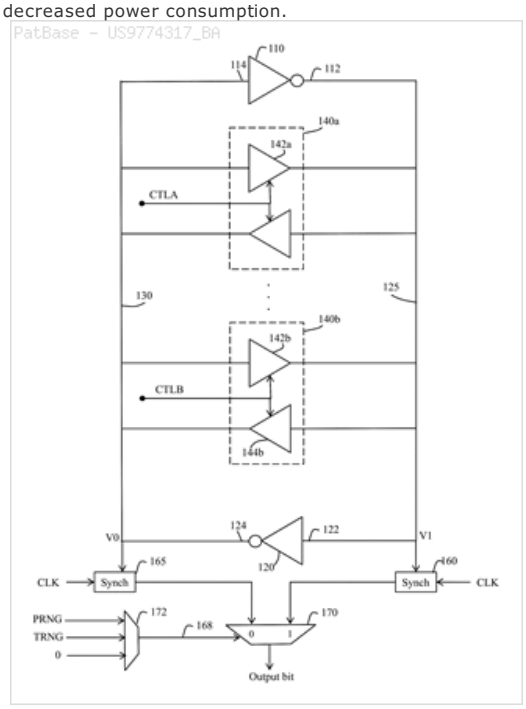
3) Family number: 67059019 (US9774317B)

Title: BISTABLE-ELEMENT FOR RANDOM NUMBER GENERATION

Abstract: A bistable cell includes a pair of inverters and multiple pairs of cross-coupled tristate buffers. Each pair of tristate buffers can be individually selected to implement an entropy harvesting state for the bistable cell. Each of the tristate buffers generally has lower strength than the inverters but the inverter-to-buffer strength ratio can be configured through selective use of one or more of the tristate buffer pairs. The resulting entropy harvesting state behavior can be varied based on the inverter-to-buffer strength ratio in terms of greater randomness of the output bits or decreased power consumption.

Classifications:
International (IPC 8-9): G06F13/40 G06F7/58 H03K19/00 H03K3/03 H03K3/84 (Advanced/Invention)
CPC: H03K3/84 G06F7/588 G06F13/4045 H03K3/03 H03K19/0002 Y02D10/14 Y02D10/151 H03K3/0315



Family:

Publication number	Publication date	Application number	Application date
US9774317 BA	20170926	US20160250574	20160829
US10187044 BA	20190122	US20170694165	20170901

Priority:
US20160250574 20160829 US20170694165 20170901

Probable Assignee: AMAZON TECHNOLOGIES INC
Assignee(s): (std): AMAZON TECH INC
Assignee(s): AMAZON TECHNOLOGIES INC
Inventor(s): (std): TROCK DAN ; VALFER ELAD ; DIAMANT RON ; ARMOZA YAIR
Agent(s): BLANK ROME LLP

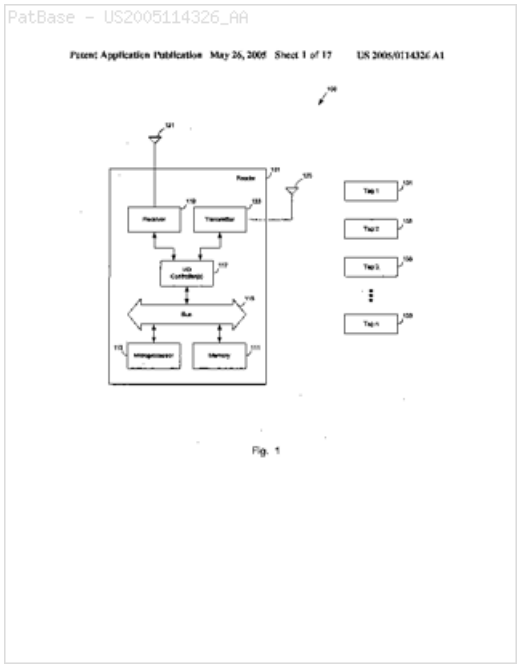
4) Family number: 31553021 (US2005114326A)

Title: METHODS AND APPARATUSES TO IDENTIFY DEVICES

Abstract: Embodiments of the present invention include systems with Readers and Tags in which a Reader queries the Tags with a parameter that includes a level of probability of reply according to which the Tags individually and randomly decide whether or not to reply. In one embodiment, the Tags can switch between two states: A and B. The query command also specifies a state (A or B) so that only the Tags in the specified state can reply. After successfully sending the Tag identification data from a Tag to the Reader, the Tag switches to the other state from the specified state. In one embodiment, the operations about the two states are symmetric. In one embodiment, the Tags can remember the parameters used in a query so that a short form of query command can be used to repeat the query with the same query parameters.

Classifications:
International (IPC 8-9): G06F17/00 G06F17/30 G06F7/00 G06K G06K17/00 G06K19/07 G06K7/00 G06K7/01 G06K7/08 G06K7/10 G08B13/14 G08B13/24 H04B1/59 H04B5/02 H04Q5/22 (Advanced/Invention);

G06F17/30 G06K17/00 G06K19/07 G06K7/00 (Advanced/Non-invention);
G06F17/00 G06F17/30 G06F7/00 G06K19/07 G06K7/00
H04Q5/00 (Core/Invention);
G06F17/30 (Core/Non-invention);
G06K (Subclass/Invention)
International (IPC 1-7): G06F17/60 G06F7/00 G06K19/07 G06K7/00 G06K7/10
CPC: G06K7/10009 Y10S707/99931 Y10S707/99933 Y10S707/99945 G06K7/0008 G06K7/10039 G06K7/10059 G06K7/10346 G06K19/0723 G06K7/10366 G08B13/2485
European: G06K19/07T G06K7/00E G06K7/10A1A1 G06K7/10A1A3 G06K7/10A8E
US: 1/1 235/385 235/385P 340/10.1 340/10.2 340/10.32 340/10.320S 340/10.33 340/10.4 340/10.400P 340/10.5 340/10.500P 340/572.1 340/870.2 707/1 707/100 707/104.1 707/2 707/3 707/4 707/5 707/6 707/707 707/713 707/769 707/770 707/999.001 707/999.003 707/999.1 707/999.104 707/999.107 709/237
JP F-Term: 5B035 5B035/AA11 5B035/BB09 5B035/CA23 5B035/CA31 5B058 5B058/CA17 5B058/CA19 5B058/CA23 5B058/KA02 5B058/KA21 5B072 5K012 5K012/AB18 5K054
JP F-Index: G06K17/00/F G06K19/00/H G06K19/07/230 G06K7/00/008 G06K7/10/112 G06K7/10/120 G06K7/10/236 H04B1/59 H04B5/02



Family:

