



- (51) **International Patent Classification:**
H04L 9/30 (2006.01) *H04W 12/04* (2009.01)
- (21) **International Application Number:**
PCT/IB2014/002161
- (22) **International Filing Date:**
24 June 2014 (24.06.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/925,299 24 June 2013 (24.06.2013) US
- (71) **Applicants:** **BLACKBERRY LIMITED** [CA/CA]; 2200 University Avenue East, Waterloo, ON N2K 0A7 (CA). **CERTICOM CORP** [CA/CA]; 4701 Tahoe Blvd, Building A, Mississauga, ON L4W 0B5 (CA).
- (72) **Inventors:** **BUCKLEY, Michael, Eoin**; 1368 Wild Indigo Road, Grayslake, IL 60030 (US). **HOLLATZ, Michael, Charles**; 10415 Fair Lane, Huntley, IL 60142 (US). **LAMBERT, Robert, John**; 63 Holm Street, Cambridge, ON N3C 3N3 (CA). **EBEID, Navine, Maurice Nassif**; 242 Briarmeadow Drive, Kitchener, ON N2A 4C4 (CA).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

[Continued on next page]

(54) **Title:** SECURING METHOD FOR LAWFUL INTERCEPTION

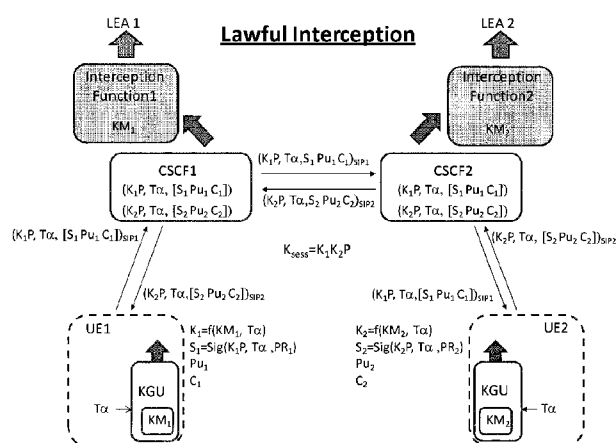


FIG. 4

(57) **Abstract:** A method is presented for secure communication, the method including generating a signature using a private key, a nonce, and at least one of an identifier and a key component; and transmitting the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key.



(88) Date of publication of the international search report:

16 July 2015

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2014/002161

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/30** (2006.01) , **H04W 12/04** (2009.01)

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)
H04L 9/30 (2006.01) , **H04W 12/04** (2009.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)

Databases: Google, Google Patents, Intellect/Canadian Patent Database, Orbit/Questel, IEEE Xplore

Keywords: key component MIKEY-IBAKE MAC tag message authentication code secure communicat* key identifier nonce signature private
IBE identity based encryption session generated certificate public random message authentication code identification ID shared secret

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US2012036567A1 (SENESE et al.), 09 February 2012 (09-02-2012)	11-14, 17-18
A	US7415606B2 (TUVELL et al.), 19 August 2008 (19-08-2008)	11-14, 17-18
A	US2012272064A1, (SUNDARAM et al.), 25 October 2012 (25-10-2012)	1-10, 15-16
A	US2009016527A1 (VIGARIE et al.), 15 January 2009 (15-01-2009)	1-10, 15-16

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

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
20 March 2015 (20-03-2015)

Date of mailing of the international search report
02 April 2015 (02-04-2015)

Name and mailing address of the ISA/CA
Canadian Intellectual Property Office
Place du Portage I, C114 - 1st Floor, Box PCT
50 Victoria Street
Gatineau, Quebec K1A 0C9
Facsimile No.: 001-819-953-2476

Authorized officer

Allan Tam (819) 953-3444

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2014/002161

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2012036567A1	09 February 2012 (09-02-2012)	AU2011289780A1 CA2807499A1 CA2807499C US2012036363A1 US8448235B2 WO2012018573A2 WO2012018573A3 WO2012018573A4 WO2012021284A2 WO2012021284A3 WO2012021284A4	28 February 2013 (28-02-2013) 16 February 2012 (16-02-2012) 19 August 2014 (19-08-2014) 09 February 2012 (09-02-2012) 21 May 2013 (21-05-2013) 09 February 2012 (09-02-2012) 12 July 2012 (12-07-2012) 07 September 2012 (07-09-2012) 16 February 2012 (16-02-2012) 12 April 2012 (12-04-2012) 07 June 2012 (07-06-2012)
US7415606B2	19 August 2008 (19-08-2008)	US2006050869A1 AT346333T AU6111701A CA2408437A1 DE60124765D1 DE60124765T2 EP1348152A2 EP1698959A1 EP1705599A2 EP1708406A2 IL152351A IL152351D0 JP2004501547A JP2012019534A KR20030010620A KR100905141B1 US6986046B1 US2006036862A1 US7171001B2 US2006041752A1 US7213147B2 WO0188674A2	09 March 2006 (09-03-2006) 15 December 2006 (15-12-2006) 26 November 2001 (26-11-2001) 22 November 2001 (22-11-2001) 04 January 2007 (04-01-2007) 14 February 2008 (14-02-2008) 01 October 2003 (01-10-2003) 06 September 2006 (06-09-2006) 27 September 2006 (27-09-2006) 04 October 2006 (04-10-2006) 03 August 2009 (03-08-2009) 29 May 2003 (29-05-2003) 15 January 2004 (15-01-2004) 26 January 2012 (26-01-2012) 05 February 2003 (05-02-2003) 29 June 2009 (29-06-2009) 10 January 2006 (10-01-2006) 16 February 2006 (16-02-2006) 30 January 2007 (30-01-2007) 23 February 2006 (23-02-2006) 01 May 2007 (01-05-2007) 22 November 2001 (22-11-2001)
US2012272064A1	25 October 2012 (25-10-2012)	CN103493427A EP2700187A1 JP2014514860A KR20130136551A WO2012145161A1	01 January 2014 (01-01-2014) 26 February 2014 (26-02-2014) 19 June 2014 (19-06-2014) 12 December 2013 (12-12-2013) 26 October 2012 (26-10-2012)
US2009016527A1	15 January 2009 (15-01-2009)	AT428236T CN101248614A CN101248614B DE602006006190D1 DK1917756T3 EP1917756A1 EP1917756B1 ES2325222T3 FR2890267A1 FR2890267B1 KR20080041279A KR101273991B1 WO2007023231A1	15 April 2009 (15-04-2009) 20 August 2008 (20-08-2008) 27 April 2011 (27-04-2011) 20 May 2009 (20-05-2009) 31 August 2009 (31-08-2009) 07 May 2008 (07-05-2008) 08 April 2009 (08-04-2009) 28 August 2009 (28-08-2009) 02 March 2007 (02-03-2007) 05 October 2007 (05-10-2007) 09 May 2008 (09-05-2008) 17 June 2013 (17-06-2013) 01 March 2007 (01-03-2007)