(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 1 月 31 日 (31.01.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/020051 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2018/097027

(22) 国际申请日: 2018 年 7 月 25 日 (25.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710632863.4 2017年7月28日 (28.07.2017) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 刘福文 (LIU, Fuwen); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。左敏 (ZUO, Min); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街32号院枫蓝国际中心2号楼10层, Beijing 100082 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) **Title:** METHOD AND APPARATUS FOR SECURITY AUTHENTICATION

(54) **发明名称:** 一种安全认证的方法及装置

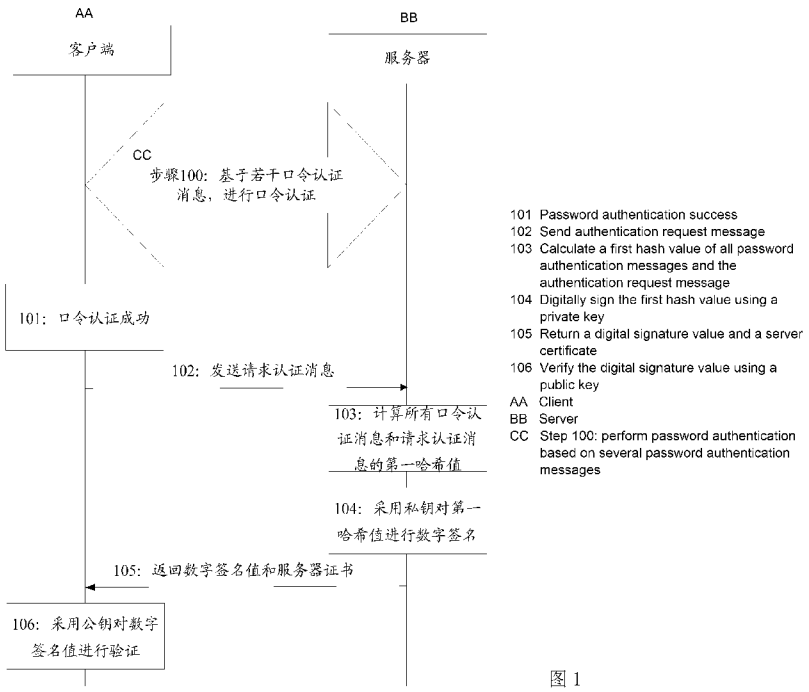

图 1

(57) **Abstract:** Disclosed are a method and apparatus for security authentication. The method comprises: based on a transmitted password authentication message, performing password authentication with a server to obtain a password authentication result; when it is determined that the password authentication result characterises password authentication success, sending an authentication request message to the server; and digitally signing all interaction messages through the server, and performing security authentication by way of the client performing digital signature verification, or by way of the client performing public key encryption a random number at the

WO 2019/020051 A1

[见续页]

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

locality and all the interaction messages and verifying the random number returned by the server.

(57) 摘要：本公开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。

一种安全认证的方法及装置

相关申请的交叉引用

本公开主张在 2017 年 7 月 28 日在中国提交的中国专利申请号 No. 201710632863.4 的优先权，其全部内容通过引用包含于此。

技术领域

本公开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

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。

相关技术下，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：

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。

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。

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。

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。

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。

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

本公开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。

本公开提供的具体技术方案如下：

第一方面，一种安全认证的方法，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；

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；

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。

可选的，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：

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。

可选的，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：

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；

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；

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。

第二方面，一种安全认证的方法，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，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；

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。

可选的，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：

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；

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。

可选的，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：

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。

第三方面，一种安全认证的方法，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；

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；

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。

可选的，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：

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；

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；

基于公钥，对随机数和哈希值进行加密，获得加密值。

第四方面，一种安全认证的方法，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，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；

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；

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。

可选的，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：

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。

第五方面，一种安全认证的装置，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；

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；

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；

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。

第六方面，一种安全认证的装置，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，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；

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；

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。

第七方面，一种安全认证的装置，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；

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；

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。

第八方面，一种安全认证的装置，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，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；

