(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109309565 B
(45)授权公告日 2021.08.10

(21)申请号 201710632863.4
(22)申请日 2017.07.28
(65)同一申请的已公布的文献号
申请公布号 CN 109309565 A
(43)申请公布日 2019.02.05
(73)专利权人 中国移动通信有限公司研究院
地址 100032 北京市西城区金融大街29号19层
专利权人 中国移动通信集团公司
(72)发明人 刘福文 左敏
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 张恺宁
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 105827412 A,2016.08.03
CN 106161032 A,2016.11.23
审查员 郑红萍

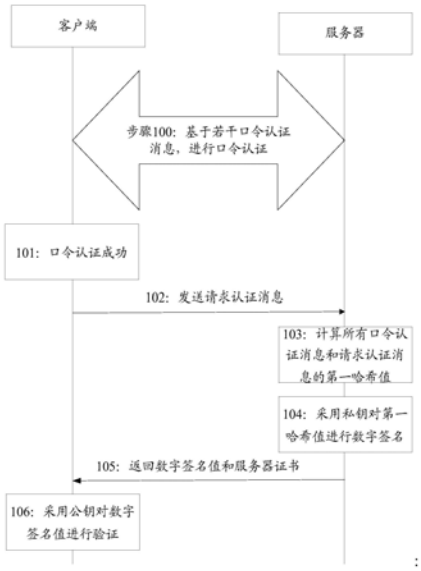
权利要求书4页 说明书11页 附图4页

(54)发明名称

一种安全认证的方法及装置

(57)摘要

本申请实施例中公开了一种安全认证的方法及装置，该方法为基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；确定所述口令认证结果表征口令认证成功时，向所述服务器发送请求认证消息；通过服务器对所有的交互消息进行数字签名，客户端进行数字签名验证的方式，或者，通过客户端对本地的随机数、所有交互消息进行公钥加密，并对服务器返回的随机数进行验证的方式，进行安全认证，这样，就可以通过将口令认证与数字签名相结合，或者，将口令认证与公钥加密相结合的方式，保证了通信双方的身份的正确性，避免了通信过程中的消息泄露以及恶意信息篡改等网络攻击，提高了网络认证的可靠度，保障了用户的通信安全。



CN 109309565 B

1.一种安全认证的方法,其特征在于,包括:

基于传输的多个交互的口令认证消息,与服务器进行口令认证,获得口令认证结果;

确定所述口令认证结果表征口令认证成功时,向所述服务器发送请求认证消息,触发所述服务器执行以下步骤:对所述口令认证消息和所述请求认证消息进行散列运算,获得第一哈希值,并基于本地的私钥,对所述第一哈希值进行数字签名,获得所述请求认证消息的数字签名值;

接收所述服务器基于接收的请求认证消息返回的包含服务器证书和数字签名值的响应认证消息,其中,所述服务器证书包含所述服务器的公钥,所述数字签名值是基于所述请求认证消息和所述口令认证消息获得的;

基于所述服务器的公钥,对所述响应认证消息中包含的数字签名值进行验证,获得安全认证结果。

2.如权利要求1所述的方法,其特征在于,基于所述服务器的公钥,对所述响应认证消息中包含的数字签名值进行验证,获得安全认证结果,具体包括:

对所述口令认证消息和所述请求认证消息进行散列运算,获得第二哈希值;

基于所述公钥和所述第二哈希值,采用预设的数字签名验证算法,获得验证数字签名值;

基于所述数字签名值与所述验证数字签名值的比较结果,获得安全认证结果。

3.一种安全认证的方法,其特征在于,包括:

接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息,其中,所述口令认证结果是基于传输的多个交互的口令认证消息进行口令认证获得的;

对所述口令认证消息和所述请求认证消息进行散列运算,获得第一哈希值;

基于本地的私钥,对所述第一哈希值进行数字签名,获得所述请求认证消息的数字签名值;

将包含本地的服务器证书和所述数字签名值的响应认证消息,发送至所述客户端,触发所述客户端基于所述服务器证书中包含的服务器的公钥对所述数字签名值进行验证并获得安全认证结果。

4.如权利要求3所述的方法,其特征在于,将包含本地的服务器证书和所述数字签名值的响应认证消息,发送至所述客户端,触发所述客户端基于所述服务器证书中包含的服务器的公钥对所述数字签名值进行验证并获得安全认证结果,具体包括:

将包含本地的服务器证书和所述数字签名值的响应认证消息,发送至所述客户端,触发所述客户端执行以下步骤:对所述口令认证消息和所述请求认证消息进行散列运算,获得第二哈希值,并基于所述公钥和所述第二哈希值,采用预设的数字签名验证算法,获得验证数字签名值,以及基于所述数字签名值与所述验证数字签名值的比较结果,获得安全认证结果。

5.一种安全认证的方法,其特征在于,包括:

基于传输的口令认证消息,与服务器进行口令认证,获得口令认证结果;

确定所述口令认证结果表征口令认证成功时,向所述服务器发送请求认证消息,并接收所述服务器基于所述请求认证消息返回的包含服务器证书的响应认证消息,其中,所述服务器证书中包含所述服务器的公钥;

生成一个随机数，对所述口令认证消息和所述请求认证消息进行散列运算，获得哈希值，然后将所述随机数与所述哈希值使用所述服务器的公钥进行加密，获得加密值，并将所述加密值发送至所述服务器；

接收所述服务器基于所述加密值返回的验证随机数，并基于所述随机数和所述验证随机数的比较结果，获得安全认证结果，其中，所述验证随机数是通过私钥对所述加密值进行解密获得的。

6.如权利要求5所述的方法，其特征在于，生成一个随机数，对所述口令认证消息和所述请求认证消息进行散列运算，获得哈希值，然后将所述随机数与所述哈希值使用所述服务器的公钥进行加密，获得加密值，具体包括：

确定接收到所述响应认证消息中包含的公钥时，获取本地生成的一个随机数；

对所述口令认证消息和所述请求认证消息进行散列运算，获得哈希值；

基于所述公钥，对所述随机数和所述哈希值进行加密，获得加密值。

7.一种安全认证的方法，其特征在于，包括：

接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，所述口令认证结果是基于传输的口令认证消息进行口令认证获得的；

基于所述请求认证消息，向所述客户端发送包含本地的服务器证书的响应认证消息；

接收所述客户端基于所述响应认证消息发送的加密值，其中，所述加密值是所述客户端生成一个随机数，并对所述口令认证消息和所述请求认证消息进行散列运算，获得哈希值后，基于所述服务器证书中包含的服务器的公钥对所随机数与所述哈希值进行加密获得的；

