

# (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  
2012年3月1日 (01.03.2012)

PCT

(10) 国际公布号  
WO 2012/024904 A1

- (51) 国际专利分类号:  
H04L 12/08 (2006.01)
- (21) 国际申请号: PCT/CN2011/070270
- (22) 国际申请日: 2011年1月14日 (14.01.2011)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201010265334.3 2010年8月25日 (25.08.2010) CN
- (71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): **张保华 (ZHANG, Bao-hua)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限

公司转交, Guangdong 518057 (CN)。 **邓方民 (DENG, Fangmin)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。  
**于松 (YU, Song)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。  
**薛涛 (XUE, Tao)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。  
**曹耀斌 (CAO, Yaobin)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

- (74) 代理人: **北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE)**; 中国北京市海淀区学清路8号B座1601A, Beijing 100192 (CN)。

[见续页]

(54) Title: METHOD AND SYSTEM FOR PRE-ACCESSING CONFERENCE TELEPHONE AND NETWORK SIDE DEVICE

(54) 发明名称: 一种会议电话预接入的方法、系统及网络侧设备

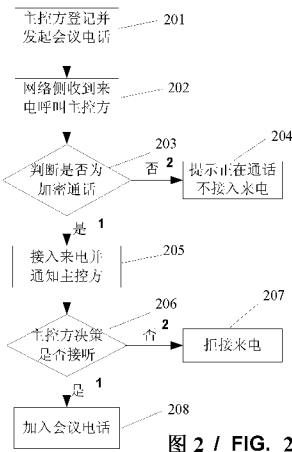


图 2 / FIG. 2

- 1 YES
- 2 NO
- 201 REGISTER AND INITIATE A CONFERENCE TELEPHONE BY A MAIN CONTROL PARTY
- 202 RECEIVE AN INCOMING CALL CALLING THE MAIN CONTROL PARTY BY A NETWORK SIDE
- 203 JUDGE WHETHER THE CALL IS AN ENCRYPTION CONVERSATION
- 204 PROMPT THAT THE CONVERSATION IS IN PROCESSING AND DO NOT ACCESS THE INCOMING CALL
- 205 ACCESS THE INCOMING CALL AND INFORM THE MAIN CONTROL PARTY
- 206 DECIDE WHETHER THE CALL IS ACCESSED BY THE MAIN CONTROL PARTY
- 207 REFUSE THE INCOMING CALL
- 208 JOIN IN THE CONFERENCE TELEPHONE

(57) Abstract: A method for pre-accessing a conference telephone is disclosed in the present invention. The method includes: a network side detects a received call with a main control party as a target after the main control party initiates an encryption conference telephone; the call is not accessed if the call is a non-encryption conversation; the call is allowed to access if the call is an encryption conversation. A system for pre-accessing a conference telephone is also disclosed in the present invention, wherein the system includes a pre-accessing processing unit and a call type detection unit in the network side. A network side device is also disclosed in the present invention. The present invention realizes pre-accessing of the encryption conference telephone, thus improving safety of encryption conversation, as well as avoiding a problem that a user is frequently interfered while performing the encryption conference telephone.

(57) 摘要: 本发明公开了一种会议电话预接入的方法, 所述方法包括: 主控方发起加密会议电话后, 网络侧对收到的目标为所述主控方的呼叫进行检测, 如果该呼叫为非加密通话, 则不予接入该呼叫; 如果该呼叫为加密通话, 则允许接入该呼叫。本发明还公开了一种会议电话预接入的系统, 所述系统包括网络侧的预接入处理单元和呼叫类型检测单元。本发明还公开了一种网络侧设备。本发明实现了加密会议电话预接入, 既提高了加密通话的安全性, 同时也避免了用户在进行加密会议电话时频繁受到干扰的问题。

WO 2012/024904 A1



(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG)。

**根据细则 4.17 的声明:**

— 发明人资格(细则 4.17(iv))

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

## 一种会议电话预接入的方法、系统及网络侧设备

### 技术领域

5 本发明涉及移动通信技术领域，更具体地，涉及一种会议电话预接入的方法、系统及网络侧设备。

### 背景技术

语音通话是移动通讯网的最基本的业务，也是最重要的业务，也最受用户和运营商的关注，其保密性和安全性也是移动网络技术的重要内容之一。  
10 目前，具有加密通话功能的手机受到越来越多的关注，尤其是政府敏感部门，以及情报机关等非常重视安全和保密的组织和个人。