Publication number	Publication date	Application number	Application date
AT523858 E	20110915	AT20040163545T	20041105
AU2004290371 AA	20050526	AU20040290371	20041105
AU2004290371 BB	20101111	AU20040290371	20041105
CA2544704 AA	20060502	CA20042544704	20041105
CN100541527 C	20090916	CN200480029427	20040809
CN100557628 C	20091104	CN200480032318	20041105
CN1864167 A	20061115	CN200480029427	20040809
CN1875371 A	20061206	CN200480032318	20041105
DE602004022077 D1	20090827	DE200460022077T	20041105
DE602004034290 D1	20111117	DE200460034290T	20041105
DE602004041800 D1	20130613	DE200460041800T	20040809
EP1665120 A1	20060607	EP20040780679	20040809
EP1665120 B1	20130417	EP20040780679	20040809
EP1683079 A1	20060726	EP20040800815	20041105
EP1683079 B1	20090715	EP20040800815	20041105
EP1683079 B9	20120222	EP20040800815	20041105
EP2098980 A1	20090909	EP20090163545	20041105
EP2098980 B1	20110907	EP20090163545	20041105
HK1136062 A1	20100618	HK20100101957	20100224
HK1136062 B	20120706	HK20100101957	20100224
IN01903CN2006 A	20070608	IN2006CN01903	20060530
IN256099 B	20130503	IN2006CN01903	20060530
JP2007514343 T2	20070531	JP20060539679T	20041105
JP4713491 B2	20110629	JP20060539679T	20041105
KR20060131773 A	20061220	KR20067011176	20041105
US2005114326 AA	20050526	US20040982557	20041105
US2005263591 AA	20051201	US20040915725	20040809
US2006117066 AA	20060601	US20050271629	20051109
US2006143163 AA	20060629	US20050271628	20051109
US2010207739 AA	20100819	US20100772922	20100503
US2012154123 AA	20120621	US20110330384	20111219
US2014354416 AA	20141204	US20140303520	20140612
US2015015375 AA	20150115	US20140284341	20140521
US7562083 BB	20090714	US20050271628	20051109
US7716160 BB	20100511	US20040982557	20041105
US7716208 BB	20100511	US20050271629	20051109
US8102244 BB	20120124	US20040915725	20040809
US8742899 BB	20140603	US20110330384	20111219
US8768952 BB	20140701	US20100772922	20100503
US9483671 BB	20161101	US20140303520	20140612
WO05015480 A2	20050217	WO2004US25883	20040809
WO05015480 C1	20060309	WO2004US25883	20040809
WO05015480 C2	20080313	WO2004US25883	20040809
WO05048180 A1	20050526	WO2004US36991	20041105

Priority:

US20030494143P 20030809 US20030518229 20031107 US20030518229P 20031107

EP20040780679 20040909 US20040015725 20040909 WO2004US25893 20040909
EP20040808815 20041105 EP20090163545 20041105 US20040982597 20041105
WO2004US36991 20041105 US20050271629 20051109 US20050271628 20051109
US20100772922 20100503 US20110330384 20111219 US20140284341 20140521
US20140303520 20140612

Probable Assignee: ALIEN TECHNOLOGY LLC

Assignee(s): (std): ALIEN TECH CORP ; RUIZHANG TECH CO LTD ; SMITH JOHN STEPHEN ; SMITH JOHN S ; RUIZHANG TECH LTD CO ; CARRENDER CURTIS L ; ALIEN TECHNOLOGY CORP

Assignee(s): ALIEN TECHNOLOGY LLC ; EAST WEST BANK ; RUIZHANG TECHNOLOGY CO LTD ; ALIEN TECHNOLOGY LLC WAS KNOWN AS ALIEN TECHNOLOGY CORPORATION.. ; QUATROTEC INC

Inventor(s): (std): CURTIS L CARRENDER ; JOHN STEPHEN SMITH ; SMITH JOHN STEPHEN ; SMITH JOHN STEPHEN CARRENDER C ; STEPHEN SMITH JOHN ; SMITH JOHN S ; SMITH JOHN ; CARRENDER CURTIS ; CARRENDER CURTIS L

Inventor(s): CARRENDER CURTIS L MORGAN HILL ; SMITH JOHN STEPHEN CARRENDER CURTIS L ; SMITH JOHN STEPHEN SAN JOSE

Agent(s): FPA PATENT ATTORNEYS PTY LTD; FREEHILLS PATENT AND TRADE MARK ATTORNEYS; FREEHILLS PATENT ATTORNEYS; FREEHILLS PATENT ATTORNEY S; HERBERT SMITH FREEHILLS; RICHES MCKENZIE AND HERBERT LLP; SAMSON AND PARTNER PATENTANWAELTE MBB; WP THOMPSON AND CO; WP THOMPSON; CALLON DE LAMARCK JEAN ROBERT; COLLIN JEROME; ELLA CHEONG HONG KONG LTD; YAMAKAWA MASAKI; BLAKELY SOKOLOFF TAYLOR AND ZAFMAN LLP; BLAKELY SOKOLOFF TAYLOR AND ZAFMAN LLP, SEVENTH FLOOR; BLAKELY SOKOLOFF TAYLOR AND ZAFMAN LLP SEVENTH FLOOR; BLAKELY SOKOLOFF TAYLOR AND ZAFMAN

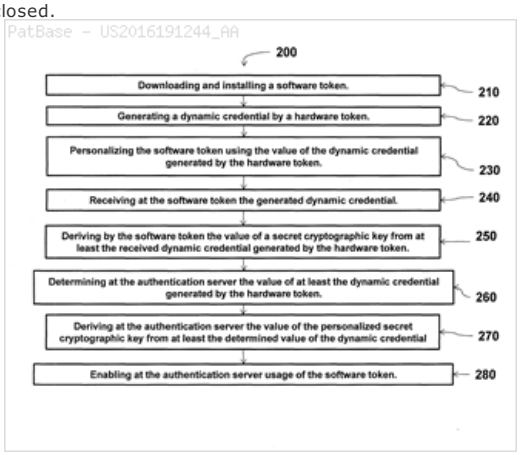
Designated states: AE AG AL AM AT AU AZ BA BB BE BF BG BJ BR BW BY BZ CA CF CG CH CI CM CN CO CR CU CY CZ DE DK DM DZ EC EE EG ES FI FR GA GB GD GE GH GM GN GQ GR GW HR HU ID IE IL IN IS IT JP KE KG KP KR KZ LC LI LK LR LS LT LU LV MA MC MD MG MK ML MN MR MW MX MZ NA NE NI NL NO NZ OM PG PH PL PT RO RU SC SD SE SG SI SK SL SN SY SZ TD TG TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

5) Family number: 62794022 (US2016191244A)

Title: METHOD AND APPARATUS FOR SECURING A MOBILE APPLICATION

Abstract: Methods, apparatus, and systems for personalizing a software token using a dynamic credential (such as a one-time password or electronic signature) generated by a hardware token are disclosed.

