(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 101523800 B
(45)授权公告日 2013.05.01

(21)申请号 200780037702.5
(22)申请日 2007.10.05
(30)优先权数据
60/850,882 2006.10.10 US
11/866,946 2007.10.03 US
(85)PCT申请进入国家阶段日
2009.04.09
(86)PCT申请的申请数据
PCT/US2007/080525 2007.10.05
(87)PCT申请的公布数据
WO2008/045773 EN 2008.04.17
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 A·佩雷斯 L·R·东代蒂
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 夏青 韩宏

(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
WO 2005/091551 A1,2005.09.29,
US 6769060 B1,2004.07.27,
US 7024690 B1,2006.04.04,
审查员 陈晨

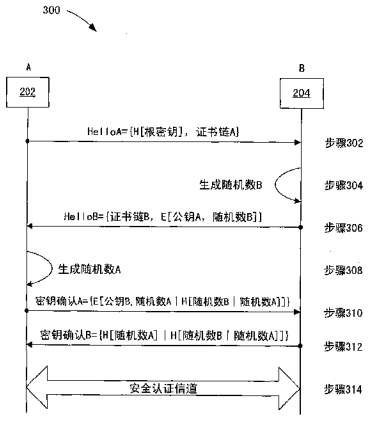
权利要求书4页 说明书6页 附图3页

(54)发明名称

用于双向认证的方法和装置

(57)摘要

本发明提供了一种在具有数字版权代理的站和安全可移动媒体设备之间进行双向认证的方法。数字版权代理通过向安全可移动媒体设备发送消息来发起双向认证。安全可移动媒体设备使用与数字版权代理相关联的公钥对第一随机数进行加密。数字版权代理对加密的第一随机数进行解密,并根据至少第一随机数对第二随机数和第一散列进行加密。安全可移动媒体设备对经加密的第二随机数和第一散列进行解密,验证第一散列以便认证数字版权代理,并根据至少第二随机数生成第二散列。数字版权代理验证第二散列,以便认证安全可移动媒体设备。



CN 101523800 B

1. 一种用于在第一实体和第二实体之间进行双向认证的方法，包括：

所述第一实体通过向所述第二实体发送消息来发起双向认证，其中，发起双向认证的所述消息包括具有至少一个信任根密钥的散列和对应的所述第一实体的证书链；

所述第二实体对与所述第一实体相关联的第一公钥进行验证，生成第一随机数，使用所述第一公钥对所述第一随机数进行加密并在消息中向所述第一实体发送经加密的第一随机数，其中，从所述第二实体向所述第一实体发送的包括所述经加密的第一随机数的所述消息还包括所述第二实体的证书链；

所述第一实体对与所述第二实体相关联的第二公钥进行验证，使用对应于所述第一公钥的第一私钥对所述经加密的第一随机数进行解密，生成第二随机数，根据至少所述第一随机数生成第一散列，使用所述第二公钥对所述第二随机数和所述第一散列进行加密，并在消息中向所述第二实体发送经加密的第二随机数和第一散列；

所述第二实体使用对应于所述第二公钥的第二私钥对所述经加密的第二随机数和第一散列进行解密，验证所述第一散列以便认证所述第一实体并且确定所述第一实体知道所述第一随机数，根据至少所述第二随机数生成第二散列，并将所述第二散列发送到所述第一实体；以及

所述第一实体验证所述第二散列以便认证所述第二实体并且确定所述第二实体知道所述第二随机数。

2. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第一实体和所述第二实体都根据密钥导出函数使用所述第一随机数和所述第二随机数导出会话加密密钥和消息认证码 (MAC) 密钥，以便在所述第一实体和所述第二实体之间的通信中使用。

3. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第一实体是数字版权代理，并且所述第二实体是安全可移动媒体设备。

4. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第一实体是移动站。

5. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第二实体具有有限的处理能力。

6. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第一散列进一步基于至少所述第二随机数，从而所述第一散列根据与所述第二随机数相级连的至少所述第一随机数生成。

7. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第二散列进一步基于至少所述第一随机数。

8. 根据权利要求 1 所述的用于双向认证的方法，其中，所述第二散列进一步基于至少所述第一散列，从而所述第二散列根据与所述第一散列相级连的至少所述第二随机数生成。

9. 一种用于双向认证的装置，包括：

用于通过发送消息来发起双向认证的模块，其中，发起双向认证的所述消息包括具有至少一个信任根密钥的散列和对应的第一证书链；

用于验证与第一实体相关联的第一公钥、生成第一随机数、使用所述第一公钥对所述第一随机数进行加密并在消息中发送经加密的第一随机数的模块，其中，包括所述经加密的第一随机数的所述消息还包括第二证书链；

用于验证与第二实体相关联的第二公钥、使用对应于所述第一公钥的第一私钥对经加密的第一随机数进行解密、生成第二随机数、根据至少所述第一随机数生成第一散列、使用所述第二公钥对所述第二随机数和所述第一散列进行加密并在消息中发送经加密的第二随机数和第一散列的模块；

用于使用对应于所述第二公钥的第二私钥对经加密的第二随机数和第一散列进行解密、验证所述第一散列以认证所述第一实体并且确定所述第一实体知道所述第一随机数、根据至少所述第二随机数生成第二散列并在消息中发送所述第二散列的模块；以及

