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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 April 2003 (03.04.2003)

PCT

(10) International Publication Number
WO 2003/027832 A3

(51) International Patent Classification[7]: G06F 7/58

(21) International Application Number:
PCT/US2002/029080

(22) International Filing Date:
13 September 2002 (13.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/963,857 26 September 2001 (26.09.2001) US

(71) Applicant: **INTEL CORPORATION** [US/US]; (a Delaware Corpporation), 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor: **RUEHLE, Mike**; 2655 Kaystone Avenue, #30, Santa Clara, CA 95051 (US).

(74) Agent: **MALLIE, Michael, J.**; Blakely, Sokoloff, Tayor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

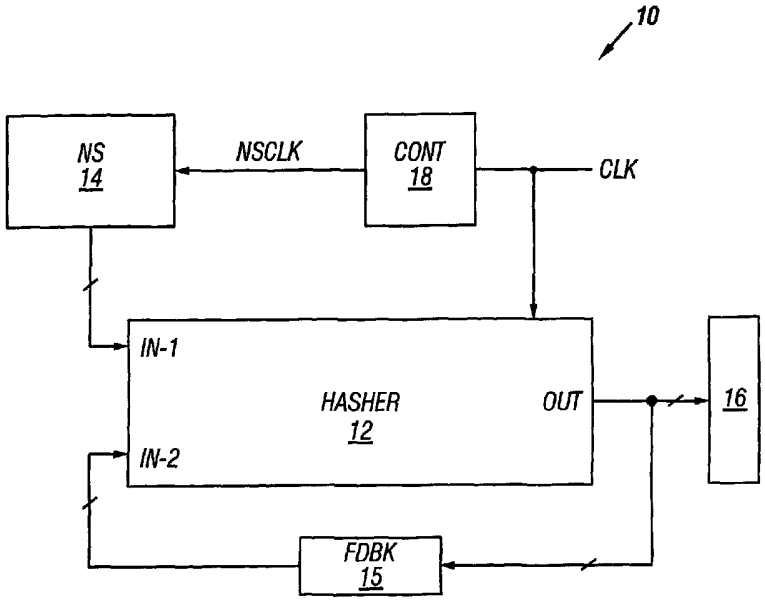
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: HASH-BASED PSEUDO-RANDOM NUMBER GENERATOR



(57) Abstract: A pseudo-random number generator (PRNG) with increased randomness. An iterative hash-based PRNG hashes in the output of a numerical sequencer, such as a counter or linear feedback shift register, in each hash stage. To improve the unpredictability of the numerical sequencer output, it may be paused for relatively unpredictable time periods. When the timing of the output of the numerical sequencer is unpredictable, elapsed time cannot be used to reliably predict what the output of the numerical sequencer will be with relation to the hash operation. The unpredictable time period may be related to when a request for a pseudo-random number is received.

WO 2003/027832 A3

(88) Date of publication of the international search report:
25 March 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/29080

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58

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)
IPC 7 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 practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 627 894 A (ALBERT BODO ET AL) 6 May 1997 (1997-05-06) column 1, line 50 -column 3, line 30	1-24
A	EP 0 365 930 A (IBM) 2 May 1990 (1990-05-02) abstract	1-24
A	EP 0 949 563 A (LUCENT TECHNOLOGIES INC) 13 October 1999 (1999-10-13) paragraphs '0004!,'0007!	8,17

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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 document 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
10 February 2004	17/02/2004

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Prins, L

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 02/29080

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5627894 A	06-05-1997	DE 4010305 A1	02-10-1991
		AT 153815 T	15-06-1997
		DE 59108715 D1	03-07-1997
		EP 0449265 A2	02-10-1991
		ES 2101701 T3	16-07-1997
		JP 7311673 A	28-11-1995
EP 0365930 A	02-05-1990	US 4905176 A	27-02-1990
		EP 0365930 A2	02-05-1990
		JP 1926190 C	25-04-1995
		JP 2128218 A	16-05-1990
		JP 6058623 B	03-08-1994
EP 0949563 A	13-10-1999	US 6285761 B1	04-09-2001
		BR 9917146 A	30-10-2001
		CA 2260683 A1	04-09-1999
		DE 69904525 D1	30-01-2003
		DE 69904525 T2	04-09-2003
		EP 0949563 A2	13-10-1999
		JP 11288214 A	19-10-1999
		TW 410310 B	01-11-2000