Classifications:
International (IPC 8-9): G06F21/30 G06F21/31 G06F21/45 G06Q20/40 G09C1/00 H04L29/06 H04L9/06 H04L9/08 H04L9/32 (Advanced/Invention)
International (IPC 1-7): H04L29/06
CPC: G06Q20/401 H04L9/0656 H04L9/3271 H04L63/0823 H04L63/083 H04L63/0876 H04L9/3213 H04L9/3247 G06F21/31 G06F21/45 H04L9/3228 H04L9/3234 H04L63/0435 H04L63/0838 H04L63/0853 H04L63/0861 H04L63/123
US: 1/1 713/155 713/159
JP F-Term: 5B285 5J104 5J104/AA07 5J104/KA01 5J104/KA04 5J104/KA21 5J104/NA02 5J104/PA07
JP F-Index: G06F21/31 G09C1/00/640/E H04L9/00/601/B H04L9/00/675/A H04L9/00/675/D



Family:

Publication number	Publication date	Application number	Application date
BR112017014014 A2	20180102	BR20171114014	20151229
CN107409049 A	20171128	CN201580077086	20151229
CN107409049 B	20200529	CN201580077086	20151229
DE602015029586 D1	20190523	DE201560029586T	20151229
EP3241335 A2	20171108	EP20150885779	20151229
EP3241335 B1	20190501	EP20150885779	20151229
EP3605997 A1	20200205	EP20190171964	20151229
IN201737022478 A	20170915	IN201737022478	20170627
JP2018507586 T2	20180315	JP20170534638T	20151229
JP6514337 B2	20190515	JP20170534638T	20151229
MX2017008651 A1	20180426	MX20170008651	20151229
US2016191244 AA	20160630	US20150982147	20151229
US2016191494 AA	20160630	US20150982166	20151229
US9525549 BB	20161220	US20150982147	20151229
US9525550 BB	20161220	US20150982166	20151229
WO16190903 A2	20161201	WO2015US67784	20151229
WO16190903 A3	20170119	WO2015US67784	20151229

Priority:

US20140097376P 20141229 EP20150885779 20151229 US20150982147 20151229
US20150982166 20151229 WO2015US67784 20151229

Probable Assignee: ONESPAN NORTH AMERICA INC

Assignee(s): (std): VASCO DATA SECURITY INT GMBH ; VASCO DATA SECURITY INT INC ; VASCO DATA SECURITY INC ; ONESPAN INT GMBH

Assignee(s): ONESPAN NORTH AMERICA INC

Inventor(s): (std): COULIER FRANK ; MATHIAS CLAES ; FRANK COULIER ; CLAES MATHIAS

Agent(s): BECK MICHAEL ANDRIES T; RATNERPRESTIA; WEED STEPHEN J

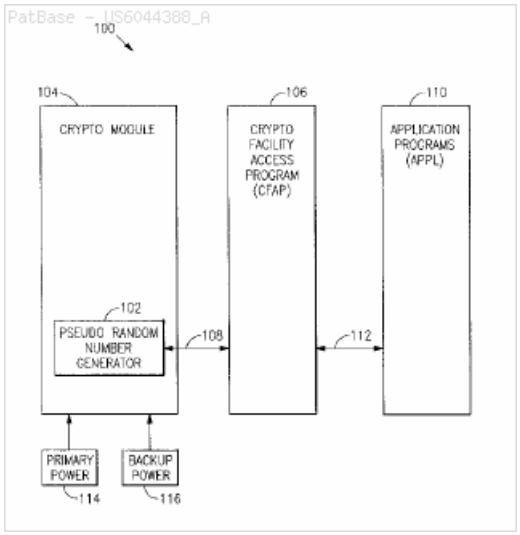
Designated states: AE AG AL AM AO AT AU AZ BA BB BE BF BG BH BJ BN BR BW BY BZ CA CF CG CH CI CL CM CN CO CR CU CY CZ DE DK DM DO DZ EC EE EG ES FI FR GA GB GD GE GH GM GN GQ GR GT GW HN HR HU ID IE IL IN IR IS IT JP KE KG KM KN KP KR KZ LA LC LI LK LR LS LT LU LV LY MA MC MD ME MG MK ML MN MR MT MW MX MY MZ NA NE NG NI NL NO NZ OM PA PE PG PH PL PT QA RO RS RU RW SA SC SD SE SG SI SK SL SM SN ST SV SY SZ TD TG TH TJ TM TN TR TT TZ UA UG US UZ VC VN ZA ZM ZW

6) Family number: 12163026 (US6044388A)

Title: PSEUDORANDOM NUMBER GENERATOR

Abstract: Pseudorandom numbers are generated in a cryptographic module in a cryptographically strong manner by combining a time-dependent value with a secret value and passing the result through a one-way hash function to generate a hash value from which a random number is generated. The secret value is continually updated whenever the cryptographic module is idle by a first feedback function that generates an updated secret value as a one-way function of the current secret value and the time-dependent value. In addition, the secret value is updated on the occurrence of a predetermined external event by a second feedback function that generates an updated secret value as a one-way function of the current secret value, the time-dependent value and an externally supplied value. Upon power-on reset, if the pseudorandom number generator has not been previously initialized, it initializes itself by resetting the time-dependent and secret values and requiring the second feedback function to perform a predetermined number of updates of the secret value in response to external events. Otherwise, the time-dependent and secret values are restored using values stored in backup registers. A hash of the current secret value that is different from either feedback function is used as a backup secret value to minimize the possibility that restoration will result in repetition of pseudorandom numbers.

Classifications:
International (IPC 8-9): G06F7/58 H04L9/22 (Advanced/Invention); G06F7/58 H04L9/18 (Core/Invention)
International (IPC 1-7): G06F1/02 G06F7/58
CPC: H04L9/0662 G06F7/582 G06F7/588 H04L2209/26
European: G06F7/58P G06F7/58R H04L9/22
US: 380/28 380/46 708/250 708/254



Family:

Publication number	Publication date	Application number	Application date
US6044388 A	20000328	US19970856562	19970515

Priority:

US19970856562 19970515

Probable Assignee: RPX CORP

Assignee(s): (std): IBM

Assignee(s): INT BUSINESS MACHINE CORP ; INT BUSINESS MACHINES CORP ; RPX CORP

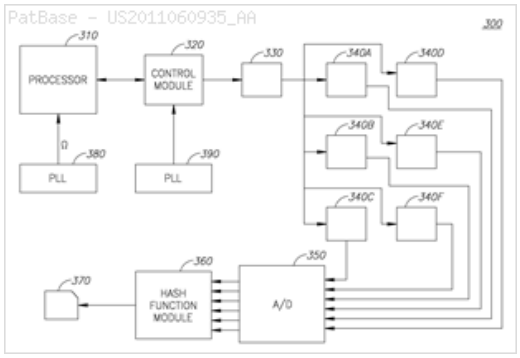
Inventor(s): (std): DEBELLIS ROBERT S ; SMITH SR RONALD M ; YEH PHIL CHI CHUNG

7) Family number: 48437037 (US2011060935A)

Title: GENERATING A RANDOM NUMBER IN AN EXISTING SYSTEM ON CHIP

Abstract: A system for generating a true random number and implemented within an existing System on Chip (SoC) is provided herein. The system includes one or more sub circuitry synchronous modules configured to operate in a specified nominal clock rate, wherein each sub circuitry synchronous modules yields expected deterministic results when operating in its nominal clock rate; and a control module configured to clock the one or more sub circuitry synchronous modules each in a clock rate higher than its respective the nominal clock rate and beyond a specified value, to yield a non deterministic behavior of the one or more sub circuitry synchronous modules, resulting in one or more random signals, wherein the system is implemented within an existing system on chip (SOC).

