(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 108900552 B
(45)授权公告日 2019.10.15

(21)申请号 201810935188.7

(22)申请日 2018.08.16

(65)同一申请的已公布的文献号
申请公布号 CN 108900552 A

(43)申请公布日 2018.11.27

(73)专利权人 北京海泰方圆科技股份有限公司
地址 100094 北京市海淀区东北旺西路8号中关村软件园9号楼国际软件大厦E座一层、二层

(72)发明人 安晓江 李鹏坤 胡伯良

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 赵囡囡 董文倩

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04L 9/08(2006.01)

(56)对比文件
CN 101568110 A,2009.10.28,
CN 104038930 A,2014.09.10,
CN 101383698 A,2009.03.11,
CN 107483388 A,2017.12.15,
CN 101056171 A,2007.10.17,
CN 107533623 A,2018.01.02,

审查员 蔡红

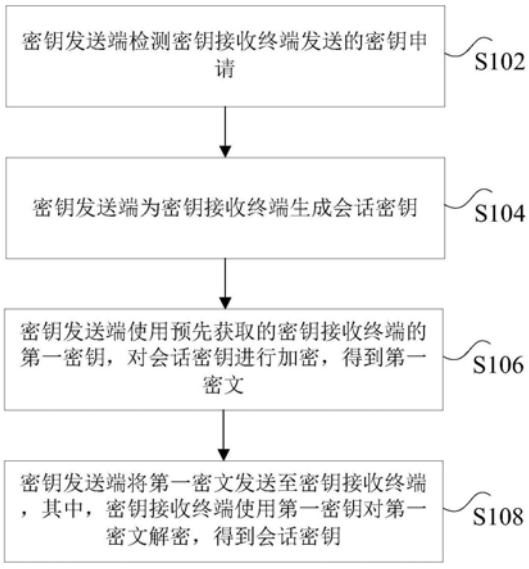
权利要求书3页 说明书8页 附图3页

(54)发明名称

密钥分发方法和装置、密钥获取方法和装置

(57)摘要

本发明公开了一种密钥分发方法和装置、密钥获取方法和装置。其中，该方法包括：密钥发送端检测所述密钥接收终端发送的密钥申请；所述密钥发送端为所述密钥接收终端生成会话密钥；所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥，对所述会话密钥进行加密，得到第一密文；所述密钥发送端将所述第一密文发送至所述密钥接收终端，其中，所述密钥接收终端使用所述第一密钥对所述第一密文解密，得到所述会话密钥。本发明解决了现有技术中的密钥分发的过程较复杂的技术问题。



CN 108900552 B

1.一种密钥分发方法,其特征在于,包括:

密钥发送端检测密钥接收终端发送的密钥申请;

所述密钥发送端为所述密钥接收终端生成会话密钥;

所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥,对所述会话密钥进行加密,得到第一密文,其中,密钥接收终端的第一密钥是密钥接收终端生成的第一密钥;

所述密钥发送端将所述第一密文发送至所述密钥接收终端,其中,所述密钥接收终端使用所述第一密钥对所述第一密文解密,得到所述会话密钥;

在密钥发送端检测所述密钥接收终端发送的密钥申请之前,所述方法还包括:

所述密钥发送端接收所述密钥接收终端的密钥信息,其中,所述密钥信息由所述密钥接收终端的第一密钥和所述密钥接收终端的终端标识构成;

所述密钥发送端使用本地的第二密钥对所述第一密钥加密,得到第二密文,其中,所述密钥发送端本地的第二密钥是所述密钥发送端所单独持有的,用于对所述密钥接收终端的所述第一密钥进行加密保存;

所述密钥发送端将所述第二密文与所述终端标识对应存储;

所述密钥发送端接收所述密钥接收终端的密钥信息,包括:

所述密钥发送端接收密钥分发应用通过HTTPS安全连接发送的所述密钥信息,其中,所述密钥分发应用通过扫描所述密钥接收终端根据所述第一密钥和所述终端标识生成的二维码,得到所述密钥信息。

2.根据权利要求1所述的方法,其特征在于,所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥,对所述会话密钥进行加密,得到第一密文,包括:

所述密钥发送端从所述密钥申请中获取所述密钥接收终端的终端标识;

所述密钥发送端根据所述终端标识查找所述密钥接收终端对应的第二密文;

所述密钥发送端使用所述第二密钥解密所述第二密文,得到所述第一密钥;

所述密钥发送端使用所述第一密钥对所述会话密钥和所述终端标识进行加密,得到所述第一密文。

3.一种密钥获取方法,其特征在于,包括:

密钥接收终端向密钥发送端发送密钥申请;

所述密钥接收终端接收所述密钥发送端返回的第一密文,其中,所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥,对为所述密钥接收终端生成的会话密钥进行加密,得到第一密文,其中,密钥接收终端的第一密钥是密钥接收终端生成的第一密钥;

所述密钥接收终端使用所述第一密钥解密所述第一密文,得到所述会话密钥;