用于验证所述第二散列以认证所述第二实体并且确定所述第二实体知道所述第二随机数的模块。

10. 根据权利要求 9 所述的用于双向认证的装置，还包括：

用于根据密钥导出函数使用所述第一随机数和所述第二随机数导出会话加密密钥和消息认证码 (MAC) 密钥以便在所述第一实体和所述第二实体之间的通信中使用的模块。

11. 根据权利要求 9 所述的用于双向认证的装置，其中，所述第一散列进一步基于至少所述第二随机数，从而所述第一散列根据与所述第二随机数相级连的至少所述第一随机数生成。

12. 根据权利要求 9 所述的用于双向认证的装置，其中，所述第二散列进一步基于至少所述第一随机数。

13. 根据权利要求 9 所述的用于双向认证的装置，其中，所述第二散列进一步基于所述第一散列，从而所述第二散列根据与所述第一散列相级连的所述第二随机数生成。

14. 一种与安全可移动媒体设备进行双向认证的站，包括：

数字版权代理，其中，

所述数字版权代理通过向所述安全可移动媒体设备发送消息来发起双向认证，其中，发起双向认证的所述消息包括具有至少一个信任根密钥的散列和对应的所述数字版权代理的证书链，并且其中，所述安全可移动媒体设备验证与所述数字版权代理相关联的第一公钥，生成第一随机数，使用所述第一公钥对所述第一随机数进行加密，并在消息中向所述数字版权代理发送经加密的第一随机数，其中，从所述安全可移动媒体设备向所述数字版权代理发送的具有所述经加密的第一随机数的所述消息还包括所述安全可移动媒体设备的证书链；

所述数字版权代理验证与所述安全可移动媒体设备相关联的第二公钥，使用对应于所述第一公钥的第一私钥对所述经加密的第一随机数进行解密，生成第二随机数，根据至少所述第一随机数生成第一散列，使用所述第二公钥对所述第二随机数和所述第一散列进行加密，并在消息中向所述安全可移动媒体设备发送经加密的第二随机数和第一散列，其中，所述安全可移动媒体设备使用对应所述第二公钥的第二私钥对所述经加密的第二随机数和第一散列进行解密，验证所述第一散列以便认证所述数字版权代理并且确定所述数字版权代理知道所述第一随机数，根据至少所述第二随机数生成第二散列，并向所述数字版权代理发送所述第二散列；以及

所述数字版权代理验证所述第二散列，以便认证所述安全可移动媒体设备并且确定所述安全可移动媒体设备知道所述第二随机数。

15. 根据权利要求 14 所述的进行双向认证的站，其中，所述数字版权代理和所述安全

可移动媒体设备都根据密钥导出函数使用所述第一随机数和所述第二随机数导出会话加密密钥和消息认证码 (MAC) 密钥，以便在所述数字版权代理和所述安全可移动媒体设备之间的通信中使用。

16. 根据权利要求 14 所述的进行双向认证的站，其中，所述数字版权代理的所述证书链包括与所述数字版权代理相关联的公钥。

17. 根据权利要求 14 所述的进行双向认证的站，其中，所述安全可移动媒体设备的所述证书链包括与所述安全可移动媒体设备相关联的所述公钥。

18. 根据权利要求 14 所述的进行双向认证的站，其中，所述站是移动站。

19. 根据权利要求 14 所述的进行双向认证的站，其中，所述第一散列进一步基于至少所述第二随机数，从而所述数字版权代理根据与所述第二随机数相级连的至少所述第一随机数生成所述第一散列。

20. 一种用于进行双向认证的装置，包括 ：

用于促使站的数字版权代理通过向安全可移动媒体设备发送消息而发起双向认证的模块，其中，发起双向认证的所述消息包括具有至少一个信任根密钥的散列和对应的所述数字版权代理的证书链，并且其中，所述安全可移动媒体设备验证与所述数字版权代理相关联的第一公钥，生成第一随机数，使用所述第一公钥对所述第一随机数进行加密并在消息中向所述数字版权代理发送经加密的第一随机数，其中，从所述安全可移动媒体设备向所述数字版权代理发送的具有所述经加密的第一随机数的所述消息还包括所述安全可移动媒体设备的证书链 ；

用于促使所述数字版权代理验证与所述安全可移动媒体设备相关联的第二公钥、使用对应于所述第一公钥的第一私钥对所述经加密的第一随机数进行解密、生成第二随机数、根据至少所述第一随机数生成第一散列、使用所述第二公钥对所述第二随机数和所述第一散列进行加密并在消息中向所述安全可移动媒体设备发送经加密的第二随机数和第一散列的模块，其中，所述安全可移动媒体设备使用对应于所述第二公钥的第二私钥对所述经加密的第二随机数和第一散列进行解密，验证所述第一散列以便认证所述数字版权代理并且确定所述数字版权代理知道所述第一随机数，根据至少所述第二随机数生成第二散列并向所述数字版权代理发送所述第二散列 ；以及

用于促使所述数字版权代理验证所述第二散列以便认证所述安全可移动媒体设备并且确定所述安全可移动媒体设备知道所述第二随机数的模块。

21. 一种用于进行双向认证的装置，包括 ：

用于促使安全可移动媒体设备验证与数字版权代理相关的第一公钥、生成第一随机数、使用所述第一公钥对所述第一随机数进行加密并在消息中向所述数字版权代理发送经加密的第一随机数的模块，其中，从所述安全可移动媒体设备向所述数字版权代理发送的具有所述经加密的第一随机数的所述消息还包括所述安全可移动媒体设备的证书链，其中，所述数字版权代理通过向所述安全可移动媒体设备发送消息来发起双向认证，其中，发起双向认证的所述消息包括具有至少一个信任根密钥的散列和对应的所述数字版权代理的证书链，并且其中，所述数字版权代理验证与所述安全可移动媒体设备相关联的第二公钥，使用对应于所述第一公钥的第一私钥对所述经加密的第一随机数进行解密，生成第二随机数，根据至少所述第一随机数生成第一散列，使用所述第二公钥对所述第二随机数和

