US 20240214213A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214213 A1

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

(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.: **18/556,931**

(22) PCT Filed: **May 21, 2021**

(86) PCT No.: **PCT/JP2021/019341**

§ 371 (c)(1),
(2) Date: **Oct. 24, 2023**

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 9/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3242*** (2013.01); ***H04L 9/0618*** (2013.01)

(57) **ABSTRACT**

The secure join system includes the first and second information-processing-apparatuses respectively holding first and second data. The second information-processing-apparatus is configured to: create third and fourth vectors in which a hash-value related to a key-value of the first data in a first vector and a ciphertext of the first data corresponding to the key-value in a second vector are rearranged by permutation; and create a fifth vector having a hash-value related to a key-value of the second data. The first information-processing-apparatus is configured to: search for j in which a hash-value of an i-th element of the fifth vector matches a j-th element value of the third vector for each i and create encrypted data in which a ciphertext of a j-th element value of the fourth vector is set when j is found and a ciphertext of a dummy value is set when j is not found.