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；

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。

第九方面，一种电子设备，包括：一个或多个处理器；以及

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。

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。

第十一方面，一种电子设备，包括：一个或多个处理器；以及

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。

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。

第十三方面，一种电子设备，包括：一个或多个处理器；以及

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。

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。

第十五方面，一种电子设备，包括：一个或多个处理器；以及

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。

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。

本公开中，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

图 1 为本公开一些实施例中安全认证的方法的流程图；

图 2 为本公开一些实施例中安全认证的方法的流程图；

图 3 为本公开一些实施例中安全认证的装置的结构示意图一；

图 4 为本公开一些实施例中安全认证的装置的结构示意图二；

图 5 为本公开一些实施例中安全认证的装置的结构示意图三；

图 6 为本公开一些实施例中安全认证的装置的结构示意图四。

具体实施方式

下面将结合本公开一些实施例中的附图，对本公开一些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公开一部分实施例，并不是全部的实施例。基于本公开一些实施例，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，都属于本公开保护的范围。

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，本公开一些实施例中，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。

以下结合说明书附图对本公开的一些实施例进行说明，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，本公开中的实施例及实施例中的特征可以相互组合。

本公开一些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。

参阅图 1 所示，为本公开一些实施例中第一种方法的流程图，本公开一些实施例中，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：

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。

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。

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。

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。

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。

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。

步骤 102：客户端向服务器发送请求认证消息。

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。

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。

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。

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。

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。。

步骤 105：服务器将数字签名值和服务器证书发送至客户端。

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。

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。

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。

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。

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。

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。

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、

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。

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。

参阅图 2 所示，为本公开一些实施例中第二种方法的流程图，本公开一些实施例中，采用口令与公钥加密相结合，对安全认证的具体流程如下：

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。

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。

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。

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。

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。

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。

步骤 202：客户端向服务器发送请求认证消息。

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。

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。

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。

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。

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。

具体，首先，客户端接收服务器发送的响应认证消息。

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。

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。

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。

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。

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。

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。

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。

步骤 207：客户端将加密值发送至服务器。

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。

步骤 209：服务器将验证随机数返回至客户端。

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。

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。

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。

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。

本公开一些实施例中，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。

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。

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。

本公开一些实施例中，一种电子设备，包括：一个或多个处理器；以及

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。

本公开一些实施例中，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。

本公开一些实施例中，一种电子设备，包括：一个或多个处理器；以及

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。

本公开一些实施例中，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。

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，本公开一些实施例中，安全认证的装置具体包括：

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；

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；

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；

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。

可选的，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：

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。

可选的，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：

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；

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；

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。

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，本公开一些实施例中，安全认证的装置具体包括：

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；

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；

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。

可选的，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：

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；

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。

可选的，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：

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。

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，本公开一些实施例中，安全认证的装置具体包括：

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；

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；

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；

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。

可选的，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：

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；

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；

基于公钥，对随机数和哈希值进行加密，获得加密值。

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，本公开一些实施例中，安全认证的装置具体包括：

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；

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；

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；

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。

可选的，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：

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。

本公开一些实施例中，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。

本领域内的技术人员应明白，本公开一些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，本公开一些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，本公开一些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。

本公开一些实施例中是参照根据本公开一些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。

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。

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。

尽管已描述了本公开一些实施例，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公开一些实施例中范围的所有变更和修改。

显然，本领域的技术人员可以对本公开一些实施例中进行各种改动和变型而不脱离本公开一些实施例的精神和范围。这样，倘若本公开一些实施例的这些修改和变型属于本公开一些实施例中权利要求及其等同技术的范围之内，则本公开一些实施例中也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种安全认证的方法，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；

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，其中，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，具体包括：

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。

3、如权利要求 1 或 2 所述的方法，其中，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。

4、一种安全认证的方法，包括：

接收所述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；

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

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。

5、如权利要求 4 所述的方法，其中，基于本地的私钥，对接收的请求认证消息和所述口令认证消息进行数字签名，获得数字签名值，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，获得第一哈希值；

基于所述私钥，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。

6、如权利要求 4 或 5 所述的方法，其中，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。

7、一种安全认证的方法，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；

基于接收的所述服务器的公钥，对本地获取的随机数、所述口令认证消息和所述请求认证消息进行加密，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。

8、如权利要求 7 所述的方法，其中，基于接收的所述服务器的公钥，对本地获取的随机数、所述口令认证消息和所述请求认证消息进行加密，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。

9、一种安全认证的方法，包括：

接收所述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，所述加密值是基于所述服务器证书中包含的服务器的公钥对本地获取的随机数、所述口令认证消息和所述请求认证消息进行加密获得的；