基于本地的私钥对所述加密值进行解密，获得验证随机数，并将所述验证随机数发送至所述客户端，触发所述客户端基于所述随机数和所述验证随机数的比较结果获得安全认证结果。

8.如权利要求7所述的方法，其特征在于，基于所述请求认证消息，向所述客户端发送包含本地的服务器证书的响应认证消息，具体包括：

基于所述请求认证消息，向所述客户端发送包含本地的服务器证书的响应认证消息，触发所述客户端执行以下步骤：对所述口令认证消息和所述请求认证消息进行散列运算获得哈希值，并基于所述公钥对本地生成的随机数和所述哈希值进行加密，获得加密值。

9.一种安全认证的装置，其特征在于，包括：

获得单元，用于基于传输的多个交互的口令认证消息，与服务器进行口令认证，获得口令认证结果；

发送单元，用于确定所述口令认证结果表征口令认证成功时，向所述服务器发送请求认证消息，触发所述服务器执行以下步骤：对所述口令认证消息和所述请求认证消息进行散列运算，获得第一哈希值，并基于本地的私钥，对所述第一哈希值进行数字签名，获得所述请求认证消息的数字签名值；

接收单元，用于接收所述服务器基于接收的请求认证消息返回的包含服务器证书和数字签名值的响应认证消息，其中，所述服务器证书包含所述服务器的公钥，所述数字签名值是基于所述请求认证消息和所述口令认证消息获得的；

认证单元，用于基于所述服务器的公钥，对所述响应认证消息中包含的数字签名值进

行验证，获得安全认证结果。

10.一种安全认证的装置，其特征在于，包括：

接收单元，用于接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，所述口令认证结果是基于传输的多个交互的口令认证消息进行口令认证获得的；

签名单元，用于对所述口令认证消息和所述请求认证消息进行散列运算，获得第一哈希值，基于本地的私钥，对所述第一哈希值进行数字签名，获得所述请求认证消息的数字签名值；

发送单元，用于将包含本地的服务器证书和所述数字签名值的响应认证消息，发送至所述客户端，触发所述客户端基于所述服务器证书中包含的服务器的公钥对所述数字签名值进行验证并获得安全认证结果。

11.一种安全认证的装置，其特征在于，包括：

获得单元，用于基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；

请求单元，用于确定所述口令认证结果表征口令认证成功时，向所述服务器发送请求认证消息，并接收所述服务器基于所述请求认证消息返回的包含服务器证书的响应认证消息，其中，所述服务器证书中包含所述服务器的公钥；

加密单元，用于生成一个随机数，对所述口令认证消息和所述请求认证消息进行散列运算，获得哈希值，然后将所述随机数与所述哈希值使用所述服务器的公钥进行加密，获得加密值，并将所述加密值发送至所述服务器；

认证单元，用于接收所述服务器基于所述加密值返回的验证随机数，并基于所述随机数和所述验证随机数的比较结果，获得安全认证结果，其中，所述验证随机数是通过私钥对所述加密值进行解密获得的。

12.一种安全认证的装置，其特征在于，包括：

第一接收单元，用于接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，所述口令认证结果是基于传输的口令认证消息进行口令认证获得的；

发送单元，用于基于所述请求认证消息，向所述客户端发送包含本地的服务器证书的响应认证消息；

第二接收单元，用于接收所述客户端基于所述响应认证消息发送的加密值，其中，所述加密值是所述客户端生成一个随机数，并对所述口令认证消息和所述请求认证消息进行散列运算，获得哈希值后，基于所述服务器证书中包含的服务器的公钥对所随机数与所述哈希值进行加密获得的；

认证单元，用于基于本地的私钥对所述加密值进行解密，获得验证随机数，并将所述验证随机数发送至所述客户端，触发所述客户端基于所述随机数和所述验证随机数的比较结果获得安全认证结果。

13.一种电子设备，其特征在于，包括：一个或多个处理器；以及

一个或多个计算机可读介质，所述可读介质上存储有用于安全认证的程序，其中，所述程序被所述一个或多个处理器执行时，实现如权利要求1或2所述的方法的步骤。

14.一个或多个计算机可读介质，其特征在于，所述可读介质上存储有用于安全认证的程序，其中，所述程序被一个或多个处理器执行时，使得通信设备执行如权利要求1或2所述

的方法。

15.一种电子设备,其特征在于,包括:一个或多个处理器;以及

一个或多个计算机可读介质,所述可读介质上存储有用于安全认证的程序,其中,所述程序被所述一个或多个处理器执行时,实现如权利要求3或4所述的方法的步骤。

16.一个或多个计算机可读介质,其特征在于,所述可读介质上存储有用于安全认证的程序,其中,所述程序被一个或多个处理器执行时,使得通信设备执行如权利要求3或4所述的方法。

17.一种电子设备,其特征在于,包括:一个或多个处理器;以及

一个或多个计算机可读介质,所述可读介质上存储有用于安全认证的程序,其中,所述程序被所述一个或多个处理器执行时,实现如权利要求5-6任一项所述的方法的步骤。

18.一个或多个计算机可读介质,其特征在于,所述可读介质上存储有用于安全认证的程序,其中,所述程序被一个或多个处理器执行时,使得通信设备执行如权利要求5-6任一项所述的方法。

19.一种电子设备,其特征在于,包括:一个或多个处理器;以及

一个或多个计算机可读介质,所述可读介质上存储有用于安全认证的程序,其中,所述程序被所述一个或多个处理器执行时,实现如权利要求7-8任一项所述的方法的步骤。

20.一个或多个计算机可读介质,其特征在于,所述可读介质上存储有用于安全认证的程序,其中,所述程序被一个或多个处理器执行时,使得通信设备执行如权利要求7-8任一项所述的方法。

一种安全认证的方法及装置

技术领域

[0001] 本申请涉及网络安全技术领域，尤其涉及一种安全认证的方法及装置。

背景技术

[0002] 随着互联网技术的发展，网络攻击也日益严重，用户在使用互联网进行通信、交易等操作时，存在信息泄露，交易信息被恶意篡改等问题。用户的网络安全受到了极大的威胁，这给用户带来了极大的不便。

[0003] 现有技术下，通常通过安全认证的方式，保证通信的安全。其中，安全认证主要采用以下两种方式：

[0004] 第一种方式为：客户端与服务器将共享的口令，作为安全认证凭证，以通过共享的口令进行安全认证。

[0005] 具体的，客户端接收服务器发送的携带口令的响应消息，确定本地的口令与接收的响应消息中包含的口令相同时，确定服务器认证成功；服务器接收客户端发送的携带口令的响应消息，确定本地的口令与接收的响应消息中包含的口令相同时，确客户端认证成功。

