

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214212 A1 HAMADA et al.

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

(54) SECURE CONSOLIDATION SYSTEM, INFORMATION PROCESSING APPARATUS, SECURE CONSOLIDATION METHOD, AND **PROGRAM**

(71) Applicant: NIPPON TELEGRAPH AND TELEPHONE CORPORATION,

Tokyo (JP)

(72) Inventors: Koki HAMADA, Tokyo (JP); Koji

CHIDA, Tokyo (JP); Masanobu KII, Tokyo (JP); Atsunori ICHIKAWA, Tokyo (JP); Junichi TOMIDA, Tokyo

(JP)

(21) Appl. No.: 18/556,518

(22) PCT Filed: May 21, 2021

PCT/JP2021/019342 (86) PCT No.:

§ 371 (c)(1),

(2) Date: Oct. 20, 2023

Publication Classification

Int. Cl. (51)H04L 9/32

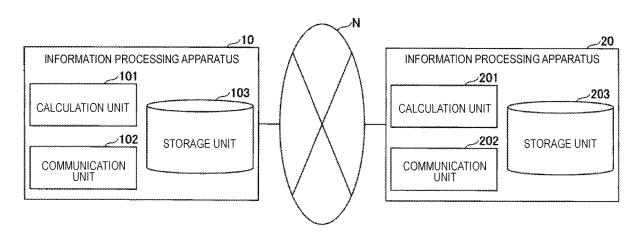
(2006.01)

(52)U.S. Cl.

CPC *H04L 9/3236* (2013.01)

(57)ABSTRACT

A secure collation system performs secure-data-collation between first and second information processing apparatuses and includes the first and second information processing apparatuses. The second information-processing-apparatus creates, when receiving a first vector having a hash value of a key value of the first information-processing-apparatus as an element, a second vector by adding a dummy hash value to the first vector and rearranging the first vector by random permutation; creates a third vector having, as elements, a hash value of a key value of the second informationprocessing-apparatus and a hash value of a dummy key value; and transmits the second and third vectors to the first information-processing-apparatus. The first informationprocessing-apparatus calculates a hash value of an element of the third vector and creates a fourth vector having the hash value as an element; and collates matched values between each element of the third vector and each element of the fourth vector.



1