A B S T R A C T

Each participant apparatus (103) encrypts a plaintext by using a secret key of secret key cryptography, encrypts the encryption key by a public key, and sends the plaintext and public key to a substitution/decryption apparatus (112). With this processing, the limitation on the length of a ciphertext to be processed can be eliminated. In this invention, a verifiable proof text using a public key by each substitution/decryption apparatus is verified by a verification apparatus (109) by using the public key. If one of a plurality of organizations to decrypt and shuffle ciphertexts has not correctly executed the operation, a third party can specify it and prove that the specified organization is unauthorized.