手机会议电话功能，以其组建简单且移动性好的优点，越来越被人们广泛使用。会议电话主要用于三个或更多用户同时进行通话。对于发起方来说，必须首先在网络侧登记三方通话的业务才能使用。

15 本发明申请的发明人发现：目前具有加密通话功能的手机基本上都是基于端到端的语音加解密，不需要网络参与，因此，也就无法利用网络中的安全密钥加密因子（Ki）或者其他由 Ki 产生的密钥如密码密钥（Cipher Key，简称为 CK）等进行加解密运算。

20 综上所述，现有手机会议电话业务的安全性不高，有可能被其他未知的非加密通话干扰。

### 发明内容

本发明解决的技术问题是提供一种会议电话预接入的方法、系统及网络侧设备，提高会议电话业务的安全性。

25 为解决上述技术问题，本发明提供了一种会议电话预接入的方法，所述方法包括：

主控方发起加密会议电话后，网络侧对收到的目标为所述主控方的呼叫

进行检测，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，则允许接入该呼叫。

其中，网络侧对收到的目标为所述主控方的呼叫进行检测的步骤包括：

5 若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密，则网络侧判定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

其中，所述呼叫类型通过所述呼叫建立消息中的用户-用户信息元素（UUIE）字段实现，且当所述 UUIE 字段内容为“加密语音（ENCRYPTION VOICE）”时，表示呼叫类型为加密。

所述方法还包括：

10 所述加密会议电话进入通话状态后，所述加密会议电话的终端和网络侧根据所述呼叫类型，对通话的语音数据进行加密和解密处理。

其中，对通话的语音数据的加密和解密处理的步骤包括：

主叫终端使用发送方密码密钥（CK）作为运算因子对上行语音数据进行加密，并将加密后的语音数据上传到网络侧；以及

15 网络侧收到所述加密后的语音数据后，使用发送方 CK 作为运算因子进行解密后，再使用接收方 CK 作为运算因子加密语音数据，并将加密后的语音数据发送给被叫终端；被叫终端使用接收方 CK 作为运算因子解密收到的下行语音数据。

所述方法还包括：

20 所述网络侧允许接入所述呼叫后，由所述主控方决定是否接听并将其加入本次加密会议电话。

为解决上述技术问题，本发明还提供了一种会议电话预接入的系统，所述系统包括网络侧的预接入处理单元和呼叫类型检测单元，其中，

25 所述呼叫类型检测单元设置为：接收到主控方发起的会议电话后，对收到的目标为所述主控方的呼叫进行检测，并将检测结果传送给所述预接入处理单元；

所述预接入处理单元设置为：根据所述呼叫类型检测单元传送的检测结  
果，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，  
则允许接入该呼叫。

5 其中，所述呼叫类型检测单元是设置为按照如下方式对所述呼叫进行检  
测：

若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密，则判  
定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

所述系统还包括终端中的呼叫类型添加模块，

10 所述呼叫类型添加模块设置为：在发起呼叫时，通过呼叫建立消息中的  
用户-用户信息元素（UUIE）字段添加呼叫类型，且当所述 UUIE 字段内容  
为“加密语音（ENCRYPTION VOICE）”时，表示呼叫类型为加密。

所述系统还包括网络侧的网络侧硬件加密模块和终端的终端硬件加密模  
块，其中：

15 所述终端硬件加密模块设置为：当所述终端为发送方终端时，使用发送  
方密码密钥（CK）作为运算因子对上行语音数据进行加密，并将加密后的语  
音数据上传到网络侧；以及，当所述终端为接收方终端时，接收到下行语音  
数据后，使用接收方 CK 作为运算因子对收到的下行语音数据进行解密；

20 所述网络侧硬件加密模块设置为：收到发送方上传的加密后的语音数据  
后，使用发送方 CK 作为运算因子进行解密后，再使用接收方 CK 作为运算  
因子加密语音数据，并将加密后的语音数据发送给接收方。

