(12) **INTER PARTES REEXAMINATION CERTIFICATE** (0160th)

United States Patent
Wilber

(10) **Number:** US 6,763,364 C1
(45) **Certificate Issued:** May 25, 2010

(54) **RANDOM NUMBER GENERATOR AND GENERATION METHOD**

(75) Inventor: **Scott A. Wilber**, Boulder, CO (US)

(73) Assignee: **Quantum World Corporation**, Roswell, NM (US)

Reexamination Request:
No. 95/000,352, Feb. 21, 2008

Reexamination Certificate for:
Patent No.:	**6,763,364**
Issued:	**Jul. 13, 2004**
Appl. No.:	**09/699,523**
Filed:	**Oct. 30, 2000**

Related U.S. Application Data

(62) Division of application No. 08/388,631, filed on Feb. 14, 1995, now Pat. No. 6,324,558.

(51) **Int. Cl.**
G06F 7/58	(2006.01)
G06F 1/02	(2006.01)

(52) **U.S. Cl.** **708/255**; 714/44

(58) **Field of Classification Search** .... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

|			
3,706,941 A	12/1972	Cohn	
4,355,366 A	10/1982	Porter	
4,799,259 A	1/1989	Ogrodski	
4,853,884 A	8/1989	Brown et al.	
4,905,176 A	2/1990	Schulz	
5,224,165 A	6/1993	Reinhardt et al.	
5,251,165 A	10/1993	James, III	
5,539,828 A	7/1996	Davis	
5,579,234 A	* 11/1996	Wiley et al.	.... 702/118

OTHER PUBLICATIONS

20090302 Rebuttal Report of Wicker (redacted images).
20090213 Expert Report of M. Ray Mercer, PH.D.
20090213 Mercer Report—Attachments A to D.
20090213 Mercer Report Attachments E to I.
Agnew, G.B., "Random Sources for Cryptographic Systems", Dept of Electrical Engineering, pp. 77–81.
May, et al., "Electronic System Perturbation Techniques", SRI International, Sep. 30, 1980, pp. 1–59.
Murray, Herschell, "A General Approach for Generating Natural Random Variables", IEEE, Dec. 1970, pp. 1210–1213.
Murray, Herschell, "Generation of Random Number from Natural Fluctuation Phenomena", Dissertation, Aug. 1966, University of Kansas.
Princeton Engineering Anomalies Research (PEAR), "Outline for Constructing A Portable Random Event Generator", Internal Document, Apr. 1993.
Princeton Engineering Anomalies Research (PEAR), "Construction and Use of Random Event Generators in Human/Machine Anomalies Experiments", Technical Note PEAR 98002, Jun. 1998.

(Continued)

Primary Examiner—Anjan K. Deb

(57) **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.
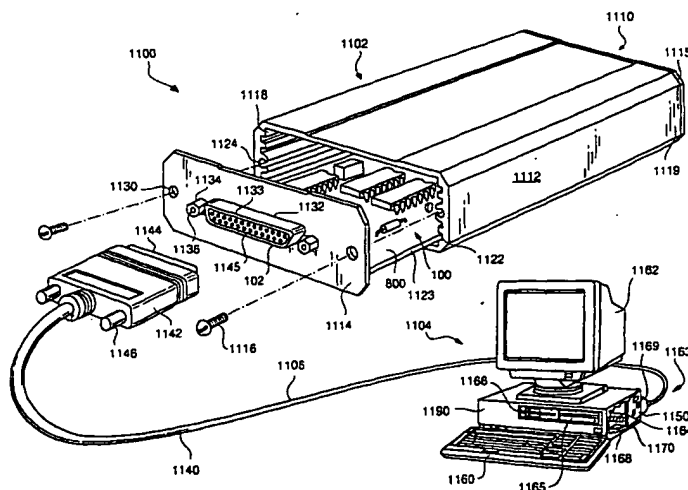
OTHER PUBLICATIONS

Radin, et al., "Towards a High Technology of the Mind: Rationale, Prototype Design and Initial Experiments", Contel Technology Center, Mar. 13, 1991.

Buslenko, N.P.; Golenko, D.I.; Shreider, Yu.A.; Sobol', I.M.; and Sragovich, V.G.; *"The Monte Carlo Method—The Method of Statistical Trials"*, University of Colorado—Boulder, Pergamon Press, pp. 257–340.

M. Richter, "A Noise Generator For Obtaining Quasi–Ideal Random Numbers For Stochastic Simulation," Dissertation RWTH Aachen (1992).

D.I. Radin, "Testing the Plausability of PSI–Mediated Computer System Failures," Journal of Parapsychology, vol. 54 (Mar. 1990), pp. 1–19 and Appendix pp. 7–9.

IBM Technical Disclosure Bulletin, "Integrated Circuit Compatible Random Number Generator," vol. 30, No. 11, Apr. 1988, pp. 333–335.

Calmos NM 810 RNG Data Sheet, Nov. 1989.

H.F. Murry, "A General Approach for Generating Natural Random Variables," IEEE Transactions on Computers (Dec. 1970), pp. 1210–1213.

M. Gude, "Concept for a High Performance Random Number Generator Based on Physical Random Phenomena," Frequenz vol. 39 (Jul./Aug. 1985), pp. 187–190.

Article 15: Installable Device Drivers, Section II: Programming in the MS–DOS Environment, MS–DOS Encyclopedia (1988), pp. 447–471.

Article 11: Terminate–and–Stay–Resident Utilities, Programming in the MS–DOS Environment, MS–DOS Encyclopedia (1988), pp. 347–359.

R. White, "How Software Works," PC Computing, (1993), pp. 2, 3, 12–20, 22–32, 43–65.

Amiga ROM Kernel Reference Manual: Libraries and Devices, Amiga Technical Reference Series (1986), pp. i–vii, 383–411, 428–437.

* cited by examiner

1

INTER PARTES
REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 316

THE PATENT IS HEREBY AMENDED AS
INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claim **8** is confirmed.

Claims **1-4** and **7** are cancelled.

New claim **11** is added and determined to be patentable.

Claims **5, 6, 9** and **10** were not reexamined.

2

11. A true random number generator system, comprising:

a hardware true random number generator circuit that implements a source of thermal or semiconductor noise for generating a true random sequence of signals; and

a personal computer including a true random number generator circuit interface, said interface consisting of one or more of the following: a device driver, a TSR, a portion of the operating system of said personal computer, and a program stored in the bios memory of said personal computer;

wherein said personal computer utilizes the true random sequence of signals received via said interface; and

wherein said interface comprises software for locating and testing said true random number generator circuit when said personal computer is turned on.

*   *   *   *   *