(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 3 月 14 日 (14.03.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/047375 A1

(51) 国际专利分类号:
H04N 21/4788 (2011.01) *H04N 21/258* (2011.01)
H04N 21/475 (2011.01)

(21) 国际申请号: PCT/CN2017/111925

(22) 国际申请日: 2017 年 11 月 20 日 (20.11.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710804202.5 2017年9月8日 (08.09.2017) CN

(71) 申请人: 武汉斗鱼网络科技有限公司 (WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.) [CN/CN]; 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430000 (CN)。

(72) 发明人: 周志刚(ZHOU, Zhigang); 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430000 (CN)。 张文明(ZHANG, Wenming); 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430000 (CN)。 陈少杰(CHEN, Shaojie); 中国湖北省武汉市东湖开发区软件园东路1号软件产业4.1期B1栋11楼, Hubei 430000 (CN)。

(74) 代理人: 北京超凡志成知识产权代理事务所（普通合伙）(CHOFN INTELLECTUAL PROPERTY); 中国北京市海淀区北四环西路68号左岸工社1215-1218室, Beijing 100080 (CN)。

WO 2019/047375 A1

(54) **Title:** AUTHENTICATION METHOD, DEVICE, SERVER AND STORAGE MEDIUM FOR PREVENTING AUTOMATED GIFT FARMING

(54) **发明名称:** 防止被刷的验证方法、装置、服务器及存储介质

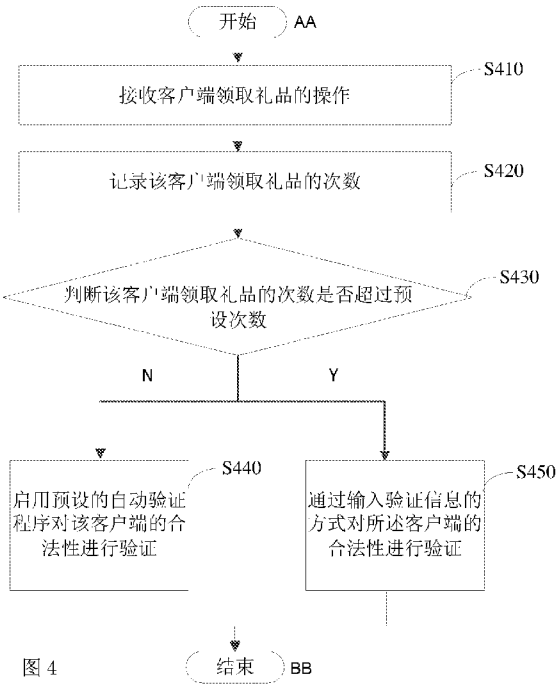

图 4

S410 Receive gift acquisition operation from user terminal
S420 Record number of gifts acquired by user terminal
S430 Has the number of gifts acquired by user terminal surpassed a preset number?
S440 Activate preset authentication program to authenticate validity of client
S450 Use manual information input method to authenticate validity of client
AA Start
BB Finish

(57) **Abstract:** The present invention provides an authentication method, a device, a server and a storage medium for preventing automated gift farming. The solution authenticates the validity of a corresponding user terminal on the basis of a number of acquired gifts. The method uses an automatic authentication method to authenticate the validity of a user terminal when the number of acquired gifts is small, and requires a manual information input authentication method to authenticate the validity of a user terminal when the number of acquired gifts is large. The invention greatly limits the automated farming of gifts by software tools and enables more viewers to participate in interactive livestream activities, thereby strengthening the audience appeal of a streaming platform and creating an

[见续页]

(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, 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))。

enjoyable user experience.

(57) 摘要：本发明提供的防止被刷的验证方法、装置、服务器及存储介质，通过领取礼品次数设置对应的客户端合法性验证方案，当领取礼品次数较少时采用自动验证的方式验证客户端的合法性，当领取礼品次数较多时需要通过手动输入验证信息的方式验证客户端的合法性，极大遏制了通过软件工具刷礼品的行为，可以让更多的观众能够参与到直播互动活动中，增加直播平台对观众的吸引力及良好的用户体验。

防止被刷的验证方法、装置、服务器及存储介质

本申请要求于2017年9月8日提交中国专利局的申请号为2017108042025、名称为“防止被刷的验证方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及网络信息安全技术领域，具体而言，涉及一种防止被刷的验证方法、装置、服务器及存储介质。

背景技术

目前，网络视频直播通过利用互联网及流媒体技术进行在线直播，随着直播平台的发展，各种各样的活动也会随之展开，例如主播直播平台（比如，斗鱼直播平台）提供观看一定时长可以领取免费礼品（比如，鱼丸），可以是通过主播打赏观众，或让观众参与进行抢宝箱等方式来促进主播与观众之间的互动。然而一部分技术人员或者黑客会编写一些脚本来实现自动领取“鱼丸”和自动抢宝箱的功能。这些编写的脚本相比其他观众手动抢礼品具有极大的优势，从而导致大多数“鱼丸”都被这些技术人员或黑客抢走，导致其他大部分观众无法获得礼品，未达到平台促进主播与观众之间互动的目的。

发明内容

为了克服现有技术中的上述不足，本发明目的在于提供一种防止被刷的验证方法、装置、服务器及存储介质，通过设置多层验证方式对客户端的合法性进行验证，在客户端领取的礼品数量次数越多时，对应的客户端合法性验证也就越严格。

为了实现上述目的，本发明较佳实施例所采用的技术方案如下所示：

第一方面，本发明较佳实施例提供一种防止被刷的验证方法，应用于与客户端通信连接的服务器，所述方法包括：

接收所述客户端领取礼品的操作；

记录该客户端领取礼品的次数；

判断该客户端领取礼品的次数是否超过预设次数；

当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对该客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

在本发明较佳实施例中，所述预设次数为两次，所述启动预设的自动验证程序对该客户端的合法性进行验证的步骤包括：

当客户端首次领取礼品时，根据接收到客户端发送的协议字段信息验证所述客户端的

合法性；

当客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性。

在本发明较佳实施例中，上述当客户端首次领取礼品时，根据接收到客户端发送的协议字段信息验证所述客户端的合法性的步骤包括：

向客户端发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及客户端加密使用的 key 值；

接收客户端上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端根据预设的加密参数进行加密得到，该加密参数包括客户端上报的用户 ID、服务器下发的礼品数量、服务器下发的礼品编号、当前客户端的时间戳、客户端的设备 ID、客户端登录时获得的令牌、客户端所属直播间的房号及客户端加密使用的 key 值；

当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致时，判定所述客户端不合法。

在本发明较佳实施例中，所述当客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性的步骤包括：

调用非对称加密算法为服务器生成一对公钥和私钥；

将服务器的公钥和客户端采用非对称加密算法生成的公钥进行互换；

下发一随机数到所述客户端，由客户端根据客户端生成的私钥和服务器的公钥对随机数进行加密；

采用服务器的私钥和客户端的公钥对客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端不合法。

在本发明较佳实施例中，所述通过输入验证信息的方式对所述客户端的合法性进行验证的步骤包括：

下发一验证信息到所述客户端；

将客户端上传的输入验证信息与下发的验证信息进行比对；

当客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法。

第二方面，本发明较佳实施例中还提供一种防止被刷的验证装置，所述装置应用于与客户端通信的服务器，所述装置包括：

接收模块，用于接收所述客户端领取礼品的操作；

记录模块，用于记录该客户端领取礼品的次数；

判断模块，用于判断该客户端领取礼品的次数是否超过预设次数；

验证模块，用于当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对该客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

