

THE INVENTION CLAIMED IS:

1. A method for authenticating a device, comprising:

coupling a first device to an interaction database, the interaction database coupled to a second device, the interaction database storing interaction data, the first device storing a first group public key, a first group private key, a first device public key, and a first device private key, the second device storing the first group public key, the first group private key, a second device public key, and a second device private key;

transmitting a first message to a remote computer system from the first device, the first message comprising challenge data associated with a challenge question corresponding to the interaction data, response data associated with a required response to the challenge question corresponding to the interaction data, and authentication data associated with the first device, the challenge data and the response data each encrypted with the first group public key, the first message encrypted with a remote computer system public key of the remote computer system;

receiving a second message at the second device from the remote computer system, the second message comprising the challenge data encrypted with the first group public key from the first message, the second message encrypted with the second device public key;

transmitting a third message to the remote computer system from the second device, the third message comprising response data associated with the required response to the challenge question corresponding to the interaction data, the response data encrypted with the first group public key, the third message encrypted with the remote computer system public key; and

in response to receiving an authentication message from the remote computer system indicating that the first device has been authenticated by the remote computer system, permitting interaction between the first device and the remote computer system.

2. The method of claim 1, wherein the interaction data comprises data associated with at least one interaction, each interaction comprising at least one of a payment transaction or a communication.

3. The method of claim 2, wherein the at least one interaction comprises at least one of an interaction between the second device and the remote computer system, an interaction between the second device and a second remote computer system, an interaction between a third device coupled to the interaction database and the remote computer system, an interaction between the third device and the second remote computer system, or a fictional interaction between a fictional device and a fictional remote computer system.

4. The method of claim 1, further comprising:
determining, by the first device, the challenge data and the response data based on the interaction data in the interaction database before transmitting the first message; and
in response to receiving the second message, determining, by the second device, the response data based on the challenge data from the second message and the interaction data in the interaction database before transmitting the third message.

5. The method of claim 1, wherein the interaction database, the first device, and the second device are each coupled to a first network.

6. The method of claim 5, wherein the first device, the second device, and the remote computer system are each coupled to a second network separate from the first network, and further wherein the first message is transmitted to the remote computer system from the first device over the second network, the second message is received at the second device from the remote computer system over the second network, and the third message is transmitted to the remote computer system from the second device over the second network.

7. The method of claim 1, wherein the remote computer system authenticates the first device based on a comparison of the response data from the first message and the response data from the third message.

8. The method of claim 1, further comprising storing the challenge data in the interaction database in response to receiving the second message with the challenge data.

9. The method of claim 1, further comprising, in response to receiving an authentication message from the remote computer system indicating that the first device has not been authenticated by the remote computer system, preventing interaction between the first device and the remote computer system.

10. A method for authenticating a device, comprising:

coupling a first device to an interaction database, the interaction database coupled to a second device, the interaction database storing interaction data, the first device storing a first group public key, a first group private key, a first device public key, and a first device private key, the second device storing the first group public key, the first group private key, a second device public key, and a second device private key;

transmitting a first message to a first remote computer system from the first device, the first message comprising challenge data associated with a challenge question corresponding to the interaction data, first remote computer system public key data associated with a first remote computer system public key, response data associated with a required response to the challenge question corresponding to the interaction data, and authentication data associated with the first device, the challenge data, the first remote computer system public key data, and the response data each encrypted with the first group public key, the first message encrypted with the first remote computer system public key of the first remote computer system;

receiving a second message at the second device from a second remote computer system, the second message comprising the challenge data and the first remote computer system public key data encrypted with the first group public key from the first message, the second message encrypted with the second device public key;

transmitting a third message to the second remote computer system from the second device, the third message comprising response data associated with the required response to the challenge question corresponding to the interaction data, the response data encrypted with the first group public key, the third message

encrypted with the first remote computer system public key from the second message;
and

in response to receiving an authentication message from the second remote computer system indicating that the first device has not been authenticated by the second remote computer system, preventing interaction between the first device and at least one of the first remote computer system and the second remote computer system.

