Title (en)

METHODS AND SYSTEMS FOR SECURE DATA COMMUNICATION

Title (de)

VERFAHREN UND SYSTEME ZUR SICHEREN DATENÜBERTRAGUNG

Title (fr)

PROCÉDÉS ET SYSTÈMES POUR UNE COMMUNICATION DE DONNÉES SÉCURISÉE

Publication

EP 3701664 A4 20210728 (EN)

Application

EP 18870501 A 20181023

Priority

- US 201715796577 A 20171027
- US 201862662819 P 20180426
- CA 2018051339 W 20181023

Abstract (en)

[origin: WO2019079890A1] A computer-implemented method, which comprises: receiving an input message comprising N-bit input segments, N being an integer greater than one; converting the N-bit input segments into corresponding N-bit output segments using a 2N-by-2N one-to-one mapping stored in a non-transitory storage medium; and generating an output message comprising the N-bit output segments. Also, a computer-implemented method for a recipient to validate a message received from a sender, the message including a first part and a second part. This method comprises receiving a token from a witnessing entity; obtaining a first data element by joint processing of the first part of the message and the token; obtaining a second data element by joint processing of the second part of the message using a key associated with the sender; and validating the message by comparing the first and second data elements.

IPC 8 full level

H04L 9/00 (2006.01); **G06Q 20/06** (2012.01); **G06Q 20/38** (2012.01); **H03M 7/00** (2006.01); **H04L 7/00** (2006.01); **H04L 9/06** (2006.01); **H04L 9/08** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

G06Q 20/06 (2013.01); **G06Q 20/381** (2013.01); **G06Q 20/382** (2013.01); **G06Q 20/38215** (2013.01); **H04L 9/0618** (2013.01); **H04L 9/0822** (2013.01); **H04L 9/3239** (2013.01); **H04L 9/50** (2022.05); H03M 7/00 (2013.01)

Citation (search report)

- [I] ZULEHNER ALWIN ET AL: "Taking one-to-one mappings for granted: Advanced logic design of encoder circuits", DESIGN, AUTOMATION & TEST IN EUROPE CONFERENCE & EXHIBITION (DATE), 2017, EDAA, 27 March 2017 (2017-03-27), pages 818 - 823, XP033096467, DOI: 10.23919/DATE.2017.7927101
- [I] WU ET AL: "One-to-one mapping matrix", APPLIED MATHEMATICS AND COMPUTATION, ELSEVIER, US, vol. 169, no. 2, 15 October 2005 (2005-10-15), pages 963 - 970, XP027747533, ISSN: 0096-3003, [retrieved on 20051015]
- [I] "Announcing the Advanced Encryption Standard (AES)", INTERNET CITATION, 26 November 2001 (2001-11-26), XP002452709, Retrieved from the Internet <URL:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> [retrieved on 20070926]
- See references of WO 2019079890A1

Cited by

US11621841B2; US11924339B2

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

WO 2019079890 A1 20190502; AU 2018355917 A1 20200213; AU 2018355917 B2 20200924; CA 3073549 A1 20190502; CA 3073549 C 20210608; CN 111201749 A 20200526; CN 111201749 B 20210928; EP 3701664 A1 20200902; EP 3701664 A4 20210728; WO 2020082160 A1 20200430

DOCDB simple family (application)

CA 2018051339 W 20181023; AU 2018355917 A 20181023; CA 2019050093 W 20190125; CA 3073549 A 20181023; CN 201880057218 A 20181023; EP 18870501 A 20181023