

Title (en)

APPARATUS FOR PROCESSING APPROXIMATELY ENCRYPTED MESSAGES AND METHODS THEREOF

Title (de)

VORRICHTUNG UND VERFAHREN ZUR VERARBEITUNG VON ANNÄHERND VERSCHLÜSSELTEN NACHRICHTEN UND VERFAHREN DAFÜR

Title (fr)

APPAREIL DE TRAITEMENT DE MESSAGES APPROXIMATIVEMENT CHIFFRÉS ET PROCÉDÉS ASSOCIÉS

Publication

EP 3909193 A4 20220928 (EN)

Application

EP 19908950 A 20191121

Priority

- US 201962790806 P 20190110
- KR 20190066572 A 20190605
- KR 20190112292 A 20190910
- KR 2019016001 W 20191121

Abstract (en)

[origin: KR20200087061A] The present invention is to provide an apparatus for efficiently performing a reboot operation on an approximate-encrypted ciphertext and a method thereof. A method of processing a ciphertext is disclosed. According to the present invention, the method of processing a ciphertext comprises the steps of: linearly transforming a homomorphic ciphertext for an approximate message containing an error; calculating an approximate modulus of the linearly modified homomorphic ciphertext using a multi-order equation set to approximate input values within a preset range to an integer point; and linearly transforming the approximate modulus calculated homomorphic ciphertext into a ciphertext form.

IPC 8 full level

H04L 9/00 (2022.01)

CPC (source: EP KR)

H04L 9/008 (2013.01 - EP KR); **H04L 9/0618** (2013.01 - KR); **H04L 9/0838** (2013.01 - KR); **H04L 9/3026** (2013.01 - KR)

Citation (search report)

- [XY] JUNG HEE CHEON ET AL: "Faster Homomorphic Discrete Fourier Transforms and Improved FHE Bootstrapping", vol. 20181109:163301, 5 November 2018 (2018-11-05), pages 1 - 18, XP061026898, Retrieved from the Internet <URL:http://eprint.iacr.org/2018/1073.pdf> [retrieved on 20181105]
- [XPY] HAN KYOOHYUNG ET AL: "Improved Homomorphic Discrete Fourier Transforms and FHE Bootstrapping", IEEE ACCESS, vol. 7, 29 April 2019 (2019-04-29), pages 57361 - 57370, XP011724114, DOI: 10.1109/ACCESS.2019.2913850
- [T] CHEON JUNG HEE ET AL: "Bootstrapping for Approximate Homomorphic Encryption", 31 March 2018, SAT 2015 18TH INTERNATIONAL CONFERENCE, AUSTIN, TX, USA, SEPTEMBER 24-27, 2015; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER, BERLIN, HEIDELBERG, PAGE(S) 360 - 384, ISBN: 978-3-540-74549-5, XP047471999
- [YP] CHEN HAO ET AL: "Improved Bootstrapping for Approximate Homomorphic Encryption", 24 April 2019, ADVANCES IN DATABASES AND INFORMATION SYSTEMS; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 34 - 54, ISBN: 978-3-319-10403-4, XP047507752
- See references of WO 2020145503A1

Cited by

CN117440103A; CN117353898A

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)

EP 3909193 A1 20211117; EP 3909193 A4 20220928; KR 102167565 B1 20201019; KR 20200087061 A 20200720

DOCDB simple family (application)

EP 19908950 A 20191121; KR 20190112292 A 20190910