Classifications:
International (IPC 8-9): G06F1/00 G06F7/58 (Advanced/Invention)
CPC: G06F7/588
European: G06F7/58R
US: 708/250 708/255 713/500 713/500P



Family:

Publication number	Publication date	Application number	Application date
US2011060935 AA	20110310	US20100876304	20100907
US8522065 BB	20130827	US20100876304	20100907

Priority:

US20090240211P 20090906 US20100876304 20100907

Probable Assignee: BROADCOM SEMICONDUCTORS ISRAEL LTD

Assignee(s): (std): CARMON RAFY ; DANIEL AVI ; MANN YEHOSHUA ; PERCELLO LTD ; REGEV GUY ; SOKOLOV RAM

Assignee(s): BROADCOM SEMICONDUCTORS ISRAEL LTD ; BROADCOM COMMUNICATIONS ISRAEL LTD

Inventor(s): (std): SOKOLOV RAM ; REGEV GUY ; MANN YEHOSHUA ; DANIEL AVI ; CARMON RAFY

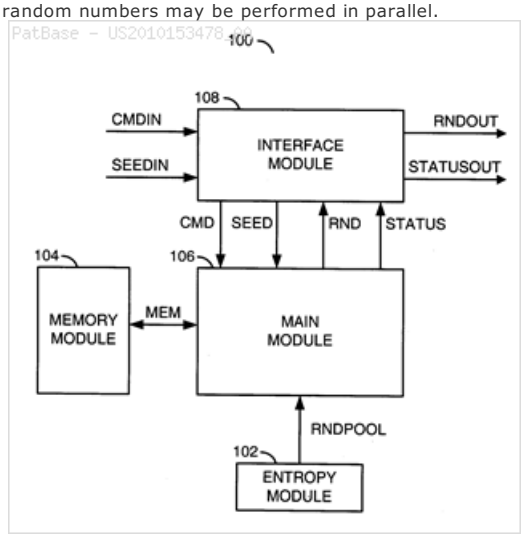
Agent(s): STERNE KESSLER GOLDSTEIN AND FOX PLLC

8) Family number: 45444039 (US2010153478A)

Title: PARALLEL TRUE RANDOM NUMBER GENERATOR ARCHITECTURE

Abstract: A system having an entropy module, a memory module and a main module is disclosed. The entropy module may be configured to generate a plurality of first random numbers. The memory module may be configured to buffer (i) the first random numbers and (ii) a plurality of second random numbers. The main module is generally configured to (i) control a first transfer of the first random numbers from the entropy module to the memory module, (ii) control a second transfer of the first random numbers from the memory module to the main module, (iii) generate the second random numbers by encrypting the first random numbers and (iv) control a third transfer of the second random numbers from the main module to the memory module. The generation of the first random numbers and the generation of the second random numbers may be performed in parallel.

Classifications:
International (IPC 8-9): G06F15/16 G06F17/30 G06F7/58 H04L9/28 (Advanced/Invention); G06F7/58 H04L9/28 (Core/Invention)
CPC: H04L9/0662 G06F7/58 G06F7/588 H04L9/0631 H04L2209/125 H04L2209/26
European: G06F7/58 G06F7/58R H04L9/08H H04L9/22
US: 380/28 380/28S 707/899 708/255 708/255P 726/9



Family:

Publication number	Publication date	Application number	Application date
US2010153478 AA	20100617	US20080335870	20081216
US8539009 BB	20130917	US20080335870	20081216

Priority:

US20080335870 20081216

Probable Assignee: AVAGO TECHNOLOGIES LTD

Assignee(s): (std): ALISEYCHIK PAVEL A ; GASANOV ELYAR E ; IZYUMIN OLEG N ; LSI CORP ; NEZNANOV ILYA V ; PANTELEEV PAVEL A

Assignee(s): AVAGO TECHNOLOGIES GENERAL IP SINGAPORE PTE LTD ; AVAGO TECHNOLOGIES LTD ; BANK OF AMERICA NA COLLATERAL AGENT AS ; DEUTSCHE BANK NEW YORK BRANCH COLLATERAL AGENT AG AS ; AGERE SYSTEMS LLC

Inventor(s): (std): PANTELEEV PAVEL A ; NEZNANOV ILYA V ; IZYUMIN OLEG N ; GASANOV ELYAR E ; ALISEYCHIK PAVEL A

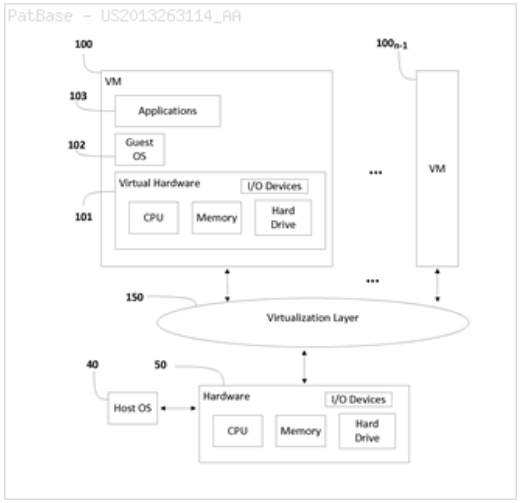
Agent(s): CHRISTOPHER P MAIORANA PC LSI CORP; CHRISTOPHER P

9) Family number: 54914041 (US2013263114A)

Title: DETECTING A REPEATING EXECUTION TIME SEQUENCE IN A VIRTUAL MACHINE

Abstract: A generation identifier is provided having a value established upon generating a new virtual machine configuration context or a snapshot of a virtual machine configuration context. The generation identifier is configured to be sampled in order to indicate whether the sampled generation is a latest generation. To use the generation identifier, a service or application persists the generation identifier upon resuming or initiating operation. During normal operation or replay, the persisted generation identifier is compared to the generation identifier sampled from a location associated with the virtual machine configuration context on which the service or application is being run before performing a requested process or committing to a transaction. When the sampled generation identifier is different than the persisted generation identifier, the service or application knows that it is running a time-shifted operation such as from a snapshot replay.

