(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114760500 B
(45)授权公告日 2024.09.13

(21)申请号 202210294411.0

(22)申请日 2022.03.24

(65)同一申请的已公布的文献号
申请公布号 CN 114760500 A

(43)申请公布日 2022.07.15

(73)专利权人 海南乾唐视联信息技术有限公司
地址 570105 海南省海口市龙华区滨海街道77号中环国际广场1201室

(72)发明人 张润青 王艳辉 沈世国 杨春晖

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
专利代理师 苏培华

(51)Int.Cl.
H04N 21/2347(2011.01)
H04N 21/233(2011.01)
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 110138749 A,2019.08.16
GB 2446173 A,2007.08.06
CN 110430043 A,2019.11.08

审查员 刘小睿

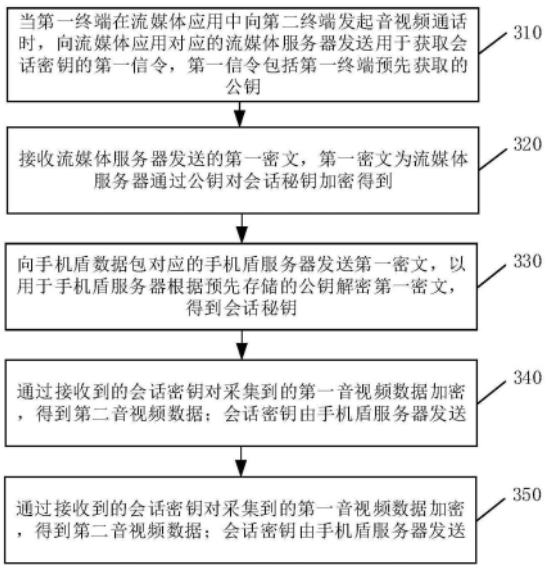
权利要求书3页 说明书10页 附图4页

(54)发明名称

一种音视频数据加密方法和装置

(57)摘要

本发明实施例提供了一种音视频数据加密方法和装置。该方法包括:当第一终端在流媒体应用中向第二终端发起音视频通话时,向流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令;接收视联网服务器发送的第一密文;向手机盾数据包对应的手机盾服务器发送第一密文,以用于手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥;通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;将第二音视频数据发给视联网服务器,以用于视联网服务器将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。根据本发明的实施例,能够保证音视频数据传输的安全性。



CN 114760500 B

1.一种音视频数据加密方法,其特征在于,应用于第一终端,所述第一终端设置有手机盾数据包,所述方法包括:

向手机盾服务器发送用户证书申请,以用于所述手机盾服务器从证书颁发机构CA服务器获取用户证书;接收所述手机盾服务器返回的用户证书,所述用户证书中包括公钥;向所述手机盾服务器发送签名请求,以用于获取签名信息;接收所述手机盾服务器返回的所述签名信息;从视联网服务器获取设备秘钥;根据所述设备秘钥、所述签名信息,以及所述第一终端保存的用户信息,向所述视联网服务器发起登录认证;

当所述第一终端在流媒体应用中向第二终端发起音视频通话时,向所述流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令,所述第一信令包括所述第一终端预先获取的公钥;

接收所述视联网服务器发送的第一密文,所述第一密文为所述视联网服务器通过所述公钥对所述会话秘钥加密得到;

向所述手机盾数据包对应的手机盾服务器发送所述第一密文,以用于所述手机盾服务器根据预先存储的所述公钥解密所述第一密文,得到所述会话秘钥;

通过接收到的所述会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;所述会话秘钥由所述手机盾服务器发送;

将所述第二音视频数据发给视联网服务器,以用于所述视联网服务器将所述第二音视频数据转发至第二终端,以用于所述第二终端根据预先获取的所述会话秘钥解析所述第二音视频数据,得到所述第一音视频数据。

2.根据权利要求1所述的方法,其特征在于,所述从所述视联网服务器获取设备秘钥,包括:

向所述视联网服务器发送用于获取设备秘钥的第二信令,所述第二信令包括所述公钥;

接收所述视联网服务器发送的第二密文,所述第二密文为所述视联网服务器通过所述公钥对所述设备秘钥加密得到;

向所述手机盾服务器发送所述第二密文,以用于所述手机盾服务器解密所述第二密文,得到所述设备秘钥;

接收所述手机盾服务器发送的所述设备秘钥。

3.根据权利要求1所述的方法,其特征在于,所述根据所述设备秘钥、所述签名信息,以及所述第一终端保存的用户信息,向所述视联网服务器发起登录认证,包括:

根据所述设备秘钥对所述第一终端的用户信息加密,得到第三密文,

向视联网服务器发送登录信令,所述登录信令包括:所述设备秘钥、所述第三密文,以及所述签名信息,以用于所述视联网服务器根据所述设备秘钥对所述第三密文解密得到所述用户信息、以及在用户信息与所述签名信息通过验证的情况下,返回登录确认信息给所述第一终端;

在接收到所述登录确认信息的情况下,登录所述流媒体应用。

4.一种音视频数据加密方法,其特征在于,应用于视联网服务器,所述方法包括:

当第一终端在流媒体应用中向第二终端发起音视频通话时;

接收第一终端发送的用于获取会话秘钥的第一信令,所述第一信令包括所述第一终端

预先获取的公钥;

向所述第一终端发送第一密文,所述第一密文为通过所述公钥对所述会话秘钥加密得到;所述第一密文用于:以使与所述第一终端中的手机盾数据包对应的手机盾服务器根据预先存储的所述公钥解密所述第一密文,得到所述会话秘钥;

接收所述第一终端发送的第二音视频数据,所述第二音视频数据为所述第一终端根据所述会话秘钥对采集的第一音视频数据加密得到;

将所述第二音视频数据转发至第二终端,以用于所述第二终端根据预先获取的所述会话秘钥解析所述第二音视频数据,得到所述第一音视频数据;

