

node P_i , k is the pre-set integer $k \geq 1$, and $e_i=(e_{i,1}, \dots, e_{i,k})$ is the random number generated for the proving node P_i , wherein $e_{i,j}$ is the j -th bit of e_i .

13. The method according to claim 12, wherein the step of determining whether authentication of the plurality of proving nodes is successful, further comprises:

- 5 determining the authentication of the plurality of proving nodes is successful if the following equation is satisfied:

$$x = y^c \prod_{i=1}^u \prod_{j=1}^k v_{i,j}^{e_{i,j}} \bmod n, \text{ if } v_{i,j} = \frac{1}{s_{i,j}^c} \bmod n$$

$$y^c = x \prod_{i=1}^u \prod_{j=1}^k v_{i,j}^{e_{i,j}} \bmod n, \text{ if } v_{i,j} = s_{i,j}^c \bmod n$$

wherein x is the first verification value, y is the second verification value, c is the pre-set integer $c \geq 2$, $v_i=(v_{i,1}, \dots, v_{i,k})$ is the public key of the proving node P_i ,

- 10 and $e_i=(e_{i,1}, \dots, e_{i,k})$ is the random number generated for the proving node P_i .

14. A method for performing collective authentication in a communication network having a verifying node and a plurality of proving nodes connected thereto, the method comprising:

- 15 calculating, by the verifying node, a first verification value based on a plurality of first values, wherein each of the first values is individually calculated by one of the plurality of proving nodes in the network based on a predetermined public system parameter and a random value selected by the proving node;

- 20 calculating, by the verifying node, a second verification value based on a plurality of second values, wherein each of the second value is individually calculated by one of the plurality of proving nodes in the network based on a

random number generated for the proving node, the random value selected by the proving node and the predetermined public system parameter; and

determining, by the verifying node, whether authentication of the plurality of proving nodes is successful based on whether the first verification value, the
5 second verification value and the random numbers generated for the plurality of proving nodes in the network satisfy a predetermined authentication condition.

15. The method according to claim 14, wherein the step of calculating the first verification value based on a plurality of first values, further comprises:

calculating, by the verifying node, the first verification value based on at
10 least one first unit value respectively received from at least one proving node directly connected to the verifying node, wherein each of the at least one first unit value is calculated based on a first value calculated by a proving node directly connected to the verifying node and at least one first value respectively
15 calculated by at least one child node of the proving node directly connected to the verifying node.

16. The method according to claim 14 or claim 15, wherein the step of calculating the second verification value based on a plurality of second values, further comprising:

calculating, by the verifying node, the second verification value based on
20 at least one second unit value respectively received from at least one proving node directly connected to the verifying node, wherein each of the at least one second unit value is calculated based on individually second value calculated by

a proving node directly connected to the verifying node and at least one second value respectively calculated by at least one child node of the proving node directly connected to the verifying node.

17. The method according to any one of claim 14 to claim 16, further comprising:

5 generating, by the verification node, a random number for each proving node in the network and sending the generated random number to the each proving node in the network.

18. The method according to any one of claim 14 to claim 16, further comprising:

 generating, by the verifying node, a root random value and sharing the
10 generated root random value in the network;

 wherein the random number for each proving node in the network is generated by the each proving node based on the root random value and a pre-determined function.

19. A method for performing collective authentication in a communication

15 network having a verifying node and a plurality of proving nodes connected thereto, the method comprising:

 calculating, by each proving node in the network, a first value based on a predetermined public system parameter and a random value selected by the each proving node and sending the calculated first value to a parent node
20 directly connected to the each proving node;

calculating, by the each proving node in the network, a second value based on a random number generated for the each proving node, the random value selected by the each proving node, the private key of the each proving node, and the predetermined public system parameter, and sending the
5 calculated second value to a parent node directly connected to the each proving node.

20. The method according to claim 19, further comprising:

receiving, by the each proving node in the network, a root random value from the verifying node, and

10 generating, by the each proving node, the random number for calculating the second value for the each proving node based on the received root random value and a pre-determined function.

15