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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 December 2016 (22.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/204846 A3

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/28* (2006.01)

(21) International Application Number:
PCT/US2016/024764

(22) International Filing Date:
29 March 2016 (29.03.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/144,027 7 April 2015 (07.04.2015) US
15/082,853 28 March 2016 (28.03.2016) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 15/082,853 (CON)
Filed on 28 March 2016 (28.03.2016)

(71) Applicant: **SECURE CHANNELS SA** [CH/CH]; 21 Ruelle des Moulins, Nyon 1260, Vaud (CH).

(72) Inventor: **COLERIDGE, Robert**; Drayton Court, Drayton Road, Solihull West Midlands B90 4NG (GB).

(74) Agents: **KOVELMAN, Robert, L.** et al.; Seed Intellectual Property Law Group PLLC, Suite 5400, 701 Fifth Avenue, Seattle, Washington 98104-7064 (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, 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:
2 February 2017

(54) Title: SYSTEM AND METHOD FOR AN ENHANCED XOR CIPHER THROUGH EXTENSIONS

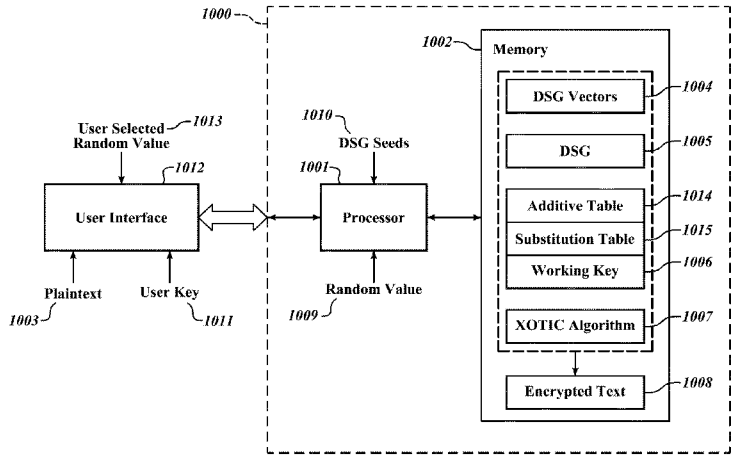

FIG.1

(57) Abstract: A system and method for providing a rapid, yet highly secure cryptographic technique, to provide enhanced protection for digital data. At least one random value and Deterministic Sequence Generator (DSG) seeds are mathematically processed to create an initialization value (IV). The initialization value (IV) is mathematically processed with a user key to generate a set of initial DSG vectors. The initial DSG vectors are then inputted into a DGS and, using the initial DSG vectors, the DSG creates an additive table and a substitution table. An initial internal working key is generated from the user key and the initial DSG vectors. An addition, an XOR and a substitution operation is applied to each byte of plaintext data in combination with the internal working key to enable the cipher to quickly and effectively encrypt the plaintext data. Once encrypted, the encrypted data may be stored in memory for subsequent use and/or transmitted to another party. Decryption of the encrypted data may be performed by applying the inverse of the above process.

WO 2016/204846 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/024764

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i, H04L 9/28(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 9/08; H04L 9/28; H04L 9/06; 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: Deterministic Sequence Generator (DSG), encryption, generation, substitution table, 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 5003596 A (MICHAEL C. WOOD) 26 March 1991 See column 5, line 59 - column 7, line 23; claims 1-10; and figure 2.	1-22
A	US 2009-0220071 A1 (SHAY GUERON et al.) 03 September 2009 See paragraphs [0019]-[0024], [0028]-[0033].	1-22
A	RAZI HOSSEINKHANI et al., "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System", International Journal of Computer Science and Security (IJCSS), Vol. 6, No. 1, pp. 19-28, February 2012 See pages 20-24.	1-22
A	US 6246768 B1 (YONG-DUK KIM) 12 June 2001 See column 3, line 36 - column 5, line 49; claim 2; and figure 2.	1-22
A	US 5623548 A (RYOTA AKIYAMA et al.) 22 April 1997 See column 11, line 56 - column 13, line 25; and figures 9, 10.	1-22

☐ 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	Date of mailing of the international search report
20 December 2016 (20.12.2016)	**02 January 2017 (02.01.2017)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
AHN, Jeong Hwan
Telephone No. +82-42-481-8633

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/024764

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5003596 A	26/03/1991	CA 2064769 A1	18/02/1991
		CA 2064769 C	08/02/2000
		EP 0489742 A1	12/11/1997
		EP 0489742 B1	19/11/1997
		JP 3188940 B2	16/07/2001
		WO 91-03113 A1	07/03/1991
US 2009-0220071 A1	03/09/2009	CN 101520965 A	02/09/2009
		CN 101520965 B	16/03/2016
		EP 2096786 A2	02/09/2009
		EP 2096786 A3	25/01/2012
		EP 2096786 B1	06/04/2016
		JP 2009-211071 A	17/09/2009
		JP 5538736 B2	02/07/2014
		KR 10-1036103 B1	19/05/2011
		KR 10-2009-0093900 A	02/09/2009
		US 8879725 B2	04/11/2014
US 6246768 B1	12/06/2001	KR 10-0296958 B1	16/05/2001
US 5623548 A	22/04/1997	GB 2285562 A	12/07/1995
		JP 3029381 B2	04/04/2000