



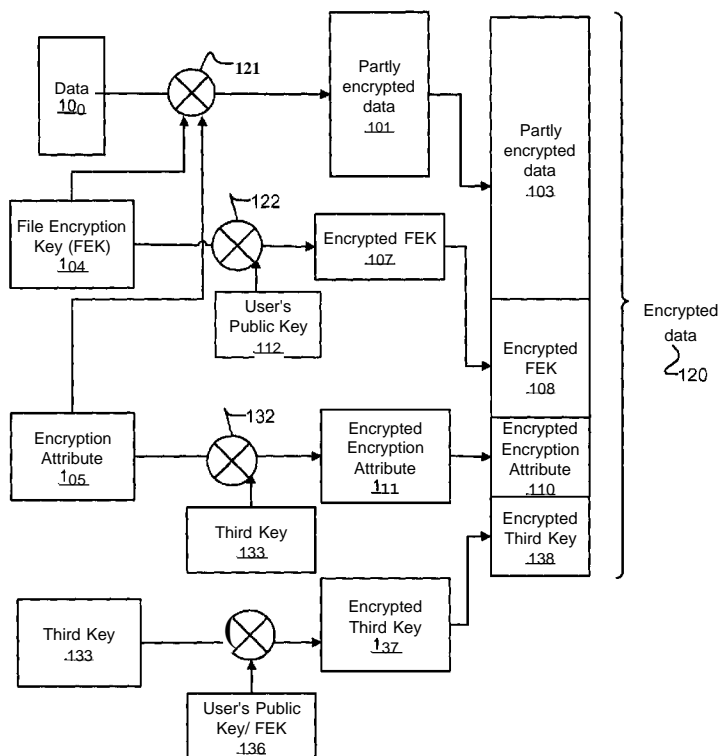
- (51) International Patent Classification:
H04L 9/08 (2006.0 1) H04L 9/30 (2006.0 1)
- (21) International Application Number:
PCT/IB20 12/002808
- (22) International Filing Date:
29 December 2012 (29. 12.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
13/292,883 9 November 2011 (09. 11.2011) US
- (71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).
- (72) Inventor: CHEW, Yen Hsiang; 216 Persiaran Gurney Georgetown, Penang 10250 (MY).
- (74) Agents: VINCENT, Lester, J. et al; Blakely, Sokoloff, Taylor & Zafman LLP, 1279 Oakmead Parkway, Sunnyvale, CA 94085-4040 (US).

- (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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, ML, MR, NE, SN, TD, TG).

[Continued on nextpage]

(54) Title: MULTI-KEY CRYPTOGRAPHY FOR ENCRYPTING FILE SYSTEM ACCELERATION

Figure 1



(57) Abstract: Embodiments of methods and systems for encrypting and decrypting with encryption attributes are presented. An encryption attribute contains information to identify one or more segments of a file to be encrypted. An encryption process encrypts those one or more segments to generate a partly encrypted file instead of encrypting the entire file. That is, the file includes some data that are encrypted and some data that are not. In one embodiment, at least three encryption keys are used such that the encryption attribute is encrypted with using a third key.



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2012/002808**A. CLASSIFICATION OF SUBJECT MATTER***H04L 9/08(2006.01)i, H04L 9/30(2006.01)1*

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 9/08; H04N 7/167; H04L 9/06; H04L 29/06; H04L 9/32

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: encrypt, decrypt, symmetric encryption key, public key, first key, second key, third key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009-0052670 A1 (YONG-KUK YOU et al.) 26 February 2009 See paras . 9-10 , 12 , 74-75 ; figures 1 , 4 ; and claims 1 , 9 .	1-27
A	wo 03-055174 A2 (INTEL CO. , LTD.) 03 July 2003 See claim 1 ; para. 22 ; and figure 3 .	1-27
A	KR 10-2011-0024788 A (LG ELECTRONICS CO. , LTD.) 09 March 2011 See paras . 30-34 ; and figure 2 .	1-27
A	wo 2005-071881 A1 (NEC CO. , LTD.) 04 August 2005 See paras . 24-27 ; and figure 2 .	1-27
A	wo 2007-028099 A2 (QUALCOMM INC.) 08 March 2007 See paras . 73-82 ; and figure 8 .	1-27

 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 but 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 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

15 May 2013 (15.05.2013)

Date of mailing of the international search report

16 May 2013 (16.05.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

BYUN, Sung Cheal

Telephone No. 82-42-481-8262



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/IB2012/002808

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0052670 A1	26.02.2009	KR 10-2009-00 19660 A	25.02.2009
Wo 03-055174 A2	03.07.2003	AU 2002-352943 A1 CN 100456765 co CN 1606854 A EP 1457016 A2 KR 10-0647 172 B1 TW 264912 B US 2003-01 1547 1 A1 Wo 03-055174 A3	09.07.2003 28.01.2009 13.04.2005 15.09.2004 23.11.2006 21.10.2006 19.06.2003 26.02.2004
KR 10-201 1-0024788 A	09.03.2011	None	
wo 2005-07188 1 A1	04.08.2005	EP 1708407 A1 JP 04687465 B2 KR 10-06680 16 B1 KR 10-2006-0033707 A US 2006-0262933 A1 US 2010-01 15285 A1 US 2012-0250855 A1 US 2012-0250868 A1 US 7672460 B2 US 8223973 B2	04.10.2006 25.02.2011 16.01.2007 19.04.2006 23.11.2006 06.05.2010 04.10.2012 04.10.2012 02.03.2010 17.07.2012
wo 2007-028099 A2	08.03.2007	CN 101297300 AO EP 1920378 A2 EP 2390815 A1 JP 049441 13 B2 JP 2009-507433 A JP 2012-134983 A KR 10-1260884 B1 KR 10-2008-00429 18 A KR 10-2010-006315 1 A KR 10-201 1-0 118737 A KR 10-2012-0 108994 A KR 10-2012-0 12048 1 A wo 2007-028099 A3	29.10.2008 14.05.2008 30.11.2011 09.03.2012 19.02.2009 12.07.2012 06.05.2013 15.05.2008 10.06.2010 31.10.2011 05.10.2012 01.11.2012 21.06.2007