

Claims

1. 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:

5 calculating, by each proving node in the network, a first value for the each proving node based on a predetermined public system parameter and a random value selected by the each proving node;

 sending, by the each proving node in the network, the calculated first value to its parent node;

10 calculating, by the verifying node, a first verification value based on a product of the plurality of first values calculated by the plurality of proving nodes in the network;

 generating a random number for the each proving node in the network;

 calculating, by the each proving node in the network, a second value for the
15 each proving node based on the random number generated for the each proving node, the random value selected by the each proving node, a private key of the each proving node, and the predetermined public system parameter;

 sending, by the each proving node in the network, the calculated second value to its parent node;

calculating, by the verifying node, a second verification value based on a product of the plurality of second values calculated by the plurality of proving nodes in the network; and

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

2. The method according to claim 1, further comprising:

if one of the proving nodes in the network is directly connected to at least
10 one child node, sending, by the proving node in the network, a first unit value to its parent node , wherein the first unit value is calculated based on a product of the first values calculated by both the proving node and the at least one child node of the proving node;

wherein the step of calculating a first verification value based on a product
15 of the plurality of first values calculated by the plurality of proving nodes, further comprises:

calculating, by the verifying node, the first verification value based on at least one first unit value, wherein each of the at least one first unit value is respectively calculated by at least one proving node directly connected to the
20 verifying node in the network.

3. The method according to claim 1 or 2, further comprising:

if one of the proving nodes in the network is directly connected to at least one child node, sending, by the proving node in the network, a second unit value to its parent node, wherein the second unit value is calculated based on a product of the second values calculated by both the proving node and the at least one child node of the proving node;

wherein the step of calculating a second verification value based on a product of the plurality of second values calculated by the plurality of proving nodes, further comprises:

calculating, by the verifying node, the second verification value based on at least one second unit value, wherein each of the at least one second unit value is respectively calculated by at least one proving node directly connected to the verifying node in the network.

4. The method according to any one of claim 1 to claim 3, wherein the step of generating a random number for the each proving node in the network, further comprises:

generating, by the verifying node, a random number for the each proving node in the network; and

sending the generated random number for the each proving node to the each proving node directly or through a parent node of the each proving node in the network.

5. The method according to any one of claim 1 to claim 3, wherein the step of generating a random number for the each proving node in the network, further comprises:

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

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

6. The method according to any preceding claim, further comprising:

calculating, by the each proving node or the verifying node or a trusted
10 party, a public key or the private key of the each proving node.

7. The method according to claim 6, wherein the public key or the private key of the each proving node is calculated based on the predetermined public system parameter and an identity of the each proving node.

8. The method according to claim 7, wherein the predetermined system parameter
15 is a public modulus which is a product of a plurality of prime numbers, wherein at least two of the prime numbers are different.

9. The method according to claim 7 or claim 8, wherein the public key or private key for the each proving node is calculated according to the following Equation:

$$v_{i,j} = \frac{1}{s_{i,j}^c} \bmod n, \text{ or } v_{i,j} = s_{i,j}^c \bmod n; \quad i = 1, \dots, u; j = 1, \dots, k$$

wherein $v_i=(v_{i,1}, \dots, v_{i,k})$ is the public key of the proving node P_i , $s_i=(s_{i,1}, \dots, s_{i,k})$ is the private key of the proving node P_i , n is the predetermined public system parameter called public modulus, u is the number of the proving nodes in the network, k is a pre-set integer no less than 1, and c is a pre-set integer no less than 2.

10. The method according to claim 9, wherein the first value is calculated by the each proving node in the network according to the following equation:

$$x_i = r_i^c \bmod n$$

wherein x_i is the first value calculated by the proving node P_i , n is the predetermined public modulus value, r_i is the random value selected by the proving node P_i , c is the pre-set integer no less than 2.

11. The method according to claim 10, wherein the first verification value is calculated according to the following equation:

$$x = \prod_{i=1}^u x_i \bmod n$$

wherein x is the first verification value, x_i is the first value calculated by the proving node P_i , n is the predetermined system parameter called public modulus, u is the number of the proving nodes in the network.

12. The method according to claim 11, wherein the second verification value is calculated according to the following equation:

$$y = \prod_{i=1}^u y_i \bmod n;$$

wherein y is the second verification value, y_i is the second value calculated by the proving node P_i , n is the predetermined public modulus value, and u is the number of the proving nodes in the network, wherein the second value y_i is calculated according to the following equation:

$$y_i = r_i \prod_{j=1}^k s_{i,j}^{e_{i,j}} \bmod n$$

wherein n is the predetermined public modulus value, r_i is the random value selected by the proving node P_i , $s_i=(s_{i,1}, \dots, s_{i,k})$ is the private key of the proving 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:

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 , 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:

calculating, by the verifying node, a first verification value based on a product of a plurality of first values calculated by the plurality of proving nodes in the network, wherein each proving node in the network calculates a first value for the each proving node based on a predetermined public system parameter and a
5 random value selected by the each proving node, and sends the calculated first value to its parent node;

calculating, by the verifying node, a second verification value based on a product of a plurality of second values calculated by the plurality of proving nodes in the network, wherein each proving node in the network calculates a second
10 value for the each proving node based on a random number generated for the each proving node, the random value selected by the each proving node, a private key of the each proving node, and the predetermined public system parameter, and sends the calculated second value to its parent node; and

determining, by the verifying node, whether authentication of the plurality of
15 proving nodes is successful based on whether the first verification value, the 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 product of a plurality of first values calculated by the
20 plurality of proving nodes in the network, further comprises:

calculating, by the verifying node, the first verification value based on at 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 product of the first value calculated by a proving node directly connected to the verifying node and at least one first value respectively calculated by at least one child node of the proving node directly
5 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 product of a plurality of second values calculated by the plurality of proving nodes in the network, further comprising:

calculating, by the verifying node, the second verification value based on
10 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 a product of the 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
15 proving node directly connected to the verifying node.

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

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.

20 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 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
5 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 its parent node directly
10 connected to the each proving node, wherein a product of the first values calculated by the plurality of the proving nodes in the network is to be used to calculate a first verification value for performing collective authentication of the plurality of proving nodes;

calculating, by the each proving node in the network, a second value based
15 on a random number generated for the each proving node, the random value selected by the each proving node, a private key of the each proving node, and the predetermined public system parameter, and sending the calculated second value to its parent node directly connected to the each proving node, wherein a product of the second values calculated by the plurality of the proving nodes in the
20 network is to be used to calculate a second verification value for performing collective authentication of the plurality of proving nodes .

20. The method according to claim 19, further comprising: if one of the proving nodes in the network is directly connected to at least one child node,

5 sending, by the proving node in the network, a first unit value to its parent node, wherein the first unit value is calculated based on a product of the first values calculated by both the proving node and the at least one child node of the proving node; and

 sending, by the proving node in the network, a second unit value to its parent node, wherein the second unit value is calculated based on a product of the second values calculated by both the proving node and the at least one child
10 node of the proving node.

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

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

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