其中,所述第一终端还用于:向所述手机盾服务器发送用户证书申请,以用于所述手机盾服务器从证书颁发机构CA服务器获取用户证书;接收所述手机盾服务器返回的用户证书,所述用户证书中包括所述公钥;向所述手机盾服务器发送签名请求,以用于获取签名信息;接收所述手机盾服务器返回的所述签名信息;从所述视联网服务器获取设备秘钥;根据所述设备秘钥、所述签名信息,以及所述第一终端保存的用户信息,向所述视联网服务器发起登录认证。

5.根据权利要求4所述的方法,其特征在于,在所述接收第一终端发送的用于获取会话秘钥的第一信令之前,所述方法还包括:

根据所述设备秘钥对所述第一终端的用户信息加密,得到第三密文;

接收所述第一终端发送的登录信令,所述登录信令包括:设备秘钥、第三密文,以及所述第一终端的签名信息;

根据所述设备秘钥对所述第三密文解密,得到所述用户信息;

在用户信息与所述签名信息通过验证的情况下,返回登录确认信息给所述第一终端。

6.一种音视频数据加密方法,其特征在于,应用于手机盾服务器,所述方法包括:

当第一终端在流媒体应用中向第二终端发起音视频通话时;

接收所述第一终端发送的第一密文;所述第一密文为视联网服务器通过公钥对会话秘钥加密得到;

根据预先存储的所述公钥解密所述第一密文,得到所述会话秘钥;

将所述会话秘钥发送至所述第一终端;

所述第一终端根据所述会话秘钥对采集的第一音视频数据加密得到第二音视频数据;

所述第一终端将所述第二音视频数据转发至第二终端,以用于所述第二终端根据预先获取的所述会话秘钥解析所述第二音视频数据,得到所述第一音视频数据;

其中,所述第一终端还用于:向所述手机盾服务器发送用户证书申请,以用于所述手机盾服务器从证书颁发机构CA服务器获取用户证书;接收所述手机盾服务器返回的用户证书,所述用户证书中包括所述公钥;向所述手机盾服务器发送签名请求,以用于获取签名信息;接收所述手机盾服务器返回的所述签名信息;从所述视联网服务器获取设备秘钥;根据所述设备秘钥、所述签名信息,以及所述第一终端保存的用户信息,向所述视联网服务器发起登录认证。

7.一种音视频数据加密装置,其特征在于,包括:

一个或多个处理器;和

其上存储有指令的一个或多个机器可读介质,当由所述一个或多个处理器执行时,使

得所述装置执行如权利要求1至3任一项或权利要求4-5任一项或权利要求6所述的音视频数据加密方法。

8.一种计算机可读存储介质,其特征在于,其存储的计算机程序使得处理器执行如权利要求1至3任一项或权利要求4-5任一项或权利要求6所述的音视频数据加密方法。

一种音视频数据加密方法和装置

技术领域

[0001] 本发明涉及音视频数据处理技术领域,特别是涉及一种音视频数据加密方法和装置。

背景技术

[0002] 由于视联网业务的不断开展,越来越多的用户利用手机来使用视联网功能,如视频会议、视频通话等等。

[0003] 目前,在视联网中开展音视频业务的需求越来越多,如何保证音视频数据传输的安全性便成为亟待解决的技术问题。

发明内容

[0004] 鉴于上述问题,提出了本发明实施例以便提供一种克服上述问题或者至少部分地解决上述问题的一种音视频数据加密方法和相应的音视频数据加密装置。

[0005] 第一方面,本发明实施例提供一种音视频数据加密方法,应用于第一终端,第一终端设置有手机盾数据包,该方法包括:

[0006] 当第一终端在流媒体应用中向第二终端发起音视频通话时,向流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥;

[0007] 接收视联网服务器发送的第一密文,第一密文为视联网服务器通过公钥对会话秘钥加密得到;

[0008] 向手机盾数据包对应的手机盾服务器发送第一密文,以用于手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥;

[0009] 通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;会话秘钥由手机盾服务器发送;

[0010] 将第二音视频数据发给视联网服务器,以用于视联网服务器将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0011] 第二方面,本发明实施例提供一种音视频数据加密方法,应用于视联网服务器,该方法包括:

[0012] 接收第一终端发送的用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥;

[0013] 向第一终端发送第一密文,第一密文为通过公钥对会话秘钥加密得到;

[0014] 接收第一终端发送的第二音视频数据,第二音视频数据为第一终端根据会话秘钥对采集的第一音视频数据加密得到;

[0015] 将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0016] 第三方面,本发明实施例提供一种音视频数据加密方法,应用于手机盾服务器,该方法包括:

[0017] 接收第一终端发送的第一密文;第一密文为视联网服务器通过公钥对会话秘钥加密得到;

[0018] 根据预先存储的公钥解密第一密文,得到会话秘钥;

[0019] 将会话秘钥发送至第一终端。

[0020] 第四方面,本发明实施例提供了一种音视频数据加密装置,该音视频数据加密装置包括:处理器以及存储有计算机程序指令的存储器;处理器执行计算机程序指令时,实现如第一方面或者第二方面或者第三方面中的方法。

[0021] 第五方面,本发明实施例提供了一种可读存储介质,该计算机可读存储介质上存储有计算机程序指令,计算机程序指令被处理器执行时实现如第一方面或者第二方面或者第三方面中的方法。

[0022] 本发明实施例包括以下优点:

[0023] 本发明实施例应用视联网的特性,当第一终端在流媒体应用中向第二终端发起音视频通话时,向流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥;接收视联网服务器发送的第一密文,第一密文为视联网服务器通过公钥对会话秘钥加密得到;这里,对会话秘钥加密后传输,可以保证会话秘钥的安全性。向手机盾数据包对应的手机盾服务器发送第一密文,以用于手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥;由于手机盾必须基于手机安全元件或可信执行环境,可以硬件级的安全性。这里,由第一终端中安装的手机盾数据包对应的手机盾服务器来解密,进一步提升安全性。最后,通过接收到的由手机盾服务器发送的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;将第二音视频数据发给视联网服务器,以用于视联网服务器将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。由此,在视联网内进行音视频数据的加密,可以保证传输的音视频数据更安全可靠。