11. A system for authenticating a device, comprising:

an interaction database configured to store interaction data;

a first device coupled to the interaction database, the first device configured to store a first group public key, a first group private key, a first device public key, and a first device private key; and

a second device coupled to the interaction database, the second device configured to store the first group public key, the first group private key, a second device public key, and a second device private key;

wherein the first device is configured to transmit a first message to a remote computer system, the first message comprising challenge data associated with a challenge question corresponding to the interaction data, response data associated with a required response to the challenge question corresponding to the interaction data, and authentication data associated with the first device, the challenge data and the response data each encrypted with the first group public key, the first message encrypted with a remote computer system public key of the remote computer system;

wherein the second device is configured to receive a second message from the remote computer system, the second message comprising the challenge data encrypted with the first group public key from the first message, the second message encrypted with the second device public key;

wherein the second device is configured to transmit a third message to the remote computer system, the third message comprising response data associated with the required response to the challenge question corresponding to the interaction data, the response data encrypted with the first group public key, the third message encrypted with the remote computer system public key; and

wherein, in response to receiving an authentication message from the remote computer system indicating that the first device has been authenticated by the

remote computer system, the first device is configured to permit interaction between the first device and the remote computer system.

12. The system of claim 11, wherein the interaction data comprises data associated with at least one interaction, each interaction comprising at least one of a payment transaction or a communication.

13. The system of claim 12, wherein the at least one interaction comprises at least one of an interaction between the second device and the remote computer system, an interaction between the second device and a second remote computer system, an interaction between a third device coupled to the interaction database and the remote computer system, an interaction between the third device and the second remote computer system, or a fictional interaction between a fictional device and a fictional remote computer system.

14. The system of claim 11, wherein:

the first device is configured to determine the challenge data and the response data based on the interaction data in the interaction database before transmitting the first message; and

in response to receiving the second message, the second device is configured to determine the response data based on the challenge data from the second message and the interaction data in the interaction database before transmitting the third message.

15. The system of claim 11, wherein the interaction database, the first device, and the second device are each coupled to a first network.

16. The system of claim 15, wherein the first device, the second device, and the remote computer system are each coupled to a second network separate from the first network, and further wherein the first message is transmitted to the remote computer system from the first device over the second network, the second message is received at the second device from the remote computer system over the second network, and the third message is transmitted to the remote computer system from the second device over the second network.

17. The system of claim 11, wherein the remote computer system authenticates the first device based on a comparison of the response data from the first message and the response data from the third message.

18. The system of claim 11, wherein the interaction database is configured to store the challenge data in response to the second device receiving the second message with the challenge data.

19. The system of claim 11, wherein, in response to receiving an authentication message from the remote computer system indicating that the first device has not been authenticated by the remote computer system, the first device is configured to prevent interaction between the first device and the remote computer system.

20. A system for authenticating a device, comprising:

an interaction database configured to store interaction data;

a first device coupled to the interaction database, the first device configured to store a first group public key, a first group private key, a first device public key, and a first device private key; and

a second device coupled to the interaction database, the second device configured to store the first group public key, the first group private key, a second device public key, and a second device private key;

wherein the first device is configured to transmit a first message to a remote computer system, the first message comprising challenge data associated with a challenge question corresponding to the interaction data, first remote computer system public key data associated with a first remote computer system public key, response data associated with a required response to the challenge question corresponding to the interaction data, and authentication data associated with the first device, the challenge data, the first remote computer system public key data, and the response data each encrypted with the first group public key, the first message encrypted with the first remote computer system public key of the remote computer system;

wherein the second device is configured to receive a second message from a second remote computer system, the second message comprising the

challenge data and the first remote computer system public key data encrypted with the first group public key from the first message, the second message encrypted with the second device public key;

wherein the second device is configured to transmit a third message to the second remote computer system, the third message comprising response data associated with the required response to the challenge question corresponding to the interaction data, the response data encrypted with the first group public key, the third message encrypted with the first remote computer system public key from the second message; and

wherein, in response to receiving an authentication message from the second remote computer system indicating that the first device has not been authenticated by the remote computer system, the first device is configured to prevent interaction between the first device and at least one of the first remote computer system and the second remote computer system.

