

CLAIMS

1. A -method for authentication in a virtual reality scenario, the method comprising:

calculating interactive environment authentication information based on random information delivered by a virtual reality server, wherein the random information comprises a random number string of a predetermined length, and the interactive environment authentication information comprises a coordinate sequence generated through mapping calculation based on the random number string;

obtaining password information entered by a user in the virtual reality scenario; and

sending the password information and the interactive environment authentication information to the virtual reality server, wherein the virtual reality server obtains random information through reverse calculation based on the interactive environment authentication information after the password information is verified, and matches the random information obtained through reverse calculation against the random information delivered to a virtual reality client, to perform security authentication on an interactive environment of the virtual reality scenario.

2. The method according to claim 1, wherein the method further comprises:

detecting that the user triggers a target service in the virtual reality scenario;

sending a service request to the virtual reality server;

obtaining encrypted random information delivered by the virtual reality server in response to the virtual reality server receiving the service request; and

decrypting the encrypted random information.

3. The method according to claim 1, wherein the coordinate sequence comprises a set of a series of coordinates generated in response to determining a displacement of an operation focus during interaction between the user and the virtual reality scenario.

4. The method according to claim 1, wherein calculating the interactive environment authentication information based on random information delivered by the virtual reality server comprises:

separately performing mapping calculation on random numbers in the random number string based on a predetermined mapping algorithm, to generate all sets of mapping coordinates respectively corresponding to the random numbers, wherein each set of mapping coordinates is used as an offset corresponding to each password character and is offsetting an

operation focus in the virtual reality scenario by an offset corresponding to a password character after the user enters the password character in the virtual reality scenario; and

splicing all sets of coordinates generated after the operation focus is offset, to obtain the coordinate sequence.

5. The method according to claim 4, wherein offsetting the operation focus in the virtual reality scenario comprises:

determining a set of coordinates of an initial location of the operation focus in a password input interface in the virtual reality scenario; and

using a set of mapping coordinates corresponding to the password character as an offset to offset the set of coordinates of the initial location once.

6. The method according to claim 2, wherein the target service is a virtual reality scenario-based fast payment service.

7. A method for authentication in a virtual reality scenario, the method comprising:

obtaining, by a virtual reality server, interactive environment authentication information and password information entered by a user in a virtual reality scenario that are sent by a virtual reality terminal, wherein the interactive environment authentication information is generated through calculation based on random information delivered to the virtual reality terminal, wherein the random information comprises a random number string of a predetermined length, and the interactive environment authentication information comprises a coordinate sequence generated through mapping calculation based on the random number string;

verifying, by the virtual reality server, the password information; and if the password information is verified, obtaining random information through reverse calculation based on the interactive environment authentication information, and verifying whether the random information obtained through reverse calculation matches the random information delivered by the virtual reality server; and

determining, by the virtual reality server, that security authentication on an interactive environment of the virtual reality scenario succeeds if the random information obtained through reverse calculation matches the random information delivered to the virtual reality terminal.

8. The method according to claim 7, wherein the method further comprises:
receiving a service request sent by a virtual reality terminal in response to the virtual reality terminal detecting that the user triggers a target service in the virtual reality scenario;
generating the random information in response to the received service request; and
encrypting the random information and delivering encrypted random information to the virtual reality terminal.

9. The method according to claim 7, wherein the coordinate sequence comprises a set of a series of coordinates generated in response to determining a displacement of an operation focus during interaction between the user and the virtual reality scenario.

10. The method according to claim 7, wherein the interactive environment authentication information comprises a coordinate sequence obtained by using a set of mapping coordinates corresponding to a password character as an offset after the user enters the password character in the virtual reality scenario to offset an operation focus in the virtual reality scenario and splicing all sets of coordinates generated after the operation focus is offset, and all sets of mapping coordinates are generated by separately performing mapping calculation on random numbers in the random number string based on a predetermined mapping algorithm and respectively correspond to the random numbers; and

obtaining the random information through reverse calculation based on the interactive environment authentication information comprises:

separately calculating offsets corresponding to the sets of coordinates in the coordinate sequence, to obtain sets of mapping coordinates corresponding to password characters in the password information;

separately performing reverse calculation on the sets of mapping coordinates corresponding to the password characters based on the predetermined mapping algorithm, to generate random numbers respectively corresponding to the sets of mapping coordinates; and
splicing the random numbers to obtain the random number string.

11. The method according to claim 10, wherein the separately calculating offsets corresponding to the sets of coordinates in the coordinate sequence comprises:

determining a set of coordinates of an initial location of the operation focus existing before the operation focus is offset in a password input interface in the virtual reality scenario; and

calculating the corresponding offsets based on the set of coordinates of the initial

location and the sets of coordinates in the coordinate sequence.

12. The method according to claim 8, wherein the target service is a virtual reality scenario-based fast payment service.

13. An apparatus for authentication in a virtual reality scenario, the apparatus comprising:

a calculation module, configured to calculate interactive environment authentication information based on random information delivered by a virtual reality server, wherein the random information comprises a random number string of a predetermined length, and the interactive environment authentication information comprises a coordinate sequence generated through mapping calculation based on the random number string;

a first acquisition module, configured to obtain password information entered by a user in a virtual reality scenario; and

a sending module, configured to send the password information and the interactive environment authentication information to the virtual reality server, so that the virtual reality server obtains random information through reverse calculation based on the interactive environment authentication information after the password information is verified, and matches the random information obtained through reverse calculation against the random information delivered to a virtual reality client, to perform security authentication on an interactive environment of the virtual reality scenario.

