(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
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
4,353,366 A 10/1982 Porter
4,799,259 A 1/1989 Ogrodski
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

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.

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

Calamos NM 810 RNG Data Sheet, Nov. 1989.


* cited by examiner
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.

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.

* * * * *