21. A computer program product for authenticating a device, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

couple a first device to an interaction database, the interaction database coupled to a second device, the interaction database storing interaction data, the first device storing a first group public key, a first group private key, a first device public key, and a first device private key, the second device storing the first group public key, the first group private key, a second device public key, and a second device private key;

transmit a first message to a remote computer system from the first device, the first message comprising challenge data associated with a challenge question corresponding to the interaction data, response data associated with a required response to the challenge question corresponding to the interaction data, and authentication data associated with the first device, the challenge data and the response data each encrypted with the first group public key, the first message encrypted with a remote computer system public key of the remote computer system, wherein:

in response to the first message, a second message is received at the second device from the remote computer system, the second message comprising the challenge data encrypted with the first group public key from the first message, the second message encrypted with the second device public key, and

in response to the second message, a third message is transmitted to the remote computer system from the second device, the third message comprising response data associated with the required response to the challenge question corresponding to the interaction data, the response data encrypted with the first group public key, the third message encrypted with the remote computer system public key; and

in response to receiving an authentication message from the remote computer system indicating that the first device has been authenticated by the remote computer system, permit interaction between the first device and the remote computer system.

22. The computer program product of claim 21, wherein the interaction data comprises data associated with at least one interaction, each interaction comprising at least one of a payment transaction or a communication.

23. The computer program product of claim 22, wherein the at least one interaction comprises at least one of an interaction between the second device and the remote computer system, an interaction between the second device and a second remote computer system, an interaction between a third device coupled to the interaction database and the remote computer system, an interaction between the third device and the second remote computer system, or a fictional interaction between a fictional device and a fictional remote computer system.

24. The computer program product of claim 21, wherein the one or more instructions, when executed by the at least one processor, further cause the at least one processor to:

determine the challenge data and the response data based on the interaction data in the interaction database before transmitting the first message,

wherein, in response to receiving the second message, the second device is configured to determine the response data based on the challenge data from

the second message and the interaction data in the interaction database before transmitting the third message.

25. The computer program product of claim 21, wherein the interaction database, the first device, and the second device are each coupled to a first network.

26. The computer program product of claim 25, wherein the first device, the second device, and the remote computer system are each coupled to a second network separate from the first network, and further wherein the first message is transmitted to the remote computer system from the first device over the second network, the second message is received at the second device from the remote computer system over the second network, and the third message is transmitted to the remote computer system from the second device over the second network.

27. The computer program product of claim 21, wherein, in response to receiving the third message, the remote computer system authenticates the first device based on a comparison of the response data from the first message and the response data from the third message.

28. The computer program product of claim 21, wherein the interaction database is configured to store the challenge data in response to the second device receiving the second message with the challenge data.

29. The computer program product of claim 21, wherein the one or more instructions, when executed by the at least one processor, further cause the at least one processor to, in response to receiving an authentication message from the remote computer system indicating that the first device has not been authenticated by the remote computer system, prevent interaction between the first device and the remote computer system.

30. A computer program product for authenticating a device, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

couple a first device to an interaction database, the interaction database coupled to a second device, the interaction database storing interaction data, the first device storing a first group public key, a first group private key, a first device public key, and a first device private key, the second device storing the first group public key, the first group private key, a second device public key, and a second device private key;

transmit a first message to a first remote computer system from the first device, the first message comprising challenge data associated with a challenge question corresponding to the interaction data, first remote computer system public key data associated with a first remote computer system public key, response data associated with a required response to the challenge question corresponding to the interaction data, and authentication data associated with the first device, the challenge data, the first remote computer system public key data, and the response data each encrypted with the first group public key, the first message encrypted with the first remote computer system public key of the first remote computer system, wherein

in response to the first message, a second message is received at the second device from a second remote computer system, the second message comprising the challenge data and the first remote computer system public key data encrypted with the first group public key from the first message, the second message encrypted with the second device public key, and

in response to the second message, a third message is transmitted to the second remote computer system from the second device, the third message comprising response data associated with the required response to the challenge question corresponding to the interaction data, the response data encrypted with the first group public key, the third message encrypted with the first remote computer system public key from the second message; and

in response to receiving an authentication message from the second remote computer system indicating that the first device has not been authenticated by the second remote computer system, prevent interaction between the first device and at least one of the first remote computer system and the second remote computer system.