US 20240214201A1

(19) **United States**

(12) **Patent Application Publication**

HOSHIZUKI et al.

(10) **Pub. No.: US 2024/0214201 A1**

(43) **Pub. Date: Jun. 27, 2024**

(54) **ENCRYPTION PROCESSING APPARATUS AND ENCRYPTION PROCESSING METHOD**

(71) Applicant: **AXELL CORPORATION**, Tokyo (JP)

(72) Inventors: **Yusuke HOSHIZUKI**, Tokyo (JP); **Kotaro MATSUOKA**, Tokyo (JP)

(73) Assignee: **AXELL CORPORATION**, Tokyo (JP)

(21) Appl. No.: **18/540,794**

(22) Filed: **Dec. 14, 2023**

(30) **Foreign Application Priority Data**

Dec. 20, 2022 (JP) 2022-203161

Publication Classification

(51) **Int. Cl.**

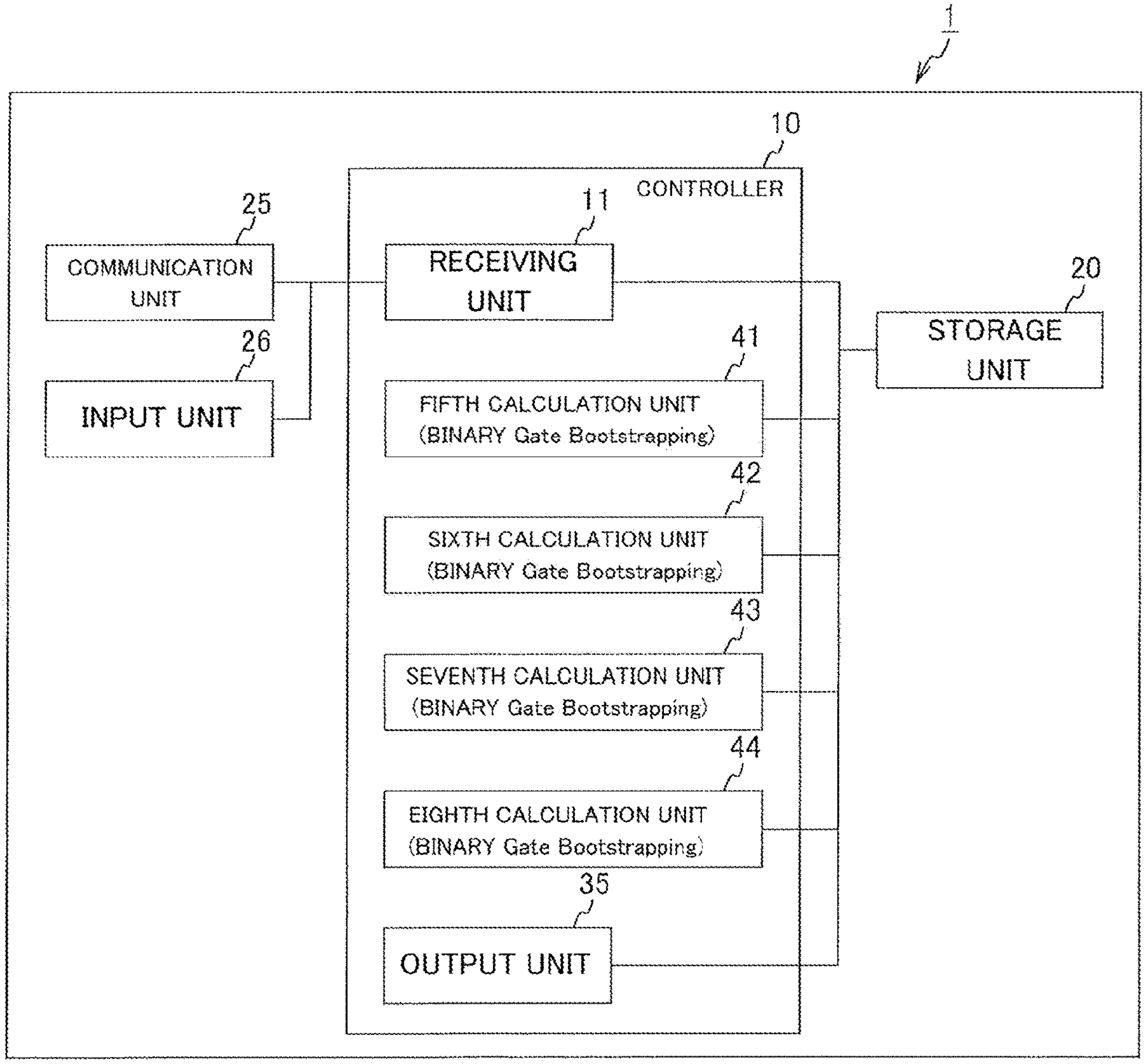
H04L 9/30	(2006.01)
H04L 9/00	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/3093*** (2013.01); ***H04L 9/008*** (2013.01)

(57) **ABSTRACT**

An encryption processing apparatus processing a ciphertext is disclosed. The ciphertext is a fully homomorphic ciphertext that has a value with an error as a plaintext associated with an integer and that enables an operation between integers without decryption. The encryption processing apparatus includes a processor which executes the following processes. The processor applies a first polynomial to a first ciphertext to obtain a second ciphertext, the first polynomial being configured to be able to select an operation result in units smaller than a divided region used as one plaintext symbol corresponding to the first ciphertext in a range. The processor further convers two or more of plaintext symbols corresponding to the second ciphertext to the same one plaintext symbol by applying a second polynomial to the second ciphertext, to obtain a third ciphertext corresponding to an operation result of a predetermined operation.


1
10
CONTROLLER
25
COMMUNICATION UNIT
11
RECEIVING UNIT
20
STORAGE UNIT
26
INPUT UNIT
41
FIFTH CALCULATION UNIT (BINARY Gate Bootstrapping)
42
SIXTH CALCULATION UNIT (BINARY Gate Bootstrapping)
43
SEVENTH CALCULATION UNIT (BINARY Gate Bootstrapping)
44
EIGHTH CALCULATION UNIT (BINARY Gate Bootstrapping)
35
OUTPUT UNIT