Classifications:
International (IPC 8-9): G06F9/455 G06F9/46 (Advanced/Invention)
CPC: G06F9/45558 G06F2009/45562
US: 1/1 718/1



Family:

Publication number	Publication date	Application number	Application date
US2013263114 AA	20131003	US20120430689	20120327
US9250945 BB	20160202	US20120430689	20120327

Priority:

US20120430689 20120327

Probable Assignee: MICROSOFT CORP

Assignee(s): (std): JOHNSON GREGORY C ; MICROSOFT CORP ; MICROSOFT TECHNOLOGY LICENSING LLC ; WATKINS DOUGLAS A

Inventor(s): (std): JOHNSON GREGORY C ; WATKINS DOUGLAS A

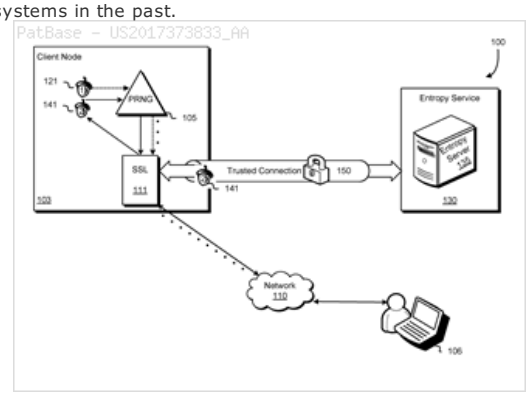
Agent(s): JOHM; MICKY; JUDY

10) Family number: 66748043 (US2017373833A)

Title: ESTABLISHING ENTROPY ON A SYSTEM

Abstract: Servers in datacenters, mobile devices and virtualized servers without human interaction may experience difficulties in establishing entropy in a virtualized computing environment. Entropy is an important foundation for cryptography and a lack of entropy has led to weaknesses that can be used to break cryptographic systems in the past.

Classifications:
International (IPC 8-9): G06F7/58 H04L29/06 H04L29/08 H04L9/00 H04L9/06 H04L9/08 (Advanced/Invention)
CPC: H04L9/002 H04L9/0662 H04L9/0877 H04L63/164 G06F7/582 H04L67/10
US: 1/1 713/150



Family:

Publication number	Publication date	Application number	Application date
US2017373833 AA	20171228	US20170685669	20170824

US9749127 BA	20170829	US20140294997	20140603
US10419205 BB	20190917	US20170685669	20170824

Priority:

US20140294997 20140603 US20170685669 20170824

Probable Assignee: AMAZON TECHNOLOGIES INC

Assignee(s): (std): AMAZON TECH INC

Assignee(s): AMAZON TECHNOLOGIES INC

Inventor(s): (std): CIGNETTI TODD LAWRENCE ; DOANE ANDREW JEFFREY

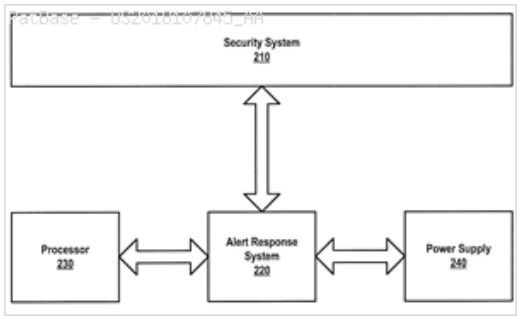
Agent(s): DAVIS WRIGHT TREMAINE LLP

11) Family number: 67439054 (US2018107845A)

Title: ACTIVE ASIC INTRUSION SHIELD

Abstract: Provided are systems, methods, and apparatus for protecting an integrated circuit against invasive attacks and various forms of tampering. A defensive mechanism is an active physical security shield that includes an array of traces at a high metal of the integrated circuit, covering a high percentage of the surface area of that layer, and a collection of digital logic components that drive signals across the traces. The driving of the signals across the traces is done in an active manner such that a short, open, or stuck-at fault on any of the traces is detected within a very short period of time. The active security system is connected to or in communication with an alert response mechanism, such that a fault detected by the security system results in a signal being sent to the alert response mechanism.

Classifications:
International (IPC 8-9): G06F1/14 G06F1/26 G06F21/00 G06F21/50 G06F21/55 G06F21/70 G06F21/76 G06F21/86 G06F21/87 H01L23/00 (Advanced/Invention)
CPC: G06F21/55 G06F21/87 H01L23/528 H01L23/576 G06F21/76 G06F21/86 G06F1/14 G06F1/26 G06F21/50
US: 1/1 726/23



Family:

Publication number	Publication date	Application number	Application date
CN107958153 A	20180424	CN201710872406	20170925
CN207380709 U	20180518	CN201721238846U	20170925
DE102017118325 A1	20180419	DE201710118325	20170811
DE202017104846 U1	20171228	DE201720104846U	20170811
GB201714963 A0	20171101	GB20170014963	20170918
GB2556411 A1	20180530	GB20170014963	20170918
GB2556411 B2	20200101	GB20170014963	20170918
TW201827979 A	20180801	TW20170128517	20170823
TWI681281 B	20200101	TW20170128517	20170823
US2018107845 AA	20180419	US20160294525	20161014
US9946899 BA	20180417	US20160294525	20161014
WO18071091 A1	20180419	WO2017US46341	20170810

Priority:

US20160294525 20161014

Probable Assignee: GOOGLE INC

Assignee(s): (std): GOOGLE LLC N D GES D STAATES DELAWARE ; GOOGLE LLC ; GOOGLE INC

Assignee(s): GOOGLE LLC NDGESD STAATES DELAWARE

Inventor(s): (std): BOS LYNN ; JOHNSON SCOTT ; JOHNSON SCOTT D ; LYNN BOS ; SCOTT JOHNSON ; WESSON WILLIAM ; WILLIAM WESSON

Agent(s): COLBY NIPPER; COLBY MICHAEL K

Designated states: AE AG AL AM AO AT AU AZ BA BB BE BF BG BH BJ BN BR BW BY BZ CA CF CG CH CI CL CM CN CO CR CU CY CZ DE DJ DK DM DO DZ EC EE EG ES FI FR GA GB GD GE GH GM GN GQ GR GT GW HN HR HU ID IE IL IN IR IS IT JO JP KE KG KH KM KN KP KR KW KZ LA LC LK LR LS LT LU LV LY MA MC MD ME MG MK ML MN MR MT MW MX MY MZ NA NE NG NI NL NO NZ OM PA PE PG PH PL PT QA RO RS RU RW SA SC SD SE SG SI SK SL SM SN ST SV SY SZ TD TG TH TJ TM TN TR TT TZ UA UG US UZ VC VN ZA ZM ZW

