



(51) International Patent Classification:

H04L 9/30 (2006.01) *H04W 12/04* (2009.01)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)

(21) International Application Number:

PCT/CA2011/050181

(22) International Filing Date:

1 April 2011 (01.04.2011)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant (for all designated States except US): **CERTICOM CORP.** [CA/CA]; 5520 Explorer Drive, 4th Floor, Mississauga, Ontario L3W 5L1 (CA).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **BROWN, Daniel Richard L.** [CA/CA]; 4th Floor, 14157 - 5520 Explorer Drive, Mississauga, Ontario L4W 5L1 (CA).

(74) Agent: **RIDOUT & MAYBEE LLP**; 225 King Street West, 10th Floor, Toronto, Ontario M5V 2M2 (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, 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

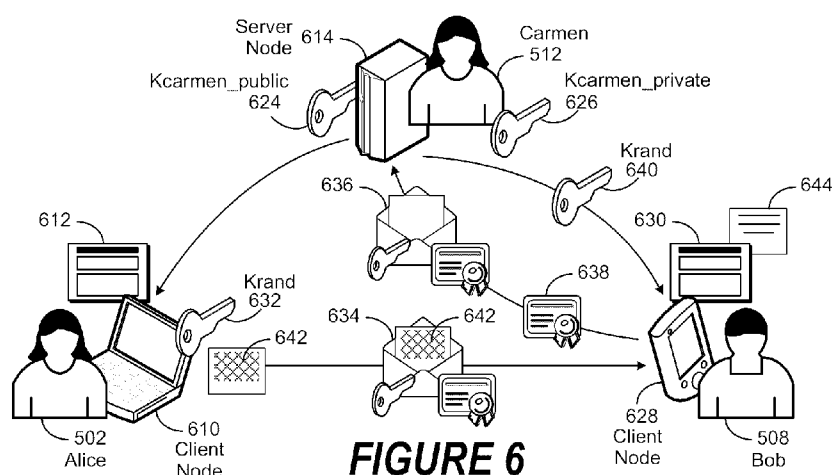
Published:

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

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

6 December 2012

(54) Title: IDENTITY-BASED DECRYPTION

**FIGURE 6**

(57) Abstract: Devices and methods are provided for managing identity-based decryption of digital content. A message sender ("Alice") uses a random key (Krand) to encrypt message content for a message recipient ("Bob"). Then Alice uses the public key of a message decryption service provider ("Carmen") to generate a wrapped key ciphertext comprising the Krand and authentication information associated with Bob. Alice then sends a message text containing the encrypted message content and the wrapped key ciphertext to Bob, who in turn sends the wrapped key ciphertext to Carmen along with his authentication information. Carmen then uses her private key to process the wrapped key ciphertext to decrypt the Krand and Bob's authentication information. If the authentication information provided by Bob matches the decrypted authentication information, then Carmen sends the decrypted Krand to Bob, who uses it to decrypt the encrypted message content.



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2011/050181

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 9/30** (2006.01) , **H04L 9/32** (2006.01) , **H04W 12/04** (2009.01) , **H04W 12/06** (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)

IPC: **H04L 9/30** (2006.01) , **H04L 9/32** (2006.01) , **H04W 12/04** (2009.01) , **H04W 12/06** (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)

Epoque, Canadian Patent Database, WEST, Internet

Keywords : IBE, IBD, encryption, decryption, decryption service provider, wrapped key, ciphertext, message content, authentication data, secure channel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US20090034714 A9; 05 February 2009 (05-02-2009); BONEH et al. [Abstract]	1-30
A	US2006095770 A; 04 May 2006 (04-05-2006); BAYLIS et al. [0029]	1-30
A	US6275936 B1; 14 August 2001 (14-08-2001); KYOJIMA et al. *** whole document ***	1-30
A	"On the Risks of IBE", Khurana, H. and Basney, J.; Fifth International Workshop on Applied PKC (IWAP), Dalian, China, Nov 2006.	1-30
T	"Identity-Based Decryption"; Brown, D.[http://eprint.iacr.org/2011/266 (accessed Oct. 31 2011)]	1-30

☐ 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

31 October 2011 (31-10-2011)

Date of mailing of the international search report

28 December 2011 (28.12.2011)

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

Lawrence J. Engel (819) 997-2936

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2011/050181

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2009034714A9	05 Feb. 2009 (05-02-2009)	AT465571T	15 May 2010 (15-05-2010)
		AU2002332671A1	03 March 2003 (03-03-2003)
		DE60236094D1	02 June 2010 (02-06-2010)
		EP1425874A2	09 June 2004 (09-06-2004)
		EP1425874A4	15 April 2009 (15-04-2009)
		EP1425874B1	21 April 2010 (21-04-2010)
		EP2224637A2	01 September 2010 (01-09-2010)
		JP2005500740A	06 January 2005 (06-01-2005)
		JP2011151866A	04 August 2011 (04-08-2011)
		US2003081785A1	01 May 2003 (01-05-2003)
		US7113594B2	26 September 2006 (26-09-2006)
		US2007041583A1	22 February 2007 (22-02-2007)
		US7634087B2	15 December 2009 (15-12-2009)
		US2010208895A1	19 August 2010 (19-08-2010)
		WO03017559A2	27 February 2003 (27-02-2003)
		WO03017559A3	10 July 2003 (10-07-2003)
US2006095770A1	04 May 2006 (04-05-2006)	US2006095770A1	04 May 2006 (04-05-2006)
		US7660987B2	09 February 2010 (09-02-2010)
US6275936B1	14 August 2001 (14-08-2001)	JP11122240A	30 April 1999 (30-04-1999)