在所述密钥接收终端向所述密钥发送端发送密钥申请之前,所述方法还包括:

所述密钥接收终端生成第一密钥;

所述密钥接收终端根据所述第一密钥和所述密钥接收终端的终端标识生成密钥信息;

所述密钥接收终端将所述密钥信息发送至所述密钥发送端,所述密钥发送端使用本地的第二密钥对所述第一密钥加密,得到第二密文,其中,所述密钥发送端本地的第二密钥是所述密钥发送端所单独持有的,用于对所述密钥接收终端的所述第一密钥进行加密保存;

在所述密钥接收终端根据所述第一密钥和所述密钥接收终端的终端标识生成密钥信息之后,所述方法还包括:

所述密钥接收终端根据所述密钥信息生成二维码，其中，由密钥分发应用通过扫描所述二维码，并将扫描结果通过HTTPS安全连接发送至所述密钥发送端。

4.根据权利要求3所述的方法，其特征在于，所述密钥发送端使用第一密钥，对所述会话密钥和所述密钥接收终端的终端标识进行加密，得到所述第一密文，所述密钥接收终端使用所述第一密钥解密所述第一密文，得到所述会话密钥，包括：

所述密钥接收终端使用所述第一密钥解密所述第一密文，得到所述会话密钥和所述密钥接收终端的终端标识；

对所述第一密钥中的终端标识进行验证；

如果验证通过，保存所述会话密钥。

5.一种密钥分发装置，其特征在于，包括：

检测模块，用于密钥发送端检测密钥接收终端发送的密钥申请；

生成模块，用于所述密钥发送端为所述密钥接收终端生成会话密钥；

第一接收模块，用于所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥，对所述会话密钥进行加密，得到第一密文，其中，密钥接收终端的第一密钥是密钥接收终端生成的第一密钥；

第一发送模块，用于所述密钥发送端将所述第一密文发送至所述密钥接收终端，其中，所述密钥接收终端使用所述第一密钥对所述第一密文解密，得到所述会话密钥；

所述装置还包括：

第三接收模块，用于在密钥发送端检测所述密钥接收终端发送的密钥申请之前，所述密钥发送端接收所述密钥接收终端的密钥信息，其中，所述密钥信息由所述密钥接收终端的第一密钥和所述密钥接收终端的终端标识构成；

加密模块，用于所述密钥发送端使用本地的第二密钥对所述第一密钥加密，得到第二密文，其中，所述密钥发送端本地的第二密钥是所述密钥发送端所单独持有的，用于对所述密钥接收终端的所述第一密钥进行加密保存；

存储模块，用于所述密钥发送端将所述第二密文与所述终端标识对应存储；

所述第三接收模块包括：发送子模块，用于所述密钥发送端接收密钥分发应用通过HTTPS安全连接发送的所述密钥信息，其中，所述密钥分发应用通过扫描所述密钥接收终端根据所述第一密钥和所述终端标识生成的二维码，得到所述密钥信息。

6.一种密钥获取装置，其特征在于，包括：

第一发送模块，用于密钥接收终端向密钥发送端发送密钥申请；

第二接收模块，用于所述密钥接收终端接收所述密钥发送端返回的第一密文，其中，所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥，对为所述密钥接收终端生成的会话密钥进行加密，得到第一密文，其中，密钥接收终端的第一密钥是密钥接收终端生成的第一密钥；

解密模块，用于所述密钥接收终端使用所述第一密钥解密所述第一密文，得到所述会话密钥；

所述装置还包括：

第四接收模块，用于在所述密钥接收终端向所述密钥发送端发送密钥申请之前，所述密钥接收终端生成第一密钥；

第一生成模块，用于所述密钥接收终端根据所述第一密钥和所述密钥接收终端的终端标识生成密钥信息；

第二发送模块，用于所述密钥接收终端将所述密钥信息发送至所述密钥发送端，所述密钥发送端使用本地的第二密钥对所述第一密钥加密，得到第二密文，其中，所述密钥发送端本地的第二密钥是所述密钥发送端所单独持有的，用于对所述密钥接收终端的所述第一密钥进行加密保存；

所述装置还包括：第二生成模块，用于所述密钥接收终端根据密钥信息生成二维码，其中，由密钥分发应用通过扫描二维码，并将扫描结果通过HTTPS安全连接发送至所述密钥发送端。

7.一种存储介质，其特征在于，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行权利要求1至2中任意一项所述的密钥分发方法或权利要求3至4中任意一项所述的密钥获取方法。

8.一种处理器，其特征在于，所述处理器用于运行程序，其中，所述程序运行时执行权利要求1至2中任意一项所述的密钥分发方法或权利要求3至4中任意一项所述的密钥获取方法。