附图说明

[0024] 图1是本发明的一种实现音视频数据加密方法的示意图;

[0025] 图2是本发明实施例提供的一种音视频数据加密方法的流程图;

[0026] 图3是本发明实施例提供的一种应用于第一终端的音视频数据加密方法的流程图;

[0027] 图4是本发明实施例提供的一种应用于视联网服务器的音视频数据加密方法的流程图;

[0028] 图5是发明实施例提供的一种应用于手机盾服务器的音视频数据加密方法的流程图;

[0029] 图6是发明实施例提供的一种第一终端的结构示意图;

[0030] 图7是发明实施例提供的一种视联网服务器的结构示意图;

[0031] 图8是发明实施例提供的一种手机盾服务器的结构示意图;

具体实施方式

[0032] 为使本发明的上述目的、特征和优点能够更加明显易懂,下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0033] 首先,对于本发明实施例涉及的技术术语进行介绍。

[0034] 视联网,视联网是网络发展的重要里程碑,是互联网的更高级形态,是一个实时网络,能够实现目前互联网无法实现的全网高清视频实时传输,将众多互联网应用推向高清视频化,高清面对面。最终将实现世界无距离,实现全球范围内人与人的距离只是一个屏幕的距离。

[0035] 手机盾数据包(手机盾SDK),通过CA服务器给APP下发CA证书,通过加密机或者PCIE加密卡进行加密的过程,做到软加密的要求。其中,软件开发工具包(Software Deve l opment Kit,SDK)一般都是一些软件工程师为特定的软件包、软件框架、硬件平台、操作系统等建立应用软件时的开发工具的集合。

[0036] 加密机是一种主机加密设备,加密机和主机之间使用TCP/IP协议通信,所以加密机对主机的类型和主机操作系统无任何特殊的要求。

[0037] 手机盾是以手机可信执行环境(TEE)和安全元件(SE)为载体实现的二代USBKEY,完全不依赖任何外部硬件设备,也无需用户安装任何额外的软件。需要注意的是,纯粹依赖软件无法满足盾级安全性的要求,手机盾必须基于手机安全元件或可信执行环境,手机盾服务商在TEE中为要保护的程序创建安全域,才可实现硬件级安全性。

[0038] CA证书,CA中心为每个使用公开秘钥的用户发放一个数字证书,数字证书作用是证明证书中列出的用户合法拥有证书中列出的公开秘钥。证书颁发机构(Cert ificate Author ity,CA)即颁发数字证书的机构。是负责发放和管理数字证书的权威机构,并作为电子商务交易中受信任的第三方,承担公钥体系中公钥的合法性检验的责任。

[0039] 流媒体服务系统:流媒体服务系统是视联网与IP网音视频传输业务的桥梁和纽带,实现了视联网业务与IP网业务的无缝融合,可以将IP网中各类音视频资源安全接入视联网,可将视联网中视频会议、监控图像、数字电视等不同的音视频流转换并以常用标准的IP网协议方式输出,是视联网与IP网手机客户端互联互通的核心设备。

[0040] 下面对本发明实施例提供的音视频数据加密方法进行整体性说明。

[0041] 第一终端100,视联网服务器200、手机盾服务器300、第二终端400以及CA服务器500。

[0042] 首先,第一终端100获取用户证书和签名信息。

[0043] 具体地,第一终端100向手机盾服务器300发送用户证书申请,以用于手机盾服务器300从CA服务器500获取用户证书;第一终端100接收手机盾服务器300返回的用户证书,用户证书中包括公钥;第一终端100向手机盾服务器300发送签名请求,以用于获取签名信息;第一终端100接收手机盾服务器300返回的签名信息。

[0044] 其次,第一终端100获取设备秘钥。

[0045] 具体地,第一终端100向视联网服务器200发送用于获取设备秘钥的第二信令,第二信令包括公钥;视联网服务器200通过公钥对设备秘钥加密得到第二密文;视联网服务器200向第一终端100发送第二密文;第一终端100向手机盾服务器300发送第二密文,以用于手机盾服务器300解密第二密文,得到设备秘钥;第一终端100接收手机盾服务器300发送的

设备秘钥。

[0046] 接着,第一终端100根据设备秘钥登录流媒体应用。

[0047] 具体地,第一终端100根据设备秘钥对第一终端100的用户信息加密,得到第三密文;向视联网服务器200发送登录信令,登录信令包括:设备秘钥、第三密文,以及签名信息。视联网服务器200根据设备秘钥对第三密文解密得到用户信息、以及在用户信息与签名信息通过验证的情况下,返回登录确认信息给第一终端100;第一终端100在接收到登录确认信息的情况下,登录流媒体应用。

[0048] 然后,第一终端100获取会话信令。

[0049] 具体地,第一终端100在流媒体应用中向第二终端400发起音视频通话时,向流媒体应用对应的视联网服务器200发送用于获取会话秘钥的第一信令,第一信令包括第一终端100预先获取的公钥。视联网服务器200向第一终端100发送第一密文,第一密文为通过公钥对会话秘钥加密得到。第一终端100向手机盾数据包对应的手机盾服务器300发送第一密文。手机盾服务器300根据预先存储的公钥解密第一密文,得到会话秘钥。

[0050] 最后,对音视频数据加密。

[0051] 具体地,通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据。将第二音视频数据发给视联网服务器200。视联网服务器200将第二音视频数据转发至第二终端400。第二终端400根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0052] 其中,本发明中涉及到的视联网服务器具体可以为流媒体服务器。

