ABSTRACT

It is an object of the present invention to enhance the security and reduce the data amount of data to be handled in a group signing system, in which when the group public key which includes: a description for four groups: group 1, group 2, group T, and group E of the same order number; a description of bilinear mapping from group 1 and group 2 to group T; each generator of group 1, group 2, group T, and group E; and a signature public key of a signature scheme using group 1, group 2, and group T, is input, the member secret key including an integer not larger than the order number, member evidence which is a value given by multiplying the generator of group E by the member secret key, and an element of group 1 or group 2 which is a value given by multiplying the generator of the group 1 or the group 2 by the member secret key are sent to the member-certificate issuing device, and thereafter upon receipt of a signature for the member secret key, which is verifiable by the signature public key, from the member-certificate issuing device, the signature is used as the member certificate.