14. The apparatus according to claim 13, wherein the coordinate sequence comprises a set of a series of coordinates generated in response to determining a displacement of an operation focus during interaction between the user and the virtual reality scenario.

15. The apparatus according to claim 13, wherein the calculation module is configured to:

separately perform mapping calculation on random numbers in the random number string based on a predetermined mapping algorithm, to generate all sets of mapping coordinates respectively corresponding to the random numbers, wherein each set of mapping coordinates is used as an offset corresponding to each password character and is used to offset an operation focus in the virtual reality scenario by an offset corresponding to a password character after the user enters the password character in the virtual reality scenario; and

splice all sets of coordinates generated after the operation focus is offset, to obtain the coordinate sequence.

16. The apparatus according to claim 15, wherein the calculation module is further configured to:

determine a set of coordinates of an initial location of the operation focus in a password input interface in the virtual reality scenario; and

use a set of mapping coordinates corresponding to the password character as an offset to offset the set of coordinates of the initial location once.

17. An apparatus for authentication in a virtual reality scenario, the apparatus comprising:

a second acquisition module, configured to obtain interactive environment authentication information and password information entered by a user in a virtual reality scenario that are sent by a virtual reality terminal, wherein the interactive environment authentication information is generated through calculation based on random information delivered to the virtual reality terminal, wherein the random information comprises a random number string of a predetermined length, and the interactive environment authentication information comprises a coordinate sequence generated through mapping calculation based on the random number string;

a verification module, configured to verify the password information; and if the password information is verified, obtain random information through reverse calculation based on the interactive environment authentication information, and verify whether the random information obtained through reverse calculation matches the random information delivered by the virtual reality server; and

a determining module, configured to determine that security authentication on an interactive environment of the virtual reality scenario succeeds if the random information obtained through reverse calculation matches the random information delivered to the virtual reality terminal.

18. The apparatus according to claim 17, wherein the coordinate sequence comprises a set of a series of coordinates generated in response to determining a displacement of an operation focus during interaction between the user and the virtual reality scenario.

19. The apparatus according to claim 18, wherein the interactive environment authentication information comprises a coordinate sequence obtained by using a set of mapping coordinates corresponding to a password character as an offset after the user enters the password character in the virtual reality scenario to offset an operation focus in the virtual reality scenario and splicing all sets of coordinates generated after the operation focus is offset, and all sets of mapping coordinates are generated by separately performing mapping calculation on random numbers in the random number string based on a predetermined mapping algorithm and respectively correspond to the random numbers; and

the verification module is configured to:

separately calculate offsets corresponding to the sets of coordinates in the coordinate sequence, to obtain sets of mapping coordinates corresponding to password characters in the password information;

separately perform reverse calculation on the sets of mapping coordinates corresponding to the password characters based on the predetermined mapping algorithm, to generate random numbers respectively corresponding to the sets of mapping coordinates; and

splice the generated random numbers to obtain the random number string.

20. The apparatus according to claim 19, wherein the verification module is further configured to:

determine a set of coordinates of an initial location of the operation focus existing before the operation focus is offset in a password input interface in the virtual reality scenario; and

calculate the corresponding offsets based on the set of coordinates of the initial location and the sets of coordinates in the coordinate sequence.

21. A virtual reality terminal device for authentication in a virtual reality scenario, the virtual reality terminal device comprising:

a processor; and

a storage, configured to store a machine-executable instruction, wherein

a machine-executable instruction that is stored in the storage and that corresponds to control logic of virtual reality scenario-based authentication is read and executed, to prompt the processor to:

calculate interactive environment authentication information based on random information delivered by a virtual reality server, wherein the random information comprises a

random number string of a predetermined length, and the interactive environment authentication information comprises a coordinate sequence generated through mapping calculation based on the random number string;

obtain password information entered by a user in a virtual reality scenario; and

send the password information and the interactive environment authentication information to the virtual reality server, so that the virtual reality server obtains random information through reverse calculation based on the interactive environment authentication information after the password information is verified, and matches the random information obtained through reverse calculation against the random information delivered to a virtual reality client, to perform security authentication on an interactive environment of the virtual reality scenario.

22. A virtual reality server device for authentication in a virtual reality scenario, the virtual reality server device comprising:

a processor; and

a storage, configured to store a machine-executable instruction, wherein

a machine-executable instruction that is stored in the storage and that corresponds to control logic of virtual reality scenario-based authentication is read and executed, to prompt the processor to:

obtain interactive environment authentication information and password information entered by a user in a virtual reality scenario that are sent by a virtual reality terminal, wherein the interactive environment authentication information is generated through calculation based on random information delivered to the virtual reality terminal, wherein the random information comprises a random number string of a predetermined length, and the interactive environment authentication information comprises a coordinate sequence generated through mapping calculation based on the random number string;

verify the password information; and if the password information is verified, obtain random information through reverse calculation based on the interactive environment authentication information, and verify whether the random information obtained through reverse calculation matches the random information delivered by the virtual reality server; and

determine that security authentication on an interactive environment of the virtual reality scenario succeeds if the random information obtained through reverse calculation matches the random information delivered to the virtual reality terminal.