(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
2017 年 3 月 30 日 (30.03.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/050150 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/098818

(22) 国际申请日: 2016 年 9 月 13 日 (13.09.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510608978.0 2015 年 9 月 22 日 (22.09.2015) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人; 及

(71) 申请人 (仅对美国): 任卿 (REN, Qing) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 陈航 (CHEN, Hang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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))。

(54) Title: SECURE VOICE COMMUNICATION METHOD AND DEVICE BASED ON INSTANT COMMUNICATION

(54) 发明名称 : 基于即时通讯的安全语音通讯方法及装置

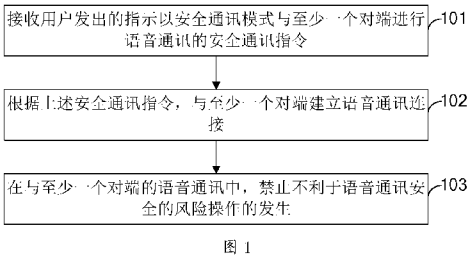


图 1

(57) Abstract: Provided are a secure voice communication method and device based on instant communication. The method comprises: receiving a secure communication instruction sent by a user to indicate voice communication with at least one opposite end in a secure communication mode; establishing a voice communication connection with the at least one opposite end according to the secure communication instruction; and during voice communication with the at least one opposite end, forbidding the occurrence of a risk operation adverse to the security of voice communication. By providing a secure communication mode, the present application can solve the security problem of voice communication in instant communication scenarios, thereby improving the security of instant communication.

(57) 摘要: 本申请提供一种基于即时通讯的安全语音通讯方法及装置。方法包括：接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令；根据安全通讯指令，与至少一个对端建立语音通讯连接；在与至少一个对端的语音通讯中，禁止不利于语音通讯安全的风险操作的发生。本申请通过提供安全通讯模式，可以解决即时通讯场景中语音通讯的安全问题，提高即时通讯的安全性。

WO 2017/050150 A1

基于即时通讯的安全语音通讯方法及装置

【技术领域】

本申请涉及通信技术领域，尤其涉及一种基于即时通讯的安全语音通讯方法及装置。

【背景技术】

随着互联网及通讯技术的发展，即时通讯逐渐兴起，并已成为目前最为流行的通讯方式。即时通讯使人们之间的通讯更加方便、及时，但同时也带来了信息安全问题。例如，在即时通讯过程中，用户可以随时截屏，将通讯内容发送给其它好友，导致信息被泄露。

为了解决即时通讯带来的信息安全问题，现有技术出现了类似澡堂模式或阅后即焚模式等方案，用以解决即时通讯场景中文本信息的安全问题。但是，对于即时通讯场景中语音通讯的安全问题，目前尚未很好的解决。

【发明内容】

本申请的多个方面提供一种基于即时通讯的安全语音通讯方法及装置，用以解决即时通讯场景中语音通讯的安全问题，提高即时通讯的安全性。

本申请的一方面，提供一种基于即时通讯的安全语音通讯方法，包括：

接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令；

根据所述安全通讯指令，与所述至少一个对端建立语音通讯连接；

在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全的风险操作的发生。

在本申请的一可选实施方式中，所述接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令，包括：

接收所述用户发出的启动安全通讯模式的启动指令；

根据所述启动指令，向所述用户展示安全通讯界面；

接收所述用户通过所述安全通讯界面发出的所述安全通讯指令。

在本申请的一可选实施方式中，所述在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯的安全的风险操作的发生，包括以下至少一种实现方式：

在实现所述安全通讯模式的过程中，禁止实现用于实现所述风险操作的应用级功能；

在与所述至少一个对端的语音通讯中，屏蔽用于实现所述风险操作的应用级功能；

在与所述至少一个对端的语音通讯中，禁止调用用于实现所述风险操作的系统级功能。

在本申请的一可选实施方式中，所述在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全的风险操作的发生，包括：

在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全且与所述语音通讯的安全等级相匹配的风险操作的发生。

在本申请的一可选实施方式中，所述在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全且与所述语音通讯的安全等级相匹配的风险操作的发生之前，包括：