所述第一散列进行加密，并在消息中向所述安全可移动媒体设备发送经加密的第二随机数和第一散列；

用于促使所述安全可移动媒体设备使用对应于所述第二公钥的第二私钥对所述经加密的第二随机数和第一散列进行解密、验证所述第一散列以便认证所述数字版权代理并且确定所述数字版权代理知道所述第一随机数、根据至少所述第二随机数生成第二散列并向所述数字版权代理发送所述第二散列的模块，其中，所述数字版权代理验证所述第二散列以便认证所述安全可移动媒体设备并且确定所述安全可移动媒体设备知道所述第二随机数。

用于双向认证的方法和装置

[0001] 基于 35U.S.C.S.119 要求优先权

[0002] 本专利申请要求 2006 年 10 月 10 日递交的、名称为“METHODS ANDAPPARATUS FOR MUTUAL AUTHENTICATION”的临时申请 No.60/850,882 的优先权。该临时申请已经转让给本申请的受让人，故以引用方式将其明确地并入本文。

技术领域

[0003] 概括地说，本发明涉及无线通信，具体地说，本发明涉及双向认证。

背景技术

[0004] 移动用户可能想要访问由需要与另一实体或代理进行认证的系统所保护的内容。通用的认证协议是 RFC 4306 中描述的因特网密钥交换 (IKE) 协议。然而，IKE 协议假设认证过程中的实体具有足够的计算或处理能力，以至于不需要担心认证的速度。

[0005] 因此，在本领域存在对以下技术的需求，即与具有有限处理能力的设备进行高效双向认证的技术。

发明内容

[0006] 本发明的一方面涉及一种在第一实体和第二实体之间进行双向认证的方法。在该方法中，第一实体通过向第二实体发送消息来发起双向认证。第二实体对与第一实体相关联的第一公钥进行验证，生成第一随机数，使用第一公钥对第一随机数进行加密并在消息中向第一实体发送经加密的第一随机数。第一实体对与第二实体相关联的第二公钥进行验证，使用对应于第一公钥的第一私钥对经加密的第一随机数进行解密，生成第二随机数，根据至少第一随机数生成第一散列，使用第二公钥对第二随机数和第一散列进行加密，并在消息中向第二实体发送经加密的第二随机数和第一散列。第二实体使用对应于第二公钥的第二私钥对经加密的第二随机数和第一散列进行解密，验证第一散列以便认证第一实体，根据至少第二随机数生成第二散列，并将第二散列发送到第一实体。第一实体验证第二散列以便认证第二实体。

[0007] 在本发明的更详细方面，第一实体和第二实体都根据密钥导出函数使用第一随机数和第二随机数导出会话加密密钥和消息认证码 (MAC) 密钥，以便在第一实体和第二实体之间的通信中使用。

[0008] 此外，发起双向认证的消息可以包括至少一个信任根密钥的散列和对应的第一实体的证书链。第一实体的证书链可以包括与第一实体相关联的公钥。同样，从第二实体到第一实体的具有经加密的第一随机数的消息还可以包括第二实体的证书链。第二实体的证书链可以包括与第二实体相关联的公钥。

[0009] 在本发明其它更详细的方面中，第一实体可以是移动站的数字版权代理，并且第二实体可以是安全可移动媒体设备。第二实体可以具有有限的处理能力。并且，第一散列可以进一步基于第二随机数，从而第一散列是根据与第二随机数级连的第一随机数生成的。

第二散列可以进一步基于第一随机数，或者进一步基于第一散列，从而第二散列可以基于与第一散列相级连的第二随机数。

[0010] 本发明的另一方面可以涉及用于双向认证的装置，该装置包括用于发起双向认证的模块，用于验证第一公钥、生成第一随机数并使用第一公钥对第一随机数进行加密的模块，用于验证第二公钥、使用对应于第一公钥的第一私钥对经加密的第一随机数进行解密、生成第二随机数、根据至少第一随机数生成第一散列以及使用第二公钥对第二随机数和第一散列进行加密的模块，用于使用对应于第二公钥的第二私钥对经加密的第二随机数和第一散列进行解密、验证第一散列用于认证以及根据至少第二随机数生成第二散列的模块，以及用于验证第二散列以用于认证的模块。

[0011] 本发明的另一方面可以涉及与安全可移动媒体设备进行双向认证的移动站，该移动站包括数字版权代理。数字版权代理通过向安全可移动媒体设备发送消息来发起双向认证，其中安全可移动媒体设备验证与数字版权代理相关联的第一公钥，生成第一随机数，使用第一公钥对第一随机数进行加密，并在消息中向数字版权代理发送经加密的第一随机数。数字版权代理验证与安全可移动媒体设备相关联的第二公钥，使用对应于第一公钥的第一私钥对经加密的第一随机数进行解密，生成第二随机数，根据至少第一随机数生成第一散列，使用第二公钥对第二随机数和第一散列进行加密，并在消息中向安全可移动媒体设备发送经加密的第二随机数和第一散列，其中，安全可移动媒体设备使用对应第二公钥的第二私钥对经加密的第二随机数和第一散列进行解密，验证第一散列以便认证数字版权代理，根据至少第二随机数生成第二散列，并向数字版权代理发送第二散列。数字版权代理验证第二散列，以便认证安全可移动媒体设备。

