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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 August 2004 (12.08.2004)

PCT

(10) International Publication Number
WO 2004/068280 A3

(51) International Patent Classification[7]: H04L 9/00, H04K 1/00

(21) International Application Number: PCT/US2004/000147

(22) International Filing Date: 6 January 2004 (06.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/248,471 22 January 2003 (22.01.2003) US

(71) Applicants and
(72) Inventors: **SZREK, Walter** [US/US]; 60 Spencer Avenue, East Greenwich, RI 02818 (US). **SZREK, Irena** [US/US]; 60 Spencer Avenue, East Greenwich, RI 02818 (US).

(74) Agents: **JOSEPHS, David, R.** et al.; Barlow, Joseph & Holmes, Ltd., 101 Dyer Street, 5th Floor, Providence, RI 02903 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

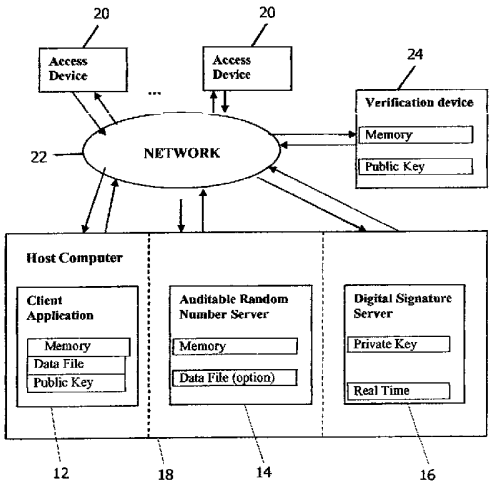
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (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*

(88) Date of publication of the international search report:
3 February 2005

*[Continued on next page]*

(54) Title: METHOD OF GENERATING UNPREDICTABLE AND AUDITABLE RANDOM NUMBERS




(57) Abstract: A system and method for generation of unpredictable and auditable random numbers includes a host computer (18), a digital signature server (16) and a verification device (24). The host computer (18) provides data to the digital signature server (16); obtains digital signature for this data; uses elements of this signature for random numbers generation; logs relevant data for audit. The verification device (24) uses logged data for auditing of the random number generation process. This invention can be applied in gaming and gambling industries where the random numbers are used for generation of game/play elements and of winning numbers elements. The game/play elements and winning numbers elements generated using this invention can be audited.

WO 2004/068280 A3

*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/US04/00147

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00; H04K 1/00

US CL : 380/28

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)

U.S. : 380/28, 262, 252; 463/29

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)

Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>---<br>Y | US 5,778,069 A (THOMLINSON et al.) 07 July 1998 (07.07.1998), see col. 5, lines 56-58, col. 7, lines 41-44. | 1, 2, 5, 7-11, 13, 20, 22<br>---<br>3, 4, 6, 12, 14-19, 21, 23-28, 30-60 |
| Y | US 2002/0161721 A1 (YUAN et al.) 31 October 2002 (31.10.2002), see page 5, paragraph 0050). | 6 |
| Y, E | US 6,685,562 B1 (RANTANEN) 03 FEBRUARY 2004 (03.02.2004), col. 4, lines 13-26; col. 6, lines 44-64. | 3, 12, 14-19, 21, 23-28, 34-38, 42-52 |
| Y, P | US 6,595,855 B2 (SAKO) 22 July 2003 (22.07.2003), see col. 6, lines 52-57. | 4, 30-33, 39-41, 51-60 |
| Y | US 2001/0038178 A1 (VANCURA) 08 November 2001 (08.11.2001), see pages 10-11, paragraph 0128. | 34-38 |
| Y | US 2002/0141590 A1 (MONTGOMERY) 03 October 2002 (03.10.2002), see page 3, paragraph 0033. | 60 |
| A | US 5,643,086 A (ALCORN et al.) 01 July 1997 (01.07.1997). | 1-60 |

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

29 November 2004 (29.11.2004)

Date of mailing of the international search report

03 DEC 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703) 305-3230

Authorized officer

Vincent Trans for Michelle R. Eason

Telephone No. (703)305-9750

Form PCT/ISA/210 (second sheet) (January 2004)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/00147

Continuation of B. FIELDS SEARCHED Item 3:
EAST
speed, digital, signature, random