为解决上述技术问题，本发明还提供了一种网络侧设备，所述设备包括  
预接入处理单元和呼叫类型检测单元，其中，

25 所述呼叫类型检测单元设置为：接收到主控方发起的会议电话后，对收  
到的目标为所述主控方的呼叫进行检测，并将检测结果传送给所述预接入处  
理单元；

所述预接入处理单元设置为：根据所述呼叫类型检测单元传送的检测结  
果，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，

则允许接入该呼叫。

其中，所述呼叫类型检测单元是设置为按照如下方式对所述呼叫进行检测：

5 若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密，则判定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

其中，所述呼叫类型检测单元通过呼叫建立消息中的用户-用户信息元素（UUIE）字段添加的呼叫类型对所述呼叫进行检测，且当所述 UUIE 字段内容为“加密语音（ENCRYPTION VOICE）”时，表示呼叫类型为加密。

所述设备还包括网络侧硬件加密模块，其中：

10 所述网络侧硬件加密模块设置为：收到发送方的终端使用发送方密码密钥（CK）作为运算因子对上行语音数据进行加密，并将加密后的语音数据上传到网络侧设备的加密后的语音数据后，使用发送方 CK 作为运算因子进行解密后，再使用接收方 CK 作为运算因子加密语音数据，并将加密后的语音数据发送给接收方。

15

本发明提供了一种会议电话预接入的方法、系统和网络侧设备，从而实现加密会议电话预接入，既提高了加密通话的安全性，同时也避免了用户在进行加密会议电话时频繁受到干扰的问题。本发明技术方案具有较强的通用性和实用性，另外该功能主要由网络侧实现，终端除了增加加密通话类型之外，几乎不需要做更多的改动。

20

## 附图概述

图 1 为本发明中的语音加解密流程图；

图 2 为本发明实施例的实现加密会议电话预接入的流程示意图。

25

## 本发明的较佳实施方式

本发明的基本思想在于，提供一种加密多方通话的预接入方案，基于终端和核心网同时使用 CK 对语音进行硬件加密，实现加密会议电话的预接入，以保证会议电话的安全性。

5 基于上述思想，本发明提供的一种实现加密会议电话预接入的方法，具体采用如下技术方案：

主控方发起加密会议电话后，网络侧对收到的目标为所述主控方的呼叫进行检测，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，则允许接入该呼叫。

其中，主控方可以是主叫终端，也可以是被叫终端。

10 进一步地，所述网络侧按照如下方式对所述呼叫进行检测：

若所述呼叫的呼叫建立消息中包含呼叫类型（Call type），且呼叫类型为加密，则判定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

进一步地，所述呼叫类型通过 UUIE 字段实现，且当所述 UUIE 字段内容为“ENCRYPTION VOICE”时，表示呼叫类型为加密。

15 进一步地，所述方法还包括：

所述网络侧允许接入所述呼叫后，由所述主控方决定是否接听并将其加入本次加密会议电话。

20 根据以上描述的加密会议电话的预接入的方法，主叫终端按照约定提供呼叫类型（主叫在发起呼叫时定义），网络对呼叫类型（Call type）进行判断并进行预接入处理。其中，加密通话类型可采用用户-用户信息元素（User-User Information Element, UUIE）字段表示，例如自定义为“加密语音（ENCRYPTION VOICE）”。终端使用 UUIE 字段表示加密通话类型，并可通过设置（SETUP）信令作为载体传输，网络和被叫终端都可以获取该  
25 字段的内容以便查询呼叫类型。会议发起方首先在网络侧注册登记三方通话的业务，当会议电话发起后，所有呼叫主控方的来电都由网络侧预处理。如果判断来电的呼叫类型是非加密的，则网络不接入此次通话，提示用户被叫

用户正在通话中，不方便接听；如果判断来电的呼叫类型是加密的，即 UUIE 字段内容为“ENCRYPTION VOICE”，则接入此次来电并通知到主控方，然后由主控方决定是否接听并将其加入会议电话。

