Название: Euclidean Division Method for the Homomorphic Scheme CKKS

Авторы: Babenko, M (Babenko, Mikhail); Golimblevskaia, E (Golimblevskaia, Elena)

Групповые авторы книг: IEEE

Источник: PROCEEDINGS OF THE 2021 IEEE CONFERENCE OF RUSSIAN YOUNG RESEARCHERS IN ELECTRICAL AND ELECTRONIC ENGINEERING (ELCONRUS) **Серия книг:** IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference **Стр.:** 217-220 **DOI:** 10.1109/ElConRus51938.2021.9396347 **Опубликовано:** 2021

Аннотация: The use of cloud computing can reduce the economic costs of maintaining IT infrastructure, but at the same time, the likelihood of confidential data theft increases. To reduce the likelihood of it, cloud computing uses homomorphic encryption. However, a homomorphic cipher only allows adding and multiplying encrypted numbers; in some cases, a division operation is required to implement algorithms. To implement the division operation with encrypted numbers it is necessary to implement the encrypted number comparison operation. Considering that the operation of comparing encrypted numbers is carried out using numerical methods, it is necessary to adapt the existing algorithms for Euclidean division. In this article, we propose a two-stage algorithm for Euclidean division of numbers encrypted using the CKKS scheme and investigate its properties.

Идентификационный номер: WOS:000669709800049

Название конференции: IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)

Дата проведения конференции: JAN 26-28, 2021

Место проведения конференции: Saint Petersburg Electrotechn Univ, RUSSIA

Спонсоры конференции: IEEE

Принимающая сторона конференции: Saint Petersburg Electrotechn Univ

ISSN: 2376-6557

ISBN: 978-1-6654-0476-1