G00002

CERTIFIED SHIFFLE-DECRYPTING SYSTEM, CERTIFIED SHUFFLE-DECRYPTING METHOD AND CERTIFIED SHUFFLE-DECRYPTION VERIFYING METHOD

ABSTRACT

A certified shuffle-decrypting system is disclosed, which does not require encrypted texts to be output, and in which the amounts of calculation and certificates are mininized to allow efficient processing. The certified shuffle-decrypting system generates shuffle-decryption certificates certifying that multiple encrypted texts have been shuffle-decrypted correctly, and verifies, based on the shuffle-decryption certificates, whether or not the shuffle-decryption has taken place correctly. This system comprises: a certified shuffle-decryption device (10) for shuffle-decrypting the multiple encrypted texts to generate the shuffle-decrypted texts, and for generating the shuffle-decryption certificates; and shuffle-decryption verification device (20) for verifying whether or not the shuffle-decryption has taken place correctly; by referring to the generated shuffle-decrypted texts and the shuffle-decryption certificates for the shuffle-decrypted texts.

FIG. 1

162162