[0053] 下面结合图2,对本发明实施例提供的音视频数据加密方法进行说明。

[0054] 210,第一终端100向视联网服务器200发送用于获取会话秘钥的第一信令。

[0055] 220,视联网服务器200向第一终端10发送第一密文,第一密文为通过公钥对会话秘钥加密得到。

[0056] 230,第一终端100向手机盾数据包对应的手机盾服务器300发送第一密文。

[0057] 240,手机盾服务器300根据预先存储的公钥解密第一密文,得到会话秘钥。

[0058] 250,手机盾服务器300向第一终端100发送会话秘钥。

[0059] 260,第一终端100通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据。

[0060] 270,第一终端100将第二音视频数据发给视联网服务器200。

[0061] 280,视联网服务器200将第二音视频数据转发至第二终端400。

[0062] 290,第二终端400根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0063] 本发明实施例应用视联网的特性,当第一终端在流媒体应用中向第二终端发起音视频通话时,向流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥;接收视联网服务器发送的第一密文,第一密文为视联网服务器通过公钥对会话秘钥加密得到;这里,对会话秘钥加密后传输,可以保证会话秘钥的安全性。向手机盾数据包对应的手机盾服务器发送第一密文,以用于手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥;由于手机盾必须基于手机安全元件或可信执行环境,可以保证硬件级的安全性。这里,由第一终端中安装的手机盾数据包对应的手机

盾服务器来解密,进一步提升安全性。最后,通过接收到的由手机盾服务器发送的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;将第二音视频数据发给视联网服务器,以用于视联网服务器将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。由此,在视联网内进行音视频数据的加密,可以保证传输的音视频数据更安全可靠。

[0064] 下面对本发明实施例提供的音视频数据加密方法进行详细说明。

[0065] 图3为本发明实施例提供的一种音视频数据加密方法的流程图。

[0066] 如图3所示,该音视频数据加密方法可以包括步骤310-步骤350,该方法应用于第一终端,第一终端设置有手机盾数据包,具体如下所示:

[0067] 步骤310,当第一终端在流媒体应用中向第二终端发起音视频通话时,向流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥。

[0068] 在一种可能的实施例中,步骤310之前,还可以包括以下步骤:

[0069] 步骤360,从手机盾服务器获取包括公钥的用户证书,以及第一终端对应的签名信息。

[0070] 步骤370,从视联网服务器获取设备秘钥。

[0071] 步骤380,根据设备秘钥、签名信息,以及第一终端保存的用户信息,向视联网服务器发起登录认证。

[0072] 从手机盾服务器获取包括公钥的用户证书,以及第一终端对应的签名信息,从视联网服务器获取设备秘钥,以及根据设备秘钥、签名信息,以及第一终端保存的用户信息,向视联网服务器发起登录认证。是为了进行用户信息鉴权。

[0073] 用户鉴权,一种用于在通信网络中对试图访问来自服务提供商的服务的用户进行鉴权的方法。用于用户准备使用数据业务时,对该用户使用数据业务的合法性和有效性进行检查。

[0074] 其中,上述涉及到的步骤360,包括:

[0075] 向手机盾服务器发送用户证书申请,以用于手机盾服务器从证书颁发机构CA服务器获取用户证书;

[0076] 接收手机盾服务器返回的用户证书,用户证书中包括公钥;

[0077] 向手机盾服务器发送签名请求,以用于获取签名信息;

[0078] 接收手机盾服务器返回的签名信息。

[0079] 为用户分配用于访问各个服务的多个服务专用标识;从用户对应的第一终端处发出用户证书申请,该用户证书申请标识出将要访问的服务;在认证机构处CA服务器,对所述请求进行鉴权,将包括公钥的用户证书返回给所述用户对应的的第一终端。

[0080] 即第一终端可以接收手机盾服务器返回的包括公钥的用户证书,然后第一终端向手机盾服务器发送签名请求,手机盾服务器向第一终端返回第一终端的签名信息。

[0081] 其中,上述涉及到的步骤370中,具体可以包括以下步骤:

[0082] 向视联网服务器发送用于获取设备秘钥的第二信令,第二信令包括公钥;

[0083] 接收视联网服务器发送的第二密文,第二密文为视联网服务器通过公钥对设备秘钥加密得到;

[0084] 向手机盾服务器发送第二密文,以用于手机盾服务器解密第二密文,得到设备秘钥;

[0085] 接收手机盾服务器发送的设备秘钥。

[0086] 秘钥是一种参数,它是在明文转换为密文或将密文转换为明文的算法中输入的参数。设备秘钥是与第一终端相关的秘钥。

[0087] 这里,将对视联网服务器通过公钥对设备秘钥加密得到的第二密文,发送至手机盾服务器,由手机盾服务器解密第二密文,得到设备秘钥,由于手机盾服务器的执行环境安全性更高,能够提升解密的安全性。

[0088] 其中,上述涉及到的步骤380中,具体可以包括以下步骤:

[0089] 根据设备秘钥对第一终端的用户信息加密,得到第三密文,

[0090] 向视联网服务器发送登录信令,登录信令包括:设备秘钥、第三密文,以及签名信息,以用于视联网服务器根据设备秘钥对第三密文解密得到用户信息、以及在用户信息与签名信息通过验证的情况下,返回登录确认信息给第一终端;

[0091] 在接收到登录确认信息的情况下,登录流媒体应用。

[0092] 根据设备秘钥对第一终端的用户信息加密,得到第三密文,这里,对第一终端的用户信息加密生成第三密文后再发送,能够保证用户信息的安全性。

[0093] 其中,设备秘钥是用于视联网服务器根据设备秘钥对第三密文解密得到用户信息的。视联网服务器比较用户信息与签名信息,在用户信息与签名信息一致,即用户信息通过验证的情况下,返回登录确认信息给第一终端;第一终端在接收到登录确认信息的情况下,就可以成功登录流媒体应用。

[0094] 步骤320,接收视联网服务器发送的第一密文,第一密文为视联网服务器通过公钥对会话秘钥加密得到。

[0095] 视联网服务器通过公钥对会话秘钥加密得到第一密文后,再发送,能够保证会话公钥在传输中的安全性。

[0096] 步骤330,向手机盾数据包对应的手机盾服务器发送第一密文,以用于手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥。

[0097] 手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥;由于手机盾必须基于可信执行环境,可以保证硬件级的安全性。这里,由第一终端中安装的手机盾数据包对应的手机盾服务器来解密,进一步提升安全性。

