Title (en)

SECURE DATA PROCESSING

Title (de)

SICHERE DATENVERARBEITUNG

Title (fr)

TRAITEMENT DE DONNÉES SÉCURISÉ

Publication

EP 3747150 A4 20210825 (EN)

Application

EP 18903892 A 20180130

Priority

CN 2018074627 W 20180130

Abstract (en)

[origin: WO2019148335A1] According to an example aspect of the present invention, there is provided there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to process, using two random numbers R1, R 2, a pair of input ciphertexts to obtain a masked ciphertext encrypted using a public key of a computation node, provide the masked ciphertext to the computation node and receive a response from the computation node, and process the response to remove the mask, to obtain at least one of: a first output ciphertext comprising a maximum value of plaintexts corresponding to the input ciphertexts and a second output ciphertext comprising a minimum value of plaintexts corresponding to the input ciphertexts, wherein the output ciphertext is encrypted under a public key.

IPC 8 full level

H04L 9/14 (2006.01); H04L 9/00 (2006.01)

CPC (source: EP)

H04L 9/008 (2013.01)

Citation (search report)

- [X] US 2011194691 A1 20110811 - RANE SHANTANU [US], et al
- [XDA] 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
- [XD] LIU XIMENG ET AL: "Hybrid privacy-preserving clinical decision support system in fog-cloud computing", FUTURE GENERATION COMPUTER SYSTEMS, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 78, 18 March 2017 (2017-03-18), pages 825 - 837, XP085191450, ISSN: 0167-739X, DOI: 10.1016/J.FUTURE.2017.03.018
- [A] DING WENXIU ET AL: "Encrypted data processing with Homomorphic Re-Encryption", INFORMATION SCIENCES, AMSTERDAM, NL, vol. 409, 7 May 2017 (2017-05-07), pages 35 - 55, XP085055393, ISSN: 0020-0255, DOI: 10.1016/J.INS.2017.05.004
- See references of WO 2019148335A1

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 2019148335 A1 20190808; EP 3747150 A1 20201209; EP 3747150 A4 20210825

DOCDB simple family (application)

CN 2018074627 W 20180130; EP 18903892 A 20180130