在本发明较佳实施例中，所述预设次数为两次，所述验证模块所述启动预设的自动验证程序对该客户端的合法性进行验证的方式包括：

当客户端首次领取礼品时，根据接收到客户端发送的协议字段信息验证所述客户端的合法性；

当客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性。

在本发明较佳实施例中，所述验证模块在客户端首次领取礼品时，根据接收到客户端发送的协议字段信息验证所述客户端的合法性的方式包括：

向客户端发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及客户端加密使用的 key 值；

接收客户端上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端根据预设的加密参数进行加密得到，该加密参数包括客户端上报的用户 ID、服务器下发的礼品数量、服务器下发的礼品编号、当前客户端的时间戳、客户端的设备 ID、客户端登录时获得的令牌、客户端所属直播间的房号及客户端加密使用的 key 值；

当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致时，判定所述客户端不合法。

在本发明较佳实施例中，所述当客户端第二次领取礼品时，所述验证模块根据非对称加密算法验证所述客户端的合法性的方式包括：

调用非对称加密算法为服务器生成一对公钥和私钥；

将服务器的公钥和客户端采用非对称加密算法生成的公钥进行互换；

下发一随机数到所述客户端，由客户端根据客户端生成的私钥和服务器的公钥对随机数进行加密；

采用服务器的私钥和客户端的公钥对客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的

数据与下发的随机数不一致时，判定所述客户端不合法。

在本发明较佳实施例中，所述验证模块通过输入验证信息的方式对所述客户端的合法性进行验证的方式包括：

下发一验证信息到所述客户端；

将客户端上传的输入验证信息与下发的验证信息进行比对；

当客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法。

第三方面，本发明较佳实施例中还提供一种防止被刷的验证方法，所述方法应用于相互通信的客户端与服务器，所述方法包括：

所述服务器接收所述客户端领取礼品的操作；

所述服务器记录该客户端领取礼品的次数；

所述服务器判断所述客户端领取礼品的次数是否超过预设次数；

当领取礼品的次数未超过预设次数时，所述服务器启动预设的自动验证程序对所述客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

在本发明较佳实施例中，所述预设次数为两次，所述服务器启动预设的自动验证程序对所述客户端的合法性进行验证的步骤包括：

当所述客户端首次领取礼品时，所述服务器根据接收到客户端发送的协议字段信息验证所述客户端的合法性；

当所述客户端第二次领取礼品时，所述服务器根据非对称加密算法验证所述客户端的合法性。

在本发明较佳实施例中，所述当客户端首次领取礼品时，所述服务器根据接收到所述客户端发送的协议字段信息验证所述客户端的合法性的步骤包括：

所述服务器向所述客户端发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及所述客户端加密使用的 key 值；

所述服务器接收所述客户端上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端根据预设的加密参数进行加密得到，该加密参数包括所述客户端上报的用户 ID、服务器下发的礼品数量、服务器下发的礼品编号、当前所述客户端的时间戳、所述客户端的设备 ID、所述客户端登录时获得的令牌、所述客户端所属直播间的房号及所述客户端加密使用的 key 值；

当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，所述服务器判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致

时，判定所述客户端不合法。

在本发明较佳实施例中，所述当所述客户端第二次领取礼品时，所述服务器根据非对称加密算法验证所述客户端的合法性的步骤包括：

调用非对称加密算法为所述服务器生成一对公钥和私钥；

将所述服务器的公钥和所述客户端采用非对称加密算法生成的公钥进行互换；

下发一随机数到所述客户端，由所述客户端根据所述客户端生成的私钥和所述服务器的公钥对随机数进行加密；

采用所述服务器的私钥和所述客户端的公钥对所述客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端不合法。

在本发明较佳实施例中，所述通过输入验证信息的方式对所述客户端的合法性进行验证的步骤包括：

所述服务器下发一验证信息到所述客户端；

所述客户端响应验证信息输入操作，将输入的验证信息发送给所述服务器；

所述服务器将客户端上传的输入验证信息与下发的验证信息进行比对；

当客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法。

第四方面，本发明较佳实施例中还提供一种服务器，包括处理器、存储器、及防止被刷的验证装置，所述防止被刷的验证装置安装于所述存储器中并包括一个或多个由所述处理器执行的软件功能模块，所述防止被刷的验证装置包括：

接收模块，被配置为接收所述客户端领取礼品的操作；

记录模块，被配置为记录所述客户端领取礼品的次数；

判断模块，被配置为判断所述客户端领取礼品的次数是否超过预设次数；

验证模块，被配置为当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对所述客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

第五方面，本发明较佳实施例中还提供一种存储介质，该存储介质包括一组指令，当执行所述指令时，引起至少一个处理器执行本发明实施例第一方面提供的防止被刷的验证方法。

相对于现有技术而言，本发明具有以下有益效果：

本发明提供的防止被刷的验证方法及装置，通过领取礼品次数设置对应的客户端合法

性验证方案，当领取礼品次数较少时采用自动验证的方式验证客户端的合法性，当领取礼品次数较多时需要通过手动输入验证信息的方式验证客户端的合法性，极大遏制了通过软件工具刷礼品的行为，让更多的观众能够参与到直播互动活动中，增加直播平台对观众的吸引力及良好的用户体验。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本发明的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

图 1 为本发明第一较佳实施例提供的客户端与服务器通信的交互示意图。

图 2 为本发明较佳实施例提供的客户端的方框示意图。

图 3 为本发明较佳实施例提供的服务器的方框示意图。

图 4 为本发明较佳实施例提供的防止被刷的验证方法的流程示意图。

图 5 为图 4 中步骤 S440 的子步骤流程示意图。

图 6 为图 5 中步骤 S441 的子步骤流程示意图。

图 7 是图 5 中步骤 S442 的子步骤流程示意图。

图 8 是图 4 中步骤 S450 的子步骤流程示意图。

图 9 为本发明第二较佳实施例提供的防止被刷的验证装置的功能模块图。

图标：100-客户端；200-服务器；300-网络；110-第一存储器；120-第一处理器；130-第一通信单元；140-存储控制器；210-第二存储器；220-第二处理器；230-第二通信单元；500-验证装置；510-接收模块；520-记录模块；530-判断模块；540-验证模块。

具体实施方式

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，所描述的实施例是本发明一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本发明实施例的组件可以以各种不同的配置来布置和设计。因此，以下对在附图中提供的本发明的实施例的详细描述并非旨在限制要求保护的本发明的范围，而是仅仅表示本发明的选定实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。同时，在本发明的描述中，术语“第一”、“第二”等仅用于区分描述，而不能理解为指示或暗示相对重要性。

下面结合附图，对本发明的一些实施方式作详细说明。在不冲突的情况下，下述的实

施例及实施例中的特征可以相互组合。

请参照图 1，图 1 是本发明较佳实施例提供的客户端 100 与服务器 200 通信的交互示意图。所述服务器 200 可通过网络 300 与所述客户端 100 进行通信，以实现服务器 200 与客户端 100 之间的数据通信或交互。

