G00002



ABSTRACT

A anonymous decryption system, the management of which is facilitated and initialization of which is readily and reliably carried out. A shuffling management center (10) transmits a security parameter and common public information generated on the basis of the security parameter to decryption shuffle centers (20-1 to 20-m). The decryption shuffle centers (20-1 to 20-m) generate public keys and decryption keys and returns the public keys to the shuffling management center (10). The shuffling management center combines the returned public key to generate an encryption public key and make the encryption key public. The shuffling management center (10) repeats transfer of encrypted data list to the decryption shuffle center (20-j) having the j-th processing priority when it decrypts the encrypted data list, transfer of a received data list of which a order-switching process and a partial decryption process are carried out to the next decryption shuffle center (20-(j+1)). Such processing is carried out for up to the last decryption shuffle center (20-m) and make the data list from there the decryption result.



162162