密钥分发方法和装置、密钥获取方法和装置

技术领域

[0001] 本发明涉及数据处理领域，具体而言，涉及一种密钥分发方法和装置、密钥获取方法和装置。

背景技术

[0002] 为了保证通信安全，通常在两个设备通信前，会进行密钥分发，即生成密钥的一方将生成的密钥分发给另一方，从而用于后续的通信。

[0003] 目前，密钥分发主要有两种方式，一种是离线密钥分发，一种是在线密钥分发。离线密钥分发一般通过光盘或者其它存储介质手动进行密钥分发，不便于大规模实施。

[0004] 在线密钥分发通过网络进行密钥分发，为了保证密钥的安全性，分发过程会对密钥进行加密，加密所使用的密钥一般通过使用证书协商获得。也即，通过证书进行密钥协商的在线密钥分发，首先需要预先为每个终端生成一张证书以及对应的密钥，因此需要额外再部署一套证书发放系统，大规模的证书发放具有较大的实施难度。

[0005] 针对现有技术中的密钥分发的过程较复杂的问题，目前尚未提出有效的解决方案。

发明内容

[0006] 本发明实施例提供了一种密钥分发方法和装置、密钥获取方法和装置，以至少解决现有技术中的密钥分发的过程较复杂的技术问题。

[0007] 根据本发明实施例的一个方面，提供了一种密钥分发方法，包括：密钥发送端检测密钥接收终端发送的密钥申请；密钥发送端为密钥接收终端生成会话密钥；密钥发送端使用预先获取的密钥接收终端的第一密钥，对会话密钥进行加密，得到第一密文；密钥发送端将第一密文发送至密钥接收终端，其中，密钥接收终端使用第一密钥对第一密文解密，得到会话密钥。

[0008] 进一步地，在密钥发送端检测密钥接收终端发送的密钥申请之前，密钥发送端接收密钥接收终端的密钥信息，其中，密钥信息由密钥接收终端的第一密钥和密钥接收终端的终端标识构成；密钥发送端使用本地的第二密钥对第一密钥加密，得到第二密文；密钥发送端将第二密文与终端标识对应存储。

[0009] 进一步地，密钥发送端从密钥申请中获取密钥接收终端的终端标识；密钥发送端根据终端标识查找密钥接收终端对应的第二密文；密钥发送端使用第二密钥解密第二密文，得到第一密钥；密钥发送端使用第一密钥对会话密钥和终端标识进行加密，得到第一密文。

[0010] 进一步地，密钥发送端接收密钥分发应用发送的密钥信息，其中，密钥分发应用通过扫描密钥接收终端根据第一密钥和终端标识生成的二维码，得到密钥信息。

[0011] 根据本发明实施例的一个方面，提供了一种密钥获取方法，密钥接收终端向密钥发送端发送密钥申请；密钥接收终端接收密钥发送端返回的第一密文，其中，密钥发送端使

用预先获取的密钥接收终端的第一密钥，对为密钥接收终端生成的会话密钥进行加密，得到第一密文；密钥接收终端使用第一密钥解密第一密文，得到会话密钥。

[0012] 进一步地，密钥发送端使用第一密钥，对会话密钥和密钥接收终端的终端标识进行加密，得到第一密文，密钥接收终端使用第一密钥解密第一密文，得到会话密钥和密钥接收终端的终端标识；对第一密钥中的终端标识进行验证；如果验证通过，保存会话密钥。

[0013] 进一步地，在密钥接收终端向密钥发送端发送密钥申请之前，密钥接收终端生成第一密钥；密钥接收终端根据第一密钥和密钥接收终端的终端标识生成密钥信息；根据密钥信息生成二维码，其中，由密钥分发应用通过扫描二维码，并将扫描结果发送至密钥发送端。

[0014] 根据本发明实施例的一个方面，提供了一种密钥分发装置，检测模块，用于密钥发送端检测密钥接收终端发送的密钥申请；生成模块，用于密钥发送端为密钥接收终端生成会话密钥；第一接收模块，用于密钥发送端使用预先获取的密钥接收终端的第一密钥，对会话密钥进行加密，得到第一密文；第一发送模块，用于密钥发送端将第一密文发送至密钥接收终端，其中，密钥接收终端使用第一密钥对第一密文解密，得到会话密钥。

[0015] 根据本发明实施例的一个方面，提供了一种密钥获取装置，第一发送模块，用于密钥接收终端向密钥发送端发送密钥申请；第二接收模块，用于密钥接收终端接收密钥发送端返回的第一密文，其中，密钥发送端使用预先获取的密钥接收终端的第一密钥，对为密钥接收终端生成的会话密钥进行加密，得到第一密文；解密模块，用于密钥接收终端使用第一密钥解密第一密文，得到会话密钥。

[0016] 根据本发明实施例的一个方面，提供了一种存储介质，存储介质包括存储的程序，其中，在程序运行时控制存储介质所在设备执行上述的密钥分发方法或密钥获取方法。