本实施例中，所述服务器 200 可以是，但不限于，web（网站）服务器、ftp（file transfer protocol，文件传输协议）服务器等。所述客户端 100 可以是，但不限于，智能手机、个人电脑（personal computer，PC）、平板电脑、个人数字助理（personal digital assistant，PDA）、移动上网设备（mobile Internet device，MID）等。所述网络 300 可以是，但不限于，有线网络或无线网络。所述客户端 100 的操作系统可以是，但不限于，安卓（Android）系统、IOS（iPhone operating system）系统、Windows phone 系统、Windows 系统等。优选地，本实施例中，所述客户端 100 的操作系统为 Android 系统。所述应用程序可以是服务器 200 提供的任何可供客户端 100 自定义下载并安装的应用程序，例如，所述应用程序可以是斗鱼直播 APP。

请参照图 2，是图 1 中所示的客户端 100 的方框示意图。

如图 2 所示，所述客户端 100 包括第一存储器 110、第一处理器 120、第一通信单元 130 以及存储控制器 140。所述第一存储器 110、第一处理器 120、第一通信单元 130 以及存储控制器 140 相互之间直接或间接地电性连接，以实现数据的传输或交互。例如，这些元件相互之间可通过一条或多条通讯总线或信号线实现电性连接。

其中，所述第一存储器 110 可以是，但不限于，随机存取存储器（Random Access Memory，RAM），只读存储器（Read Only Memory，ROM），可编程只读存储器（Programmable Read-Only Memory，PROM），可擦除只读存储器（Erasable Programmable Read-Only Memory，EPROM），电可擦除只读存储器（Electric Erasable Programmable Read-Only Memory，EEPROM）等。其中，第一存储器 110 用于存储程序，所述第一处理器 120 在接收到执行指令后，执行所述程序。

所述第一处理器 120 可以是一种集成电路芯片，具有信号的处理能力。上述的第一处理器 120 可以是通用处理器，包括中央处理器 (Central Processing Unit，CPU)、网络处理器 (Network Processor，NP)等。还可以是数字信号处理器（DSP)）、专用集成电路（ASIC）、现成可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

所述第一通信单元 130 用于建立所述客户端 100 与所述服务器 200 二者之间的通信连接。例如，所述第一通信单元 130 可以利用射频单元发送的射频信号连接到网络 300，进

而通过网络 300 与服务器 200 的第一通信单元 130 建立通信连接，将采集到的用户行为信息发送到服务器 200，比如，将用户在客户端 100 抢礼品的行为或输入验证信息等发送到服务器 200。

可以理解，图 2 所示的结构仅为示意，所述客户端 100 还可以包括比图 2 中所示更多或者更少的组件，或者具有与图 2 所示不同的配置。图 2 中所示的各组件可以采用硬件、软件或其组合实现。

请参照图 3，是图 1 中所示的服务器 200 的方框示意图。所述服务器 200 包括第二存储器 210、第二处理器 220 以及第二通信单元 230。

所述第二存储器 210、第二处理器 220 以及第二通信单元 230 各元件相互之间直接或间接地电性连接，以实现数据的传输或交互。例如，这些元件相互之间可通过一条或多条通讯总线或信号线实现电性连接。所述第二处理器 220 用于执行所述第二存储器 210 中存储的可执行模块。

第二存储器 210 中存储有防止被刷的验证装置 500，所述防止被刷的验证装置 500 包括至少一个可以软件或固件（firmware）的形式存储于所述第二存储器 210 中的软件功能模块，所述第二处理器 220 通过运行存储在第二存储器 210 内的软件程序以及模块，如本发明实施例中的防止被刷的验证装置 500，从而执行各种功能应用以及数据处理，即实现本发明实施例中的防止被刷的验证方法。所述第二处理器 220 在接收到执行指令后，执行所述程序。所述第二通信单元 230 用于通过所述网络 300 建立所述服务器 200 与客户端 100 之间的通信连接，并用于通过所述网络 300 接收所述客户端 100 发送的采集到的用户操作信息。

第一实施例

请参照图 4，图 4 是本发明较佳实施例提供的防止被刷的验证方法的流程示意图。所述方法应用于服务器 200，所述方法的具体流程如下：

步骤 S410，接收所述客户端 100 领取礼品的操作。

在直播平台中，在进行互动活动时，所述客户端 100 会显示互动活动的界面，比如，会有宝箱图案和/或提醒观众抢礼品的控件。当观众点击这样的图案或者控件时，就会触发客户端 100 领取礼品的逻辑。此时客户端 100 就会发送一应答协议到服务器 200，告知服务器 200 客户端 100 上有领取礼品的操作。

步骤 S420，记录该客户端 100 领取礼品的次数。

服务器 200 对客户端 100 的每一次应答都会进行记录，记录下客户端 100 的身份信息（比如，设备识别号）及应答的时间，通过上述记录信息可以得知每一客户端 100 对应领取礼品的次数，以便后续采用不同的验证方式对客户端 100 的合法性进行验证。

步骤 S430，判断该客户端 100 领取礼品的次数是否超过预设次数。

在本实施例中所述预设次数可以根据盗刷的严重程度进行设置，具体地，可以设置为 2 次或 3 次。当次数没有超过预设次数，进入步骤 S440，当次数超过预设次数，进入步骤 S450。

步骤 S440，启动预设的自动验证程序对该客户端 100 的合法性进行验证。

请参照图 5，本实施例给出了当预设次数为 2 次的情形，所述步骤 S440 包括子步骤 S441 及子步骤 S442。

子步骤 S441，当客户端 100 首次领取礼品时，根据接收到客户端 100 发送的协议字段信息验证所述客户端 100 的合法性。

可选地，请参照图 6，所述子步骤 S440 可以包括以下步骤：

步骤 S441a，向直播间内所有客户端 100 发送领取礼品的协议。

在本实施例中，服务器 200 会下发当前可以领取礼品的数量、当前礼品编号、客户端 100 加密使用的 KEY 值。其中，当前礼品编号可以每一次都不一样，可以通过随机生成的方式以保证和之前没有重复。

可选地，采用以下形式表示：

Server_send_client:30 + yw10005 + bacdef;

其中 30 则标示客户端 100 可以领取的礼品数目，yw10005 标示礼品的编号，bacdef 则标示客户端 100 加密使用的 key 值。

步骤 S441b，接收客户端 100 上报的客户端协议，对所述客户端 100 协议中的协议字段进行验证。

所述客户端协议在客户端 100 上生成，所述客户端 100 根据客户端 100 上报的用户 ID、服务器 200 下发的礼品数量、服务器 200 下发的礼品编号、当前客户端 100 的时间戳、客户端 100 的设备 ID、客户端 100 登录时获得的令牌、客户端 100 所属直播间的房号及客户端 100 加密使用的 key 值进行加密得到。

可选地，所述客户端协议的形式可以如下：

encryptData = TEA.encrypt(UID + 30 +TIME +RoomID+DeviceID + Token +yw10005 , bacdef);