[0012] 本发明的另一方面涉及一种包括计算机可读介质的计算机程序产品，该计算机可读介质包括：用于使计算机促使具有数字版权代理的站通过向安全可移动媒体设备发送消息而发起双向认证的代码，其中安全可移动媒体设备验证与数字版权代理相关联的第一公钥，生成第一随机数，使用第一公钥对第一随机数进行加密，并在消息中向数字版权代理发送经加密的第一随机数；用于使计算机促使数字版权代理验证与安全可移动媒体设备相关联的第二公钥、使用对应于第一公钥的第一私钥对经加密的第一随机数进行解密、生成第二随机数、根据至少第一随机数生成第一散列、使用第二公钥对第二随机数和第一散列进行加密并在消息中向安全可移动媒体设备发送经加密的第二随机数和第一散列的代码，其中安全可移动媒体设备使用对应于第二公钥的第二私钥对经加密的第二随机数和第一散列进行解密，验证第一散列以便认证数字版权代理，根据至少第二随机数生成第二散列，并向数字版权代理发送第二散列；以及使计算机促使数字版权代理验证第二散列以便认证安全可移动媒体设备的代码。

[0013] 本发明的另一方面可以涉及一种包括计算机可读介质的计算机程序产品，该计算机可读介质包括：用于使计算机促使安全可移动媒体设备验证与数字版权代理相关联的第一公钥、生成第一随机数、使用第一公钥对第一随机数进行加密并在消息中向数字版权代理发送经加密的第一随机数的代码，其中，数字版权代理验证与安全可移动媒体设备相关联的第二公钥，使用对应于第一公钥的第一私钥对经加密的第一随机数进行解密，生成第二随机数，根据至少第一随机数生成第一散列，使用第二公钥对第二随机数和第一散列进行加密，并在消息中向安全可移动媒体设备发送经加密的第二随机数和第一散列；使计算

机促使安全可移动媒体设备使用对应于第二公钥的第二私钥对经加密的第二随机数和第一散列进行解密、验证第一散列以便认证数字版权代理、根据至少第二随机数生成第二散列并向数字版权代理发送第二散列的代码，其中数字版权代理验证第二散列以便认证安全可移动媒体设备。

附图说明

[0014] 图 1 为无线通信系统的例子；

[0015] 图 2 为进行双向认证的移动站和安全可移动媒体设备的方框图；

[0016] 图 3 为在移动站和安全可移动媒体设备之间进行双向认证的方法的流程图。

具体实施方式

[0017] 本申请中提到的“示例性”一词是指“举一个例子、实例或作为说明”。本申请中描述为“示例性”的任何实施例不应被理解为比其它实施例更优选或更具优势。

[0018] 远程站（也称为移动站 (MS)、接入终端 (AT)、用户设备或用户单元）可以是移动的或固定的，并可以与一个或多个基站（也称为基站收发机 (BTS) 或节点 B) 进行通信。远程站通过一个或多个基站向基站控制器（也称为无线网络控制器 (RNC)）发送并从基站控制器接收数据分组。基站和基站控制器是被称为接入网的网络的一部分。接入网在多个远程站之间传输数据分组。接入网可进一步连接到接入网外部的其它网络（诸如企业内联网或因特网），并在每个远程站和这些外部网络之间传输数据分组。与一个或多个基站建立了激活的业务信道连接的远程站称为激活的远程站，并称为处于业务状态。处于与一个或多个基站建立激活业务信道连接的过程中的远程站称为处于连接建立状态。远程站可以是通过无线信道进行通信的任意数据设备。远程站还可以是多种类型的设备中的任意一种设备，包括但不局限于 PC 卡、紧凑式闪存、外部或内部调制解调器或无绳电话。远程站向基站发送信号的通信链路称为上行链路，也称为反向链路。基站向远程站发送信号的通信链路称为下行链路，也称为前向链路。

[0019] 参照图 2，无线通信系统 100 包括一个或多个无线移动站 (MS)102、一个或多个基站 (BS)104、一个或多个基站控制器 (BSC)106 以及核心网络 108。核心网络通过合适的回程 (backhauls) 连接到因特网 110 和公共交换电话网 (PSTN)112。典型的无线移动站包括手持电话或膝上型计算机。无线通信系统 100 可以使用多种接入技术中的任意一种，诸如码分多址 (CDMA)、时分多址 (TDMA)、频分多址 (FDMA)、空分多址 (SDMA)、极分多址 (PDMA) 或本领域公知的其它调制技术。

[0020] 多种具有有限计算能力的低成本设备（以多种不同的形式特征）出现在市场中，诸如智能卡和闪存。这种设备可能需要认证。例如，希望这些设备保持有与数字版权管理 (DRM) 系统一起使用的权利。在与这些设备交换权利之前，应该存在与交换相关的双方实体的双向认证，用以将交换限制在经认证的实体中。这些实施例提供了一种完成双向认证的高效方法，并且也提供了经确认的密钥交换，该密钥进一步用于相关实体之间的通信。高效体现在计算能力和计算速度上。