[0017] 根据本发明实施例的一个方面，提供了一种处理器，处理器用于运行程序，其中，程序运行时执行上述的密钥分发方法或密钥获取方法。

[0018] 在本发明实施例中，密钥发送端检测所述密钥接收终端发送的密钥申请；所述密钥发送端为所述密钥接收终端生成会话密钥；所述密钥发送端使用预先获取的所述密钥接收终端的第一密钥，对所述会话密钥进行加密，得到第一密文；所述密钥发送端将所述第一密文发送至所述密钥接收终端，其中，所述密钥接收终端使用所述第一密钥对所述第一密文解密，得到所述会话密钥。上述方案提供的密钥分发方法无需人工参与，也无需为每个密钥接收终端生成证书，能够安全简便的在线进行密钥分发，提高了密钥分发的效率，从而解决了现有技术中的密钥分发的过程较复杂的技术问题。

附图说明

[0019] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0020] 图1是根据本发明实施例的密钥分发方法的流程图；

[0021] 图2是根据本发明实施例的密钥分发方法的流程图；

[0022] 图3是根据本发明实施例1和实施例2的一种密钥分发方法的信息交互图；

[0023] 图4是根据本发明实施例的密钥分发装置的示意图；以及

[0024] 图5是根据本发明实施例的密钥分发装置的示意图。

具体实施方式

[0025] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明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发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，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，都应当属于本发明保护的范围。

[0026] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0027] 实施例1

[0028] 根据本发明实施例，提供了一种密钥分发方法的实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0029] 图1是根据本发明实施例的密钥分发方法的流程图，如图1所示，该方法包括如下步骤：

[0030] 步骤S102，密钥发送端检测密钥接收终端发送的密钥申请。

[0031] 具体的，上述密钥发送端可以是密钥分发服务器，也可以是密钥分发终端。密钥接收终端向密钥发送端发送密钥申请，用于获取会话密钥，从而在之后的数据通信中，使用会话密钥对会话内容进行加密。

[0032] 在一种可选的实施例中，密钥发送端为银行服务器，密钥接收终端为ATM机，ATM机可以向银行服务器发起密钥申请，请求银行服务器向其下发会话密钥。

[0033] 步骤S104，密钥发送端为密钥接收终端生成会话密钥。

[0034] 步骤S106，密钥发送端使用预先获取的密钥接收终端的第一密钥，对会话密钥进行加密，得到第一密文。

[0035] 具体的，密钥接收终端的第一密钥是密钥接收终端生成的第一密钥，即密钥发送端和密钥接收终端都具有该第一密钥。密钥发送端使用第一密钥对生成的会话密钥进行加密，从而避免会话密钥在传输的过程中被窃取或篡改。

[0036] 步骤S108，密钥发送端将第一密文发送至密钥接收终端，其中，密钥接收终端使用第一密钥对第一密文解密，得到会话密钥。

[0037] 具体的，由于密钥接收终端也具有第一密钥，因此密钥接收终端在获取到第一密文后，可以使用第一密钥对第一密文进行解密，从而得到会话密钥。

[0038] 在一种可选的实施例中，仍以上述银行服务器和ATM机为例说明，ATM在首次与银行服务器通信之前，需要获取对通信数据进行加密的会话密钥。因此，ATM机向银行服务器发送密钥申请，银行服务器接收到密钥申请后，为该ATM生成属于该ATM机的会话密钥，并使

用ATM机的第一密钥对会话密钥进行加密，得到第一密文后，服务器再将第一密文发送至银行服务器，银行服务器获取到第一密文后使用第一密钥进行解密，从而能够得到会话密钥。

[0039] 在上述示例中，需要说明的是，上述示例以一个ATM机向银行服务器发送密钥申请为例进行说明，在多个ATM机向银行服务器发送密钥申请时，银行服务器为每个ATM机生成的会话密钥不同。

[0040] 还需要说明的是，在不同的场景中，为密钥接收终端生成会话密钥的服务器和使用会话密钥与密钥接收终端进行通信的服务器可以为同一个服务器，也可以为不同的服务器。

[0041] 由上可知，本申请上述实施例密钥发送端检测密钥接收终端发送的密钥申请；密钥发送端为密钥接收终端生成会话密钥；密钥发送端使用预先获取的密钥接收终端的第一密钥，对会话密钥进行加密，得到第一密文；密钥发送端将第一密文发送至密钥接收终端，其中，密钥接收终端使用第一密钥对第一密文解密，得到会话密钥。上述方案提供的密钥分发方法无需人工参与，也无需为每个密钥接收终端生成证书，能够安全简便的在线进行密钥分发，提高了密钥分发的效率，从而解决了现有技术中的密钥分发的过程较复杂的技术问题。

[0042] 作为一种可选的实施例，在密钥发送端检测密钥接收终端发送的密钥申请之前，上述方法还包括：密钥发送端接收密钥接收终端的密钥信息，其中，密钥信息由密钥接收终端的第一密钥和密钥接收终端的终端标识构成。密钥发送端使用本地的第二密钥对第一密钥加密，得到第二密文；密钥发送端将第二密文与终端标识对应存储。

[0043] 具体的，上述密钥信息是密钥接收终端根据自身生成的第一密钥和自身的终端标识生成的，密钥发送端的本地密钥是密钥发送端所单独持有的，用于对密钥接收终端的第一密钥进行加密保存。