此外，本发明中，在进入通话（Conversion）状态之后，加密会议电话的终端和网络侧需要对语音通话的上下行语音数据进行加密、和解密处理，具体包括：

主叫终端使用发送方 CK 作为运算因子对上行语音数据进行加密，并将加密后的语音数据上传到网络侧；以及

网络侧收到所述加密后的语音数据后，使用发送方 CK 作为运算因子进行解密后，再使用接收方 CK 作为运算因子加密语音数据，并将加密后的语音数据发送给被叫终端；被叫终端使用接收方 CK 作为运算因子解密收到的下行语音数据。

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

本发明实施例所使用的加密会议电话的语音通话加解密流程如图 1 所示。由于 Ki 作为移动通讯网的根密钥，具有非常高的保密性和安全性，因此，本发明实施例中采用运算因子 CK 对语音数据进行加密和解密处理。参见图 1，本实施例的会议电话的加、解密流程描述如下：

主叫终端使用主叫侧的运算因子  $CK_1$  对采集的原始数据进行加密，并将加密的自适应多速率（Adaptive Multi Rate, AMR）语音数据上传到网络，网络侧收到 AMR 语音数据后，使用相同的运算因子  $CK_1$  解密语音数据，然后再使用被叫侧的运算因子  $CK_2$  加密语音数据，并将数据发送到被叫终端，被叫终端使用同样的运算因子  $CK_2$  解密收到的 AMR 语音数据。图中的  $CK_3$  和  $CK_4$  则用于一个反向的过程，其功能与  $CK_1$  和  $CK_2$  功能相同。其中 CK 在每次通话建立的过程中是可变的。

图 2 为本发明实施例的实现加密会议电话的预接入流程示意图，结合图 2，该流程具体步骤描述如下：

步骤 201：主控方在网络侧登记三方通话业务，并发起会议电话；

5 步骤 202：网络侧收到来电，被叫用户是本次会议电话的主控方；

步骤 203：网络检测本次来电的通话类型，本实施例中具体是检测 UUIE 字段是否为自定义的加密类型“ENCRYPTION VOICE”，如果是，执行步骤 205，如果不是，执行步骤 204；

10 步骤 204：如果此次通话类型为普通呼叫，则提示主叫用户被叫正在通话中，不方便接听，然后结束来电；

步骤 205：如果此次通话类型为加密呼叫，则接入来电并通知会议电话的主控方；

步骤 206：主控方根据实际情况决策是否要接入新的来电，比如和会议电话的其他成员商量是否接受；

15 步骤 207：主控方接听本次来电，并将其加入会议电话；

步骤 208：主控方不方便接听本次来电，直接拒绝来电。

按照以上步骤，可实现本发明所述方法及过程。

20 本发明实施例提供的实现加密会议电话预接入的系统是在终端和核心网交换单元都配置硬件加密模块，对上下行语音数据进行加解密。

发送方终端将 AMR 语音送入终端硬件加密模块进行 X 加密运算，加密运算因子采用发送方 CK，从而得到加密 AMR 语音帧，并将加密 AMR 语音帧上传到网络侧；

25 网络侧将此加密语音帧及发送方 CK 送入网络侧硬件加密模块，网络硬件加密模块使用 X 算法，以发送方 CK 为运算因子对语音数据进行解密，然后再使用 X 算法，以接收方 CK 为运算因子对语音数据进行加密，并返回给

网络设备运算结果，然后网络设备将此加密语音帧发送给接收方终端；

接收方在得到下行语音数据后，将此加密语音数据和接收方 CK 送入终端硬件加密模块进行解密，从而得到普通语音帧，接下来的处理则与普通语音呼叫处理相同，将解密后的 AMR 语音数据送入 DSP (Digital Signal Processor, 数字信号处理器) 中得到 PCM (Pulse Code Modulation, 脉冲编码调制录音) 数据，将 PCM 数据送入声码器发声即可。

采用这种加密电话方式，在网络侧无法监听，而且在无线环境传输也是相当于双加密的，更加保密和安全。

具体地，本发明实施例的实现加密会议电话预接入的系统包括网络侧的预接入处理单元和呼叫类型检测单元，其中：

所述呼叫类型检测单元设置为：收到主控方发起的会议电话后，对收到的目标为所述主控方的呼叫进行检测，并将检测结果传送给所述预接入处理单元；

所述预接入处理单元设置为：根据所述呼叫类型检测单元传送的检测结果，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，则允许接入该呼叫。

