

(51) International Patent Classification:
H04L 9/14 (2006.01)(21) International Application Number:
PCT/US2014/040727(22) International Filing Date:
3 June 2014 (03.06.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/830,399 3 June 2013 (03.06.2013) US(71) Applicant (for all designated States except US): **BROWN UNIVERSITY** [US/US]; 47 George Street, Providence, RI 02912 (US).

(72) Inventors; and

(71) Applicants (for US only): **KELLY, James** [US/US]; 109 Linden St., Apt. 35, Waltham, MA 02452 (US). **TAMAS-SIA, Roberto** [US/US]; 115 Waterman St., Providence, RI 02912 (US).(74) Agent: **BRUESS, Steven, C.**; Merchant & Gould P.C., P.O. Box 2903, Minneapolis, MN 55402-0903 (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, 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))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

[Continued on next page]

(54) Title: SECURE COMPRESSION

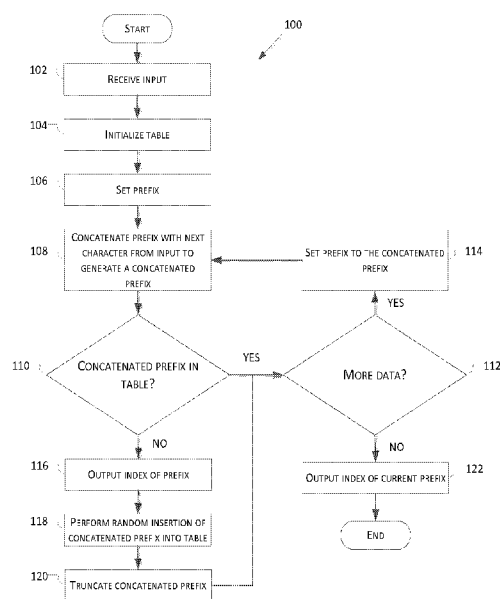


FIGURE 1

(57) Abstract: In embodiments, secure compression algorithms are provided that may be employed as a single operation on raw data to produce compressed and encrypted data. In embodiments, the algorithms described herein may be performed using any type of dictionary based encryption. In one embodiment, upon adding a new prefix to a dictionary table, the dictionary table may be permuted to randomize the entries into the table. The randomization may be based upon a permutation value generated by a deterministic pseudo-random generator and/or pseudo-random function. Other embodiments of randomization may be employed to provide secure compression. For example, instead of permuting the entire table upon adding a prefix, the prefix may be randomly added to the table.



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

23 April 2015

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/040727**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/14(2006.01)i**

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 9/14; G06K 9/36; H03M 7/30; G06F 15/00; H03M 7/34; G06F 7/00; H04L 9/00

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: secure compression, dictionary table, prefix, random insertion, random permutation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009-0309769 A1 (OSCAR CHI LIM AU et al.) 17 December 2009 See paragraphs [0028]-[0071]; and figures 1-5.	1-20
Y	US 2011-0103703 A1 (DAVID KARLOV) 05 May 2011 See paragraphs [0043]-[0205]; and figures 1A-14.	1-18
Y	US 2010-0127902 A1 (JAMES P. SCHNEIDER) 27 May 2010 See paragraphs [0027]-[0175]; and figures 1-5.	19, 20
A	US 2007-0028088 A1 (COSKUN BAYRAK et al.) 01 February 2007 See paragraphs [0034]-[0061]; and figures 1-8.	1-20
A	US 6624762 B1 (JOSEPH H END, III) 23 September 2003 See column 6, line 35 - column 55, line 35; and figures 1-30.	1-20



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 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

27 February 2015 (27.02.2015)

Date of mailing of the international search report

27 February 2015 (27.02.2015)

Name and mailing address of the ISA/KR

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

Facsimile No. ++82 42 472 3473

Authorized officer

KIM, Do Weon

Telephone No. +82-42-481-5560



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/040727

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0309769 A1	17/12/2009	CN 101610088 A CN 101610088 B US 7868788 B2	23/12/2009 24/07/2013 11/01/2011
US 2011-0103703 A1	05/05/2011	AU 2009-233627 A1 AU 2009-233627 B2 US 8600180 B2	19/05/2011 29/03/2012 03/12/2013
US 2010-0127902 A1	27/05/2010	US 7764202 B2	27/07/2010
US 2007-0028088 A1	01/02/2007	None	
US 6624762 B1	23/09/2003	None	