[0044] 密钥发送端将第二密文与终端标识对应存储，从而使得通过终端标识可以找到对应的第二密文。

[0045] 作为一种可选的实施例，密钥发送端使用预先获取的密钥接收终端的第一密钥，对会话密钥进行加密，得到第一密文，包括：密钥发送端从密钥申请中获取密钥接收终端的终端标识；密钥发送端根据终端标识查找密钥接收终端对应的第二密文；密钥发送端使用第二密钥解密第二密文，得到第一密钥；密钥发送端使用第一密钥对会话密钥和终端标识进行加密，得到第一密文。

[0046] 具体的，上述密钥申请中包括密钥接收终端的终端标识，由于密钥发送端将第二密文与终端标识对应存储，因此密钥发送端可以根据终端标识找到密钥接收终端对应的第二密文。

[0047] 由于第二密文是密钥发送端使用本地的第二密钥加密的，因此密钥发送端可以使用第二密钥解密第二密文，从而得到第一密钥。

[0048] 在密钥发送端得到第一密钥后，即可对会话密钥和密钥接收终端的终端标识进行加密，从而得到第一密钥。

[0049] 作为一种可选的实施例，密钥发送端接收密钥接收终端的密钥信息，包括：密钥发送端接收密钥分发应用发送的密钥信息，其中，密钥分发应用通过扫描密钥接收终端根据第一密钥和终端标识生成的二维码，得到密钥信息。

[0050] 具体的，上述密钥分发应用可以安装在移动终端上。

[0051] 在一种可选的实施例中，密钥接收终端根据第一密钥和终端标识生成二维码后，用于密钥分发的移动终端扫描二维码，并将扫描得到的密钥信息通过HTTPS安全连接将发送至密钥发送端。

[0052] 实施例2

[0053] 根据本发明实施例，提供了一种密钥分发方法的实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0054] 图2是根据本发明实施例的密钥分发方法的流程图，如图2所示，该方法包括如下步骤：

[0055] 步骤S202，密钥接收终端向密钥发送端发送密钥申请。

[0056] 具体的，上述密钥发送端可以是密钥分发服务器，也可以是密钥分发终端。密钥接收终端向密钥发送端发送密钥申请，用于获取会话密钥，从而在之后的数据通信中，使用会话密钥对会话内容进行加密。

[0057] 步骤S204，密钥接收终端接收密钥发送端返回的第一密文，其中，密钥发送端使用预先获取的密钥接收终端的第一密钥，对为密钥接收终端生成的会话密钥进行加密，得到第一密文。

[0058] 具体的，密钥接收终端的第一密钥是密钥接收终端生成的第一密钥，即密钥发送端和密钥接收终端都具有该第一密钥。密钥发送端使用第一密钥对生成的会话密钥进行加密，从而避免会话密钥在传输的过程中被窃取或篡改。由于密钥接收终端也具有第一密钥，因此第一密钥终端在获取到第一密文后，可以使用第一密钥对第一密文进行解密，从而得到会话密钥。

[0059] 步骤S206，密钥接收终端使用第一密钥解密第一密文，得到会话密钥。

[0060] 由上可知，本申请上述实施例密钥接收终端向密钥发送端发送密钥申请；密钥接收终端接收密钥发送端返回的第一密文，其中，密钥发送端使用预先获取的密钥接收终端的第一密钥，对为密钥接收终端生成的会话密钥进行加密，得到第一密文；密钥接收终端使用第一密钥解密第一密文，得到会话密钥。上述方案提供的密钥分发方法无需人工参与，也无需为每个密钥接收终端生成证书，过程便捷，提高了密钥分发的效率，从而解决了现有技术中的密钥分发的过程较复杂的技术问题。

[0061] 作为一种可选的实施例，密钥发送端使用第一密钥，对会话密钥和密钥接收终端的终端标识进行加密，得到第一密文，密钥接收终端使用第一密钥解密第一密文，得到会话密钥，包括：密钥接收终端使用第一密钥解密第一密文，得到会话密钥和密钥接收终端的终端标识；对第一密钥中的终端标识进行验证；如果验证通过，保存会话密钥。

[0062] 具体的，密钥接收终端对第一密钥中的终端标识进行验证，指的是接收第一密文的密钥接收终端，将第一密文中的终端标识，与自身的终端标识进行比对，如果相同，则验证通过，保存第一密文中的终端标识，并可以使用该终端标识进行会话；如果不同，则验证失败，禁止使用该会话密钥进行通信。

[0063] 作为一种可选的实施例，在密钥接收终端向密钥发送端发送密钥申请之前，方法

还包括:密钥接收终端生成第一密钥;密钥接收终端根据第一密钥和密钥接收终端的终端标识生成密钥信息;根据密钥信息生成二维码,其中,由密钥分发应用通过扫描二维码,并将扫描结果发送至密钥发送端。