接收所述用户发出的安全等级指令；

根据所述安全等级指令，确定所述语音通讯的安全等级。

在本申请的一可选实施方式中，所述风险操作包括以下至少一种：

录音操作、外放操作、外接设备操作、通讯记录保存操作、显示所述用户与所述至少一个对端的身份信息的操作以及截屏操作。

本申请的另一方面，提供一种基于即时通讯的安全语音通讯装置，包括：

指令接收模块，用于接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令；

连接建立模块，用于根据所述安全通讯指令，与所述至少一个对端建立

语音通讯连接;

安全处理模块，用于在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全的风险操作的发生。

在本申请的一可选实施方式中，所述指令接收模块具体用于:

接收所述用户发出的启动安全通讯模式的启动指令;

根据所述启动指令，向所述用户展示安全通讯界面;

接收所述用户通过所述安全通讯界面发出的所述安全通讯指令。

在本申请的一可选实施方式中，所述安全处理模块具体用于执行以下至少一种操作:

在实现所述安全通讯模式的过程中，禁止实现用于实现所述风险操作的应用级功能;

在与所述至少一个对端的语音通讯中，屏蔽用于实现所述风险操作的应用级功能;

在与所述至少一个对端的语音通讯中，禁止调用用于实现所述风险操作的系统级功能。

在本申请的一可选实施方式中，所述安全处理模块具体用于:

在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全且与所述语音通讯的安全等级相匹配的风险操作的发生。

在本申请的一可选实施方式中，所述指令接收模块还用于:

接收所述用户发出的安全等级指令;

根据所述安全等级指令，确定所述语音通讯的安全等级。

在本申请的一可选实施方式中，所述风险操作包括以下至少一种:

录音操作、外放操作、外接设备操作、通讯记录保存操作、显示所述用户与所述至少一个对端的身份信息的操作以及截屏操作。

在本申请中，允许用户以安全通讯模式与至少一个对端进行语音通讯，则当用户需要与至少一个对端以安全通讯模式进行语音通讯时，可以发出安全通讯指令;根据用户发出的指示以安全通讯模式与至少一个对端进行语音

通讯的安全通讯指令，与至少一个对端建立语音通讯连接，并在与至少一个对端的语音通讯中，禁止不利于该语音通讯安全的风险操作的发生，从而解决即时通讯场景中语音通讯的安全问题，提高即时通讯的安全性。

【附图说明】

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请一实施例提供的基于即时通讯的安全语音通讯方法的流程示意图;

图 2 为本申请一实施例提供的基于即时通讯的安全语音通讯装置的结构示意图。

【具体实施方式】

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

图 1 为本申请一实施例提供的基于即时通讯的安全语音通讯方法的流程示意图。如图 1 所示，该方法包括:

101、接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令。

102、根据上述安全通讯指令，与至少一个对端建立语音通讯连接。

103、在与至少一个对端的语音通讯中，禁止不利于语音通讯安全的风险操作的发生。

本实施例提供一种基于即时通讯的安全语音通讯方法，可由基于即时通讯的安全语音通讯装置（简称为安全语音通讯装置）来实现，主要用于解决即时通讯场景中语音通讯的安全问题，满足用户通话隐私的保密需求，提高即时通讯的安全性。本实施例的方法可用于各种类型的即时通讯应用，例如钉钉、旺旺、来往、QQ、微信等。本实施例所述的语音通讯泛指即时通讯场景中一切包括语音的通讯场景，例如视频聊天、语音聊天、免费电话、实时对讲、电话会议、视频会议以及应用提供的语音提醒等。

在本实施例中，安全语音通讯装置向用户提供一种安全通讯模式，允许用户在安全通讯模式下与至少一个对端进行语音通讯。本实施例中的安全通讯模式是一种通过禁止不利于语音通讯安全的风险操作来保证语音通讯的安全性的通讯模式。值得说明的是，根据即时通讯应用的不同，该安全通讯模式的名称可以不同。以钉钉为例，其提供的安全通讯模式称为澡堂模式，但不限于此名称。举例说明，本实施例提供的安全通讯模式的名称还可以是私聊模式、安全模式、保密模式等。

