ABSTRACT

An integrated shuffle validity proving device (300) is provided correspondingly to an ordinal number κ which is an integer representing an order. The device (300) has a permutation proof commitment unit (310) which, on receiving a commitment public key and a permutation storage commitment containing a permutation proof text made by first to (κ-1)-th integrated shuffle validity proving devices from outside, encrypts a permutation proof commitment created by adding a permutation proof text made by the κ-th integrated shuffle validity proving device to the received permutation storage commitment with the commitment public key and sends the encrypted permutation proof commitment to the outside.