[0064] 具体的,上述密钥分发应用可以安装在移动终端上。

[0065] 在一种可选的实施例中,密钥接收终端根据第一密钥和终端标识生成二维码后,用于密钥分发的移动终端扫描二维码,并将扫描得到的密钥信息通过HTTPS安全连接将发送至密钥发送端。

[0066] 图3是根据本发明实施例1和实施例2的一种密钥分发方法的信息交互图,下面结合图3,对上述密钥分发方法进行说明。

[0067] S31,密钥接收终端在本地生成一个随机密钥。

[0068] 具体的,上述随机密钥即为实施例1和实施例2中的第一密钥。

[0069] S32,密钥接收终端根据随机密钥和终端ID生成密钥信息,并通过二维码展示。

[0070] S33,用于密钥分发的移动终端扫描二维码。

[0071] S34,用于密钥分发的移动终端将扫描得到的密钥信息发送至密钥发送端。

[0072] S35,密钥发送端接收到密钥信息后,对随机密钥使用本地密钥进行加密,并和终端ID对应存储至数据库。

[0073] 上述步骤中,对随机密钥使用本地密钥进行加密得到的即为实施例1和实施例2中的第二密文。

[0074] S36,密钥接收终端向密钥发送端发送密钥申请。

[0075] S37,密钥发送端根据密钥申请中密钥接收终端的终端ID,在数据库中找到密钥接收终端加密后的随机密钥,对数据库中找到的内容进行解密,得到密钥接收终端的随机密钥。

[0076] S38,密钥发送端为密钥接收终端生成会话密钥。

[0077] S39,密钥发送端使用密钥接收终端的随机密钥对会话密钥和终端ID进行加密。

[0078] S310,密钥发送端将S39中加密的结果发送至密钥接收终端。

[0079] S311,密钥接收终端解密接收到的内容,并对接收到的内容中的终端ID进行验证。

[0080] 验证成功后,则确定该会话密钥是可信的,密钥接收终端即能够使用该会话密钥与密钥发送端进行数据通信。

[0081] 实施例3

[0082] 根据本发明实施例,还提出了一种用于执行实施例1中的密钥分发方法的密钥分发装置,图4是根据本发明实施例的密钥分发装置的示意图,如图4所示,该装置包括:

[0083] 检测模块40,用于密钥发送端检测密钥接收终端发送的密钥申请。

[0084] 生成模块42,用于密钥发送端为密钥接收终端生成会话密钥。

[0085] 第一接收模块44,用于密钥发送端使用预先获取的密钥接收终端的第一密钥,对会话密钥进行加密,得到第一密文。

[0086] 第一发送模块46,用于密钥发送端将第一密文发送至密钥接收终端,其中,密钥接收终端使用第一密钥对第一密文解密,得到会话密钥。

[0087] 作为一种可选的实施例,上述装置还包括:第三接收模块,用于在密钥发送端检测密钥接收终端发送的密钥申请之前,密钥发送端接收密钥接收终端的密钥信息,其中,密钥

信息由密钥接收终端的第一密钥和密钥接收终端的终端标识构成;加密模块,用于密钥发送端使用本地的第二密钥对第一密钥加密,得到第二密文;存储模块,用于密钥发送端将第二密文与终端标识对应存储。

[0088] 作为一种可选的实施例,第一接收模块包括:接收子模块,用于密钥发送端从密钥申请中获取密钥接收终端的终端标识;查询子模块,用于密钥发送端根据终端标识查找密钥接收终端对应的第二密文;第一解密子模块,用于密钥发送端使用第二密钥解密第二密文,得到第一密钥;加密子模块,用于密钥发送端使用第一密钥对会话密钥和终端标识进行加密,得到第一密文。

[0089] 作为一种可选的实施例,第三接收模块包括:发送子模块,用于密钥发送端接收密钥分发应用发送的密钥信息,其中,密钥分发应用通过扫描密钥接收终端根据第一密钥和终端标识生成的二维码,得到密钥信息。

[0090] 实施例4

[0091] 根据本发明实施例,还提出了一种用于执行实施例2中的密钥分发方法的密钥分发装置,图5是根据本发明实施例的密钥分发装置的示意图,如图5所示,该装置包括:

[0092] 第一发送模块50,用于密钥接收终端向密钥发送端发送密钥申请。

[0093] 第二接收模块52,用于密钥接收终端接收密钥发送端返回的第一密文,其中,密钥发送端使用预先获取的密钥接收终端的第一密钥,对为密钥接收终端生成的会话密钥进行加密,得到第一密文。

[0094] 解密模块54,用于密钥接收终端使用第一密钥解密第一密文,得到会话密钥。

[0095] 作为一种可选的实施例,密钥发送端使用第一密钥,对会话密钥和密钥接收终端的终端标识进行加密,得到第一密文,解密模块包括:第二解密子模块,用于密钥接收终端使用第一密钥解密第一密文,得到会话密钥和密钥接收终端的终端标识;验证子模块,用于对第一密钥中的终端标识进行验证;保存子模块,用于如果验证通过,保存会话密钥。