具体的，当用户与至少一个对端之间的语音通讯需要保密时，可以发出指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令。对安全语音通讯装置来说，接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令。

可选的，安全语音通讯装置可以为安全通讯模式设置一安全通讯界面，以安全通讯模式进行的语音通话在安全通讯界面上完成。当用户需要以安全通讯模式与至少一个对端进行语音通讯时，可以发出启动该安全通讯模式的启动指令。例如，用户可以通过安全语音通讯装置提供的安全通讯入口发出启动指令，所述安全通讯入口可以是一菜单项、图标或按钮等。对安全语音通讯装置来说，接收用户发出的启动安全通讯模式的启动指令；根据该启动指令，向用户展示安全通讯界面。用户通过该安全通讯界面发出安全通讯指

令。可选的，在该安全通讯界面上，设置有供用户发出安全通讯指令的控件，例如图标或按钮，用户通过点击该控件发出安全通讯指令。或者，预先设置安全通讯指令对应的手势，用户可以在安全通讯界面上发出指示以安全通讯模式进行语音通讯的手势，从而发出安全通讯指令。

以钉钉为例，用户与至少一个对端之间的语音通讯可以是用户发起的与至少一个对端用户进行语音交互的通讯过程，也可以是用户通过钉钉提供的语音提醒功能对至少一个对端用户进行语音提醒（简称为钉电话）的过程。

当用户需要与至少一个对端进行语音交互时，可以在通讯录中找到至少一个对端用户，点击该至少一个对端用户进入与该至少一个对端用户的即时通讯界面，在该即时通讯界面的导航栏上显示一指向安全通讯界面（或进入安全通讯模式）的图标，在钉钉中，该图标具体为一“眼镜”图标，但不限于此。用户通过点击该“眼镜”图标可以发出启动安全通讯模式的启动指令。安全语音通讯装置根据该启动指令，向用户展示安全通讯界面，该安全通讯界面为澡堂模式的通讯界面。用户通过澡堂模式的通讯界面上设置的控件发出安全通讯指令，或者用户通过发出预设的手势从而发出安全通讯指令。

当用户通过钉钉提供的语音提醒功能对至少一个对端用户进行语音提醒时，可以在通讯录中找到至少一个对端用户，点击至少一个对端用户进入至少一个对端用户的个人信息页，在该个人信息页上设置有钉一下图标或按钮。用户点击钉一下图标或按钮可以发出启动安全通讯模式的启动指令，安全语音通讯装置根据该启动指令，向用户展示安全通讯界面，该安全通讯界面实际上为一钉界面。在该钉界面上可以设置普通钉提醒按钮和安全钉提醒按钮，以供用户选择普通钉电话和安全钉电话。用户可以在录入语音提醒信息后，点击安全钉按钮发出安全通讯指令，安全语音通讯装置以安全通讯模式将语音提醒信息发送给至少一个对端。

在接收到用户发出的安全通讯指令后，安全语音通讯装置根据该安全通讯指令，与至少一个对端建立语音通讯连接。该安全通信指令携带有至少一个对端的标识，所述至少一个对端的标识可以是账号或手机号或 IP 地址等任

何能够唯一标识对端身份的信息。所述至少一个对端可以是一个，适用于端到端的安全通话场景；所述至少一个对端也可以是多个，适用于多人进行安全通话的场景，例如群聊、电话会议、视频会议等场景。其中，安全语音通讯装置可以采用传输控制协议（Transmission Control Protocol，TCP）和用户数据包协议（User Datagram Protocol，UDP）这两种协议与至少一个对端建立语音通讯连接。或者，安全语音通讯装置也可以通过网络套接字（Socket）与至少一个对端建立语音通讯连接。

在建立语音通讯连接后，用户可以与至少一个对端进行语音通讯。在现有即时通讯应用中，一些操作可能会对语音通讯的安全性产生不利影响，例如录音操作、外放操作、外接设备操作、通讯记录保存操作、显示用户与至少一个对端的身份信息的操作以及截屏操作等可能会造成语音通讯的相关信息的泄露，给语音通讯带来安全隐患。

