US 20240214178A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214178 A1

TAMIYA et al. (43) Pub. Date: Jun. 27, 2024

(54) **HOMOMORPHIC CYCLIC OPERATION SYSTEM, HOMOMORPHIC CYCLIC OPERATION APPARATUS, HOMOMORPHIC CYCLIC OPERATION METHOD, AND HOMOMORPHIC CYCLIC OPERATION PROGRAM**

(71) Applicant: **NEC Corporation**, Minato-ku, Tokyo (JP)

(72) Inventors: **Hiroto TAMIYA**, Tokyo (JP); **Toshiyuki ISSHIKI**, Tokyo (JP); **Kengo MORI**, Tokyo (JP); **Sanami NAKAGAWA**, Tokyo (JP)

(73) Assignee: **NEC Corporation**, Minato-ku, Tokyo (JP)

(21) Appl. No.: **18/291,341**

(22) PCT Filed: **Jul. 29, 2021**

(86) PCT No.: **PCT/JP2021/028209**

§ 371 (c)(1),
(2) Date: **Jan. 23, 2024**

Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/008*** (2013.01)

(57) **ABSTRACT**

A homomorphic cyclic operation system performs a homomorphic cyclic operation on a periodic array of data using homomorphic encryption having a homomorphic operation defined with respect to at least one multiplication and comprises: an encryption apparatus that encrypts the periodic array of data by storing it in the coefficients of an indeterminate polynomial to generate a ciphertext of periodic data; and a homomorphic cyclic operation apparatus that shifts the periodic array of data in the ciphertext of the periodic data by applying the indeterminate raised to the power of a shift amount to the ciphertext of the periodic data.