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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 July 2015 (09.07.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/102694 A3

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2014/058424

(22) International Filing Date:
30 September 2014 (30.09.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/884,753 30 September 2013 (30.09.2013) US

(72) Inventors; and
(71) Applicants : **HUGHES, Richard, J.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **NORDHOLT, Jane E.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **PETERSON, Charles G.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **TYAGI, Kush T.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **WIPF, Christopher C.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **NEWELL, Raymond T.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **MCCABE, Kevin P.** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US). **DALLMANN, Nicholas** [US/US]; P.O. Box 1663, Los Alamos National Laboratory, Los Alamos, NM 87545 (US).

(74) Agents: **SEEVE, Brian M.** et al.; Wilmer Cutler Pickering Hale and Dorr LLP, 60 State Street, Boston, MA 02109 (US).

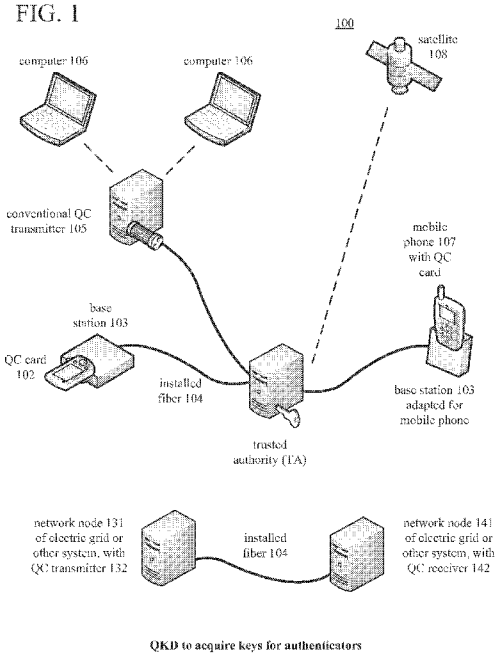
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, ST, 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,

[Continued on next page]

(54) Title: STREAMING AUTHENTICATION AND MULTI-LEVEL SECURITY FOR COMMUNICATIONS NETWORKS USING QUANTUM CRYPTOGRAPHY

FIG. 1



(57) Abstract: Message authenticators for quantum-secured communications facilitate low-latency authentication with assurances of security. Low-latency message authenticators are especially valuable in infrastructure systems where security and latency constraints are difficult to satisfy with conventional non-quantum cryptography. For example, a message transmitter receives a message and derives an authentication tag for the message based at least in part on an authenticator that uses one or more quantum keys. The message transmitter outputs the message and its authentication tag. A message receiver receives a message and authentication tag for the message. The message receiver derives a comparison tag for the message based at least in part on an authenticator that uses one or more quantum keys. The message receiver checks whether the message is authentic based on a comparison of the authentication tag and the comparison tag. In example implementations, the authenticator uses stream-wise cyclic redundancy code operations.

WO 2015/102694 A3

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))*

(88) Date of publication of the international search report:
20 August 2015

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 14/58424

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2015.01)
CPC - H04L9/3281
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(8): H04L 9/32 (2015.01); CPC: H04L9/3281

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/2, 713/170; IPC(8): H04L 9/32 (2015.01); CPC: H04L9/3281, H04L63/0428, H04L63/0823, H04L9/32, H04L63/08

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, ProQuest Dialog, Google Web, Google Patents (Search terms: quantum key, irreducible binary polynomial, single fiber, fibre, one, multiplex, authentication, Toeplitz matrix, Hankel, catalecticant, persymmetric, circulant, hash, encrypt, MixColumn, Rijndael, diffusion, etc.)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 7,933,905 B2 (Obana et al.) 26 April 2011 (26.04.2011), col. 11, ln. 35-37, 44-45, and 48-50, col. 12, ln. 47-52, 59, and 62-64, col. 15, ln. 41-51, col. 19, ln. 18-19 and 32-33, col. 20, ln. 19-20, col. 22, ln. 60-67, col. 23, ln. 4-6, 18-28, 40-47, and 66-67, col. 24, ln. 25-26, col. 25, ln. 19-27 and 55-60, and col. 26, ln. 35-36, and Figs. 1-2 and 7, and claim 4.	1-2, 11-13, 22-23, 32, 59-60 --- 3-10, 14-21, 24-31, 33-58
Y	US 7,787,623 B2 (Akiyama et al.) 31 August 2010 (31.08.2010), col. 5, ln. 67 to col. 6, ln. 2, col. 11, ln. 54-57, col. 22, ln. 27-36, 47-65, and ln. 67 to col. 23, ln. 5, and col. 23, ln. 23-25, and claim 3.	3-7, 14-18, 24-28, 33-37, 42-46, 51-55
Y	US 2010/0115277 A1 (Roscoe) 06 May 2010 (06.05.2010), para. [0004], [0026]-[0027], [0041], [0043], and [0099]-[0103], and claim 20.	5, 8, 16, 19, 26, 29, 35, 38, 44, 47, 53, 56
Y	US 7,639,947 B2 (Luo et al.) 29 December 2009 (29.12.2009), col. 3, ln. 54-55 and 67, and col. 4, ln. 1-3, and Fig. 2.	7, 9-10, 18, 20-21, 28, 30-31, 37, 39-58

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

* 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	Date of mailing of the international search report
27 May 2015 (27.05.2015)	25 JUN 2015
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. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)