此外，所述呼叫类型检测单元是设置为按照如下方式对所述呼叫进行检测：

若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密，则判定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

此外，所述系统还包括终端中的呼叫类型添加模块，

所述呼叫类型添加模块设置为：在发起呼叫时，通过呼叫建立消息中的 UUIE 字段添加呼叫类型，且当所述 UUIE 字段内容为“ENCRYPTION VOICE”时，表示呼叫类型为加密。

此外，所述系统还包括网络侧硬件加密模块和终端硬件加密模块，其中：

所述终端硬件加密模块设置为：使用发送方 CK 作为运算因子对上行语音数据进行加密，并将加密后的语音数据上传到网络侧；以及，接收到下行

语音数据后,使用接收方 CK 作为运算因子对收到的下行语音数据进行解密;

所述网络侧硬件加密模块设置为:收到发送方上传的加密后的语音数据后,使用发送方 CK 作为运算因子进行解密后,再使用接收方 CK 作为运算因子加密语音数据,并将加密后的语音数据发送给接收方。

5

本实施例还提供了一种网络侧设备,所述设备包括预接入处理单元和呼叫类型检测单元,其中,

所述呼叫类型检测单元设置为:接收到主控方发起的会议电话后,对收到的目标为所述主控方的呼叫进行检测,并将检测结果传送给所述预接入处理单元;

所述预接入处理单元设置为:根据所述呼叫类型检测单元传送的检测结果,如果该呼叫为非加密通话,则不予接入该呼叫;如果该呼叫为加密通话,则允许接入该呼叫。

所述呼叫类型检测单元是设置为按照如下方式对所述呼叫进行检测:

15 若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密,则判定所述呼叫为加密通话;否则,判定所述呼叫为非加密通话。

所述呼叫类型检测单元通过呼叫建立消息中的用户-用户信息元素(UUIE)字段添加的呼叫类型对所述呼叫进行检测,且当所述 UUIE 字段内容为“加密语音(ENCRYPTION VOICE)”时,表示呼叫类型为加密。

20 所述设备还包括网络侧硬件加密模块,其中:

所述网络侧硬件加密模块设置为:收到发送方的终端使用发送方密码密钥(CK)作为运算因子对上行语音数据进行加密,并将加密后的语音数据上传到网络侧设备的加密后的语音数据后,使用发送方 CK 作为运算因子进行解密后,再使用接收方 CK 作为运算因子加密语音数据,并将加密后的语音数据发送给接收方。

25

以上仅为本发明的优选实施案例而已，并不用于限制本发明，本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员可根据本发明做出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

- 5 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何
- 10 特定形式的硬件和软件的结合。

### 工业实用性

- 15 本发明实现加密会议电话预接入，既提高了加密通话的安全性，同时也避免了用户在进行加密会议电话时频繁受到干扰的问题。本发明技术方案具有较强的通用性和实用性，另外该功能主要由网络侧实现，终端除了增加加密通话类型之外，几乎不需要做更多的改动。

## 权 利 要 求 书

1、一种会议电话预接入的方法，所述方法包括：

5 主控方发起加密会议电话后，网络侧对收到的目标为所述主控方的呼叫进行检测，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，则允许接入该呼叫。

2、如权利要求 1 所述的方法，其中，

网络侧对收到的目标为所述主控方的呼叫进行检测的步骤包括：

若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密，则网络侧判定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

10 3、如权利要求 2 所述的方法，其中，

所述呼叫类型通过所述呼叫建立消息中的用户-用户信息元素（UUIE）字段实现，且当所述 UUIE 字段内容为“加密语音（ENCRYPTION VOICE）”时，表示呼叫类型为加密。

4、如权利要求 1、2 或 3 所述的方法，所述方法还包括：

15 所述加密会议电话进入通话状态后，所述加密会议电话的终端和网络侧根据所述呼叫类型，对通话的语音数据进行加密和解密处理。

5、如权利要求 4 所述的方法，其中，

对通话的语音数据的加密和解密处理的步骤包括：

20 主叫终端使用发送方密码密钥（CK）作为运算因子对上行语音数据进行加密，并将加密后的语音数据上传到网络侧；以及

网络侧收到所述加密后的语音数据后，使用发送方 CK 作为运算因子进行解密后，再使用接收方 CK 作为运算因子加密语音数据，并将加密后的语音数据发送给被叫终端；被叫终端使用接收方 CK 作为运算因子解密收到的

