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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 June 2005 (09.06.2005)

PCT

(10) International Publication Number
WO 2005/053209 A3

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

(21) International Application Number: PCT/US2004/039594

(22) International Filing Date: 24 November 2004 (24.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/524,959	24 November 2003 (24.11.2003)	US
60/536,133	13 January 2004 (13.01.2004)	US
60/545,678	18 February 2004 (18.02.2004)	US

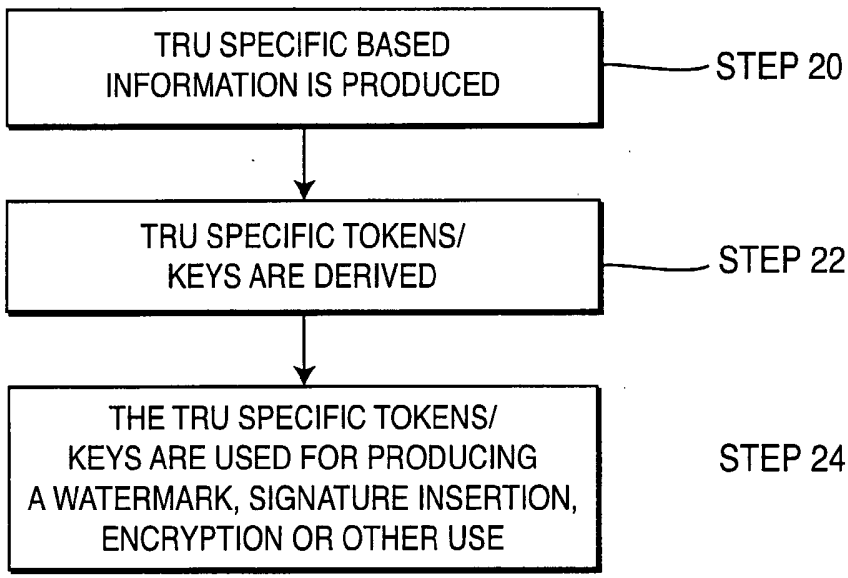
(71) Applicant *(for all designated States except US)*: **INTERDIGITAL TECHNOLOGY CORPORATION** [US/US]; 300 Delaware Avenue, Suite 527, Wilmington, Delaware 19801 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHITRAPU, Prabhakar, R.** [US/US]; 135 Brochant Drive, Blue Bell, Pennsylvania 19422 (US). **BRIANCON, Alain, Charles, Louis** [US/US]; 19328 Cissel Manor Drive, Poolesville, Maryland 20837 (US). **KUMOLUYI, Akin, O.** [GB/US]; 1601 Watchung Avenue, Plainfield, NJ 07060 (US). **CARLTON, Alan, Gerald** [GB/US]; 12 Wisteria Avenue, Mineola, New York 11501 (US). **VANGANURU, Kiran, Kumar, S.** [IN/US]; 640 American Avenue #E508, King of Prussia, Pennsylvania 19406 (US). **HERSCHAFT, Richard, Dan** [US/US]; 157-04 22 Avenue, Whitestone, New York 11357 (US). **HOFFMANN, John, Erich** [US/US]; 516 Latania Palm Drive, Indialantic, Florida 32903-3816 (US). **THOMMANA, John** [IN/US]; 10122 Vaquero Trail, Austin, Texas 78759 (US). **ZHANG, Guodong** [CN/US]; 490 Main Street, Apt. C8, Farmingdale, New York 11735 (US). **OLESEN, Robert, Lind** [US/US]; 3 Country Club Drive, Huntington, New York 11743 (US). **REZNIK, Alexander** [US/US]; 1212 River Road, Titusville, New Jersey 08660 (US). **SHAN, TieJun** [US/US]; 3060 Thompson Road, Upper Salford, PA 18969 (US). **SHIN, Sung-Hyuk** [US/US]; 104 Elder Way, Northvale, New Jersey 07647 (US). **SINGHAL, Amit** [US/US]; 918 Mystic Lane, Norristown, Pennsylvania 19403 (US). **PURKAYASTHA, Debashish** [IN/US]; 1045 Fallbrook Lane, Pottstown, Pennsylvania 19464 (US).