[0006] 但是，采用这种方式，口令存在泄漏的问题，例如，非法分子可以通过恶意软件和攻破系统等方式非法获取用户的口令。当非法分子获取用户的口令后，就可以通过安全认证，与用户进行通信。显然，非法分子与用户通信，会给用户带来隐私泄露或者金融损失等问题，无法保证用户的通信安全。

[0007] 第二种方式为：将安全传输层协议(Transport Layer Security，TLS)与口令认证相结合，进行安全认证。

[0008] 具体的，首先，客户端使用服务器证书对服务器进行认证后，与服务器建立安全的TLS链路，然后，服务器在上述TLS链路上使用口令对客户端进行认证。

[0009] 但是，采用这种方式，需要对已经部署的口令认证系统进行完全替换和修改，这浪费了已有的认证系统资源，提高了认证系统的使用成本，不具备实用性。

发明内容

[0010] 本申请实施例提供一种安全认证的方法及装置，用于保证通信双方的身份的正确性，避免通信过程中的消息泄露以及恶意信息篡改等网络攻击，提高网络认证的可靠度，保障用户的通信安全。

[0011] 本申请实施例提供的具体技术方案如下：

[0012] 第一方面，一种安全认证的方法，包括：

[0013] 基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；

[0014] 确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息；

[0015] 接收服务器基于接收的请求认证消息返回的包含服务器证书和数字签名值的响应认证消息，其中，服务器证书包含服务器的公钥，数字签名值是基于请求认证消息和口令

认证消息获得的；

[0016] 基于服务器的公钥，对响应认证消息中包含的数字签名值进行验证，获得安全认证结果。

[0017] 较佳的，确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息，具体包括：

[0018] 确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息，触发服务器执行以下步骤：对口令认证消息和请求认证消息进行散列运算，获得第一哈希值，并基于本地的私钥，对第一哈希值进行数字签名，获得请求认证消息的数字签名值。

[0019] 较佳的，基于服务器的公钥，对响应认证消息中包含的数字签名值进行验证，获得安全认证结果，具体包括：

[0020] 对口令认证消息和请求认证消息进行散列运算，获得第二哈希值；

[0021] 基于公钥和第二哈希值，采用预设的数字签名验证算法，获得验证数字签名值；

[0022] 基于数字签名值与验证数字签名值的比较结果，获得安全认证结果。

[0023] 第二方面，一种安全认证的方法，包括：

[0024] 接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，口令认证结果是基于传输的口令认证消息进行口令认证获得的；

[0025] 基于本地的私钥，对接收的请求认证消息和口令认证消息进行数字签名，获得数字签名值；

[0026] 将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客户端基于服务器证书中包含的服务器的公钥对数字签名值进行验证并获得安全认证结果。

[0027] 较佳的，基于本地的私钥，对接收的请求认证消息和口令认证消息进行数字签名，获得数字签名值，具体包括：

[0028] 对口令认证消息和请求认证消息进行散列运算，获得第一哈希值；

[0029] 基于私钥，对第一哈希值进行数字签名，获得请求认证消息的数字签名值。

[0030] 较佳的，将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客户端基于服务器证书中包含的服务器的公钥对数字签名值进行验证并获得安全认证结果，具体包括：

[0031] 将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客户端执行以下步骤：对口令认证消息和请求认证消息进行散列运算，获得第二哈希值，并基于公钥和第二哈希值，采用预设的数字签名验证算法，获得验证数字签名值，以及基于数字签名值与验证数字签名值的比较结果，获得安全认证结果。

[0032] 第三方面，一种安全认证的方法，包括：

[0033] 基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；

[0034] 确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息，并接收服务器基于请求认证消息返回的包含服务器证书的响应认证消息，其中，服务器证书中包含服务器的公钥；

[0035] 基于接收的服务器的公钥，对本地获取的随机数、口令认证消息和请求认证消息进行加密，获得加密值，并将加密值发送至服务器；

[0036] 接收服务器基于加密值返回的验证随机数，并基于随机数和验证随机数的比较结

果，获得安全认证结果，其中，验证随机数是通过私钥对加密值进行解密获得的。

[0037] 较佳的，基于接收的服务器的公钥，对本地获取的随机数、口令认证消息和请求认证消息进行加密，获得加密值，具体包括：

[0038] 确定接收到响应认证消息中包含的公钥时，获取本地生成的一个随机数；

[0039] 对口令认证消息和请求认证消息进行散列运算，获得哈希值；

[0040] 基于公钥，对随机数和哈希值进行加密，获得加密值。

[0041] 第四方面，一种安全认证的方法，包括：

[0042] 接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，口令认证结果是基于传输的口令认证消息进行口令认证获得的；

[0043] 基于请求认证消息，向客户端发送包含本地的服务器证书的响应认证消息；

[0044] 接收客户端基于响应认证消息发送的加密值，其中，加密值是基于服务器证书中包含的服务器的公钥对本地获取的随机数、口令认证消息和请求认证消息进行加密获得的；

[0045] 基于本地的私钥对加密值进行解密，获得验证随机数，并将验证随机数发送至客户端，触发客户端基于随机数和验证随机数的比较结果获得安全认证结果。

[0046] 较佳的，基于请求认证消息，向客户端发送包含本地的服务器证书的响应认证消息，具体包括：

[0047] 基于请求认证消息，向客户端发送包含本地的服务器证书的响应认证消息，触发客户端执行以下步骤：对口令认证消息和请求认证消息进行散列运算获得哈希值，并基于公钥对本地生成的随机数和哈希值进行加密，获得加密值。

[0048] 第五方面，一种安全认证的装置，包括：

[0049] 获得单元，用于基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；

[0050] 发送单元，用于确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息；

[0051] 接收单元，用于接收服务器基于接收的请求认证消息返回的包含服务器证书和数字签名值的响应认证消息，其中，服务器证书包含服务器的公钥，数字签名值是基于请求认证消息和口令认证消息获得的；

[0052] 认证单元，用于基于服务器的公钥，对响应认证消息中包含的数字签名值进行验证，获得安全认证结果。

[0053] 第六方面，一种安全认证的装置，包括：

[0054] 接收单元，用于接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，口令认证结果是基于传输的口令认证消息进行口令认证获得的；

[0055] 签名单元，用于基于本地的私钥，对接收的请求认证消息和口令认证消息进行数字签名，获得数字签名值；

[0056] 发送单元，用于将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客户端基于服务器证书中包含的服务器的公钥对数字签名值进行验证并获得安全认证结果。