下行语音数据。

6、如权利要求 1、2 或 3 所述的方法，所述方法还包括：

所述网络侧允许接入所述呼叫后，由所述主控方决定是否接听并将其加入本次加密会议电话。

5 7、一种会议电话预接入的系统，所述系统包括网络侧的预接入处理单元和呼叫类型检测单元，其中，

所述呼叫类型检测单元设置为：接收到主控方发起的会议电话后，对收到的目标为所述主控方的呼叫进行检测，并将检测结果传送给所述预接入处理单元；

10 所述预接入处理单元设置为：根据所述呼叫类型检测单元传送的检测结果，如果该呼叫为非加密通话，则不予接入该呼叫；如果该呼叫为加密通话，则允许接入该呼叫。

8、如权利要求 7 所述的系统，其中，

所述呼叫类型检测单元是设置为按照如下方式对所述呼叫进行检测：

15 若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密，则判定所述呼叫为加密通话；否则，判定所述呼叫为非加密通话。

9、如权利要求 8 所述的系统，所述系统还包括终端中的呼叫类型添加模块，

20 所述呼叫类型添加模块设置为：在发起呼叫时，通过呼叫建立消息中的用户-用户信息元素（UUIE）字段添加呼叫类型，且当所述 UUIE 字段内容为“加密语音（ENCRYPTION VOICE）”时，表示呼叫类型为加密。

10、如权利要求 7、8 或 9 所述的系统，所述系统还包括网络侧的网络侧硬件加密模块和终端的终端硬件加密模块，其中：

所述终端硬件加密模块设置为：当所述终端为发送方终端时，使用发送

方密码密钥 (CK) 作为运算因子对上行语音数据进行加密, 并将加密后的语音数据上传到网络侧; 以及, 当所述终端为接收方终端时, 接收到下行语音数据后, 使用接收方 CK 作为运算因子对收到的下行语音数据进行解密;

5 所述网络侧硬件加密模块设置为: 收到发送方上传的加密后的语音数据后, 使用发送方 CK 作为运算因子进行解密后, 再使用接收方 CK 作为运算因子加密语音数据, 并将加密后的语音数据发送给接收方。

11、一种网络侧设备, 所述设备包括预接入处理单元和呼叫类型检测单元, 其中,

10 所述呼叫类型检测单元设置为: 接收到主控方发起的会议电话后, 对收到的目标为所述主控方的呼叫进行检测, 并将检测结果传送给所述预接入处理单元;

所述预接入处理单元设置为: 根据所述呼叫类型检测单元传送的检测结果, 如果该呼叫为非加密通话, 则不予接入该呼叫; 如果该呼叫为加密通话, 则允许接入该呼叫。

15 12、如权利要求 11 所述的设备, 其中,

所述呼叫类型检测单元是设置为按照如下方式对所述呼叫进行检测:

若所述呼叫的呼叫建立消息中包含呼叫类型、且呼叫类型为加密, 则判定所述呼叫为加密通话; 否则, 判定所述呼叫为非加密通话。

13、如权利要求 12 所述的设备, 其中,

20 所述呼叫类型检测单元通过呼叫建立消息中的用户-用户信息元素 (UUIE) 字段添加的呼叫类型对所述呼叫进行检测, 且当所述 UUIE 字段内容为“加密语音 (ENCRYPTION VOICE)”时, 表示呼叫类型为加密。

14、如权利要求 11、12 或 13 所述的设备, 所述设备还包括网络侧硬件加密模块, 其中:

所述网络侧硬件加密模块设置为：收到发送方的终端使用发送方密码密钥（CK）作为运算因子对上行语音数据进行加密，并将加密后的语音数据上传到网络侧设备的加密后的语音数据后，使用发送方 CK 作为运算因子进行解密后，再使用接收方 CK 作为运算因子加密语音数据，并将加密后的语音数据发送给接收方。