例如，现有即时通讯一般都支持对语音通讯过程进行录音，该录音内存要么存储于终端设备本地，要么上传至服务器，在这些过程中，录音内容很容易被不法分子或第三人获取，例如不法分子通过木马盗取终端设备本地的录音内容，或者通过拦截上传过程获取录音内容，从而造成该语音通讯内容的泄露，给用户带来不可估量的损失。因此，为了保证语音通讯的安全，在语音通讯过程中，可以禁止录音操作。

例如，现有即时通讯一般都支持外放功能，例如扬声器或免提功能，使用外放功能，能够更加清晰的听到至少一个对端的声音，但是通讯内容可能被其它用户听到，造成语音通讯内容的泄露，从而给用户带来不可估量的损失或者造成用户隐私的泄露。因此，为了保证语音通讯的安全，在语音通讯过程中，可以禁止外放操作。例如，可以禁止用户使用扬声器或免提功能。在产品具体实现上，可以将扬声器或免提功能的按钮灰度处理，对用户变得不可操作，从而禁止用户使用扬声器或免提功能。

例如，现有即时通讯一般都支持耳麦或蓝牙耳机功能，而且一些用户在语音通讯过程中喜欢使用耳麦或蓝牙耳机，这样可以排除外界干扰，更加清

晰的听到对方的声音，但是如果用户将耳麦或蓝牙耳机等外接设备接入其它设备上，例如接入录音设备上对语音通讯过程进行录音等，也会造成语音通讯内容的泄露。因此，为了保证语音通讯的安全，在语音通讯过程中，可以禁止外接设备操作。例如，可以禁用外接设备功能，当用户外接耳麦或蓝牙耳机时，可以提示用户该功能不可用。

例如，现有即时通讯一般都具有自动保存通话记录的功能，所保存的通话记录要么存储于终端设备本地，要么上传至服务器，在这些过程中，通话记录很容易被不法分子或第三人获取，例如不法分子通过木马盗取终端设备本地的通话记录，或者通过拦截上传过程获取通话记录，从而造成该语音通讯内容的泄露，给用户带来不可估量的损失。因此，为了保证语音通讯的安全，在语音通讯过程中，可以禁止通讯记录保存操作。

例如，现有即时通讯一般都支持截屏操作，用户在语音通讯过程中可能会在与至少一个对端的即时通讯界面中传输或输入其它内容，用户通过截屏可以轻易将聊天信息发送给其它用户，从而造成语音通讯过程中有关信息的泄露。因此，为了保证语音通讯的安全，在语音通讯过程中，可以禁止截屏操作。

本实施例将上述不利于语音通讯安全的操作称为风险操作，风险操作主要是指能够或者可能对语音通讯造成泄露的各种操作。所述不利于语音通讯安全的风险操作可以包括以下至少一种：录音操作、外放操作、外接设备操作、通讯记录保存操作、显示用户与至少一个对端的身份信息的操作以及截屏操作等。

在本实施例中，为了降低风险操作给语音通讯带来的安全隐患，实现以安全通讯模式与至少一个对端进行语音通讯，安全语音通讯装置在用户与至少一个对端的语音通讯中，禁止不利于该语音通讯安全的风险操作的发生，从而保证语音通讯的安全性。

其中，根据不利于语音通讯安全的风险操作的实现形式的不同，在与至少一个对端的语音通讯中，禁止这些风险操作的实现方式也会有所不同。

可选的，在与至少一个对端的语音通讯中，禁止不利于该语音通讯安全的风险操作的发生的实现方式包括以下至少一种：

一种实现方式为：在实现安全通讯模式的过程中，禁止实现用于实现上述不利于语音通讯安全的风险操作的应用级功能。该实现方式主要针对那些由安全语音通讯装置自身实现的功能所实现的风险操作。安全语音通讯装置自身可以实现一些功能，这些功能是由安全语音通讯装置自身实现的，所以称为应用级功能。如果这些应用级功能能够产生不利于语音通讯安全的风险操作，则在实现安全通讯模式时可以禁止实现用于实现这些风险操作的应用级功能。举例说明，假设安全语音通讯装置自身实现录音功能，但通过该录音功能产生的录音操作不利于语音通讯的安全，因此，在实现安全通讯模式时，禁止实现录音功能，即在安全通讯模式下，安全语音通讯装置不具有录音功能，也就不会对语音通讯产生录音操作。