其中，UID 为客户端 100 上报的用户 ID，TIME 为当前客户端 100 的时间戳，RoomID 为客户端 100 所属直播间的房号，DeviceID 为客户端 100 的设备 ID，Token 为客户端 100 登录时获得的令牌。

在验证时，服务器 200 对所述客户端协议进行解密得到客户端 100 上报的协议字段，并对客户端 100 上报的协议字段进行验证。可选地，将解密得到的协议字段与服务器 200 中存储的数据进行比对。

步骤 S441c，当所述客户端协议中的协议字段与所述服务器 200 中的存储数据一致时，

判定所述客户端 100 合法，当所述客户端协议中的协议字段与所述服务器 200 存储数据不一致时，判定所述客户端 100 不合法。

在判定客户端 100 合法时，可以告知客户端 100 可以成功领取礼品，在判定客户端 100 不合法时，拒绝客户端 100 的领取操作并给出相应提醒信息。

子步骤 S442，当客户端 100 第二次领取礼品时，根据非对称加密算法验证所述客户端 100 的合法性。

可选地，请参照图 7，所述子步骤 S442 可以包括以下步骤：

步骤 S442a，调用非对称加密算法为服务器 200 生成一对公钥和私钥。

在本实施例中，服务器 200 和客户端 100 都会调用非对称加密算法各自生成一对公钥和私钥。

可选地，私钥可以使用随机数生成，对应的公钥可以调用 RSA 的接口函数生成，私钥和公钥是唯一配对的关系。

Privatekey=rand()；//私钥使用随机数生成。

Publickey=RSA.CreatePair(Privatekey)；公钥为调用 RSA 生成的。

步骤 S442b，将服务器 200 的公钥和客户端 100 采用非对称加密算法生成的公钥进行互换。

步骤 S442c，下发一随机数到所述客户端 100，由客户端 100 根据客户端 100 的私钥和服务器 200 的公钥对随机数进行加密。

其中，所述客户端 100 获得加密数据方式可以是：

客户端 100 对服务器 200 下发的随机数进行 MD5 计算，计算完成后，会使用加密算法对数据进行加密。

加密过程可以如下：

客户端 100 可以使用客户端 100 的私钥和服务器 200 的公钥生成一个共享的密钥。

KEY = RSA.Sharekey(客户端 privatekey, 服务器 publickey)；

客户端 100 计算出服务器 200 下发数据的 MD5 值。

Md5Result=MD5.Create(Server_randdate)；

通过对服务器 200 下发的随机数计算 MD5 值得到最终的 Md5Result 结果。

采用加密算法（比如，TEA 加密算法）对 Md5Result 结果加密后上报到服务器 200。

EncryptData = TEA.Encrypt(MD5Result, KEY)；

使用的 KEY 值通过客户端私钥和服务器公钥计算得到，此 KEY 值则没有在网络 300 中传输，非常安全。

步骤 S442d，采用服务器 200 的私钥和客户端 100 的公钥对客户端 100 基于下发随机

数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对。

服务器 200 将自己的私钥和服务器 200 的公钥生成一个共享的秘钥。

KEY=RSA.Sharekey(服务器 privatekey，客户端 publickey)；

服务器 200 使用 Key 值对客户端 100 上报的加密数据进行解密。

MD5Result=TEA.Encrypt(EncryptDate，Key)；

服务器 200 将解密得到的 MD5Result 与服务器 200 下发的随机数进行比对。

步骤 S442e，当解密后得到的数据与下发的随机数一致时，判定所述客户端 100 合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端 100 不合法。

在判定客户端 100 合法时，可以告知客户端 100 可以成功领取礼品，在判定客户端 100 不合法时，拒绝客户端 100 的领取操作并给出相应提醒信息。

步骤 S450，通过输入验证信息的方式对所述客户端 100 的合法性进行验证。

请参照图 8，在本实施例中，步骤 S450 可以包括以下子步骤：

子步骤 S451，下发一验证信息到所述客户端 100。

当客户端 100 领取了超过预设次数（比如，2 次）的礼物，此时，服务器 200 会对客户端 100 做进一步的合法性验证。以防止客户端 100 通过使用软件工具盗刷礼品。可选地，在本实施例中，服务器 200 会使客户端 100 弹出输入验证码的界面，同时服务器 200 通过与该客户端 100 绑定的手机号码将验证信息发送给手机。其中，所述验证信息包括但不限于，数字串、字符串及词组等。

子步骤 S452，将客户端 100 上传的输入验证信息与下发的验证信息进行比对。

观众在客户端 100 输入验证码的界面输入验证码之后，客户端 100 将输入的验证码上传给服务器 200，服务器 200 将接收的验证码与下发的验证码信息进行比对。

子步骤 S453，当客户端 100 上传的输入验证信息与下发的验证信息一致时，判定所述客户端 100 合法，当客户端 100 上传的输入验证信息与下发的验证信息不一致时，判定所述客户端 100 不合法。

在判定客户端 100 合法时，可以告知客户端 100 可以成功领取礼品，在判定客户端 100 不合法时，拒绝客户端 100 的领取操作并给出相应提醒信息。

第二实施例

请参照图 9，图 9 为为本发明较佳实施例提供的防止被刷的验证装置 500 的一种功能模块图。所述防止被刷的验证装置 500 包括接收模块 510、记录模块 520、判断模块 530 及验证模块 540。

所述接收模块 510，用于接收所述客户端 100 领取礼品的操作。

所述接收模块 510 用于执行图 5 中的步骤 S410，具体描述请参照步骤 S410，再此就不

再赘述。

所述记录模块 520，用于记录该客户端 100 领取礼品的次数。

所述记录模块 520 用于执行图 5 中的步骤 S420，具体描述请参照步骤 S420，再此就不再赘述。

所述判断模块 530，用于判断该客户端 100 领取礼品的次数是否超过预设次数。

所述验证模块 540，用于当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对该客户端 100 的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端 100 的合法性进行验证。

所述预设次数为两次，所述验证模块 540 启动自动验证的方式对该客户端 100 的合法性进行验证的方式包括：

当客户端 100 首次领取礼品时，根据接收到客户端 100 发送的协议字段信息验证所述客户端 100 的合法性；

当客户端 100 第二次领取礼品时，根据非对称加密算法验证所述客户端 100 的合法性。

所述验证模块 540 在为首次领取礼品时，根据接收到客户端 100 发送的协议字段信息验证所述客户端 100 的合法性的方式包括：

向直播间内所有客户端 100 发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及客户端 100 加密使用的 key 值；

接收客户端 100 上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端 100 根据预设的加密参数进行加密得到，该加密参数包括由所述客户端 100 根据客户端 100 上报的用户 ID、服务器 200 下发的礼品数量、服务器 200 下发的礼品编号、当前客户端 100 的时间戳、客户端 100 的设备 ID、客户端 100 登录时获得的令牌、客户端 100 所属直播间的房号及客户端 100 加密使用的 key 值。

当所述客户端协议中的协议字段与所述服务器 200 中的存储数据一致时，判定所述客户端 100 合法，当所述客户端协议中的协议字段与所述服务器 200 存储数据不一致时，判定所述客户端 100 不合法。