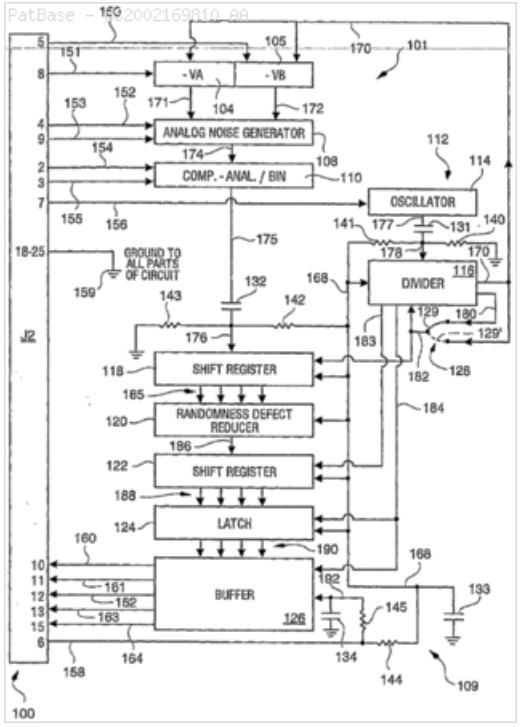
12) Family number: 28301063 (US2002169810A)

Title: RANDOM NUMBER GENERATOR AND GENERATION METHOD

Abstract: An RNG circuit is connected to the parallel port of a computer. The circuit includes a flat source of white noise and a CMOS amplifier circuit compensated in the high frequency range. A low-frequency cut-off is selected to maintain high band-width yet eliminate the 1/f amplifier noise tail. A CMOS comparator with a 10 nanosecond rise time converts the analog signal to a binary one. A shift register converts the serial signal to a 4-bit parallel one at a sample rate selected at the knee of the serial dependence curve. Two levels of XOR defect correction produce a BRS at 20 kHZ, which is converted to a 4-bit parallel word,

latched and buffered. The entire circuit is powered from the data pins of the parallel port. A device driver interface in the computer operates the RNG. The randomness defects with various levels of correction and sample rates are calculated and the RNG is optimized before manufacture.

Classifications:
International (IPC 8-9): A63F3/00 G06F1/02 G06F7/58 (Advanced/Invention); A63F3/00 (Core/Invention)
International (IPC 1-7): A63F1/00 G06F1/02 G06F7/58
CPC: G06F7/58 G06F7/588 A63F3/00157
European: A63F3/00A32 G06F7/58 G06F7/58R
US: 273/292 273/292P 708/250 708/250P 708/255 714/44



Family:

Publication number	Publication date	Application number	Application date
US2002169810 AA	20021114	US20020173520	20020617
US2004173967 AA	20040909	US20040776700	20040212
US2007033242 AA	20070208	US20060507959	20060821
US6324558 BA	20011127	US19950388631	19950214
US6763364 BA	20040713	US20000699523	20001030
US6763364 C1	20100525	US20000699523	20001030
US7096242 BB	20060822	US20020173520	20020617
US7096242 C1	20130222	US20020173520	20020617
US7752247 BB	20100706	US20060507959	20060821

Priority:

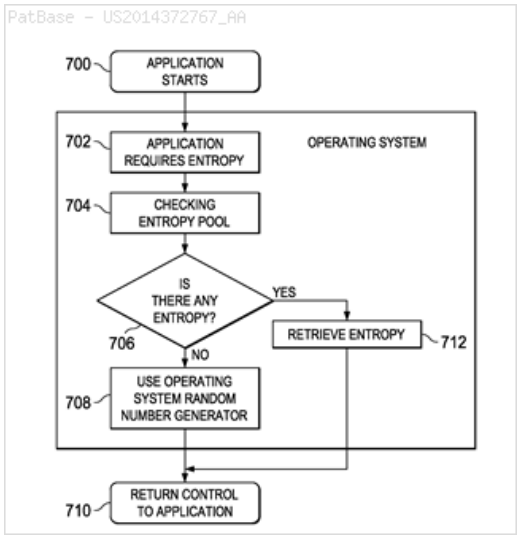
US19950388631 19950214 US20000699523 20001030 US20020173520 20020617
US20040776700 20040212 US20060507959 20060821

Probable Assignee: QUANTUM WORLD CORP
Assignee(s): (std): QUANTUM WORLD CORP ; WILBER SCOTT A
Assignee(s): NAMA DINH DUC
Inventor(s): (std): WILBER SCOTT A ; NAMA DINH DUC
Inventor(s): SCOTT A WILBER
Agent(s): THOMAS SWENSON; PATTON BOGGA LLP; CARL A; THOMAS

13) Family number: 58069063 (US2014372767A)

Title: POOLING ENTROPY TO FACILITATE MOBILE DEVICE-BASED TRUE RANDOM NUMBER GENERATION

Abstract: A mobile device operating system pools any available entropy. The resulting entropy pool is stored in device memory. When storing entropy in memory, preferably memory addresses are randomly allocated to prevent an attacker from capturing entropy that might have already been used to create a random number. The stored entropy pool provides a readily-available entropy source for any entropy required by the operating system or device applications. Then, when a cryptographic application requests a true random number, the operating system checks to determine whether the pool has available entropy and, if so, a portion of the entropy is provided to enable generation (e.g., by a TRNG) of a true random number that, in turn, may then be used for some cryptographic operation. After providing the entropy, the operating system clears the address locations that were used to provide it so that another entity cannot re-use the entropy.
Classifications:
International (IPC 8-9): G06F21/72 G06F7/58 (Advanced/Invention)
CPC: G06F21/72 G06F7/588 G06F21/73
US: 1/1 713/189



Family:

Publication number	Publication date	Application number	Application date
US2014372767 AA	20141218	US20130916655	20130613
US9449197 BB	20160920	US20130916655	20130613

Priority:

US20130916655 20130613

Probable Assignee: GLOBALFOUNDRIES INC

Assignee(s): (std)**:** GLOBAL FOUNDRIES INC ; GLOBALFOUNDRIES INC ; IBM

Assignee(s): INT BUSINESS MACHINES CORP ; WILMINGTON TRUST NATIONAL ASSOCIATION ; GLOBALFOUNDRIES US 2 LLC

Inventor(s): (std)**:** WALTENBERG PETER THEODORE ; GREEN MATTHEW JOHN ; MCLEAN LEIGH STUART

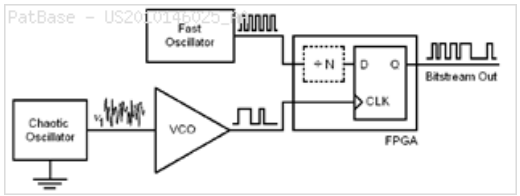
Agent(s): DELIO PETERSON AND CURCIO LLC; DAVID R

14) Family number: 42574063 (US2010146025A)

Title: METHOD AND HARDWARE FOR GENERATING RANDOM NUMBERS USING DUAL OSCILLATOR ARCHITECTURE AND CONTINUOUS-TIME CHAOS

Abstract: Novel random number generation methods and novel random number generators based on continuous-time chaotic oscillators with dual oscillator architecture are presented. Numerical and experimental results not only verify the feasibility of the proposed circuits, but also encourage their use as a high-performance IC TRNG. In comparison with RNG's based on discrete-time chaotic maps, amplification of a noise source and jittered oscillator sampling, which are advantageous in the sense that true random behavior can be mathematically proven thanks to an analytical model that has been developed, it is seen that RNG's based on continuous-time' chaotic oscillators can offer much higher and constant data rated without post-processing. The proposed innovation increases the throughput, maximizes the statistical quality of the output sequence and is robust against against external interference, parameter variations and attacks aimed to force throughout. The proposed circuits can be integrated on today process at GHz range.