另一种实现方式为：在与至少一个对端的语音通讯中，屏蔽用于实现上述不利于语音通讯安全的风险操作的应用级功能。该实现方式主要针对那些由安全语音通讯装置自身实现的功能所实现的风险操作。在实际应用中，安全语音通讯装置自身可以实现一些功能，这些功能是由安全语音通讯装置自身实现的，所以称为应用级功能。如果这些功能中有一些功能产生的操作不利于语音通讯，则可以在用户与至少一个对端的语音通讯中，屏蔽用于实现这些风险操作的应用级功能。例如，假设安全语音通讯装置自身实现截屏功能、通讯记录保存功能等，但截屏功能、通讯记录保存功能所实现的截屏操作、通讯记录保存操作可能会对语音通讯的安全性带来不利影响，于是在语音通讯过程中，可以屏蔽掉这些功能。在该实施方式中，安全语音通讯装置可以实现这些功能，这样便于其它通讯模式使用，而在安全通讯模式下，将这些功能屏蔽掉可以保证语音通讯的安全性。

又一种实现方式为：在用户与至少一个对端的语音通讯中，禁止调用用于实现上述不利于语音通讯安全的风险操作的系统级功能。该实现方式主要针对那些需要调用操作系统提供的功能所实现的风险操作。有一些功能是由

操作系统提供的，安全语音通讯装置需要调用操作系统提供的相应功能完成相应操作，这些由操作系统提供的功能称为系统级功能。如果系统级功能所实现的操作不利于语音通讯安全，则安全语音通讯装置可以在安全通讯模式下禁止调用实现这些风险操作的系统级功能。例如，假设录音功能是由操作系统提供的，但通过该录音功能产生的录音操作不利于语音通讯的安全，因此，在安全通讯模式下，可以禁止调用该录音功能，从而不会对语音通讯产生录音操作，以保证语音通讯的安全性。

在一可选实施方式中，安全语音通讯装置除了向用户提供安全通讯模式之外，还可以为用户设置安全通讯的等级，允许用户选择语音通讯的安全等级。例如，安全语音通讯装置可以预先设定安全等级，例如安全等级 1-3，则用户可以选择其语音通讯的安全等级为等级 1-3 中之一。不同安全等级对应不同的风险操作，安全等级越高，在语音通讯过程中需要禁止的风险操作越多。例如，安全等级 1 对应的风险操作包括：录音操作和外放操作；安全等级 2 对应的风险操作包括：录音操作、外放操作、外接设备操作、通讯记录保存操作；安全等级 3 对应的风险操作包括：录音操作、外放操作、外接设备操作、通讯记录保存操作、显示用户与至少一个对端的身份信息的操作以及截屏操作。值得说明的是，这里的安全等级并不限于 3 级，同理，每一安全等级对应的风险操作仅仅是示例性的，并不受限于此。

基于上述，安全语音通讯装置还可以接收用户发出的安全等级指令，该安全等级指令指示用户为其语音通讯选择的安全等级；安全语音通讯装置根据用户的安全等级指令，确定语音通讯的安全等级。相应的，安全语音通讯装置在用户与至少一个对端的语音通讯中，禁止不利于该语音通讯安全且与该语音通讯的安全等级相匹配的风险操作的发生。在该实施方式中，允许用户进行安全等级的选择，使用起来更加灵活。例如，如果用户的语音通讯安全性较高，可以选择较高的安全等级，保证语音通讯的安全性；如果用户的语音通讯需要保证一定安全性，但对安全性要求又不是特别高，此时可以选择较低的安全等级，在保证安全性需求的同时，用户可以选择使用一些功能，

例如通讯记录保存操作、显示用户与至少一个对端的身份信息的操作等，有利于提高即时通讯的灵活性。由此可见，在本实施例中，安全语音通讯装置在与至少一个对端的语音通讯中，禁止不利于该语音通讯安全的风险操作的发生，解决了即时通讯场景中语音通讯的安全问题，提高即时通讯的安全性。

