

A B S T R A C T

A re-encryption key generator according to an embodiment generates a re-encryption key required to re-encrypt, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first public key of a first user device to obtain re-encrypted text data which can be decrypted by a second private key of a second user device. The first storage device stores a first private key corresponding to the first public key. The second storage device stores a second public key corresponding to the second private key. The re-encryption key generation means generates the re-encryption key based on the first private key, the second public key, and the first random number.



162162

G00002

