

METHOD AND SYSTEM FOR PERFORMING COLLECTIVE AUTHENTICATION IN A COMMUNICATION NETWORK

Abstract

5 The invention provides method, system and apparatus for performing collective authentication in a communication network having a verifying node and a plurality of proving nodes. The method comprises: calculating by each proving node a first value based on a predetermined public modulus value and a random value selected by each proving node; calculating by the verifying node a first
10 verification value based on the first values calculated by the plurality of the proving nodes; generating a random number for each proving node; calculating, by each proving node, a second value based on the generated random number, the selected random value, the private key of the each proving node, and the predetermined public modulus value; calculating, by the verifying node, a second
15 verification value based on the second values calculated by the plurality of proving nodes; and determining whether authentication is successful based on whether the first verification value, the second verification value and the generated random numbers satisfy a predetermined authentication condition.

20 (Figure 1)