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。

10，如权利要求 9 所述的方法，其中，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。

11、一种安全认证的装置，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；

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；

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。

12、一种安全认证的装置，包括：

接收单元，用于接收所述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；

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

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。

13、一种安全认证的装置，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，用于基于接收的所述服务器的公钥，对本地获取的随机数、所述口令认证消息和所述请求认证消息进行加密，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。

14、一种安全认证的装置，包括：

第一接收单元，用于接收所述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，所述加密值是基于所述服务器证书中包含的服务器的公钥对本地获取的随机数、所述口令认证消息和所述请求认证消息进行加密获得的；

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。

15、一种电子设备，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 1~3 中任意一项所述的方法的步骤。

16、一个或多个计算机可读介质，其中，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 至 3 中任一项所述的方法。

17、一种电子设备，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 4-6 所述的方法的步骤。

18、一个或多个计算机可读介质，其中，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 4-6 所述的方法。

19、一种电子设备，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 所述的方法的步骤。

20、一个或多个计算机可读介质，其中，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 所述的方法。

21、一种电子设备，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 9-10 所述的方法的步骤。

22、一个或多个计算机可读介质，其中，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 9-10 所述的方法。

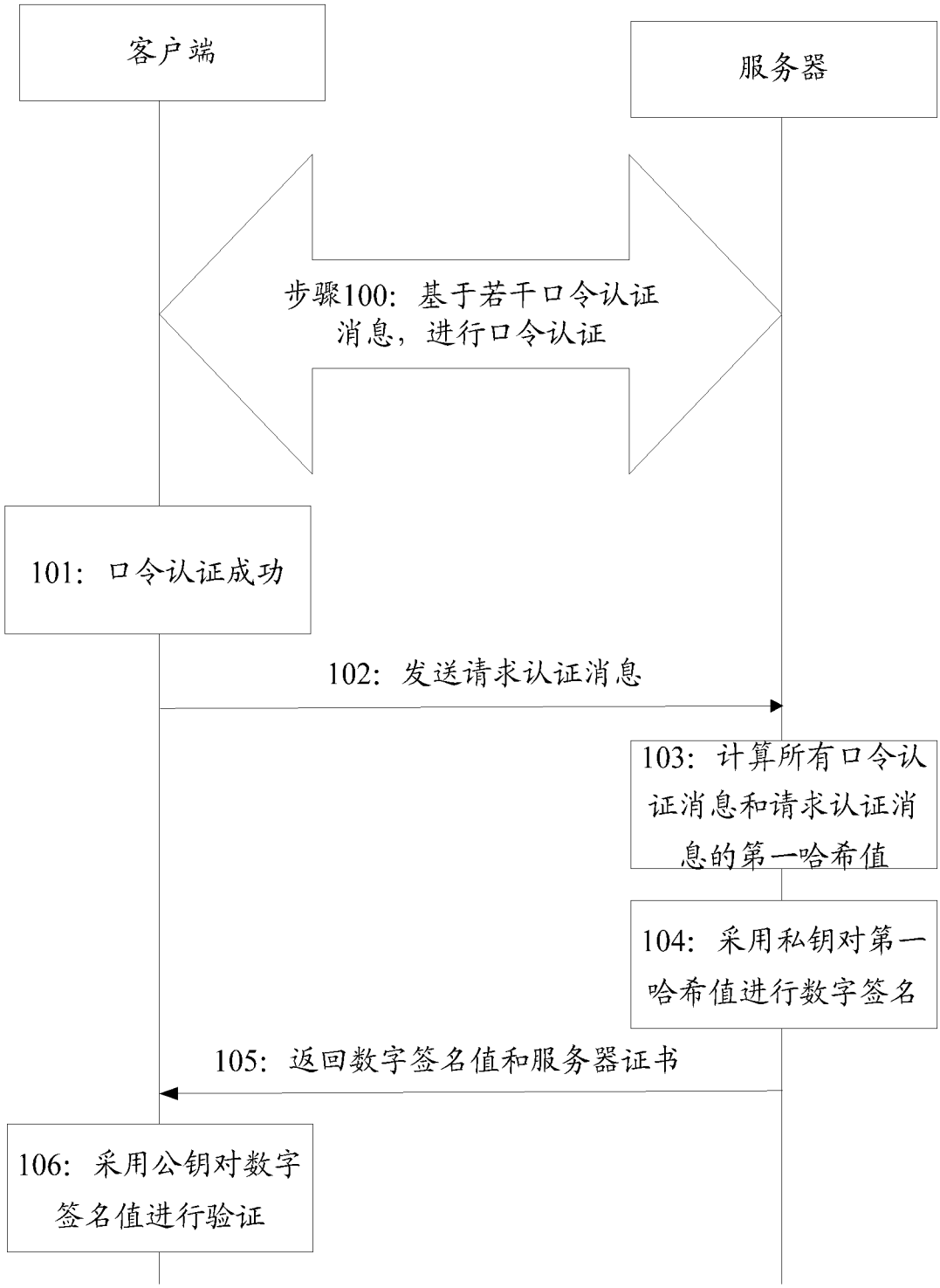
客户端
服务器
步骤100：基于若干口令认证消息，进行口令认证
101：口令认证成功
102：发送请求认证消息
103：计算所有口令认证消息和请求认证消息的第一哈希值
104：采用私钥对第一哈希值进行数字签名
105：返回数字签名值和服务器证书
106：采用公钥对数字签名值进行验证