[0098] 步骤340,通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;会话秘钥由手机盾服务器发送。

[0099] 第一终端通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据,能够保证传输的音视频数据更安全可靠。

[0100] 步骤350,将第二音视频数据发给视联网服务器,以用于视联网服务器将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0101] 其中,第二终端处保存的会话秘钥与第一终端一致,在此不再赘述,所以可以解析第二音视频数据得到第一终端采集的第一音视频数据。

[0102] 其中,第二终端获取会话秘钥的过程与第一终端获取会话秘钥的过程基本一致,

在此不再赘述。

[0103] 需要说明的是,在视频会议等应用场景中,即第一终端采集第一音视频数据并发送至第二终端,第二终端播放该第一音视频数据。由于终端之间的通信是持续的,因此,第一视联网终端采集的第一多媒体数据是持续的。

[0104] 下面对本发明实施例提供的音视频数据加密方法进行详细说明。

[0105] 图4为本发明实施例提供的一种音视频数据加密方法的流程图。

[0106] 如图4所示,该音视频数据加密方法可以包括步骤410-步骤440,该方法应用于视联网服务器,具体如下所示:

[0107] 步骤410,接收第一终端发送的用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥。

[0108] 在一种可能的实施例中,在步骤410之前,还可以包括以下步骤:

[0109] 根据设备秘钥对第一终端的用户信息加密,得到第三密文;

[0110] 接收第一终端发送的登录信令,登录信令包括:设备秘钥、第三密文,以及第一终端的签名信息;

[0111] 根据设备秘钥对第三密文解密,得到用户信息;

[0112] 在用户信息与签名信息通过验证的情况下,返回登录确认信息给第一终端。

[0113] 其中,设备秘钥是用于视联网服务器根据设备秘钥对第三密文解密得到用户信息的。视联网服务器比较用户信息与签名信息,在用户信息与签名信息一致,即用户信息通过验证的情况下,返回登录确认信息给第一终端;第一终端在接收到登录确认信息的情况下,就可以成功登录流媒体应用。

[0114] 步骤420,向第一终端发送第一密文,第一密文为通过公钥对会话秘钥加密得到。

[0115] 视联网服务器通过公钥对会话秘钥加密得到第一密文后,再发送,能够保证会话公钥在传输中的安全性。

[0116] 步骤430,接收第一终端发送的第二音视频数据,第二音视频数据为第一终端根据会话秘钥对采集的第一音视频数据加密得到。

[0117] 第二音视频数据是第一终端通过接收到的会话秘钥对采集到的第一音视频数据加密得到的,能够保证传输的音视频数据更安全可靠。

[0118] 步骤440,将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0119] 媒体服务器负责将接收到的第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。其中,第二终端处保存的会话秘钥与第一终端一致,在此不再赘述,所以可以解析第二音视频数据得到第一终端采集的第一音视频数据。

[0120] 在本发明的实施例中,视联网服务器响应于第一终端发送的用于获取会话秘钥的第一信令,通过公钥对会话秘钥加密得到第一密文并向第一终端发送,可以保证会话公钥在传输中的安全性。然后接收第一终端发送的根据会话秘钥对采集的第一音视频数据加密得到的安全可靠的第二音视频数据。并将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。能够保证第一终端和第二终端之间进行安全稳定的音视频数据传输。

[0121] 下面对本发明实施例提供的音视频数据加密方法进行详细说明。

[0122] 图5为本发明实施例提供的一种音视频数据加密方法的流程图。

[0123] 如图5所示,该音视频数据加密方法可以包括步骤510-步骤520,该方法应用于手机盾服务器,具体如下所示:

[0124] 步骤510,接收第一终端发送的第一密文;第一密文为视联网服务器通过公钥对会话秘钥加密得到。

[0125] 步骤520,根据预先存储的公钥解密第一密文。

[0126] 在本发明的实施例中,手机盾服务器接收第一终端发送的由视联网服务器通过公钥对会话秘钥加密得到第一密文,手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥;由于手机盾必须基于可信执行环境,安全性更高。这里,由第一终端中安装的手机盾数据包对应的手机盾服务器来解密,能够保证提升安全性。

[0127] 需要说明的是,对于方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明实施例并不受所描述的动作顺序的限制,因为依据本发明实施例,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作并不一定是本发明实施例所必须的。

[0128] 参照图6,示出了本发明的一种第一终端实施例的结构框图,第一终端设置有手机盾数据包,该第一终端600可以应用于视联网中,具体可以包括如下模块:

[0129] 发送模块610,用于当第一终端在流媒体应用中向第二终端发起音视频通话时,向流媒体应用对应的视联网服务器发送用于获取会话秘钥的第一信令,第一信令包括第一终端预先获取的公钥。

[0130] 接收模块620,用于接收视联网服务器发送的第一密文,第一密文为视联网服务器通过公钥对会话秘钥加密得到。

[0131] 发送模块610,用于向手机盾数据包对应的手机盾服务器发送第一密文,以用于手机盾服务器根据预先存储的公钥解密第一密文,得到会话秘钥。

[0132] 加密模块630,用于通过接收到的会话秘钥对采集到的第一音视频数据加密,得到第二音视频数据;会话秘钥由手机盾服务器发送。

[0133] 发送模块610,用于将第二音视频数据发给视联网服务器,以用于视联网服务器将第二音视频数据转发至第二终端,以用于第二终端根据预先获取的会话秘钥解析第二音视频数据,得到第一音视频数据。

[0134] 在本发明的一种可选的实施例中,该第一终端600还可以包括:

[0135] 获取模块,用于:

[0136] 从手机盾服务器获取包括公钥的用户证书,以及第一终端对应的签名信息;从视联网服务器获取设备秘钥;

[0137] 登录模块,用于根据设备秘钥、签名信息,以及第一终端保存的用户信息,向视联网服务器发起登录认证。

[0138] 在本发明的一种可选的实施例中,获取模块,具体用于:

[0139] 向视联网服务器发送用于获取设备秘钥的第二信令,第二信令包括公钥;

[0140] 接收视联网服务器发送的第二密文,第二密文为视联网服务器通过公钥对设备秘

钥加密得到；

[0141] 向手机盾服务器发送第二密文，以用于手机盾服务器解密第二密文，得到设备秘钥；

[0142] 接收手机盾服务器发送的设备秘钥。

[0143] 在本发明的一种可选的实施例中，登录模块，具体用于：

[0144] 根据设备秘钥对第一终端的用户信息加密，得到第三密文，

[0145] 向视联网服务器发送登录信令，登录信令包括：设备秘钥、第三密文，以及签名信息，以用于视联网服务器根据设备秘钥对第三密文解密得到用户信息、以及在用户信息与签名信息通过验证的情况下，返回登录确认信息给第一终端；

[0146] 在接收到登录确认信息的情况下，登录流媒体应用。

[0147] 在本发明的一种可选的实施例中，获取模块，具体用于：

[0148] 向手机盾服务器发送用户证书申请，以用于手机盾服务器从证书颁发机构CA服务器获取用户证书；

[0149] 接收手机盾服务器返回的用户证书，用户证书中包括公钥；

[0150] 向手机盾服务器发送签名请求，以用于获取签名信息；

[0151] 接收手机盾服务器返回的签名信息。

[0152] 参照图7，示出了本发明的一种视联网服务器实施例的结构框图，该视联网服务器700可以应用于视联网中，具体可以包括如下模块：

[0153] 接收模块710，用于接收第一终端发送的用于获取会话秘钥的第一信令，第一信令包括第一终端预先获取的公钥。

[0154] 发送模块720，用于向第一终端发送第一密文，第一密文为通过公钥对会话秘钥加密得到。

[0155] 接收模块710，用于接收第一终端发送的第二音视频数据，第二音视频数据为第一终端根据会话秘钥对采集的第一音视频数据加密得到。

[0156] 发送模块720，用于将第二音视频数据转发至第二终端，以用于第二终端根据预先获取的会话秘钥解析第二音视频数据，得到第一音视频数据。

[0157] 在本发明的一种可选的实施例中，视联网服务器700还可以包括：

[0158] 加密模块，用于根据设备秘钥对第一终端的用户信息加密，得到第三密文；

[0159] 接收模块710，还用于：接收第一终端发送的登录信令，登录信令包括：设备秘钥、第三密文，以及第一终端的签名信息；

[0160] 解密模块，用于根据设备秘钥对第三密文解密，得到用户信息；

[0161] 发送模块720，还用于在用户信息与签名信息通过验证的情况下，返回登录确认信息给第一终端。

[0162] 参照图8，示出了本发明的一种手机盾服务器实施例的结构框图，该手机盾服务800可以应用于视联网中，具体可以包括如下模块：

[0163] 接收模块810，用于接收第一终端发送的第一密文；第一密文为视联网服务器通过公钥对会话秘钥加密得到。

[0164] 解密模块820，用于根据预先存储的公钥解密第一密文。

[0165] 对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关

之处参见方法实施例的部分说明即可。

[0166] 本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。

[0167] 本领域内的技术人员应明白,本发明实施例的实施例可提供为方法、装置、或计算机程序产品。因此,本发明实施例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,本发明实施例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。

[0168] 本发明实施例是参照根据本发明实施例的方法、终端设备(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终端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终端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。

[0169] 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终端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。

[0170] 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终端设备上,使得在计算机或其他可编程终端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终端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。

[0171] 尽管已描述了本发明实施例的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例做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发明实施例范围的所有变更和修改。

[0172] 最后,还需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0173] 以上对本发明所提供的一种摄像头的电子聚焦方法和一种摄像头的电子聚焦装置,进行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