当客户端 100 第二次领取礼品时，所述验证模块 540 根据非对称加密算法验证所述客户端 100 的合法性的方式包括：

调用非对称加密算法为服务器 200 生成一对公钥和私钥；

将服务器 200 的公钥和客户端 100 采用非对称加密算法生成的公钥进行互换，其中，客户端 100 也调用非对称加密算法生成一对公钥和私钥；

下发一随机数到所述客户端 100，由客户端 100 根据客户端 100 生成的私钥和服务器 200 的公钥对随机数进行加密；

采用服务器 200 的私钥和客户端 100 的公钥对客户端 100 基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端 100 合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端 100 不合法。

所述验证模块 540 还用于当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端 100 进行验证。

所述验证模块 540 通过输入验证信息的方式对所述客户端 100 的合法性进行验证的方式包括：

下发一验证信息到所述客户端 100；

将客户端 100 上传的输入验证信息与下发的验证信息进行比对；

当客户端 100 上传的输入验证信息与下发的验证信息一致时，判定所述客户端 100 合法，当客户端 100 上传的输入验证信息与下发的验证信息不一致时，判定所述客户端 100 不合法。

本发明实施例还提供了一种存储介质，该存储介质包括一组指令，当执行所述指令时，引起至少一个处理器执行本发明实施例提供的防止被刷的验证方法。

综上所述，本发明提供的防止被刷的验证方法、装置、服务器及存储介质，通过领取礼品次数设置对应的客户端 100 合法性验证方案，当领取礼品次数较少时采用自动验证的方式验证客户端 100 的合法性，当领取礼品次数较多时需要通过手动输入验证信息的方式验证客户端 100 的合法性，极大遏制了通过软件工具刷礼品的行为，让更多的观众能够参与到直播互动活动中，增加直播平台对观众的吸引力及良好的用户体验。

对于本领域技术人员而言，显然本发明不限于上述示范性实施例的细节，而且在不背离本发明的精神或基本特征的情况下，能够以其他的具体形式实现本发明。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本发明的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化囊括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。

工业实用性

本申请解决现有直播互动中礼物被软件工具刷走的问题，极大地提高了直播平台对观众的吸引力和用户体验，具有极大地实用价值。

权利要求书

1.一种防止被刷的验证方法，其特征在于，所述方法应用于与客户端通信连接的服务器，所述方法包括：

接收所述客户端领取礼品的操作；

记录所述客户端领取礼品的次数；

判断所述客户端领取礼品的次数是否超过预设次数；

当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对所述客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

2.如权利要求 1 所述的验证方法，其特征在于，所述预设次数为两次，所述启动预设的自动验证程序对所述客户端的合法性进行验证的步骤包括：

当所述客户端首次领取礼品时，根据接收到客户端发送的协议字段信息验证所述客户端的合法性；

当所述客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性。

3.如权利要求 2 所述的验证方法，其特征在于，所述当客户端首次领取礼品时，根据接收到所述客户端发送的协议字段信息验证所述客户端的合法性的步骤包括：

向所述客户端发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及所述客户端加密使用的 key 值；

接收所述客户端上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端根据预设的加密参数进行加密得到，该加密参数包括所述客户端上报的用户 ID、服务器下发的礼品数量、服务器下发的礼品编号、当前所述客户端的时间戳、所述客户端的设备 ID、所述客户端登录时获得的令牌、所述客户端所属直播间的房号及所述客户端加密使用的 key 值；

当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致时，判定所述客户端不合法。

4.如权利要求 2 所述的验证方法，其特征在于，所述当所述客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性的步骤包括：

调用非对称加密算法为所述服务器生成一对公钥和私钥；

将所述服务器的公钥和所述客户端采用非对称加密算法生成的公钥进行互换；

下发一随机数到所述客户端，由所述客户端根据所述客户端生成的私钥和所述服

务器的公钥对随机数进行加密；

采用所述服务器的私钥和所述客户端的公钥对所述客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端不合法。

5.如权利要求 1-4 中任意一项所述的验证方法，其特征在于，所述通过输入验证信息的方式对所述客户端的合法性进行验证的步骤包括：

下发一验证信息到所述客户端；

将所述客户端上传的输入验证信息与下发的验证信息进行比对；

当所述客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当所述客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法。

6.一种防止被刷的验证装置，其特征在于，所述装置应用于与客户端通信的服务器，所述装置包括：

接收模块，被配置为接收所述客户端领取礼品的操作；

记录模块，被配置为记录所述客户端领取礼品的次数；

判断模块，被配置为判断所述客户端领取礼品的次数是否超过预设次数；

验证模块，被配置为当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对所述客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

7.如权利要求 6 所述的验证装置，其特征在于，所述预设次数为两次，所述验证模块启动预设的自动验证程序对该客户端的合法性进行验证的方式包括：

当所述客户端首次领取礼品时，根据接收到所述客户端发送的协议字段信息验证所述客户端的合法性；

当所述客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性。

8.如权利要求 7 所述的验证装置，其特征在于，所述验证模块在客户端首次领取礼品时，根据接收到所述客户端发送的协议字段信息验证所述客户端的合法性的方式包括：

向所述客户端发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及所述客户端加密使用的 key 值；

接收所述客户端上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端根据预设的加密参数进行加密得到，该加密

参数包括所述客户端上报的用户 ID、服务器下发的礼品数量、服务器下发的礼品编号、当前所述客户端的时间戳、所述客户端的设备 ID、所述客户端登录时获得的令牌、所述客户端所属直播间的房号及客户端加密使用的 key 值；

当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致时，判定所述客户端不合法。

9.如权利要求 7 所述的验证装置，其特征在于，当客户端第二次领取礼品时，所述验证模块根据非对称加密算法验证所述客户端的合法性的方式包括：

调用非对称加密算法为所述服务器生成一对公钥和私钥；

将所述服务器的公钥和所述客户端采用非对称加密算法生成的公钥进行互换；

下发一随机数到所述客户端，由所述客户端根据客户端生成的私钥和服务器的公钥对随机数进行加密；

采用所述服务器的私钥和所述客户端的公钥对所述客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端不合法。

10.如权利要求 6-9 中任意一项所述的验证装置，其特征在于，所述验证模块通过输入验证信息的方式对所述客户端的合法性进行验证的方式包括：

下发一验证信息到所述客户端；

将所述客户端上传的输入验证信息与下发的验证信息进行比对；

当所述客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法。

11.一种防止被刷的验证方法，其特征在于，所述方法应用于相互通信的客户端与服务器，所述方法包括：

所述服务器接收所述客户端领取礼品的操作；

所述服务器记录该客户端领取礼品的次数；

所述服务器判断所述客户端领取礼品的次数是否超过预设次数；

当领取礼品的次数未超过预设次数时，所述服务器启动预设的自动验证程序对所述客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

12.如权利要求 11 所述的验证方法，其特征在于，所述预设次数为两次，所述服务

器启动预设的自动验证程序对所述客户端的合法性进行验证的步骤包括：

当所述客户端首次领取礼品时，所述服务器根据接收到客户端发送的协议字段信息验证所述客户端的合法性；

当所述客户端第二次领取礼品时，所述服务器根据非对称加密算法验证所述客户端的合法性。

13.如权利要求 12 所述的验证方法，其特征在于，所述当客户端首次领取礼品时，所述服务器根据接收到所述客户端发送的协议字段信息验证所述客户端的合法性的步骤包括：