图 1

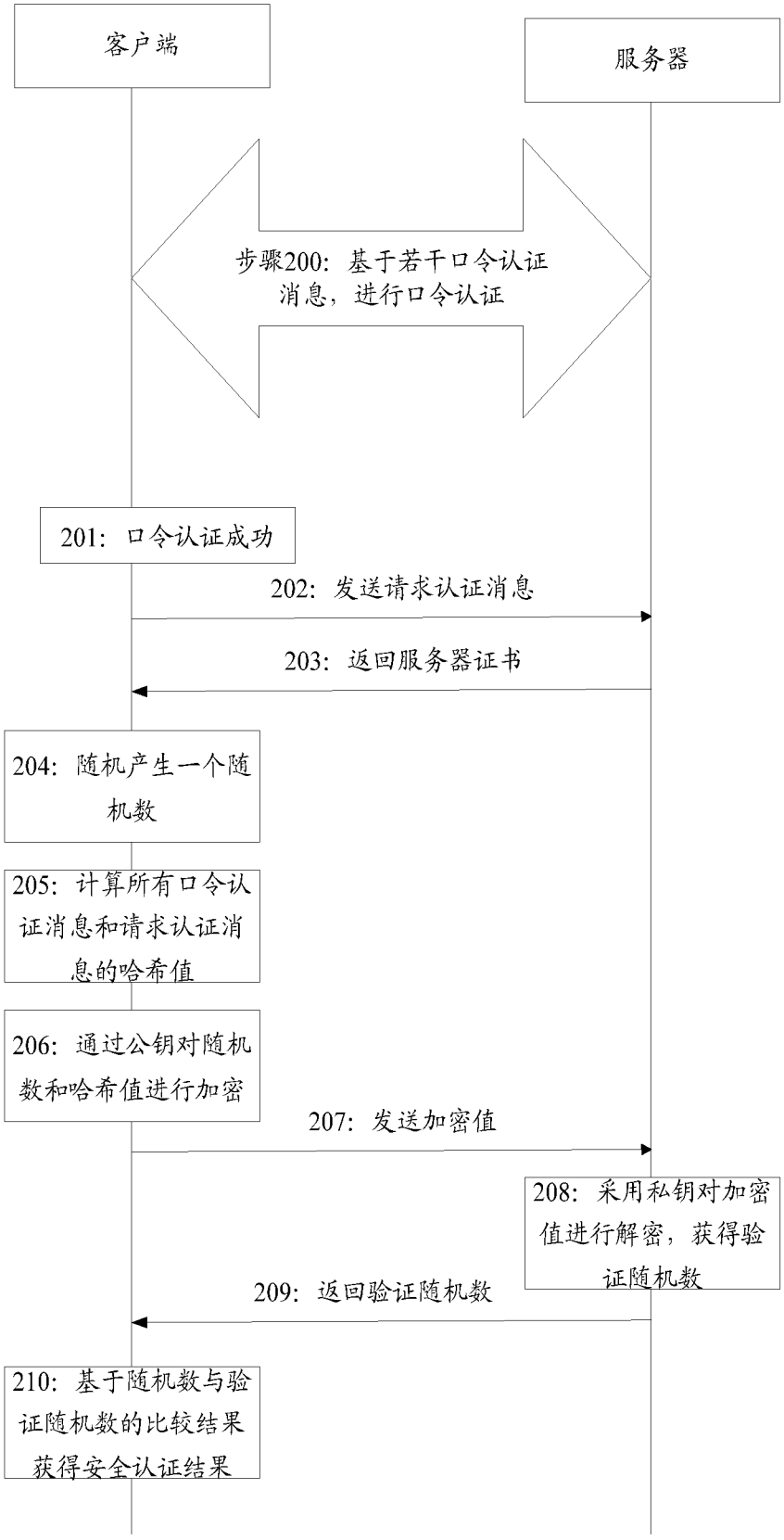
客户端
服务器
步骤200：基于若干口令认证消息，进行口令认证
201：口令认证成功
202：发送请求认证消息
203：返回服务器证书
204：随机产生一个随机数
205：计算所有口令认证消息和请求认证消息的哈希值
206：通过公钥对随机数和哈希值进行加密
207：发送加密值
208：采用私钥对加密值进行解密，获得验证随机数
209：返回验证随机数
210：基于随机数与验证随机数的比较结果获得安全认证结果