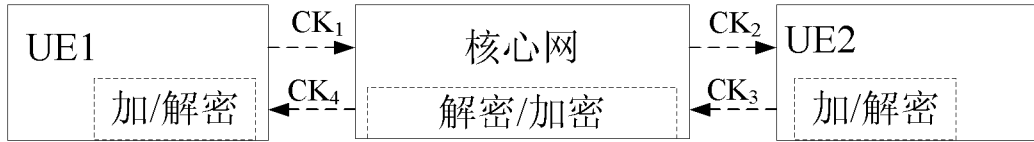


图 1

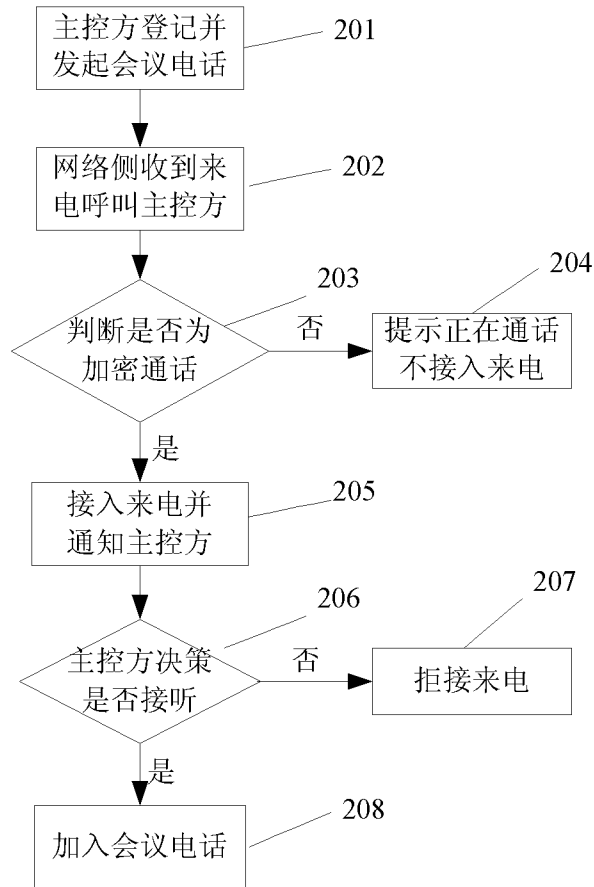


图 2

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2011/070270

## A. CLASSIFICATION OF SUBJECT MATTER

H04W12/08(2009.01)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)

IPC: H04W, H04Q

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)

VEN, CNABS, CNTXT, CNKI: conference, session, phone, call, encryption, cipher, access, network

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN101370251A (HUAWEI TECHNOLOGIES CO LTD.) 18 Feb. 2009(18.02.2009) the whole document	1-14
A	CN1889767A (HUAWEI TECHNOLOGIES CO LTD.) 03 Jan. 2007(03.01.2007) the whole document	1-14
A	CN101500229A (HUAWEI TECHNOLOGIES CO LTD.) 05 Aug. 2009(05.08.2009) the whole document	1-14

 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

“&amp;” document member of the same patent family

Date of the actual completion of the international search

18 May 2011(18.05.2011)

Date of mailing of the international search report

**09 Jun. 2011 (09.06.2011)**Name and mailing address of the ISA/CN  
The State Intellectual Property Office, the P.R.China  
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China  
100088  
Facsimile No. 86-10-62019451

Authorized officer

**PAN, Yun**

Telephone No. (86-10)62411505

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/CN2011/070270

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101370251A	18.02.2009	WO2009024060A1	26.02.2009
CN1889767A	03.01.2007	CN100527875C	12.08.2009
CN101500229A	05.08.2009	WO2009094942A1	06.08.2009
		CN101926151A	22.12.2010



国际检索报告  
关于同族专利的信息

国际申请号  
**PCT/CN2011/070270**

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101370251A	18.02.2009	WO2009024060A1	26.02.2009
CN1889767A	03.01.2007	CN100527875C	12.08.2009
CN101500229A	05.08.2009	WO2009094942A1	06.08.2009
		CN101926151A	22.12.2010