所述服务器向所述客户端发送领取礼品的协议，其中，协议内容包括礼品数量、礼品编号及所述客户端加密使用的 key 值；

所述服务器接收所述客户端上报的所述客户端协议，对所述客户端协议中的协议字段进行验证，其中，所述客户端协议由所述客户端根据预设的加密参数进行加密得到，该加密参数包括所述客户端上报的用户 ID、服务器下发的礼品数量、服务器下发的礼品编号、当前所述客户端的时间戳、所述客户端的设备 ID、所述客户端登录时获得的令牌、所述客户端所属直播间的房号及所述客户端加密使用的 key 值；

当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，所述服务器判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致时，判定所述客户端不合法。

14.如权利要求 12 所述的验证方法，其特征在于，所述当所述客户端第二次领取礼品时，所述服务器根据非对称加密算法验证所述客户端的合法性的步骤包括：

调用非对称加密算法为所述服务器生成一对公钥和私钥；

将所述服务器的公钥和所述客户端采用非对称加密算法生成的公钥进行互换；

下发一随机数到所述客户端，由所述客户端根据所述客户端生成的私钥和所述服务器的公钥对随机数进行加密；

采用所述服务器的私钥和所述客户端的公钥对所述客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对；

当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端不合法。

15.如权利要求 11-14 中任意一项所述的验证方法，其特征在于，所述通过输入验证信息的方式对所述客户端的合法性进行验证的步骤包括：

所述服务器下发一验证信息到所述客户端；

所述客户端响应验证信息输入操作，将输入的验证信息发送给所述服务器；

所述服务器将客户端上传的输入验证信息与下发的验证信息进行比对；

当客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法。

16.一种服务器，其特征在于，包括：

处理器；

存储器；及

防止被刷的验证装置，所述防止被刷的验证装置安装于所述存储器中并包括一个或多个由所述处理器执行的软件功能模块，所述防止被刷的验证装置包括：

接收模块，被配置为接收所述客户端领取礼品的操作；

记录模块，被配置为记录所述客户端领取礼品的次数；

判断模块，被配置为判断所述客户端领取礼品的次数是否超过预设次数；

验证模块，被配置为当领取礼品的次数未超过预设次数时，启动预设的自动验证程序对所述客户端的合法性进行验证，当领取礼品的次数超过预设次数，通过输入验证信息的方式对所述客户端的合法性进行验证。

17.一种存储介质，该存储介质包括一组指令，当执行所述指令时，引起至少一个处理器执行权利要求 1-5 任一项所述的方法。

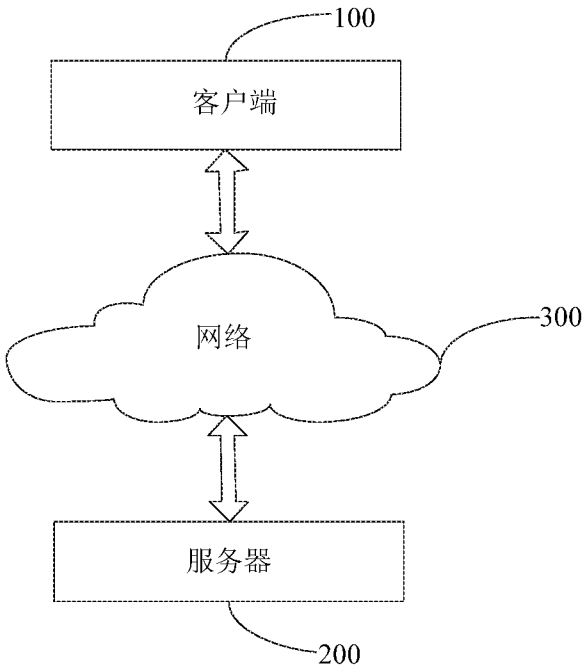

图 1

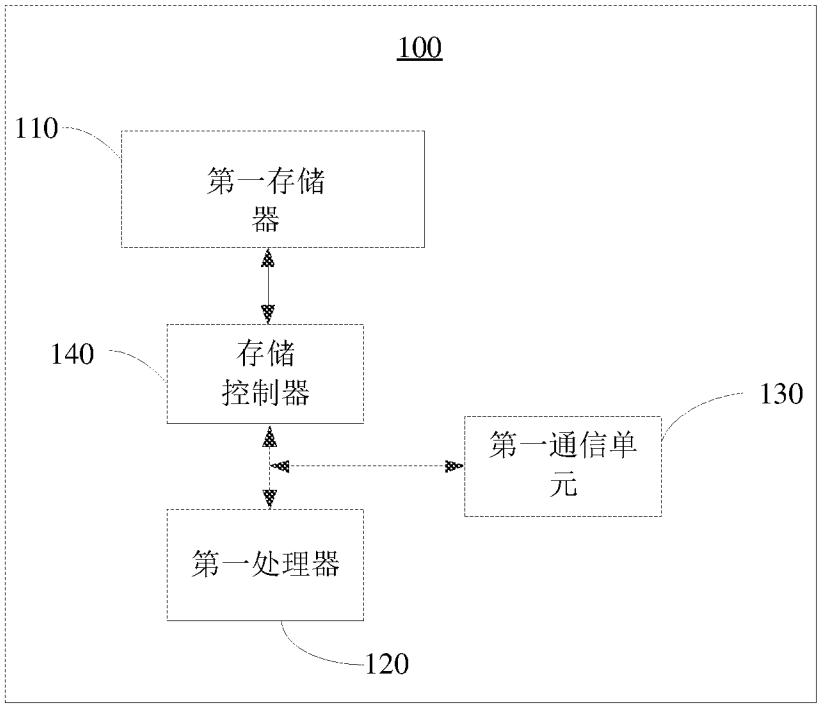

图 2

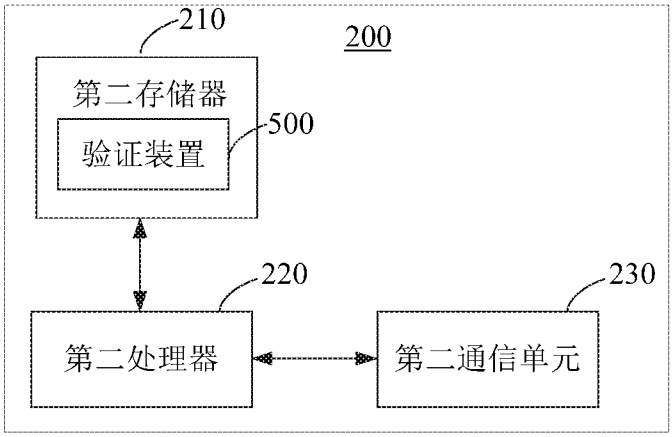
210
200
第二存储器
500
验证装置
220
230
第二处理器
第二通信单元