图 2

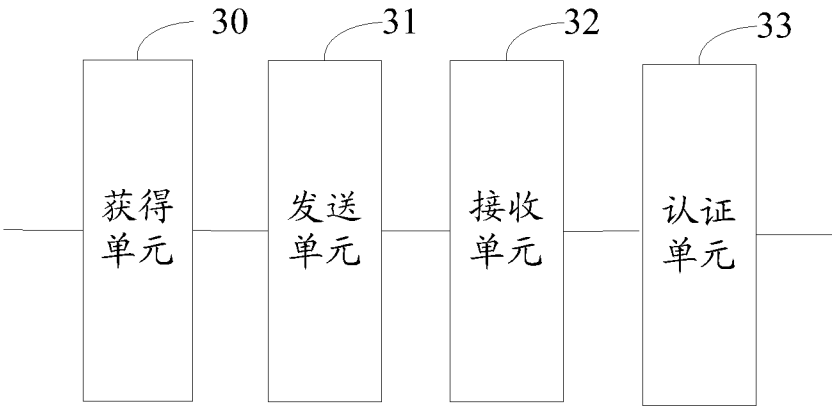

图 3

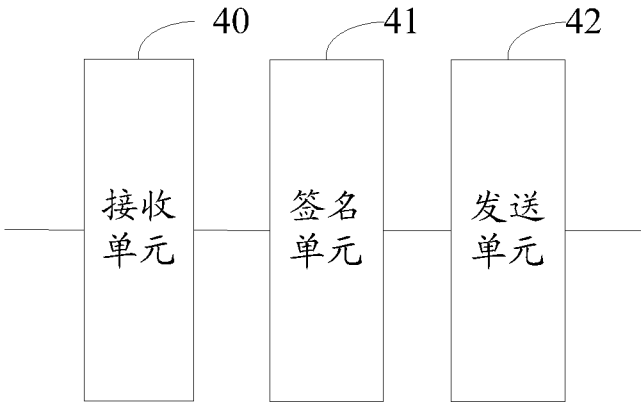

图 4

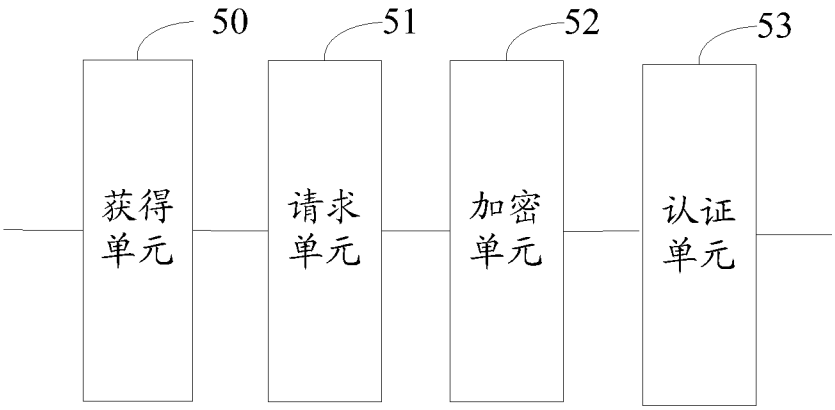
50
51
52
53
获得单元
请求单元
加密单元
认证单元

图 5

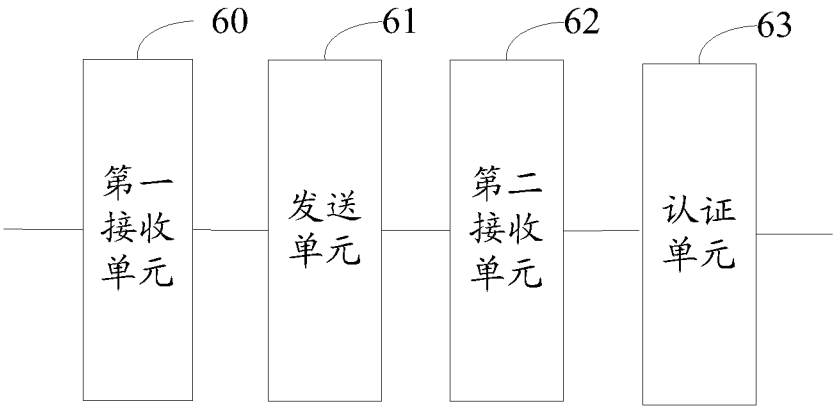
60
61
62
63
第一接收单元
发送单元
第二接收单元
认证单元

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/097027

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 口令, 密码, 数字签名, 认证, 验证, 授权, 公钥, 密钥, 私钥, 加密, password, authenti+, certif +, digital signature, public, private, Key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103795542 A (INDUSTRIAL AND COMMERCIAL BANK OF CHINA LIMITED) 14 May 2014 (2014-05-14) description, paragraphs 0029-0049	1-22
A	CN 106100848 A (NORTHEASTERN UNIVERSITY) 09 November 2016 (2016-11-09) entire document	1-22
A	CN 105933280 A (TENDYRON CORPORATION) 07 September 2016 (2016-09-07) entire document	1-22
A	US 2017070350 A1 (MARKANY INC.) 09 March 2017 (2017-03-09) entire document	1-22
A	WO 2009002963 A1 (GENERAL INSTRUMENT CORPORATION) 31 December 2008 (2008-12-31) entire document	1-22

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 September 2018	**29 September 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/097027

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	103795542	A	14 May 2014	None			
CN	106100848	A	09 November 2016	None			
CN	105933280	A	07 September 2016	None			