[0021] 本领域的技术人员能够看出，可以在两个实体之间请求双向认证的任何时间使用双向认证方案。双向认证方案不局限于本文中用于描述实施例的特定方法（诸如数字版权

管理）、系统和设备。

[0022] 本发明的一个实施例通过使用 4 个消息的交换来利用经确认的密钥交换进行双向认证。这需要 2 次公钥签名验证（每次中间确认 +1）、2 次公钥加密、2 次公钥解密、2 次散列生成以及 2 次散列验证。特定数量的消息交换、公钥验证、公钥解密、散列生成以及散列验证可以进行分解或改变，以便达到所需数量的安全性和效率。

[0023] 通过对公钥密码运算进行最小化并使用散列函数提供对交换的密钥材料的拥有证明，来提高协议的效率。

[0024] 上文描述的高效双向认证和经确认的密钥交换协议与受计算限制的设备一起使用。所述的高效是通过对公钥运算的次数进行最小化并使用加密散列提供拥有证明来实现的。

[0025] 参照图 2 和 3 所示的双向认证的方法 300（图 3）来说明该协议。下文中的步骤对应于图 3 中编号的箭头。

[0026] 在方法 300 中，实体 A（例如，MS 102 的 DRM 代理 202）向实体 B（例如，具有 SRM 代理 206 的安全可移动媒体 (SRM) 设备 204）发送 HelloA 消息（步骤 302）。SRM 代理管理对 SRM 设备中的安全存储器 208 的访问。(MS 的操作系统 210 可直接访问 SRM 设备的普通存储器 212。)HelloA 包括信任根密钥的散列（或根密钥自身）以及对应的证书链。接收这一消息之后，实体 B 从这一消息中找到它所信任的根密钥并根据选择的根密钥找到证书链。实体 B 根据选择的根密钥验证实体 A 的证书链。

[0027] 实体 B 生成随机数 RanB（步骤 304）。

[0028] 实体 B 向实体 A 发送 HelloB 消息（步骤 306）。HelloB 包括根据选择的根密钥的 B 的证书链以及由实体 A 的公钥加密的随机数 B，由实体 A 的公钥从步骤 302 之后选择的证书链中获得。接收这一消息之后，实体 A 验证实体 B 的证书链。如果正确，则使用其私钥（对应于选择的根密钥）对随机数 B 进行解密。

[0029] 注意到，一旦进行了根密钥选择和证书链交换，实体 A 和实体 B 就具有彼此的证书链。从而，就不需要在后续 HelloA 和 HelloB 消息中在实体 A 与实体 B 之间发送这些参数来用于之后的双向认证。在这种情况下，步骤 302 和 306 中的证书链交换是可选择的。

[0030] 实体 A 生成随机数 RanA（步骤 308）。

[0031] 实体 A 向实体 B 发送密钥确认 A(KeyConfirmA) 消息（步骤 310）。密钥确认 A 包括随机数 A，随机数 A 与随机数 B 和随机数 A 的级连的散列 (H[随机数 A| 随机数 B]) 相级连，并且上述的全部内容由 B 的公钥进行加密。接收这一消息之后，实体 B 对其进行解密。使用经解密的随机数 A，实体 B 验证随机数 B 与随机数 A 相级连的散列。注意 :在这一步骤，实体 B 认证了实体 A，并确定实体 A 知道随机数 B。

[0032] 实体 B 向实体 A 发送密钥确认 B(KeyConfirmB) 消息（步骤 312）。密钥确认 B 包括密钥确认 A 消息经解密的部分的散列。接收到这一消息之后，实体 A 验证这一散列。注意 :在这一步，实体 A 认证了实体 B，并确定实体 B 知道随机数 A。

[0033] 这时，两个实体已经相互认证，并确认它们都共用相同的随机数 A 和随机数 B。现在，可使用随机数 A 和随机数 B 根据密钥导出函数 (KDF) 推导出会话加密密钥 (SK) 以及 MAC 密钥 (MK)，以用于实体间后续的通信（步骤 314）。

[0034] 下文中将给出各个消息的详细说明。发送 HelloA 消息以使用密钥确认协议发起

双向认证。Hello A 具有“版本”参数和“根与链 [](rootAndChains[])”参数。版本参数可以是包括这一消息的协议版本的 8 比特值。将其映射为 5 个 MSB 用于主版本，3 个 LSB 用于次版本。根与链 [] 参数可以是 A 所支持的所有信任模型的实体 A 的根散列和证书链的阵列。参数的结构——根散列和证书链 (RootHashAndCerChain) 是参数根散列以及参数证书链，参数根散列是信任模型的根公钥的 SHA-1 散列，参数证书链是根公钥的实体的证书链。首先是实体的证书，后面是任意 CA 证书（以信令的顺序），直到但不包括根证书。

[0035] HelloB 消息由实体 B 利用密钥确认协议继续进行双向认证。下面描述各个参数。HelloB 的参数有 :“版本”、“状态”、“证书链”和“加密随机数 B”。版本参数可以是包括这一消息的协议版本的 8 比特值。将其映射为 5 个 MSB 用于主版本，3 个 LSB 用于次版本。状态参数可以是包括处理 HelloA 消息的实体 B 的状态的 8 比特值。状态参数的值可以是 :0 用于成功 - 以往的消息中没有遇到错误，而 1 用于无共用根密钥 - 实体 B 没有找到与实体 A 共用的根密钥。值 2-255 保留作为其它用途。证书链参数是根据从 HelloA 消息中选择的根密钥的实体 B 的证书链。如果状态参数的值不是成功，则证书链参数不体现。加密随机数 B 参数是使用实体 A 的公钥（来自所选择的证书链）的 RSA-OAEP 加密的随机数 B。随机数 B 可以是由实体 B 生成的 20 个字节的随机数。如果状态的值不是成功，则加密随机数 B 参数不体现。