[0096] 作为一种可选的实施例,上述装置还包括:第四接收模块,用于在密钥接收终端向密钥发送端发送密钥申请之前,密钥接收终端生成第一密钥;第一生成模块,用于密钥接收终端根据第一密钥和密钥接收终端的终端标识生成密钥信息;第二生成模块,用于根据密钥信息生成二维码,其中,由密钥分发应用通过扫描二维码,并将扫描结果发送至密钥发送端。

[0097] 实施例5

[0098] 根据本发明实施例,提供了一种存储介质,存储介质包括存储的程序,其中,在所述程序运行时控制所述存储介质所在设备执行实施例1中所述的密钥分发方法或实施例2所述的密钥获取方法。

[0099] 实施例6

[0100] 根据本发明实施例,提供了一种处理器,处理器用于运行程序,其中,所述程序运行时执行实施例1中所述的密钥分发方法或实施例2所述的密钥获取方法。

[0101] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0102] 在本发明的上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0103] 在本申请所提供的几个实施例中,应该理解到,所揭露的技术内容,可通过其它的

方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，可以为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0104] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0105] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0106] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0107] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

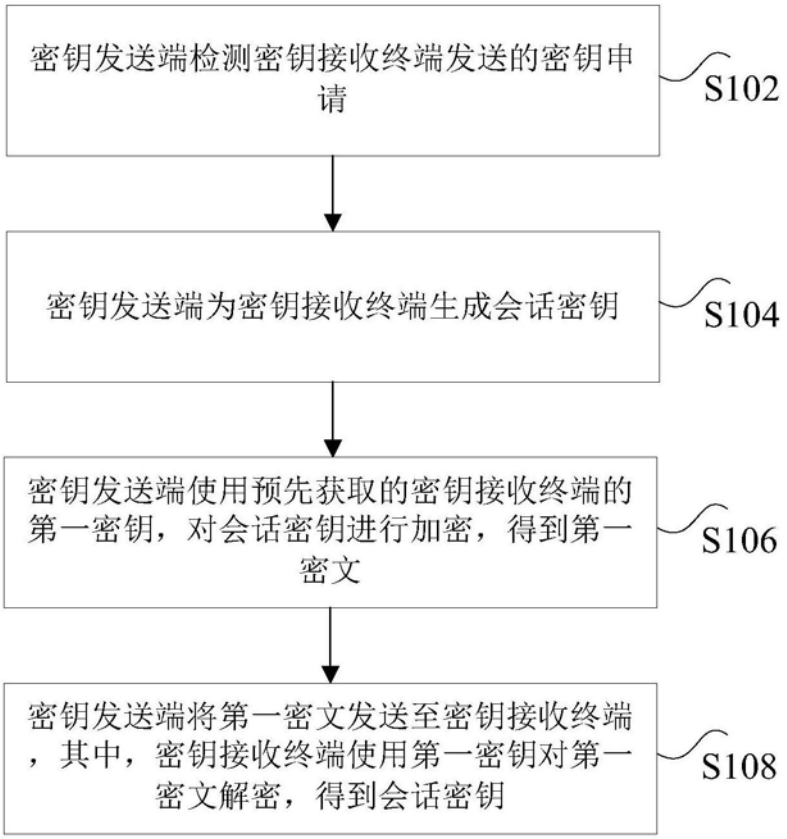

密钥发送端检测密钥接收终端发送的密钥申请
S102
密钥发送端为密钥接收终端生成会话密钥
S104
密钥发送端使用预先获取的密钥接收终端的第一密钥，对会话密钥进行加密，得到第一密文
S106
密钥发送端将第一密文发送至密钥接收终端，其中，密钥接收终端使用第一密钥对第一密文解密，得到会话密钥
S108