[0057] 第七方面，一种安全认证的装置，包括：

[0058] 获得单元，用于基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；

[0059] 请求单元，用于确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息，并接收服务器基于请求认证消息返回的包含服务器证书的响应认证消息，其中，服务器证书中包含服务器的公钥；

[0060] 加密单元，用于基于接收的服务器的公钥，对本地获取的随机数、口令认证消息和请求认证消息进行加密，获得加密值，并将加密值发送至服务器；

[0061] 认证单元，用于接收服务器基于加密值返回的验证随机数，并基于随机数和验证随机数的比较结果，获得安全认证结果，其中，验证随机数是通过私钥对加密值进行解密获得的。

[0062] 第八方面，一种安全认证的装置，包括：

[0063] 第一接收单元，用于接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，口令认证结果是基于传输的口令认证消息进行口令认证获得的；

[0064] 发送单元，用于基于请求认证消息，向客户端发送包含本地的服务器证书的响应认证消息；

[0065] 第二接收单元，用于接收客户端基于响应认证消息发送的加密值，其中，加密值是基于服务器证书中包含的服务器的公钥对本地获取的随机数、口令认证消息和请求认证消息进行加密获得的；

[0066] 认证单元，用于基于本地的私钥对加密值进行解密，获得验证随机数，并将验证随机数发送至客户端，触发客户端基于随机数和验证随机数的比较结果获得安全认证结果。

[0067] 第九方面，一种电子设备，包括：一个或多个处理器；以及

[0068] 一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，实现上述第一方面中任一项的方法的步骤。

[0069] 第十方面，一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，使得通信设备执行上述第一方面中任一项的方法。

[0070] 第十一方面，一种电子设备，包括：一个或多个处理器；以及

[0071] 一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，实现上述第二方面中任一项的方法的步骤。

[0072] 第十二方面，一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，使得通信设备执行上述第二方面中任一项的方法。

[0073] 第十三方面，一种电子设备，包括：一个或多个处理器；以及

[0074] 一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，实现上述第三方面中任一项的方法的步骤。

[0075] 第十四方面，一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，使得通信设备执行上述第三方面中任一项的方法。

[0076] 第十五方面，一种电子设备，包括：一个或多个处理器；以及

[0077] 一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序

被一个或多个处理器执行时，实现上述第四方面中任一项的方法的步骤。

[0078] 第十六方面，一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，使得通信设备执行上述第四方面中任一项的方法。

[0079] 本申请实施例中，先与服务器进行口令认证，然后，通过服务器对所有的交互消息进行数字签名，客户端进行数字签名验证的方式，或者，通过客户端对本地的随机数、所有交互消息进行公钥加密，并对服务器返回的随机数进行验证的方式，进行安全认证，这样，就可以通过将口令认证与数字签名相结合，或者，将口令认证与公钥加密相结合的方式，保证了通信双方的身份的正确性，避免了通信过程中的消息泄露以及恶意信息篡改等网络攻击，提高了网络认证的可靠度，保障了用户的通信安全。

附图说明

[0080] 图1为本申请实施例一中安全认证的方法的流程图；

[0081] 图2为本申请实施例二中安全认证的方法的流程图；

[0082] 图3为本申请实施例中安全认证的装置的结构示意图一；

[0083] 图4为本申请实施例中安全认证的装置的结构示意图二；

[0084] 图5为本申请实施例中安全认证的装置的结构示意图三；

[0085] 图6为本申请实施例中安全认证的装置的结构示意图四。

具体实施方式

[0086] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，并不是全部的实施例。基于本申请实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0087] 为了保证通信双方的身份的正确性，避免通信过程中的消息泄露以及恶意信息篡改等网络攻击，提高网络认证的可靠度，保障用户的通信安全，本申请实施例中，设计了一种安全认证的方法，该方法为通过口令与数字签名相结合的方式进行安全认证，或通过口令与公钥加密的方式进行安全认证。

[0088] 以下结合说明书附图对本申请的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明，并且在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0089] 本申请实施例中采用了两种方法进行安全认证，第一种方法为：将口令与数字签名相结合的方式，进行安全认证；第二种方法为：将口令与公钥加密相结合的方式，进行安全认证。

[0090] 参阅图1所示，为本申请实施例中第一种方法的流程图，本申请实施例一中，采用口令与数字签名相结合的方式，对安全认证的具体流程如下：

[0091] 步骤100：客户端基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果。

[0092] 具体的，执行步骤100时，口令认证消息中包含指定口令。其中，客户端与服务器之

间通过共享的指定口令,进行口令认证。

[0093] 实际应用中,服务器和客户端之间通过若干口令认证消息进行相互认证,,获得口令认证结果。

[0094] 其中,口令认证消息的数目与应用的口令协议有关,可以根据实际应用场景进行相应的调整。

[0095] 步骤101:客户端基于口令认证结果,确定口令一致时,判定口令认证成功。

[0096] 这样,客户端与服务器通过口令认证,初步确定认证成功,在后续的过程中,就可以通过数字签名进行再次认证。

[0097] 步骤102:客户端向服务器发送请求认证消息。

[0098] 步骤103:服务器对所有的口令认证消息和接收的请求认证消息进行散列运算,获得第一哈希值。

[0099] 具体的,首先,服务器获得上述客户端与服务器之间交互的所有消息,即请求认证消息,以及所有交互的口令认证消息。

[0100] 然后,服务器对获取的所有消息进行散列运算,获得第一哈希值。

[0101] 这样,就可以将客户端与服务器之间所有的交互的消息进行绑定,获得相应的哈希值。其中,由于每一次获得的哈希值都是由所有已经交互的消息共同确定的,因此,哈希值随交互的消息的变化而实时变化,这可以避免非法分子通过一个已经传输过的有效消息进行不断传输造成的重放攻击。

[0102] 步骤104:服务器基于本地的私钥,对第一哈希值进行数字签名,获得数字签名值。。

[0103] 步骤105:服务器将数字签名值和服务器证书发送至客户端。

[0104] 具体的,执行步骤105时,服务器发送的服务器证书中包含服务器的公钥,可用于对数据进行数字签名或加密。

[0105] 其中,所谓服务器证书是通过第三方的可信任机构认证中心颁发的,依赖于公钥基础设施((Public Key Infrastructure,PKI)技术,把用户的公钥和用户的其他标识信息(如名称、e-mail、身份证号等)捆绑在一起,用于通过包含的公钥对数据进行数字签名或加密,提高网络安全。

