A B S T R A C T

A re-encryption key generator according to an embodiment generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device by re-encrypting ciphertext obtained by encrypting plaintext by a first public key of a first user device without decryption. The re-encryption key generator stores a first private key corresponding to the first public key. The re-encryption key generator stores a second re-encryption key generation key of the second user device that is different from a second public key corresponding to the second private key. The re-encryption key generator generates the re-encryption key based on the first private key and the second re-encryption key generation key.