Title: METHOD OF KEY MANAGEMENT

Abstract: A method of key management for group-based controlled access to encrypted data, in which a decryption key for the encrypted data can be obtained by a party if the party is a member of at least one group which is authorized to access the data, the groups being organized in a hierarchical tree in which each non-leaf node represents a group and each leaf node represents a member of all groups represented by nodes hierarchically superior to the leaf node in question, characterized in that the leaf nodes are each assigned a respective arbitrarily chosen private key and corresponding public key, in that the private key associated with a particular non-leaf node is obtained by executing a key agreement protocol using a private key associated with a first child of the particular non-leaf node and a public key associated with a second child of the particular non-leaf node, and in that the private key for a group associated with a particular node is obtained by recursively obtaining the group private keys of the nodes on a path from the leaf node corresponding to the party in question and the node corresponding to the authorized group.