Classifications:
International (IPC 8-9): G06F7/58 H03K3/84 (Advanced/Invention); G06F7/58 H03K3/00 (Core/Invention)
CPC: G06F7/588 H03K3/84 H04L9/001
European: G06F7/58R H03K3/84 H04L9/00C
US: 708/251 708/251P



Family:

Publication number	Publication date	Application number	Application date
EP2176739 A1	20100421	EP20070735990	20070522
EP2176739 B1	20170719	EP20070735990	20070522
EP2605126 A1	20130619	EP20120006948	20070522
EP2618253 A1	20130724	EP20120006949	20070522
EP2618253 B1	20190213	EP20120006949	20070522
ES2644485 T3	20171129	ES20070735990T	20070522
TR201716176 T4	20180221	TR20170016176T	20070522
TR201907170 T4	20190621	TR20190007170T	20070522
US2010146025 AA	20100610	US20070601453	20070522
US8612501 BB	20131217	US20070601453	20070522
WO08142488 A1	20081127	WO2007IB51938	20070522

Priority:

EP20070735990 20070522 EP20120006948 20070522 WO2007IB51938 20070522
EP20120006949 20070522

Probable Assignee: SCIENTIFIC AND TECHNOLOGICAL RESEARCH COUNCIL OF TURKEY TUBITAK

Assignee(s): (std)**:** ERGUN SALIH ; SCIENT AND TECHNOLOGICAL RES COU ; SCIENT TECHNOLOGICAL RES COUNCIL OF TURKEY TUBITAK ; TUBITAK TURKIYE BILIMSEL VE TE ; TUBITAK

Assignee(s): TUERKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU TUEBITAK ; SCIENTIFIC TECHNOLOGICAL RESEARCH COUNCIL OF TURKEY TUBITAK ; TUBITAK TURKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU ; TUBITAK TURKIYE BILIMSEL VE TEKNOLOJIK VE ARASTIMA KURUMU ; SCIENTIFIC AND TECHNOLOGICAL RESEARCH COUNCIL OF T ; SCIENTIFIC AND TECHNOLOGICAL RESEARCH COUNCIL OF TURKEY (TUBITAK) ; SCIENTIFIC AND TECHNOLOGICAL RESEARCH COUNCIL OF TURKEY TUBITAK

Inventor(s): (std)**:** ERGUN SALIH

Inventor(s): SALIH ERGUN

Agent(s): MARTIN VICTORIA SOFIA; ARENT FOX LLP

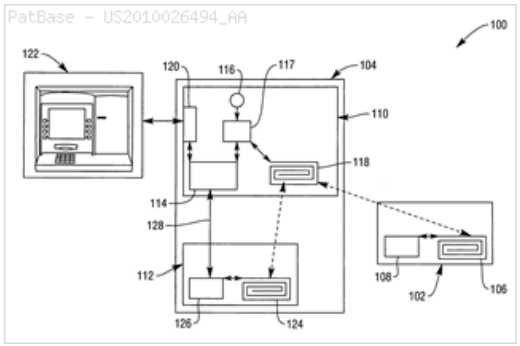
Designated states: AE AG AL AM AT AU AZ BA BB BE BF BG BH BJ BR BW BY BZ CA CF CG CH CI CM CN CO CR CU CY CZ DE DK DM DZ EC EE EG ES FI FR GA GB GD GE GH GM GN GQ GR GT GW HN HR HU ID IE IL IN IS IT JP KE KG KM KN KP KR KZ LA LC LI LK LR LS LT LU LV LY MA MC MD MG MK ML MN MR MT MW MX MY MZ NA NE NG NI NL NO NZ OM PG PH PL PT RO RS RU SC SD SE SG SI SK SL SM SN SV SY SZ TD TG TJ TM TN TR TT TZ UA UG US UZ VC VN ZA ZM ZW

15) Family number: 44312083 (US2010026494A)

Title: RADIO FREQUENCY DATA READER

Abstract: An RFID or NFC reader is associated via a data link with a tag module such that when the reader transmits an interrogation signal the tag module responds with a random, or constrained random, information signal. The information signal masks a signal transmitted by an RFID or NFC tag which the reader is interrogating, making fraudulently obtaining details contained in the tag transmission more difficult.

Classifications:
International (IPC 8-9): G06K7/00 G08B13/14 H04L9/00 H04Q5/22 (Advanced/Invention);
G08B13/14 H04Q5/00 (Core/Invention)
CPC: G06K7/0008 H04L9/0819
European: G06K7/00E
US: 235/375 235/376 235/377 235/380 235/385 340/10.1 340/10.100S 340/572.1 340/572.100P 340/572.2 340/572.3 340/572.4 340/572.5 340/572.6



Family:

Publication number	Publication date	Application number	Application date
EP2149851 A1	20100203	EP20090158988	20090428
US2010026494 AA	20100204	US20080220845	20080729
US8035521 BB	20111011	US20080220845	20080729

Priority:

US20080220845 20080729

Probable Assignee: NCR CORP

Assignee(s): (std)**:** NCR CORP

Assignee(s): JPMORGAN CHASE BANK NA ADMINISTRATIVE AGENT AS ; JPMORGAN CHASE BANK NA

Inventor(s): (std)**:** LEES STEWART ; LEES STEWART D

Agent(s): MACLEOD RODERICK WILLIAM; MICHAEL CHAN NCR CORP; PAUL W

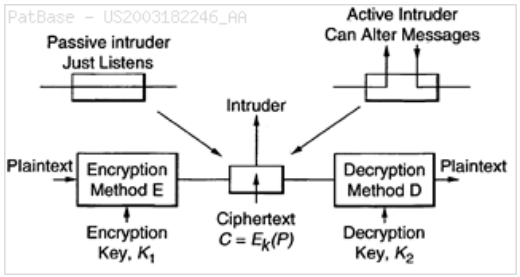
Designated states: AL AT BA BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK TR

16) Family number: 31477084 (US2003182246A)

Title: APPLICATIONS OF FRACTAL AND/OR CHAOTIC TECHNIQUES

Abstract: This invention relates to the application of techniques based upon the mathematics of fractals and chaos in various fields including document verification, data encryption and weather forecasting. The invention also relates, in one of its aspects, to image processing.

