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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 November 2007 (08.11.2007)

PCT

(10) International Publication Number
WO 2007/127576 A3

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

(21) International Application Number:
PCT/US2007/065588

(22) International Filing Date: 30 March 2007 (30.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/379,815 24 April 2006 (24.04.2006) US

(71) Applicant *(for all designated States except US)*: **MOTOROLA, INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BUSKEY, Ronald F.,** [US/US]; 923 Saratoga Parkway, Sleepy Hollow, Illinois 60118 (US). **FROSIK, Barbara B.** [US/US]; 3306 Daniels Court, Arlington Heights, Illinois 60004 (US). **KUHLMAN, Douglas A.** [US/US]; 328 Windsor Lane, Inverness, Illinois 60010 (US).

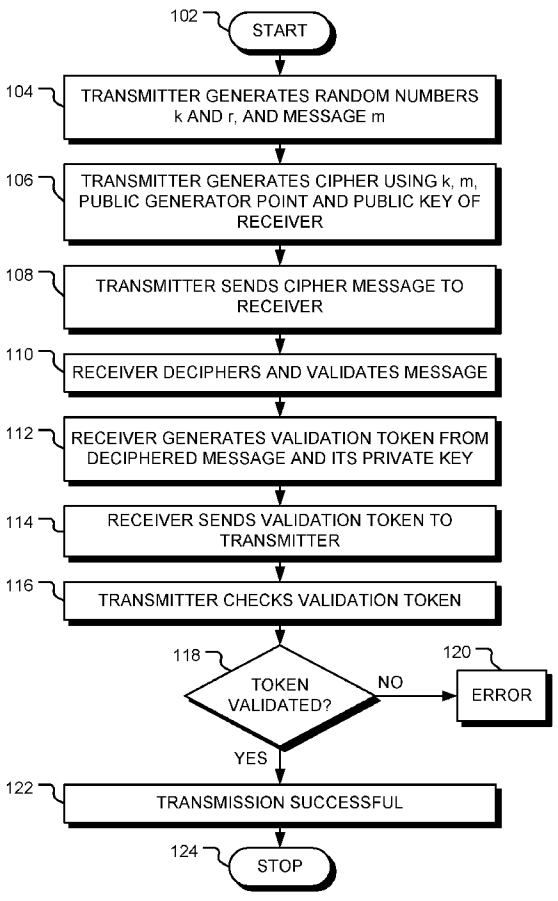
(74) Agents: **LAMB, James, A.** et al.; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(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, 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, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, 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.

(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, 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).

[Continued on next page]

(54) Title: METHOD FOR ELLIPTIC CURVE PUBLIC KEY CRYPTOGRAPHIC VALIDATION



(57) Abstract: Communication and validation of information transfer from a transmitter to a receiver is achieved by generating a cipher (400) from a message *m* (410) using parameters of an elliptic curve, a generator point *P* (406) on the elliptic curve and a public key *Q* (416) of the receiver. The cipher includes a first element that is the product *kP* of a random number *k* (404) with the generator point *P* and a second element that is the product of m and the x-coordinate of the product *kQ*. The message m is generated from two mathematically independent representations of the information and, optionally, a random number. The cipher is communicated to the receiver and decoded to recover a message *m'* (502). A validation token (500) is generated by the receiver and passed to the transmitter, which validates communication of the information to the receiver if the product *mkQ* is equal to the validation token.

WO 2007/127576 A3

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:
17 April 2008

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/65588

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01)

USPC: 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

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	US 2005/0195973 A1 (Ibrahim) 08 September 2005, paragraphs 0180-0190 and 0194-0206	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
28 December 2007 (28.12.2007)

Date of mailing of the international search report
05 FEB 2008

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
Beemnet W Dada

Telephone No. (571) 272-3847

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