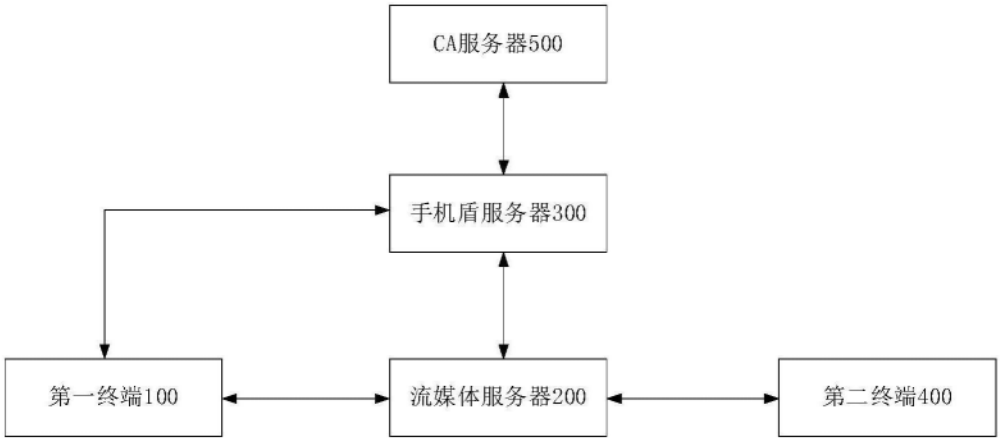

CA服务器500
手机盾服务器300
第一终端100
流媒体服务器200
第二终端400

图1

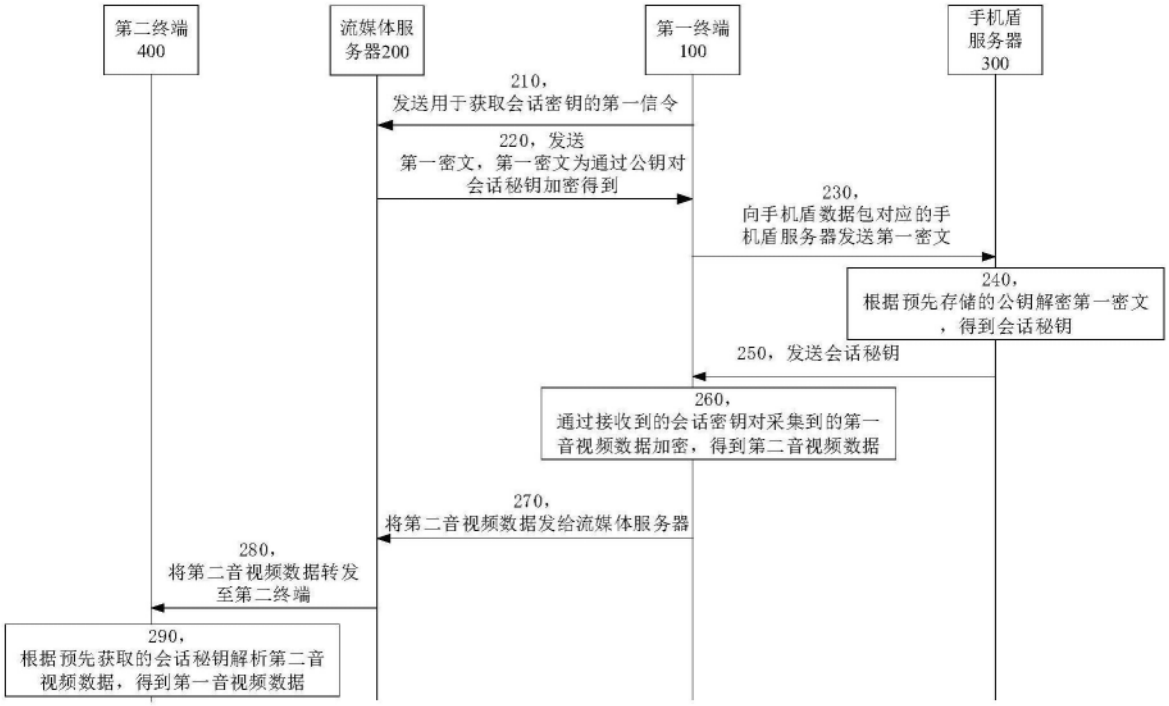

第二终端 400
流媒体服务器200
第一终端 100
手机盾服务器 300
210，发送用于获取会话密钥的第一信令
220，发送第一密文，第一密文为通过公钥对会话秘钥加密得到
230，向手机盾数据包对应的手机盾服务器发送第一密文
240，根据预先存储的公钥解密第一密文，得到会话秘钥
250，发送会话秘钥
260，通过接收到的会话密钥对采集到的第一音视频数据加密，得到第二音视频数据
270，将第二音视频数据发给流媒体服务器
280，将第二音视频数据转发至第二终端
290，根据预先获取的会话秘钥解析第二音视频数据，得到第一音视频数据

图2

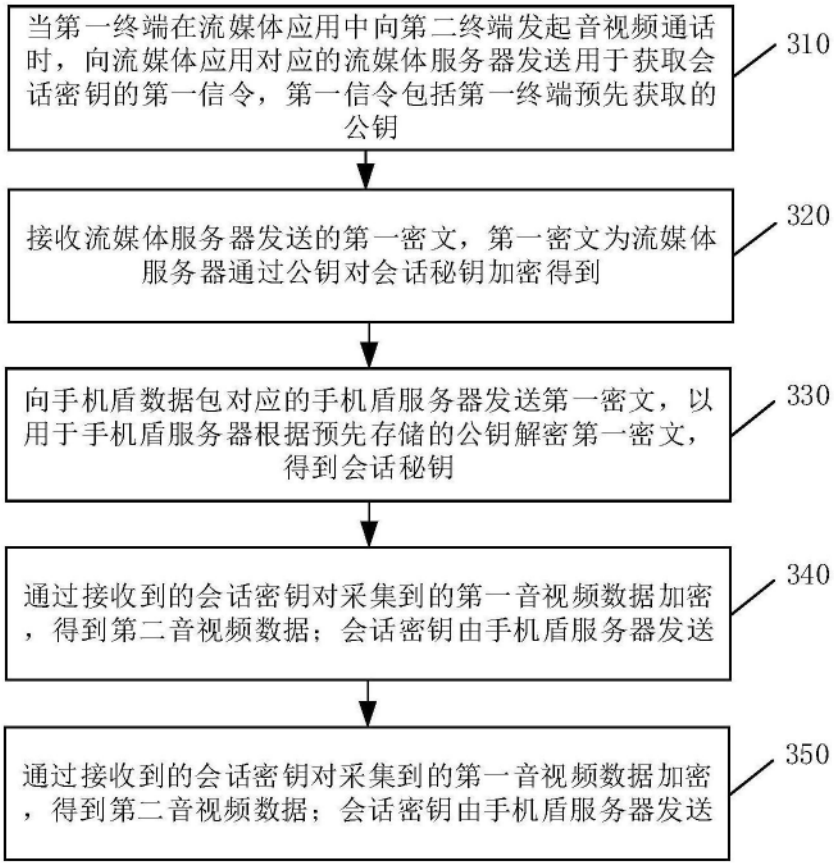

当第一终端在流媒体应用中向第二终端发起音视频通话时，向流媒体应用对应的流媒体服务器发送用于获取会话密钥的第一信令，第一信令包括第一终端预先获取的公钥
310
接收流媒体服务器发送的第一密文，第一密文为流媒体服务器通过公钥对会话秘钥加密得到
320
向手机盾数据包对应的手机盾服务器发送第一密文，以用于手机盾服务器根据预先存储的公钥解密第一密文，得到会话秘钥
330
通过接收到的会话密钥对采集到的第一音视频数据加密，得到第二音视频数据；会话密钥由手机盾服务器发送
340
通过接收到的会话密钥对采集到的第一音视频数据加密，得到第二音视频数据；会话密钥由手机盾服务器发送
350