[0036] 密钥确认 A 消息由实体 A 利用密钥确认协议继续进行双向认证。密钥确认 A 消息具有“版本”参数和“加密随机数 B”参数。版本参数可以是包括这一消息的协议版本的 8 比特值。将其映射为 5 个 MSB 用于主版本，3 个 LSB 用于次版本。加密随机数 B 参数可以是 RSA-OAEP 加密的密钥确认数据结构，包括“随机数 A”参数和“散列 BA”参数。随机数 A 参数可以是由实体 A 生成的 20 个字节的随机数，散列 BA 参数是随机数 B 与随机数 A 相级联的 SHA-1 散列。

[0037] 密钥确认 B 消息由实体 B 利用密钥确认协议结束双向认证。密钥确认 B 消息具有“版本”参数、状态参数和“散列密钥确认”参数。版本参数可以是包括这一消息的协议版本的 8 比特值。将其映射为 5 个 MSB 用于主版本，3 个 LSB 用于次版本。状态参数可以是包括处理该消息的实体 B 的状态的 8 比特值。散列密钥确认参数可以是由实体 B 解密的密钥确认数据结构的 SHA-1 散列。如果状态参数的值不是成功，则这个参数不体现。

[0038] 本发明的另一方面可以涉及包括控制处理器 216 和 OS 210 的移动站 102，控制处理器 216 和 OS 210 用于使 DRM 代理 202 实现方法 300。本发明的另一方面可以涉及一种包括计算机可读介质（诸如存储设备 218）的计算机程序产品，该计算机可读介质包括用于使计算机促使 DRM 代理执行方法 300 的步骤的代码。

[0039] 本领域技术人员应当理解，信息和信号可以使用多种不同的技术和方法来表示。例如，在贯穿上面的描述中所提及的数据、指令、命令、信息、信号、比特、符号和码片可以用电压、电流、电磁波、磁场或磁性粒子、光场或光粒子或者其任意组合来表示。

[0040] 本领域技术人员还应当明白，结合本申请的实施例描述的各种示例性的逻辑块、模块、电路和算法步骤均可以实现成电子硬件、计算机软件或其组合。为了清楚地表示硬件和软件之间的这种可互换性，上面对各种示例性的部件、块、模块、电路和步骤均围绕其功能进行了总体描述。至于这种功能是实现成硬件还是实现成软件，取决于特定的应用和对整个系统所施加的设计约束。熟练的技术人员可以针对每个特定应用，以变通的方式实现

所描述的功能，但是，这种实现决策不应解释为背离本发明的保护范围。

[0041] 用于执行本申请所述功能的通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑器件、分立门或者晶体管逻辑、分立硬件组件或者其任意组合，可以实现或执行结合本申请的实施例所描述的各种示例性的逻辑块、模块和电路。通用处理器可以是微处理器，或者可替换地，该处理器也可以是任何常规的处理器、控制器、微控制器或者状态机。处理器也可以实现为计算设备的组合，例如，DSP 和微处理器的组合、多个微处理器、一个或多个微处理器与 DSP 内核的结合，或者任何其它此种构成。

[0042] 结合本申请的实施例所描述的方法或者算法的步骤可直接体现为硬件、由处理器执行的软件模块或其组合。软件模块可以位于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、移动磁盘、CD-ROM 或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质连接至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。可替换地，存储介质也可以集成到处理器中。处理器和存储介质可以位于 ASIC 中。该 ASIC 可以位于用户终端中。当然，处理器和存储介质也可以作为分立组件存在于用户终端中。

[0043] 在一个或多个示例实施例中，所描述的功能可以实现为硬件、软件、固件或它们的任何组合。当作为计算机程序产品以软件实现时，该功能可以作为一个或多个指令或代码存储计算机可读介质上或者通过其进行传输。计算机可读介质包括计算机存储介质和通信介质，包括任何便于将计算机程序从一个地方转移到另一个地方的介质。存储介质可以是计算机能够访问的任何可用介质。举例但非限制地来说，这样的计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储器、磁盘存储器或其它磁存储设备，或者能够用于以指令或数据结构的形式携带或存储所需程序代码并能够由计算机访问的任何其它介质。而且，任何连接都可以适当地称为计算机可读介质。举个例子，如果用同轴电缆、纤维光缆、双绞线、数字用户线路 (DSL)，或诸如红外、无线和微波之类的无线技术，从网站、服务器或其它远程源传输软件，则该同轴电缆、纤维光缆、双绞线、DSL，或诸如红外、无线和微波之类的无线技术也包含在介质的定义中。本申请所用的磁盘和盘，包括压缩盘 (CD)、镭射光盘、光盘、数字多用途光盘 (DVD)、软盘和蓝光盘，其中磁盘通常通过磁性再现数据，而光盘通过激光光学地再现数据。上述的组合也包括在计算机可读介质的范围内。

[0044] 为使本领域技术人员能够实现或者使用本发明，上面提供了对本发明实施例的描述。对于本领域技术人员来说，对这些实施例的各种修改都是显而易见的，并且，本申请定义的一般原理也可以在不脱离本发明的精神和范围的基础上适用于其它实施例。因此，本发明并不限于本申请给出的实施例，而是与本申请公开的原理和新颖性特征的最广范围相一致。