Classifications:
International (IPC 8-9): G06N7/08 (Advanced/Invention);
G06N7/00 (Core/Invention)
International (IPC 1-7): B42D15/10 G06F17/60 G06N7/08 G06N7/8 G06T9/00 G07D7/00 G07D7/12 G07F7/08 H04K1/00 H04L9/00 H04N7/167
CPC: H04L9/001 G06Q20/3821 G06N7/08 H04L9/00
European: G06N7/08 G06Q20/3821
US: 380/201 380/201S 380/278 380/278S 705/76 705/76P



Family:

Publication number	Publication date	Application number	Application date
AU200121941 A1	20010618	AU20010021941	20001211
AU200121941 A5	20010618	AU20010021941D	20001211
CN1433559 A	20030730	CN20008018888	20001211
EP1236183 A2	20020904	EP20000985528	20001211
GB199929364 A0	20000202	GB19990029364	19991210
GB200000952 A0	20000308	GB20000000952	20000117
GB200006239 A0	20000503	GB20000006239	20000315
GB200006964 A0	20000510	GB20000006964	20000322
GB200226052 A0	20021218	GB20020026052	20021107
GB9929364 A0	20000202	GB19990029364	19991210
GB9929940 A0	20000209	GB19990029940	19991217
US2003182246 AA	20030925	US20030149526	20030220
WO0143067 A2	20010614	WO2000GB04736	20001211
WO0143067 A3	20020510	WO2000GB04736	20001211

Priority:

GB19990029364 19991210 GB19990029940 19991217 GB20000000952 20000117
GB20000006239 20000315 GB20000006964 20000322 WO2000GB04736 20001211

Probable Assignee: MICROBAR SECURITY LTD

Assignee(s): (std): LARM CORPOATION LIMITED E ; MICROBAR SECURITY LIMITED ; MICROBAR SECURITY LTD ; MICROLBAR SECURITY LIMITED ; MURRAY BRUCE LAWRENCE JOHN ; BLACKLEDGE JONATHAN MICHAEL ; JOHNSON WILLIAM N H ; DURAND TECHNOLOGY LTD ; BANK OF ENGLAND ; GOVERNOR AND COMPANY OF THE BANK OF ENGLAND THE

Assignee(s): JOHNSON WILLIAM NEVIL HEATON ; DURAND TECHNOLOGY LIMITED ; E LARM CORPOATION LIMITED

Inventor(s): (std): WNH JOHNSON ; MURRAY BRUCE LAWRENCE JOHN ; MURRAY B L J ; JOHNSON WILLIAM NEVIL HEATON ; JOHNSON W N H ; JM BLACKLEDGE ; BLJ MURRAY ; BLACKLEDGE JONATHAN MICHAEL ; BLACKLEDGE J M ; BLACKLEDGE JONATHAN M

Inventor(s): WILLIAM NEVIL HEATON JOHNSON ; JONATHAN MICHAEL BLACKLEDGE ; BRUCE LAWRENCE JOHN MURRAY ; W N H JOHNSON ; J M BLACKLEDGE ; B L J MURRAY

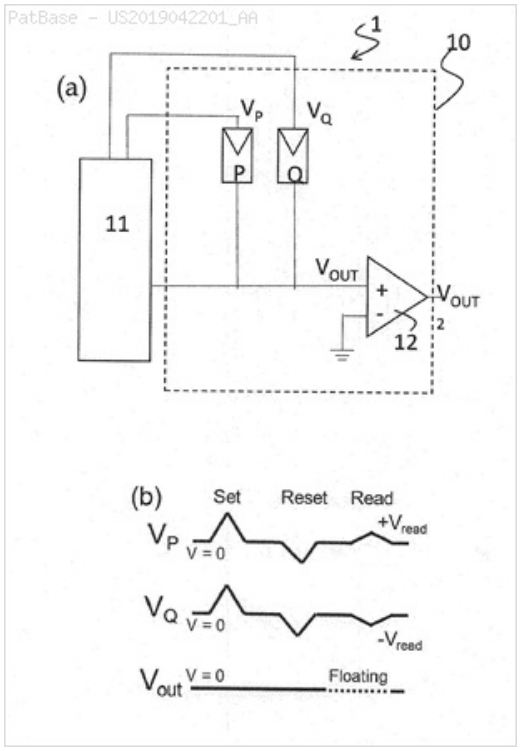
Designated states: AE AG AL AM AT AU AZ BA BB BE BF BG BJ BR BY BZ CA CF CG CH CI CM CN CR CU CY CZ DE DK DM DZ EE ES FI FR GA GB GD GE GH GM GN GR GW HR HU ID IE IL IN IS IT JP KE KG KP KR KZ LC LI LK LR LS LT LU LV MA MC MD MG MK ML MN MR MW MX MZ NE NL NO NZ PL PT RO RU SD SE SG SI SK SL SN SZ TD TG TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

17) Family number: 66945097 (US2019042201A)

Title: DEVICE AND METHOD FOR GENERATING RANDOM NUMBERS

Abstract: The invention relates to a device for generating random numbers, comprising a pair of memristors. The pair of memristors comprises a first and a second memristor, each memristor of the pair in turn comprises a top electrode, a bottom electrode and an intermediate layer adapted to switch resistance in response to predetermined voltage values applied between the top electrode and the bottom electrode. Each memristor is operatively connected to an output terminal by means of its bottom electrode. A control logic is connected to the memristors for applying suitable voltages necessary to determine a change of resistance in at least one memristor of the pair.

Classifications:
International (IPC 8-9): G06F7/58 G09C1/00 G09C1/10 G11C13/00 H04L9/08 (Advanced/Invention)
CPC: G09C1/10 G11C13/0007 G11C13/0038 G11C13/004 G11C13/0059 G11C13/0069 G11C2013/0092 G06F7/588 G09C1/00 H04L9/0866 H04L2209/12
US: 1/1 708/250



Family:

Publication number	Publication date	Application number	Application date
EP3427249 A1	20190116	EP20170714290	20170303
ITUA20161468 A1	20170908	IT2016UA01468	20160308
US2019042201 AA	20190207	US20170077514	20170303
WO17153875 A1	20170914	WO2017IB51250	20170303

Priority:

IT2016UA01468 20160308 WO2017IB51250 20170303

Probable Assignee: MILANO POLITECNICO

Assignee(s): (std)**:** MILANO POLITECNICO

Assignee(s): POLITECNICO DI MILANO

Inventor(s): (std)**:** AMBROGIO STEFANO ; BALATTI SIMONE ; IELMINI DANIELE

Agent(s): POSTIGLIONE FERRUCCIO; LISA ELISABETTA ET AL

Designated states: AE AG AL AM AO AT AU AZ BA BB BE BF BG BH BJ BN BR BW BY BZ CA CF CG CH CI CL CM CN CO CR CU CY CZ DE DJ DK DM DO DZ EC EE EG ES FI FR GA GB GD GE GH GM GN GQ GR GT GW HN HR HU ID IE IL IN IR IS IT JP KE KG KH KM KN KP KR KW KZ LA LC LI LK LR LS LT LU LV LY MA MC MD ME MG MK ML MN MR MT MW MX MY MZ NA NE NG NI NL NO NZ OM PA PE PG PH PL PT QA RO RS RU RW SA SC SD SE SG SI SK SL SM SN ST SV SY SZ TD TG TH TJ TM TN TR TT TZ UA UG US UZ VC VN ZA ZM ZW