089 A	28-02-2013
		PT 2100219 E	05-01-2011
		US 2010036899 A1	11-02-2010
		WO 2009074889 A1	18-06-2009