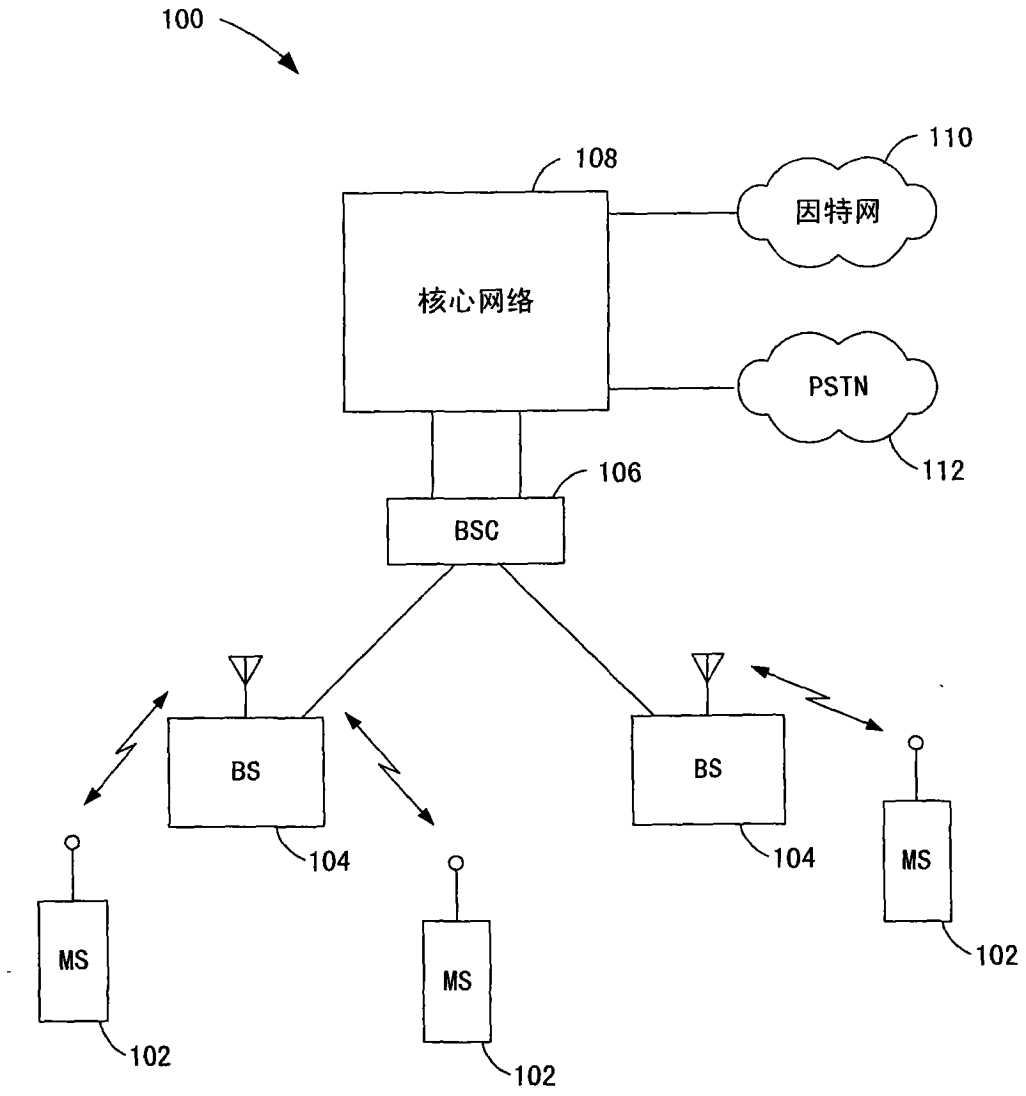

100
108
110
因特网
核心网络
PSTN
112
106
BSC
BS
BS
104
104
MS
MS
MS
102
102
102

图 1

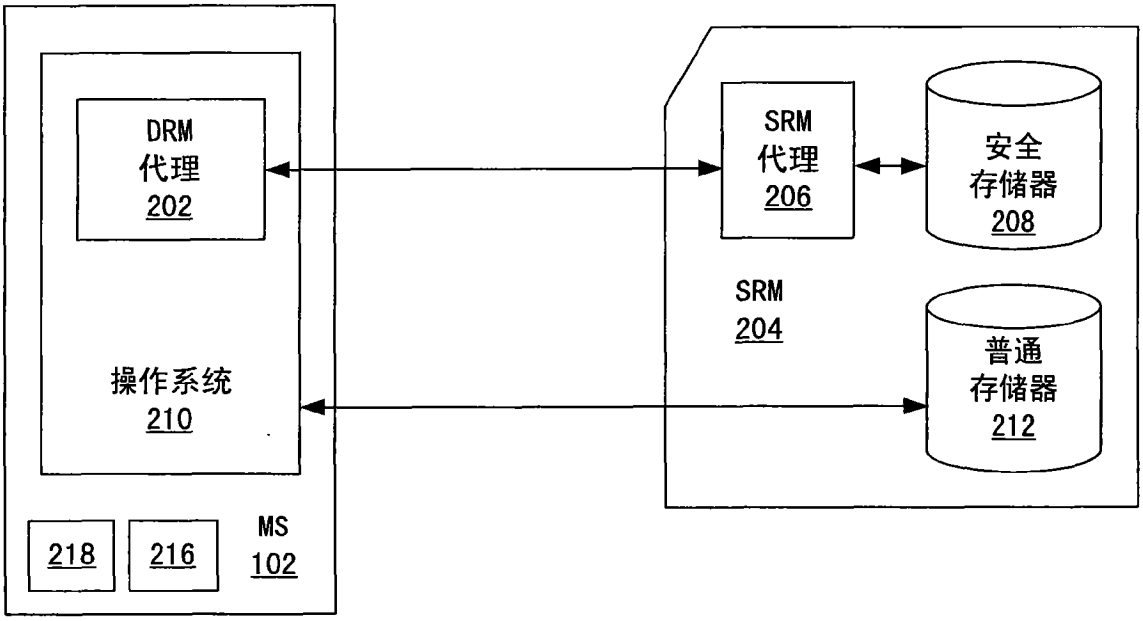

DRM
代理
202
操作系统
210
218
216
MS
102
SRM
代理
206
安全
存储器
208
SRM
204
普通
存储器
212

图 2

