Title (en)

SECURE DISTRIBUTED DATA PROCESSING

Title (de)

SICHERE VERTEILTE DATENVERARBEITUNG

Title (fr)

TRAITEMENT DE DONNÉES DISTRIBUÉ SÉCURISÉ

Publication

EP 3535924 A4 20200617 (EN)

Application

EP 16920471 A 20161104

Priority

CN 2016104553 W 20161104

Abstract (en)

[origin: WO2018082008A1] According to an example aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program codes, the at least one memory and the computer program codes being configured to, with the at least one processing core, cause the apparatus at least to receive, from at least one data provider, at least one ciphertext, the at least one ciphertext comprising a first ciphertext, perform a mathematical manipulation of the first ciphertext to modify the first ciphertext without decrypting the first ciphertext, the mathematical manipulation being selected in the apparatus in dependence of a mathematical operation to be performed on plaintext underlying the first ciphertext, obtain a second ciphertext from the modified first ciphertext by performing a cryptographic operation, wherein at least one number is randomly generated and used in masking plaintext underlying the second ciphertext, and provide the second ciphertext to an access control node.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP)

H04L 9/008 (2013.01); **H04L 9/0827** (2013.01); **H04L 9/088** (2013.01); **H04L 9/0894** (2013.01); **H04L 9/302** (2013.01); H04L 2209/46 (2013.01); H04L 2209/76 (2013.01)

Citation (search report)

- [XI] XIMENG LIU ET AL: "Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, vol. 15, no. 1, 1 March 2016 (2016-03-01), US, pages 27 - 39, XP055686573, ISSN: 1545-5971, DOI: 10.1109/TDSC.2016.2536601
- [A] MING LI ET AL: "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS., vol. 24, no. 1, 1 January 2013 (2013-01-01), US, pages 131 - 143, XP055378272, ISSN: 1045-9219, DOI: 10.1109/TPDS.2012.97
- [A] "RoboCup 2008: RoboCup 2008: Robot Soccer World Cup XII", vol. 2894, 1 January 2003, SPRINGER INTERNATIONAL PUBLISHING, Cham, ISBN: 978-3-319-10403-4, article EMMANUEL BRESSON ET AL: "A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications", pages: 37 - 54, XP055604158, 032682, DOI: 10.1007/978-3-540-40061-5_3
- See references of WO 2018082008A1

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 2018082008 A1 20180511; CN 110089071 A 20190802; CN 110089071 B 20230217; EP 3535924 A1 20190911; EP 3535924 A4 20200617

DOCDB simple family (application)

CN 2016104553 W 20161104; CN 201680091521 A 20161104; EP 16920471 A 20161104