US	2017070350	A1	09 March 2017	US	9819494	B2	14 November 2017
				KR	101658501	B1	22 September 2016
WO	2009002963	A1	31 December 2008	US	2009006852	A1	01 January 2009
				US	8171527	B2	01 May 2012

国际检索报告

国际申请号 PCT/CN2018/097027

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC:口令，密码，数字签名，认证，验证，授权，公钥，密钥，私钥，加密，password，authenti+，certif+，digital signature，public,private,Key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 103795542 A（中国工商银行股份有限公司）2014年 5月 14日（2014 - 05 - 14） 说明书第0029-0049段	1-22
A	CN 106100848 A（东北大学）2016年 11月 9日（2016 - 11 - 09） 全文	1-22
A	CN 105933280 A（天地融科技股份有限公司）2016年 9月 7日（2016 - 09 - 07） 全文	1-22
A	US 2017070350 A1（MARKANY INC.）2017年 3月 9日（2017 - 03 - 09） 全文	1-22
A	WO 2009002963 A1（GENERAL INSTRUMENT CORPORATION）2008年 12月 31日（2008 - 12 - 31） 全文	1-22

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 9月 7日	2018年 9月 29日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	蒋莉
传真号 (86-10)62019451	电话号码 （86-10）53961751

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/097027

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	103795542	A	2014年 5月 14日	无			
CN	106100848	A	2016年 11月 9日	无			
CN	105933280	A	2016年 9月 7日	无			
US	2017070350	A1	2017年 3月 9日	US	9819494	B2	2017年 11月 14日
				KR	101658501	B1	2016年 9月 22日
WO	2009002963	A1	2008年 12月 31日	US	2009006852	A1	2009年 1月 1日
				US	8171527	B2	2012年 5月 1日