

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 February 2008 (21.02.2008)

PCT

(10) International Publication Number
WO 2008/022158 A3

(51) **International Patent Classification:**
H04L 9/00 (2006.01) H04K 1/00 (2006.01)

(21) **International Application Number:**
PCT/US2007/075940

(22) **International Filing Date:** 14 August 2007 (14.08.2007)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
60/822,365 14 August 2006 (14.08.2006) US

(71) **Applicants (for all designated States except US):** **THE REGENTS OF THE UNIVERSITY OF CALIFORNIA** [US/US]; 1111 Franklin Street, 5th Floor, Oakland, California 94607-5200 (US). **SRI INTERNATIONAL** [US/US]; 333 Ravenswood Avenue, Menlo Park, California 94025 (US).

(72) **Inventors; and**

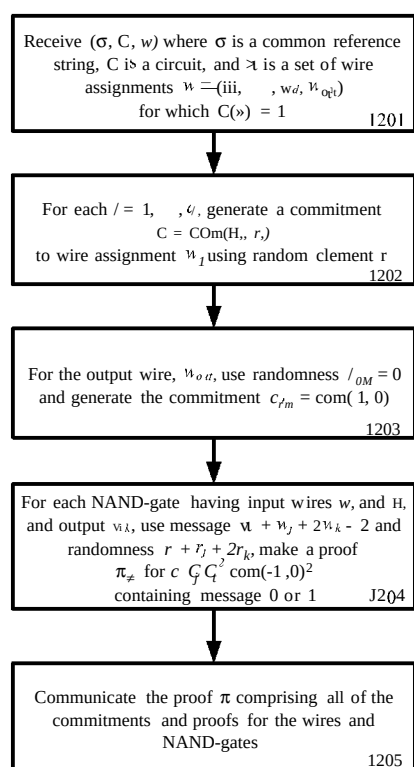
(75) **Inventors/Applicants (for US only):** **GROTH, Jens** [DK/DK]; Ildervej 15A, DK-8270 Højebjerg (DK). **OSTROVSKY, Rafail** [US/US]; P.O. Box 241631, Los Angeles, California 90024 (US). **SAHAI, Amit** [US/US]; 10847 Weyburn Avenue, Los Angeles, California 90024 (US). **WATERS, Brent** [US/US]; c/o SRI International, 333 Ravenswood Avenue, Menlo Park, California 94025 (US).

(74) **Agents:** **WOODCOCK WASHBURN LLP** et al; Cira Centre, 2929 Arch Street, 15th Floor, Philadelphia, Pennsylvania 19104-2891 (US).

(81) **Designated States (unless otherwise indicated, for every kind of national protection available):** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, **BR**, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, **HR**, HU, **ID**, IL, IN, IS, **JP**, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL,

[Continued on next page]

(54) **Title:** SYSTEM FOR NON-INTERACTIVE ZERO-KNOWLEDGE PROOFS



(57) **Abstract:** Systems and methods for generating non-interactive zero-knowledge (NIZK) proofs. A homomorphic commitment scheme provides a NIZK proof that a commitment contains 0 or 1. A NIZK proof that a triple of wire assignments satisfies a NAND-gate is generated relying on the homomorphic property of the commitment scheme. A NIZK proof of circuit satisfiability is provided that uses NIZK proofs of NAND-gate satisfiability and the homomorphic commitment scheme.

Figure 12

WO 2008/022158 A3



PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,
PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, 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,

Published:

— with international search report

(88) Date of publication of the international search report:
12 September 2008

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/75940

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 9/00**(2006.01);H04K **1/00**(2006.01)

USPC: 713/172-174,1 80;705/69

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. : 713/172, 173, 174, 180; 705/69

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)

EAST - USGPUB; USPAT, USOCR; FPRS; EPP; JPO, DERWENT; IBMJTDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/09367 1 A2 (Salomonsen et al.), 6 October 2005, abstract, pages 4, 9-13, 15-16, 26-29, 40 and 42	1-16

☐

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

07 May 2008 (07 05.2008)

Date of mailing of the international search report

94 JIN 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn ISA/US
Commissioner for Patents
P O Box 1450
Alexandria, Virginia 223 13-1450

Facsimile No. (57 1) 273-3201

Authorized officer

April Shan

Telephone No (57 1) 270-101 4

DEBORAH A. THOMAS
PARALEGAL SPECIALIST

DWT