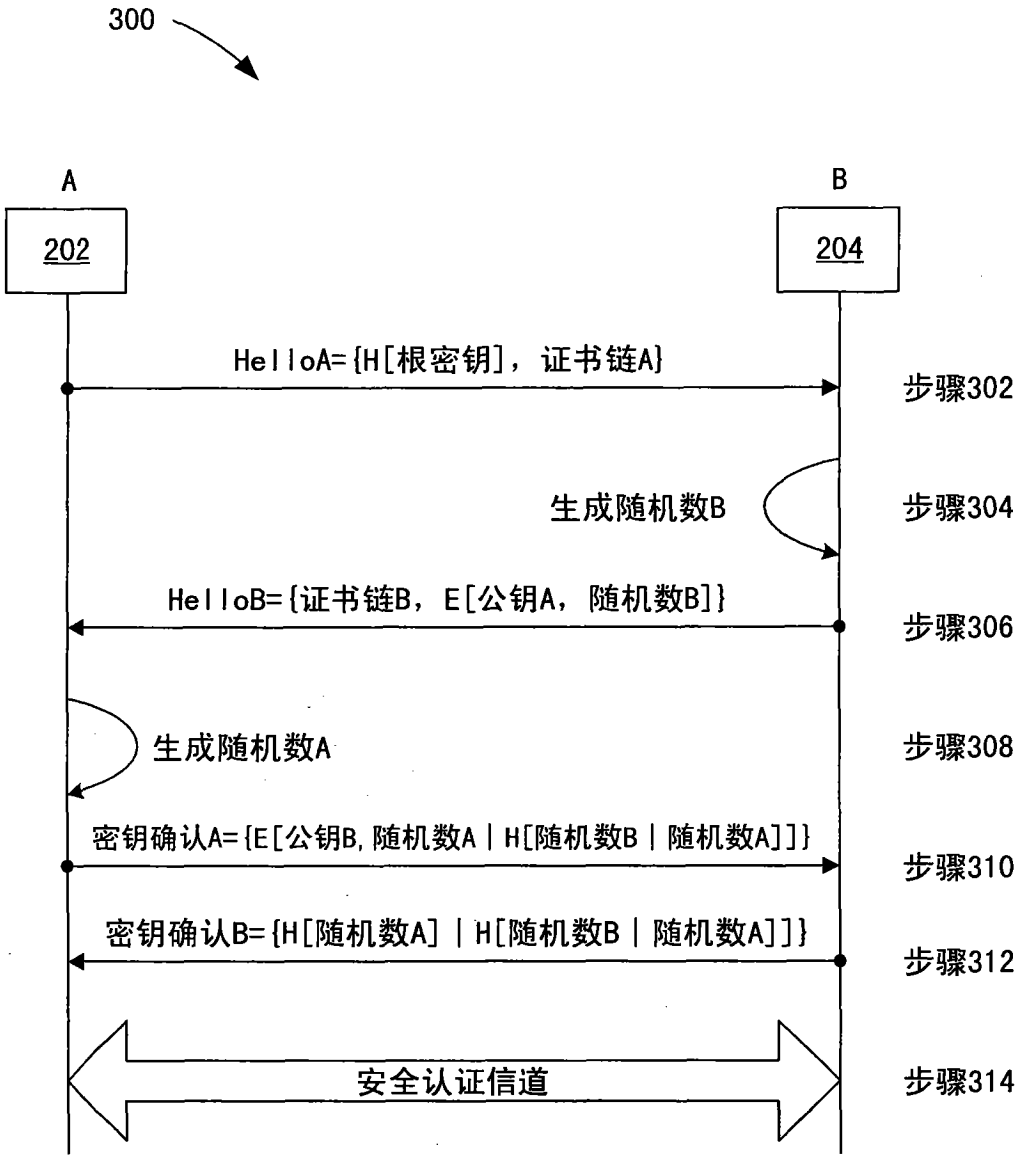

300
A
202
B
204
HelloA={H[根密钥]，证书链A}
步骤302
生成随机数B
步骤304
HelloB={证书链B，E[公钥A，随机数B]}
步骤306
生成随机数A
步骤308
密钥确认A={E[公钥B,随机数A | H[随机数B | 随机数A]]}
步骤310
密钥确认B={H[随机数A] | H[随机数B | 随机数A]]}
步骤312
安全认证信道
步骤314

图 3