图3

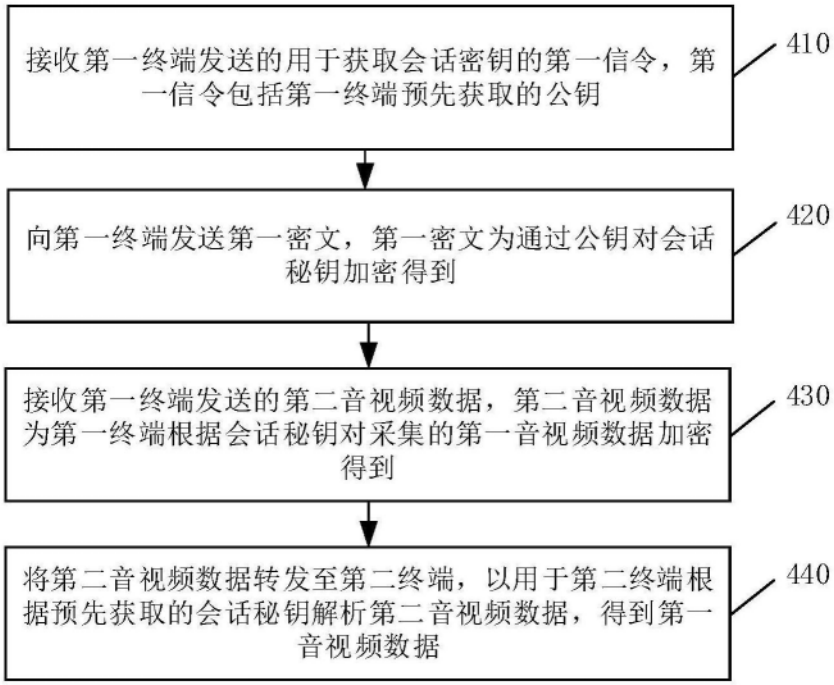

接收第一终端发送的用于获取会话密钥的第一信令，第一信令包括第一终端预先获取的公钥
410
向第一终端发送第一密文，第一密文为通过公钥对会话秘钥加密得到
420
接收第一终端发送的第二音视频数据，第二音视频数据为第一终端根据会话秘钥对采集的第一音视频数据加密得到
430
将第二音视频数据转发至第二终端，以用于第二终端根据预先获取的会话秘钥解析第二音视频数据，得到第一音视频数据
440

图4

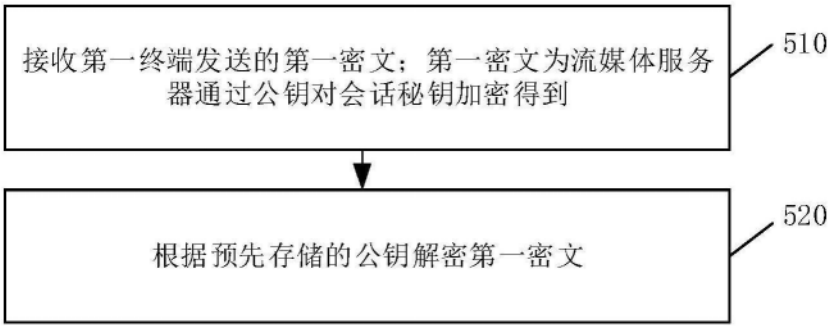

接收第一终端发送的第一密文；第一密文为流媒体服务器通过公钥对会话秘钥加密得到
510
根据预先存储的公钥解密第一密文
520

图5

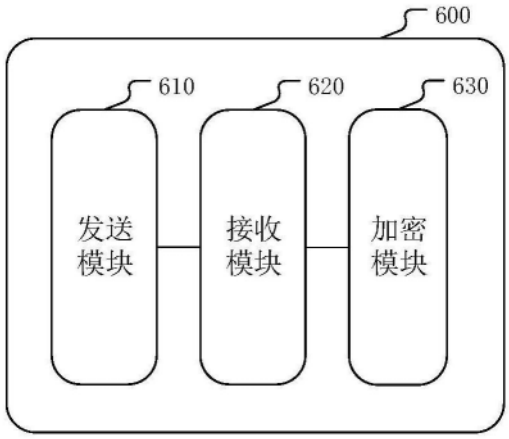

600
610
620
630
发送模块
接收模块
加密模块

图6

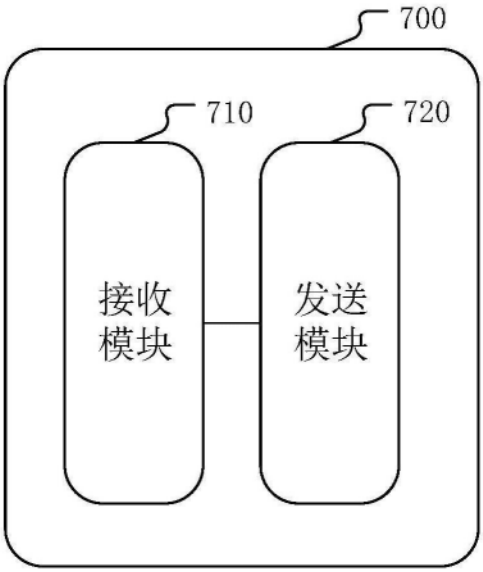

700
710
720
接收模块
发送模块

图7

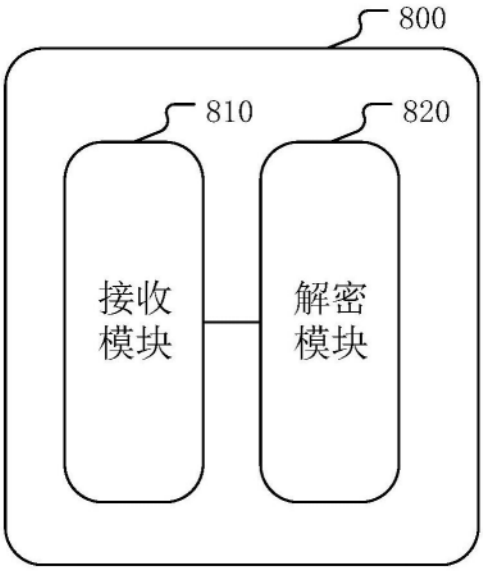


图8