图 3

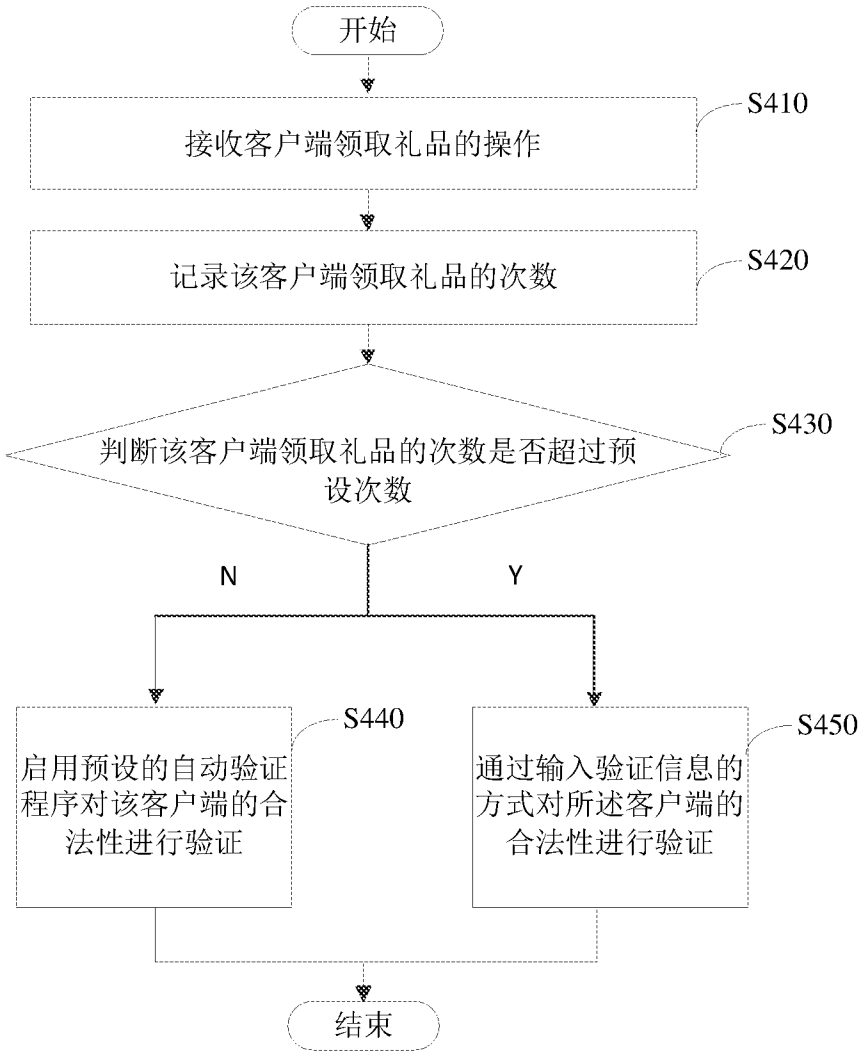
开始
S410
接收客户端领取礼品的操作
S420
记录该客户端领取礼品的次数
S430
判断该客户端领取礼品的次数是否超过预设次数
N
Y
S440
启用预设的自动验证程序对该客户端的合法性进行验证
S450
通过输入验证信息的方式对所述客户端的合法性进行验证
结束

图 4

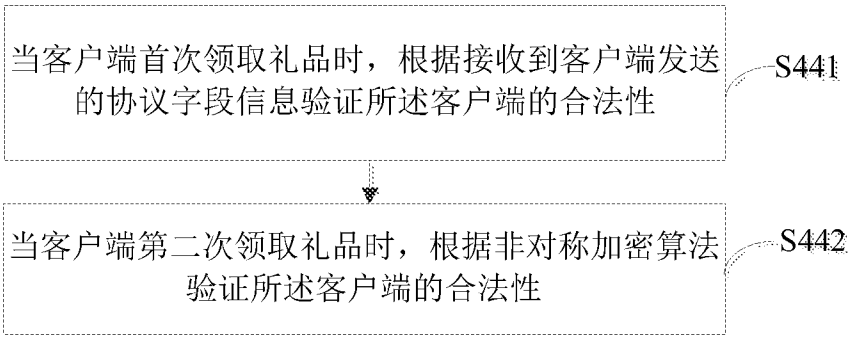
当客户端首次领取礼品时，根据接收到客户端发送的协议字段信息验证所述客户端的合法性
S441
当客户端第二次领取礼品时，根据非对称加密算法验证所述客户端的合法性
S442

图 5

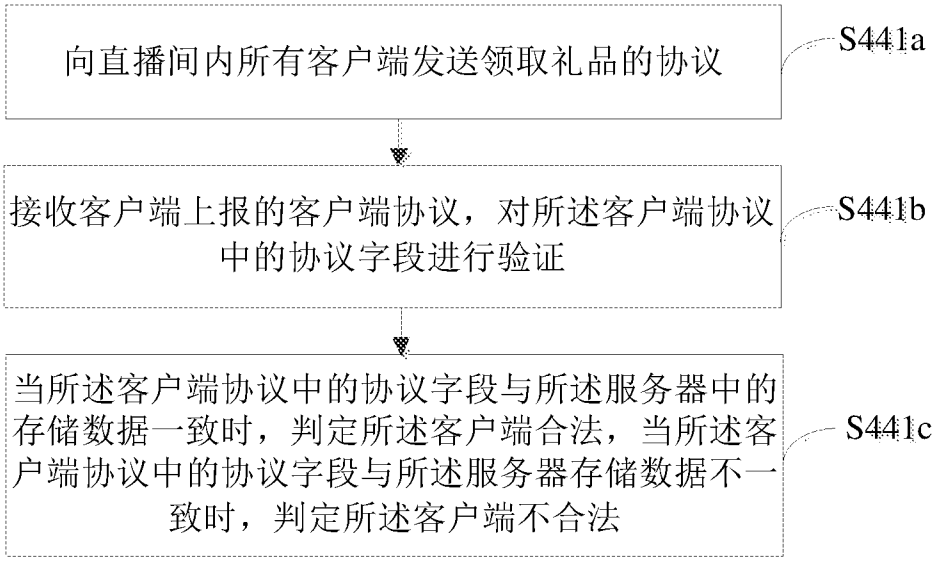
向直播间内所有客户端发送领取礼品的协议
S441a
接收客户端上报的客户端协议，对所述客户端协议中的协议字段进行验证
S441b
当所述客户端协议中的协议字段与所述服务器中的存储数据一致时，判定所述客户端合法，当所述客户端协议中的协议字段与所述服务器存储数据不一致时，判定所述客户端不合法
S441c

图 6


调用非对称加密算法为服务器生成一对公钥和私钥
S442a
将服务器的公钥和客户端采用非对称加密算法生成的公钥进行互换
S442b
下发一随机数到所述客户端，由客户端根据客户端的私钥和服务器的公钥对随机数进行加密
S442c
采用服务器的私钥和客户端的公钥对客户端基于下发随机数处理后得到的加密数据进行解密，将解密后得到的数据与下发的随机数进行比对
S442d
当解密后得到的数据与下发的随机数一致时，判定所述客户端合法，当解密后得到的数据与下发的随机数不一致时，判定所述客户端不合法
S442e