[Continued on next page]

(54) Title: TOKENS/KEYS FOR WIRELESS COMMUNICATIONS



(57) Abstract: Tokens/keys are produced for wireless communications. These tokens/keys are used for watermarks, signature insertion, encryption and other uses. In one embodiment, contextual information is used to generate tokens/keys. The tokens/keys may be derived directly from the contextual information. The contextual information may be used in conjunction with other information to derive the tokens/keys. Tokens/keys may be exchanged between transmit/receive units. The exchange of these tokens/keys may be encrypted.

WO 2005/053209 A3

(74) **Agent: BALLARINI, Robert, J.**; United Plaza, Suite 1600, 30 S. 17th Street, Philadelphia, Pennsylvania 19103 (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, 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, FR, GB, GR, HU, IE, IS, IT, LU, MC, 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).

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:** 16 February 2006

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/US04/39594

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00; H04K 1/00
US CL : 380/44, 270, 283; 713/176; 726/1, 34
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. : 380/44, 270, 283; 713/176; 726/1, 34

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2003/0072450 A1 (MAGGENTI) 17 April 2003 (17.04.2003), paragraph 10 and abstract.	1 and 12-14 ---------- 2-11,19-21,23-24,39-41 and 15,35
Y	US 5,201,000 (MATYAS et al) 06 April 1993 (06.04.1993), column 11 line 34 through column 12 line 17.	22
Y	Menezes, Alfred J. et al. Handbook of Applied Cryptography, 1997, page 172.	2 and 9
Y	US 5,953,424 (VOGELESANY et al.) 14 September 1999 (14.09.1999), column 6 lines 25-38 and column 9 lines 13-28.	15
Y	US 2003/0030680 A1 (COFTA et al.) 13 February 2003 (13.02.2003). paragraph 23.	35
X --- Y	Schneier, Bruce, Applied Cryptography Second Edition, 1996, pages 180 and 426-428.	16-18 ---------- 3-11, 19-30, 33-34, and 36-41
X	US 2003/0009683 A1 (SCHWENCK et al.) 9 January 2003 (09.01.2003), paragraphs 15 and 30.	31-32

☒ 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	Date of mailing of the international search report
28 November 2005 (28.11.2005)	27 DEC 2005
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. (571) 273-3201	Authorized officer Dale Hall for Emmanuel Moise Telephone No. (571) 272-3578

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/39594

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,492,897 B1 (MOWERY, JR.) 10 December 2002 (10.12.2002), column 7 lines 34-37.	25-30 and 33-34
Y	US 6115580 (CHUPRUN et al) 05 September 2000 (05.09.2000), column 2 lines 24-39.	36-38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/39594

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of any additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/39594

BOX III. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group 1, claim(s) 1-18 and 40-41, drawn to a method and apparatus for producing a token/key.

Group 2, claim(s) 19-21 and 39, drawn to a method for verifying a watermark/signature.

Group 3, claim(s) 22, drawn to determining if a change in criteria in token/key generation is needed.

Group 4, claim(s) 23-24, 34, and 36-38, drawn to a method for exchanging tokens/keys.

Group 5, claim(s) 25-30, 33, and 35, drawn to a method of varying security using security levels.

Group 6, claim(s) 31-32, drawn to a method for detecting tampering with sensors.

The inventions listed as Groups 1-6 do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group 1 relates to producing a token/key using TRU specific information which is not present in groups 2-6. Group 2 relates to verifying a watermark/signature, which is not present in groups 1 or 3-6. Group 3 relates to determining if a change in criteria in token/key generation is needed a feature that is not present in groups 1-2 or 4-6. Group 4 relates to exchanging a token/key a feature that is not present in groups 1-3 or 5-6. Group 5 relates to varying security using security levels a method not present in groups 1-4 or 6. Group 6 relates to a method for detecting tampering with sensors, which is not present in groups 1-5.