图1

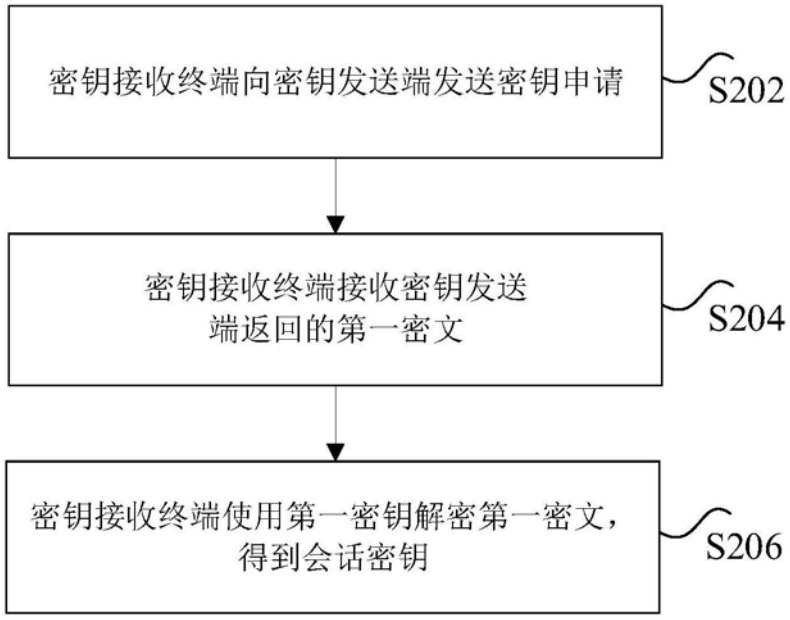

密钥接收终端向密钥发送端发送密钥申请
S202
密钥接收终端接收密钥发送端返回的第一密文
S204
密钥接收终端使用第一密钥解密第一密文，得到会话密钥
S206

图2

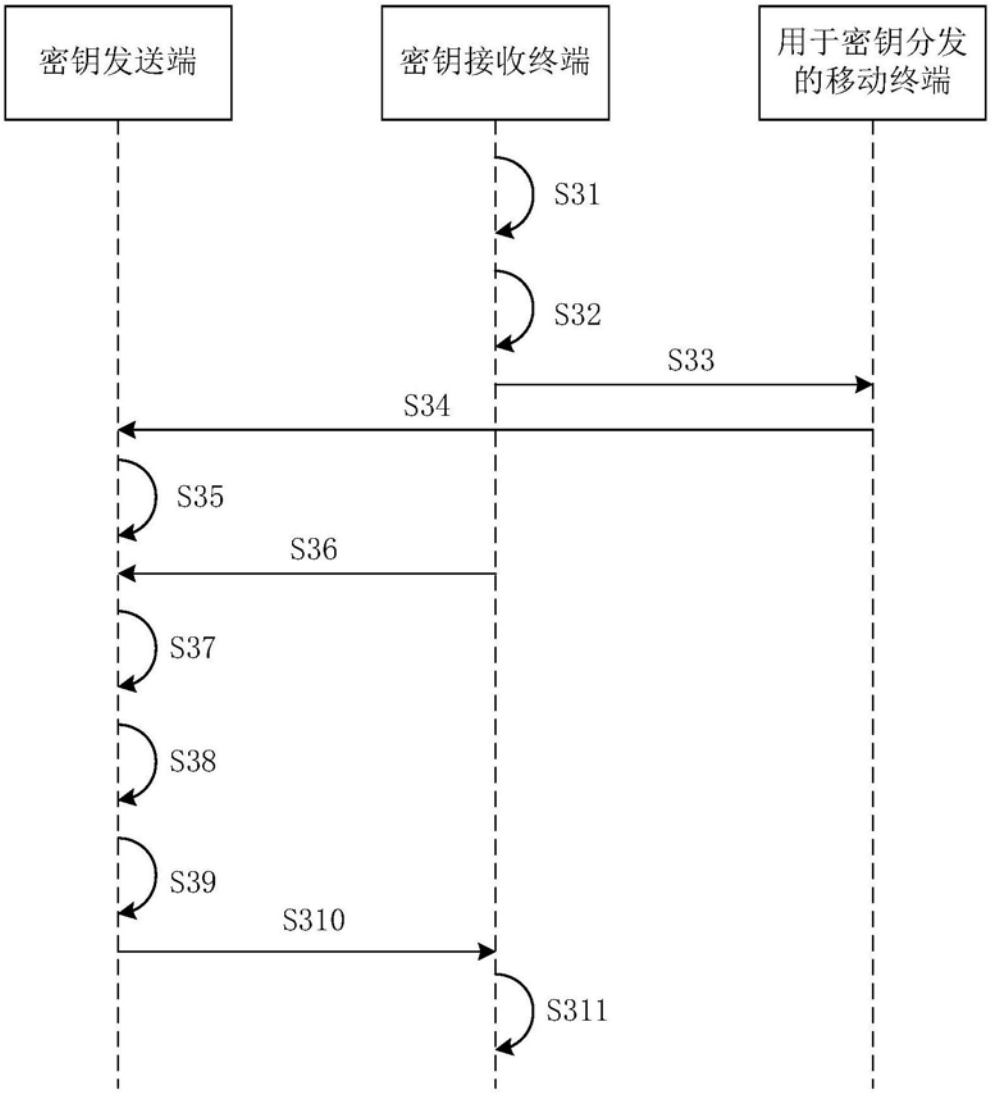

密钥发送端
密钥接收终端
用于密钥分发的移动终端
S31
S32
S33
S34
S35
S36
S37
S38
S39
S310
S311

图3


检测模块40
生成模块42
第一接收模块44
第一发送模块46

图4

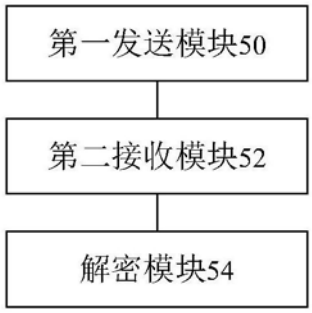


图5