[0106] PKI是一个用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施,是一种遵循标准的利用公钥加密技术为网上电子商务、电子政务的开展,提供一整套安全的基础平台。PKI技术就是利用公钥理论和技术建立的提供网络信息安全服务的基础设施。PKI管理平台能够为网络中所有需要采用加密和数字签名等密码服务的用户提供所需的密钥和证书管理,用户可以利用PKI平台提供的安全服务进行安全通信。

[0107] 步骤106:客户端基于接收服务器证书中包含的公钥,对接收的数字签名值进行验证,获得安全认证结果。

[0108] 具体的,首先,客户端接收服务器发送的服务器证书和数字签名值。

[0109] 然后,客户端获取与服务器交互的所有口令认证消息,并对请求认证消息,以及所有口令认证消息,进行散列运算,获得第二哈希值。

[0110] 接着,客户端将公钥和第二哈希值,输入数字签名验证算法,获得验证数字签名值、

[0111] 最后，客户端基于数字签名值与验证数字签名值的比较结果，获得安全认证结果，客户端确定数字签名值与验证数字签名值相同时，判定安全认证成功，否则，判定安全认证失败。

[0112] 这样，就可以将口令与数字签名相结合，对客户端和服务器先通过口令进行初步认证，然后通过数字签名进行再次认证，从而保证了通信双方的身份的正确性，避免了通信过程中的通信泄露以及信息篡改，提高了网络安全。

[0113] 参阅图2所示，为本申请实施例中第二种方法的流程图，本申请实施例二中，采用口令与公钥加密相结合，对安全认证的具体流程如下：

[0114] 步骤200：客户端基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果。

[0115] 具体的，执行步骤200时，口令认证消息中包含指定口令。其中，客户端与服务器之间通过共享的指定口令，进行口令认证。

[0116] 实际应用中，服务器和客户端之间通过若干口令认证消息进行相互认证，，获得口令认证结果。

[0117] 其中，口令认证消息的数目与应用的口令协议有关，可以根据实际应用场景进行相应的调整。

[0118] 步骤201：客户端基于口令认证结果，确定口令一致时，判定口令认证成功。

[0119] 这样，客户端与服务器通过口令认证，初步确定认证成功，在后续的过程中，就可以通过数字签名进行再次认证。

[0120] 步骤202：客户端向服务器发送请求认证消息。

[0121] 步骤203：服务器基于接收的请求认证消息，向客户端发送包含服务器证书的响应认证消息。

[0122] 具体的，服务器证书中包含服务器的公钥，可用于对数据进行数字签名或加密。

[0123] 其中，所谓服务器证书是通过第三方的可信任机构认证中心颁发的，依赖于公钥基础设施((Public Key Infrastructure,KPI)技术，把用户的公钥和用户的其他标识信息(如名称、e-mail、身份证号等)捆绑在一起，用于通过包含的公钥对数据进行数字签名或加密，提高网络安全。

[0124] PKI是一个用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施，是一种遵循标准的利用公钥加密技术为网上电子商务、电子政务的开展，提供一整套安全的基础平台。PKI技术就是利用公钥理论和技术建立的提供网络信息安全服务的基础设施。PKI管理平台能够为网络中所有需要采用加密和数字签名等密码服务的用户提供所需的密钥和证书管理，用户可以利用PKI平台提供的安全服务进行安全通信。

[0125] 步骤204：客户端确定接收到服务器证书中包含的公钥时，获取本地的一个随机数。

[0126] 具体，首先，客户端接收服务器发送的响应认证消息。

[0127] 然后，客户端获取响应认证消息中包含的数字证书，以及数字证书中包含的服务器的公钥和服务器名称。

[0128] 最后，客户端确定接收到公钥时，获取本地随机的产生一个随机数。

[0129] 步骤205：客户端对请求认证消息，以及所有的口令认证消息，进行散列运算，获得

哈希值。

[0130] 具体的，首先，客户端获得上述客户端与服务器之间交互的所有消息，即请求认证消息，以及所有交互的口令认证消息。

[0131] 然后，客户端对获取交互的所有消息进行散列运算，获得哈希值。

[0132] 这样，就可以将客户端与服务器之间所有的交互的消息进行绑定，获得相应的哈希值。由于每一次获得的哈希值都是由所有已经交互的消息共同确定的，因此，哈希值会随着交互的消息的变化而实时变化，这可以避免非法分子通过一个已经传输过的有效消息进行不断传输造成的重放攻击。

[0133] 步骤206：客户端通过公钥，对获取的随机数和哈希值进行加密，获得加密值。

[0134] 步骤207：客户端将加密值发送至服务器。

[0135] 步骤208：服务器基于本地的私钥，对接收的加密值进行解密，获得验证随机数。

[0136] 步骤209：服务器将验证随机数返回至客户端。

[0137] 步骤210：客户端基于本地的随机数和接收的验证随机数比较结果，获得安全认证结果。

[0138] 具体的，首先，客户端获取本地的随机数和接收的验证随机数的比较结果。

[0139] 然后，客户端基于获取的比较结果，确定本地的随机数与验证随机数相同时，判定安全认证成功，否则，判定安全认证失败。

[0140] 这样，就可以通过将口令与公钥加密相结合的方式，对客户端和服务器进行口令进行口令认证，然后通过公钥加密进行再次认证，这保证了通信双方的身份的正确性，避免了通信过程中的通信泄露以及信息篡改，提高了网络安全。

[0141] 本申请实施例中，通过口令与数字签名相结合的方式，以及通过口令与公钥加密相结合的方式进行安全认证，即使非法分子获取相应的口令，也无法通过数字签名或公钥加密的再次认证。

[0142] 进一步地，通过对客户端与服务器之间所有的交互消息进行散列运算获得相应的哈希值，由于哈希值可以随交互消息的变化而实时变化，这样，可以防止非法分子通过获取的一个传输过的有效消息进行重放攻击，进一步提高了网络安全。

[0143] 最后，在原有的口令认证系统的基础上进行再次认证，可以兼容原有的口令认证系统，不需要对系统进行大幅度的修改，降低了研发成本和使用成本，提高了实用性。

[0144] 本申请实施例中，一种电子设备，包括：一个或多个处理器；以及

[0145] 一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，实现上述实施例一中的各个步骤。

[0146] 本申请实施例中，一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，使得通信设备可以执行上述实施例一中的各个步骤。

[0147] 本申请实施例中，一种电子设备，包括：一个或多个处理器；以及

[0148] 一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，实现上述实施例二中的各个步骤。

[0149] 本申请实施例中，一个或多个计算机可读介质，可读介质上存储有用于安全认证的程序，其中，程序被一个或多个处理器执行时，使得通信设备可以执行上述实施例二中的