图 7

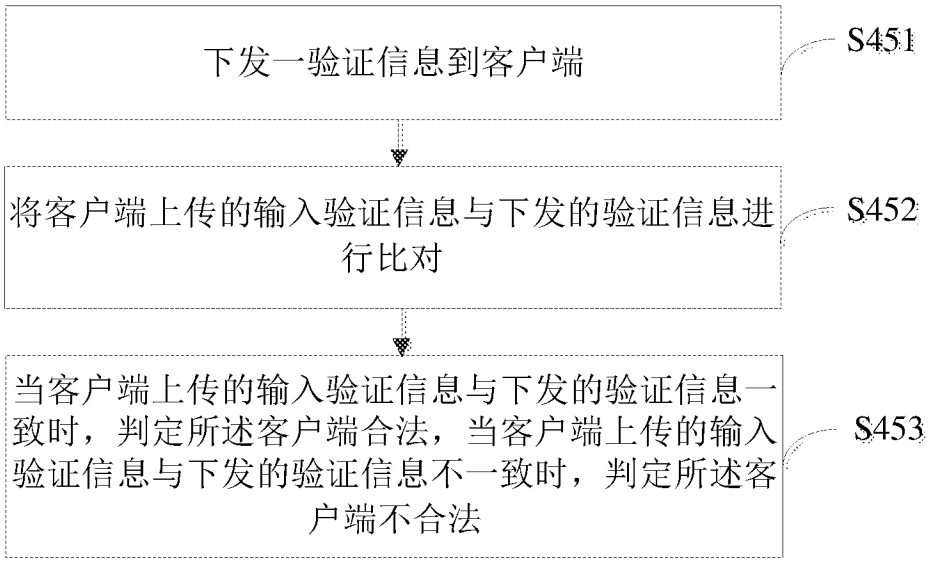
下发一验证信息到客户端
S451
将客户端上传的输入验证信息与下发的验证信息进行比对
S452
当客户端上传的输入验证信息与下发的验证信息一致时，判定所述客户端合法，当客户端上传的输入验证信息与下发的验证信息不一致时，判定所述客户端不合法
S453

图 8

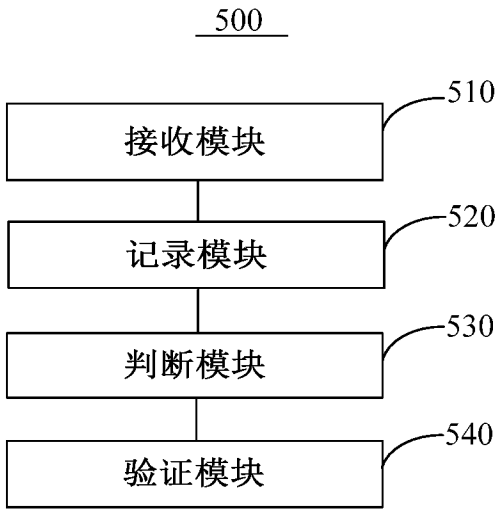
500
接收模块
510
记录模块
520
判断模块
530
验证模块
540

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/111925

A. CLASSIFICATION OF SUBJECT MATTER

H04N 21/4788(2011.01)i; H04N 21/475(2011.01)i; H04N 21/258(2011.01)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)

H04N

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)

CNABS; CNTXT; CNKI; VEN; USTXT: 直播, 互动, 交互, 礼品, 礼物, 赠品, 点击, 领取, 获取, 次数, 阈值, 验证, 认证, 黑客, 盗刷, 非对称, 加密, 公钥, 私钥, 输入, 验证码, 首次, 第一次, 第二, gift, present, get, acquisition, win, time, frequency, threshold, verification, certification, steal, hacker, encrypt, key, first, second

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102624677 A (ALIBABA GROUP HOLDING LIMITED) 01 August 2012 (2012-08-01) description, paragraphs [0031]-[0062]	1-17
Y	CN 106022826 A (WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.) 12 October 2016 (2016-10-12) description, paragraphs [0037]-[0063]	1-17
Y	CN 106452756 A (WANG, DONG) 22 February 2017 (2017-02-22) claim 4	2-5, 7-10, 12-15, 17
A	CN 105447715 A (BEIJING JINGDONG SHANGKE INFORMATION TECHNOLOGY CO., LTD. ET AL.) 30 March 2016 (2016-03-30) entire document	1-17
A	CN 106228410 A (WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.) 14 December 2016 (2016-12-14) entire document	1-17
A	US 2010034383 A1 (TURK DOUGHAN) 11 February 2010 (2010-02-11) entire document	1-17

☐ 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
22 January 2018	**31 January 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China (ISA/CN) **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/CN2017/111925

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	102624677	A	01 August 2012	CN	102624677	B	10 December 2014
				HK	1168953	A1	31 July 2015
CN	106022826	A	12 October 2016		None		
CN	106452756	A	22 February 2017		None		
CN	105447715	A	30 March 2016		None		
CN	106228410	A	14 December 2016		None		
US	2010034383	A1	11 February 2010	US	2012069996	A1	22 March 2012
				CA	2531411	C	14 February 2017
				US	2014331047	A1	06 November 2014
				CA	2531411	A1	23 June 2007
				US	9350713	B2	24 May 2016

国际检索报告

国际申请号
PCT/CN2017/111925

A. 主题的分类

H04N 21/4788(2011.01)i; H04N 21/475(2011.01)i; H04N 21/258(2011.01)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)

H04N

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）)

CNABS; CNTXT; CNKI; VEN; USTXT: 直播，互动，交互，礼品，礼物，赠品，点击，领取，获取，次数，阈值，验证，认证，黑客，盗刷，非对称，加密，公钥，私钥，输入，验证码，首次，第一次，第二，gift, present, get, acquisition, win, time, frequency, threshold, verification, certification, steal, hacker, encrypt, key, first, second

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
Y	CN 102624677 A (阿里巴巴集团控股有限公司) 2012年 8月 1日 (2012-08-01) 说明书第[0031]-[0062]段	1-17
Y	CN 106022826 A (武汉斗鱼网络科技有限公司) 2016年 10月 12日 (2016-10-12) 说明书第[0037]-[0063]段	1-17
Y	CN 106452756 A (王栋) 2017年 2月 22日 (2017-02-22) 权利要求4	2-5, 7-10, 12-15, 17
A	CN 105447715 A (北京京东尚科信息技术有限公司等) 2016年 3月 30日 (2016-03-30) 全文	1-17
A	CN 106228410 A (武汉斗鱼网络科技有限公司) 2016年 12月 14日 (2016-12-14) 全文	1-17
A	US 2010034383 A1 (TURK DOUGHAN) 2010年 2月 11日 (2010-02-11) 全文	1-17

☐ 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 1月 22日	2018年 1月 31日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 杨浩 电话号码 (86-10)62411449

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/111925

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	102624677	A	2012年 8月 1日	CN	102624677	B	2014年 12月 10日
				HK	1168953	A1	2015年 7月 31日
CN	106022826	A	2016年 10月 12日		无		
CN	106452756	A	2017年 2月 22日		无		
CN	105447715	A	2016年 3月 30日		无		
CN	106228410	A	2016年 12月 14日		无		
US	2010034383	A1	2010年 2月 11日	US	2012069996	A1	2012年 3月 22日
				CA	2531411	C	2017年 2月 14日
				US	2014331047	A1	2014年 11月 6日
				CA	2531411	A1	2007年 6月 23日
				US	9350713	B2	2016年 5月 24日