## ABSTRACT

The present invention is aimed at performing shuffle-decrypting certification which is made more secure by not allowing any knowledge of secret information to leak when certifying the legitimacy of shuffling and decryption. A shuffle-decrypting legitimacy certifying apparatus is supplied with a plurality of encrypted texts, a public key, a decrypting secret key, and a random number, encrypts the encrypted texts with the public key, shuffles the order of the encrypted texts, generates a plurality of decrypted texts produced by decrypting the encrypted texts with the secret key, and certifies the legitimacy of the encryption, the shuffling of the order, and the decryption to a shuffle-decrypting verifying apparatus. Data to communicate with the shuffle-decrypting verifying apparatus includes a commitment of a shuffled encrypted text which is an encrypted text produced by encrypting the encrypted texts with the public key and shuffling the order thereof.