各个步骤。

[0150] 基于上述实施例，参阅图3所示，安全认证的装置的结构示意图，本申请实施例中，安全认证的装置具体包括：

[0151] 获得单元30，用于基于传输的口令认证消息，与服务器进行口令认证，获得口令认证结果；

[0152] 发送单元31，用于确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息；

[0153] 接收单元32，用于接收服务器基于接收的请求认证消息返回的包含服务器证书和数字签名值的响应认证消息，其中，服务器证书包含服务器的公钥，数字签名值是基于请求认证消息和口令认证消息获得的；

[0154] 认证单元33，用于基于服务器的公钥，对响应认证消息中包含的数字签名值进行验证，获得安全认证结果。

[0155] 较佳的，在确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息时，发送单元31具体用于：

[0156] 确定口令认证结果表征口令认证成功时，向服务器发送请求认证消息，触发服务器执行以下步骤：对口令认证消息和请求认证消息进行散列运算，获得第一哈希值，并基于本地的私钥，对第一哈希值进行数字签名，获得请求认证消息的数字签名值。

[0157] 较佳的，在基于服务器的公钥，对响应认证消息中包含的数字签名值进行验证，获得安全认证结果时，认证单元33具体用于：

[0158] 对口令认证消息和请求认证消息进行散列运算，获得第二哈希值；

[0159] 基于公钥和第二哈希值，采用预设的数字签名验证算法，获得验证数字签名值；

[0160] 基于数字签名值与验证数字签名值的比较结果，获得安全认证结果。

[0161] 基于上述实施例，参阅图4所示，安全认证的装置的结构示意图，本申请实施例中，安全认证的装置具体包括：

[0162] 接收单元40，用于接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息，其中，口令认证结果是基于传输的口令认证消息进行口令认证获得的；

[0163] 签名单元41，用于基于本地的私钥，对接收的请求认证消息和口令认证消息进行数字签名，获得数字签名值；

[0164] 发送单元42，用于将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客户端基于服务器证书中包含的服务器的公钥对数字签名值进行验证并获得安全认证结果。

[0165] 较佳的，在基于本地的私钥，对接收的请求认证消息和口令认证消息进行数字签名，获得数字签名值时，签名单元41具体用于：

[0166] 对口令认证消息和请求认证消息进行散列运算，获得第一哈希值；

[0167] 基于私钥，对第一哈希值进行数字签名，获得请求认证消息的数字签名值。

[0168] 较佳的，在将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客户端基于服务器证书中包含的服务器的公钥对数字签名值进行验证并获得安全认证结果时，发送单元42具体用于：

[0169] 将包含本地的服务器证书和数字签名值的响应认证消息，发送至客户端，触发客

户端执行以下步骤:对口令认证消息和请求认证消息进行散列运算,获得第二哈希值,并基于公钥和第二哈希值,采用预设的数字签名验证算法,获得验证数字签名值,以及基于数字签名值与验证数字签名值的比较结果,获得安全认证结果。

[0170] 基于上述实施例,参阅图5所示,安全认证的装置的结构示意图,本申请实施例中,安全认证的装置具体包括:

[0171] 获得单元50,用于基于传输的口令认证消息,与服务器进行口令认证,获得口令认证结果;

[0172] 请求单元51,用于确定口令认证结果表征口令认证成功时,向服务器发送请求认证消息,并接收服务器基于请求认证消息返回的包含服务器证书的响应认证消息,其中,服务器证书中包含服务器的公钥;

[0173] 加密单元52,用于基于接收的服务器的公钥,对本地获取的随机数、口令认证消息和请求认证消息进行加密,获得加密值,并将加密值发送至服务器;

[0174] 认证单元53,用于接收服务器基于加密值返回的验证随机数,并基于随机数和验证随机数的比较结果,获得安全认证结果,其中,验证随机数是通过私钥对加密值进行解密获得的。

[0175] 较佳的,在基于接收的服务器的公钥,对本地获取的随机数、口令认证消息和请求认证消息进行加密,获得加密值时,加密单元52具体用于:

[0176] 确定接收到响应认证消息中包含的公钥时,获取本地生成的一个随机数;

[0177] 对口令认证消息和请求认证消息进行散列运算,获得哈希值;

[0178] 基于公钥,对随机数和哈希值进行加密,获得加密值。

[0179] 基于上述实施例,参阅图6所示,安全认证的装置的结构示意图,本申请实施例中,安全认证的装置具体包括:

[0180] 第一接收单元60,用于接收客户端基于表征口令认证成功的口令认证结果发送的请求认证消息,其中,口令认证结果是基于传输的口令认证消息进行口令认证获得的;

[0181] 发送单元61,用于基于请求认证消息,向客户端发送包含本地的服务器证书的响应认证消息;

[0182] 第二接收单元62,用于接收客户端基于响应认证消息发送的加密值,其中,加密值是基于服务器证书中包含的服务器的公钥对本地获取的随机数、口令认证消息和请求认证消息进行加密获得的;

[0183] 认证单元63,用于基于本地的私钥对加密值进行解密,获得验证随机数,并将验证随机数发送至客户端,触发客户端基于随机数和验证随机数的比较结果获得安全认证结果。

[0184] 较佳的,在基于请求认证消息,向客户端发送包含本地的服务器证书的响应认证消息时,发送单元61具体用于:

[0185] 基于请求认证消息,向客户端发送包含本地的服务器证书的响应认证消息,触发客户端执行以下步骤:对口令认证消息和请求认证消息进行散列运算获得哈希值,并基于公钥对本地生成的随机数和哈希值进行加密,获得加密值。

[0186] 本申请实施例中,先与服务器进行口令认证,然后,通过服务器对所有的交互消息进行数字签名,客户端进行数字签名验证的方式,或者,通过客户端对本地的随机数、所有

交互消息进行公钥加密，并对服务器返回的随机数进行验证的方式，进行安全认证，这样，就可以通过将口令认证与数字签名相结合，或者，将口令认证与公钥加密相结合的方式，保证了通信双方的身份的正确性，避免了通信过程中的消息泄露以及恶意信息篡改等网络攻击，提高了网络认证的可靠度，保障了用户的通信安全。

[0187] 本领域内的技术人员应明白，本申请实施例中的实施例可提供为方法、系统、或计算机程序产品。因此，本申请实施例中可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例中可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0188] 本申请实施例中是参照根据本申请实施例中实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0189] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0190] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0191] 尽管已描述了本申请实施例中的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例中范围的所有变更和修改。

[0192] 显然，本领域的技术人员可以对本申请实施例中实施例进行各种改动和变型而不脱离本申请实施例中实施例的精神和范围。这样，倘若本申请实施例中实施例的这些修改和变型属于本申请实施例中权利要求及其等同技术的范围之内，则本申请实施例中也意图包含这些改动和变型在内。

