

ABSTRACT

[Subject] To provide an anonymous electronic voting system which is capable of securing secrecy of the vote from a device
5 such as a cellular phone having a smaller storage capacity and a lower processing throughput, and verifying the electorates in the case where there is no common-key verification base for all the electorates.

[Solving Means] A voting server (200) transmits a list of
10 plaintext and encrypted voting data obtained by encrypting the plaintext to a voter terminal (100), and the voter terminal (100) transmits a selected encrypted candidate name corresponding to the plaintext elected by the voter to an encryption server (400). The encryption server (400) returns encrypted voting data
15 obtained by re-encrypting the encrypted candidate name to the voter terminal (100), and the voter terminal (100) transmits the encrypted voting data received from the encryption server (400) for voting. Decryption of the encrypted voting data is performed by an anonymous decryption system (500). The
20 voter terminal (100) certifies the voter to an authentication server (300), and affixes a digital signature to the encrypted voting data based on a common-key authentication base, transmitting the same to the voting server (200).