需要说明的是，对于前述的各方法实施例，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，本申请并不受所描述的动作顺序的限制，因为依据本申请，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，所涉及的动作和模块并不一定是本申请所必须的。

在上述实施例中，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。

图 2 为本申请一实施例提供的基于即时通讯的安全语音通讯装置的结构示意图。如图 2 所示，该装置包括：指令接收模块 21、连接建立模块 22 和安全处理模块 23。

指令接收模块 21，用于接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令。

连接建立模块 22，用于根据指令接收模块 21 接收的安全通讯指令，与至少一个对端建立语音通讯连接。

安全处理模块 23，用于在与至少一个对端的语音通讯中，禁止不利于该语音通讯安全的风险操作的发生。

在一可选实施方式中，指令接收模块 21 具体用于：

接收用户发出的启动安全通讯模式的启动指令；

根据启动指令，向用户展示安全通讯界面；

接收用户通过安全通讯界面发出的安全通讯指令。

在一可选实施方式中，安全处理模块 23 具体用于执行以下至少一种操作：

在实现安全通讯模式的过程中，禁止实现用于实现风险操作的应用级功能；

在与至少一个对端的语音通讯中，屏蔽用于实现风险操作的应用级功能；

在与至少一个对端的语音通讯中，禁止调用用于实现风险操作的系统级功能。

在一可选实施方式中，安全处理模块 23 具体用于:

在与至少一个对端的语音通讯中，禁止不利于语音通讯安全且与语音通讯的安全等级相匹配的风险操作的发生。

基于上述，指令接收模块 21 还用于:

接收用户发出的安全等级指令;

根据安全等级指令，确定语音通讯的安全等级。

在一可选实施方式中，上述风险操作包括以下至少一种:

录音操作、外放操作、外接设备操作、通讯记录保存操作、显示用户与至少一个对端的身份信息的操作以及截屏操作。

本实施例提供的基于即时通讯的安全语音通讯装置可以作为各种即时通讯应用的客户端实现，但不限于此。

本实施例提供的基于即时通讯的安全语音通讯装置，允许用户以安全通讯模式与至少一个对端进行语音通讯，可以根据用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令，与至少一个对端建立语音通讯连接，并在与至少一个对端的语音通讯中，禁止不利于该语音通讯安全的风险操作的发生，从而解决即时通讯场景中语音通讯的安全问题，提高即时通讯的安全性。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，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，仅仅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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

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网络单元上。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。

另外，在本申请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，也可以采用硬件加软件功能单元的形式实现。

上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元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（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施例所述方法的部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权 利 要 求 书

1、一种基于即时通讯的安全语音通讯方法，其特征在于，包括:

接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令;

根据所述安全通讯指令，与所述至少一个对端建立语音通讯连接;

在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全的风险操作的发生。

2、根据权利要求 1 所述的方法，其特征在于，所述接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令，包括:

接收所述用户发出的启动安全通讯模式的启动指令;

根据所述启动指令，向所述用户展示安全通讯界面;

接收所述用户通过所述安全通讯界面发出的所述安全通讯指令。

3、根据权利要求 1 所述的方法，其特征在于，所述在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯的安全的风险操作的发生，包括以下至少一种实现方式:

在实现所述安全通讯模式的过程中，禁止实现用于实现所述风险操作的应用级功能;

在与所述至少一个对端的语音通讯中，屏蔽用于实现所述风险操作的应用级功能;

在与所述至少一个对端的语音通讯中，禁止调用用于实现所述风险操作的系统级功能。

4、根据权利要求 1 所述的方法，其特征在于，所述在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全的风险操作的发生，包括:

在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全且与所述语音通讯的安全等级相匹配的风险操作的发生。

5、根据权利要求 4 所述的方法，其特征在于，所述在与所述至少一个对端

的语音通讯中，禁止不利于所述语音通讯安全且与所述语音通讯的安全等级相匹配的风险操作的发生之前，包括:

接收所述用户发出的安全等级指令;

根据所述安全等级指令，确定所述语音通讯的安全等级。

6、根据权利要求 1-5 任一项所述的方法，其特征在于，所述风险操作包括以下至少一种:

录音操作、外放操作、外接设备操作、通讯记录保存操作、显示所述用户与所述至少一个对端的身份信息的操作以及截屏操作。

7、一种基于即时通讯的安全语音通讯装置，其特征在于，包括:

指令接收模块，用于接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令;

连接建立模块，用于根据所述安全通讯指令，与所述至少一个对端建立语音通讯连接;

安全处理模块，用于在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全的风险操作的发生。

8、根据权利要求 7 所述的装置，其特征在于，所述指令接收模块具体用于:

接收所述用户发出的启动安全通讯模式的启动指令;

根据所述启动指令，向所述用户展示安全通讯界面;

接收所述用户通过所述安全通讯界面发出的所述安全通讯指令。

9、根据权利要求 7 所述的装置，其特征在于，所述安全处理模块具体用于执行以下至少一种操作:

在实现所述安全通讯模式的过程中，禁止实现用于实现所述风险操作的应用级功能;

在与所述至少一个对端的语音通讯中，屏蔽用于实现所述风险操作的应用级功能;

在与所述至少一个对端的语音通讯中，禁止调用用于实现所述风险操作的系统级功能。

10、根据权利要求 7 所述的装置，其特征在于，所述安全处理模块具体用于：

在与所述至少一个对端的语音通讯中，禁止不利于所述语音通讯安全且与所述语音通讯的安全等级相匹配的风险操作的发生。

11、根据权利要求 10 所述的装置，其特征在于，所述指令接收模块还用于：

接收所述用户发出的安全等级指令；

根据所述安全等级指令，确定所述语音通讯的安全等级。

12、根据权利要求 7-11 任一项所述的装置，其特征在于，所述风险操作包括以下至少一种：

录音操作、外放操作、外接设备操作、通讯记录保存操作、显示所述用户与所述至少一个对端的身份信息的操作以及截屏操作。

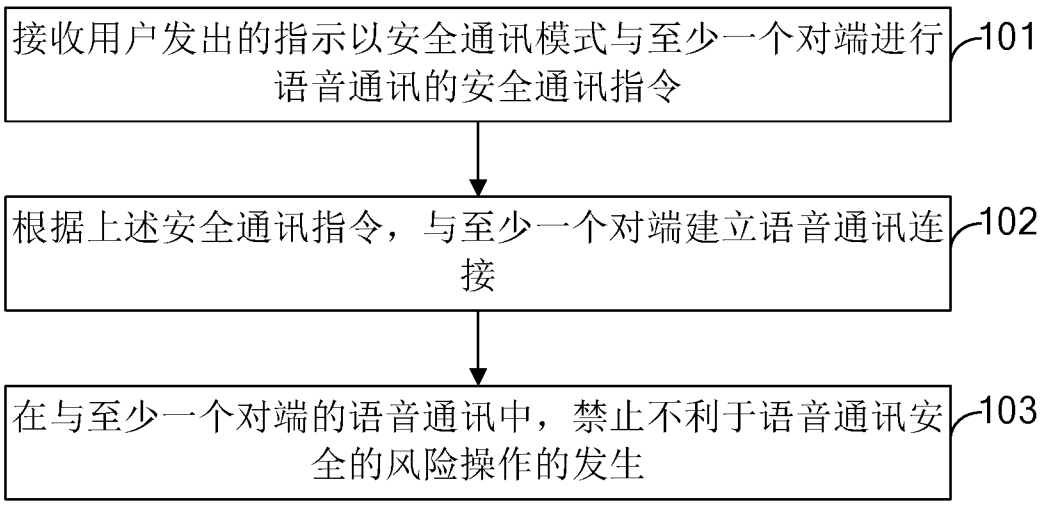

接收用户发出的指示以安全通讯模式与至少一个对端进行语音通讯的安全通讯指令
101
根据上述安全通讯指令，与至少一个对端建立语音通讯连接
102
在与至少一个对端的语音通讯中，禁止不利于语音通讯安全的风险操作的发生
103