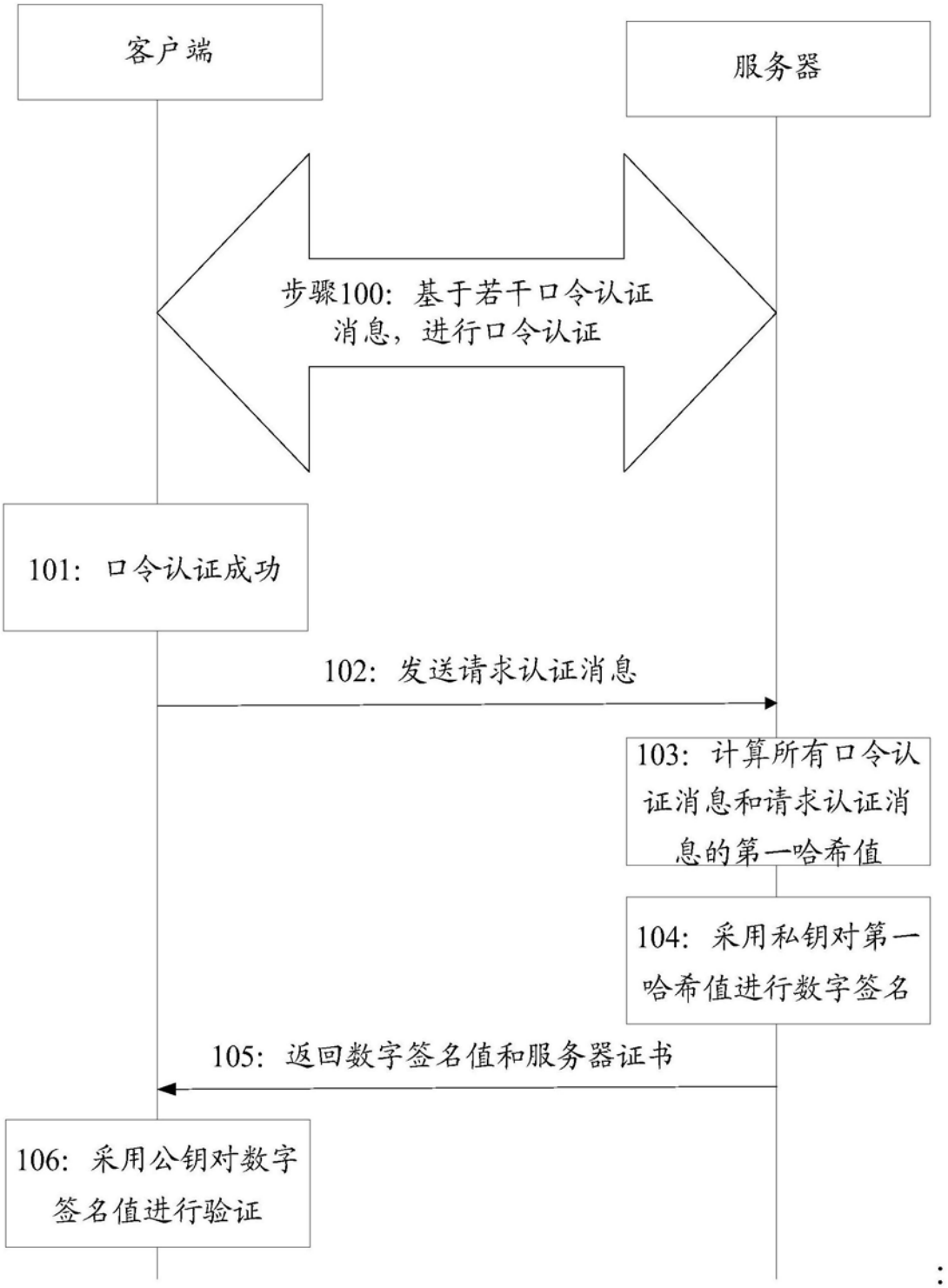

客户端
服务器
步骤100：基于若干口令认证消息，进行口令认证
101：口令认证成功
102：发送请求认证消息
103：计算所有口令认证消息和请求认证消息的第一哈希值
104：采用私钥对第一哈希值进行数字签名
105：返回数字签名值和服务器证书
106：采用公钥对数字签名值进行验证

图1

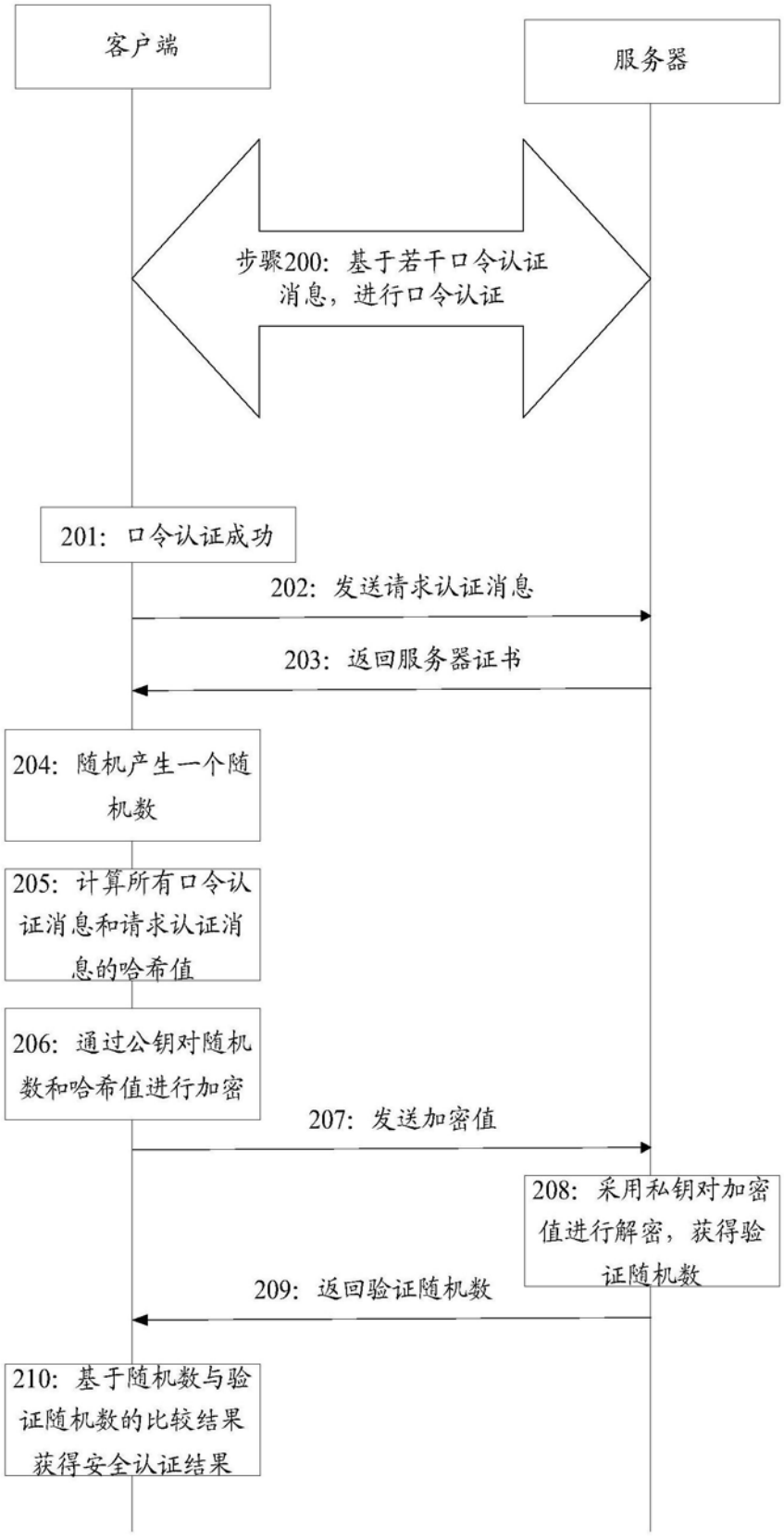

客户端
服务器
步骤200：基于若干口令认证消息，进行口令认证
201：口令认证成功
202：发送请求认证消息
203：返回服务器证书
204：随机产生一个随机数
205：计算所有口令认证消息和请求认证消息的哈希值
206：通过公钥对随机数和哈希值进行加密
207：发送加密值
208：采用私钥对加密值进行解密，获得验证随机数
209：返回验证随机数
210：基于随机数与验证随机数的比较结果获得安全认证结果

图2

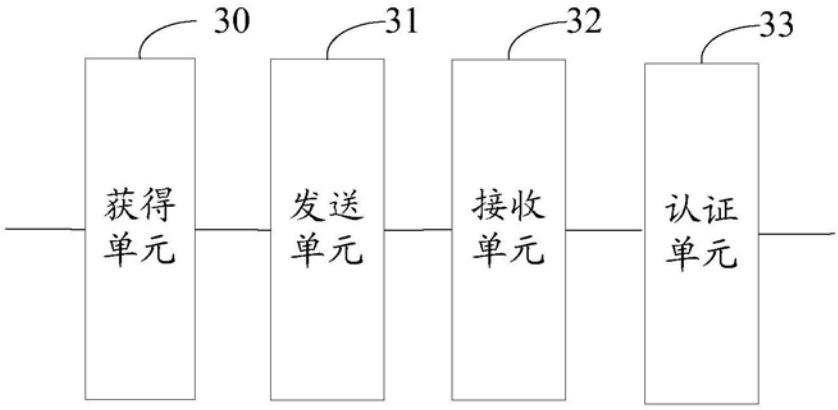

30
31
32
33
获得单元
发送单元
接收单元
认证单元

图3

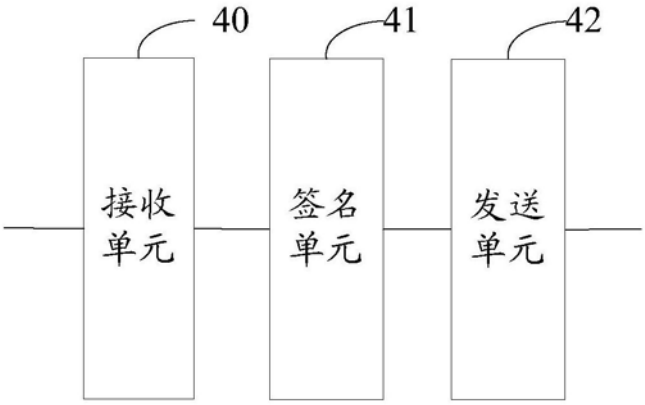

40
41
42
接收单元
签名单元
发送单元

图4

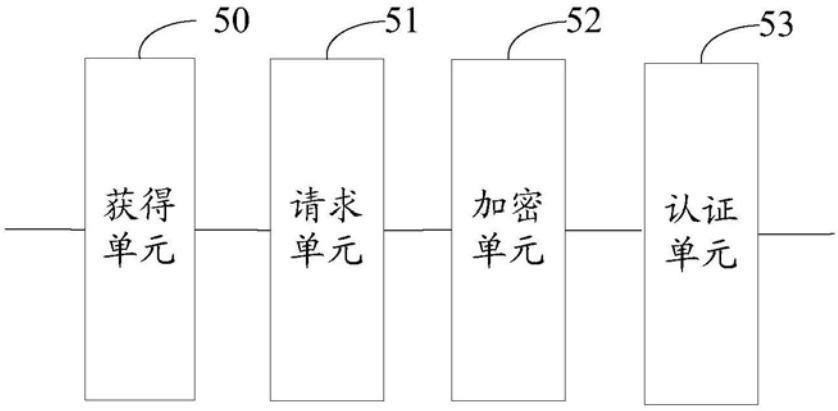

50
51
52
53
获得单元
请求单元
加密单元
认证单元

图5

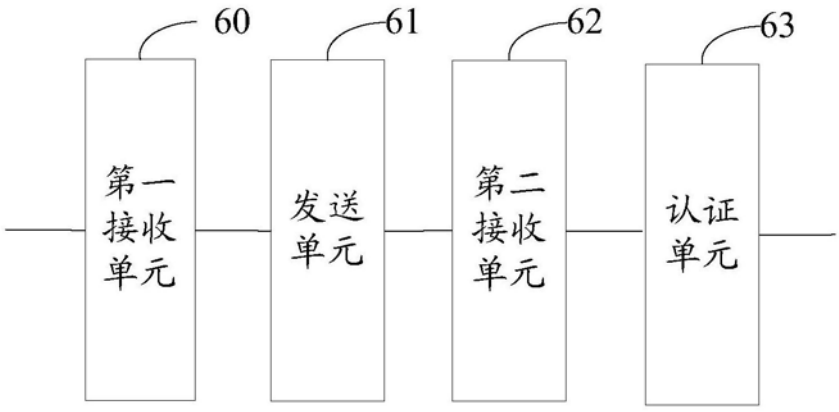


图6