图 1

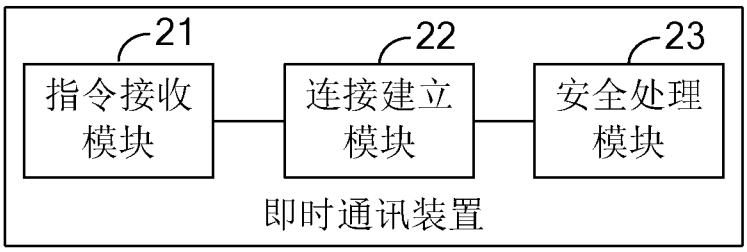

21
指令接收模块
22
连接建立模块
23
安全处理模块
即时通讯装置

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/098818

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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 H04W

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: screenshot mobile phone safe?? activation close forbid record secrecy video terminal phone call

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105323243 A (ALIBABA GROUP HOLDING LIMITED), 10 February 2016 (10.02.2016), claims 1-12	1-12
Y	CN 102045712 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 04 May 2011 (04.05.2011), description, paragraphs [0016]-[0030]	1-12
Y	CN 104038614 A (TECHFAITH WIRELESS COMMUNICATION TECHNOLOGY LIMITED), 10 September 2014 (10.09.2014), description, paragraphs [0004]-[0010]	1-12
A	CN 102955904 A (BEIJING NETQIN TECHNOLOGY COMPANY LTD.), 06 March 2013 (06.03.2013), the whole document	1-12
A	US 2013347084 A1 (FUTUREWEI TECHNOLOGIES, INC.), 26 December 2013 (26.12.2013), the whole document	1-12

☐ 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
19 October 2016 (19.10.2016)	**27 October 2016 (27.10.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **FANG, Ting** Telephone No.: (86-10) **62413316**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/098818

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105323243 A	10 February 2016	None	
CN 102045712 A	04 May 2011	CN 103152740 A	12 June 2013
		CN 103108084 A	15 May 2013
CN 104038614 A	10 September 2014	None	
CN 102955904 A	06 March 2013	US 2013047256 A1	21 February 2013
US 2013347084 A1	26 December 2013	KR 20150024388 A	06 March 2015
		EP 2850554 A1	25 March 2015
		WO 2013189291 A1	27 December 2013
		JP 2015524223 A	20 August 2015
		CA 2877409 A1	27 December 2013
		CN 104364793 A	18 February 2015

国际检索报告

国际申请号
PCT/CN2016/098818

A. 主题的分类

H04L 29/06(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 H04W

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:安全 激活 关闭 禁止 录音 截屏 保密 视频 终端 手机 电话 通话 safe?? activation close forbid record secrecy video terminal phone call

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
PX	CN 105323243 A (阿里巴巴集团控股有限公司) 2016年 2月 10日 (2016-02-10) 权利要求1-12	1-12
Y	CN 102045712 A (奇智软件北京有限公司) 2011年 5月 4日 (2011-05-04) 说明书第[0016]-[0030]段	1-12
Y	CN 104038614 A (德信无线通讯科技北京有限公司) 2014年 9月 10日 (2014-09-10) 说明书第[0004]-[0010]段	1-12
A	CN 102955904 A (网秦无限北京科技有限公司) 2013年 3月 6日 (2013-03-06) 全文	1-12
A	US 2013347084 A1 (FUTUREWEI TECHNOLOGIES, INC.) 2013年 12月 26日 (2013-12-26) 全文	1-12

☐ 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
2016年 10月 19日	2016年 10月 27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	方婷
传真号 (86-10)62019451	电话号码 (86-10)62413316

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/098818

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	105323243	A	2016年 2月 10日	无			
CN	102045712	A	2011年 5月 4日	CN	103152740	A	2013年 6月 12日
				CN	103108084	A	2013年 5月 15日
CN	104038614	A	2014年 9月 10日	无			
CN	102955904	A	2013年 3月 6日	US	2013047256	A1	2013年 2月 21日
US	2013347084	A1	2013年 12月 26日	KR	20150024388	A	2015年 3月 6日
				EP	2850554	A1	2015年 3月 25日
				WO	2013189291	A1	2013年 12月 27日
				JP	2015524223	A	2015年 8月 20日
				CA	2877409	A1	2013年 12月 27日
				CN	104364793	A	2015年 2月 18日