

(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
2006 年 6 月 29 日 (29.06.2006)

(10) 国际公布号
WO 2006/066455 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2004/001497

(22) 国际申请日: 2004 年 12 月 22 日 (22.12.2004)

(25) 申请语言: 中文

(26) 公布语言: 中文

(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): 胡宪利(HU, Xianli) [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)。苏登军(SU, Dengjun) [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)。倪明(NI, Ming) [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)。陆纪文(LU, Jiwen) [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)。

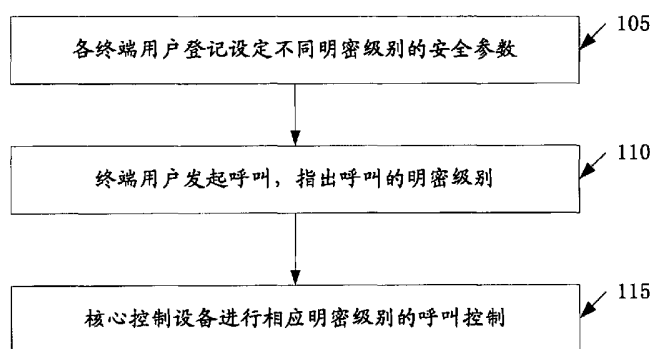
(74) 代理人: 北京市中咨律师事务所(BEIJING ZHONGZI LAW OFFICE); 中国北京市西城区阜成门北大街6号-9国际投资大厦C座17层, Beijing 100034 (CN)。

(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, AT, AU, AZ, BA, BB, BG,

[续页]

(54) Title: A METHOD FOR ACHIEVING SESSION WITH DIFFERENT PLAIN AND SECURITY LEVEL IN THE COMMUNICATION NETWORK

(54) 发明名称: 在通信网络中实现不同明密级别通话的方法



105 EACH TERMINAL USER REGISTERED THE SECURITY PARAMETER SETTING DIFFERENT PLAIN AND SECURITY LEVEL
110 THE TERMINAL USER ORIGINATE THE CALL, SPECIFY THE PLAIN AND SECURITY LEVEL OF THE CALL
115 THE CORE CONTROL DEVICE CONTROL THE CALL CORRESPONDING TO THE PLAIN AND SECURITY LEVEL

(57) Abstract: The invention discloses a method for achieving the session of the different plain and security levels in the communication network. The terminal device of this network can support the communication at one or plurality of security levels. The method comprises: registering the security parameter of a set or plurality sets of the security levels corresponding to the session plain and security level what each terminal user had in the core control device of said network; the terminal users originate the call to said core control device, wherein there is the security parameter corresponding to the current session plain and security level specified by said user in the call request; said core control device controls the call of plain and security level based on the security parameter in the call request and the security parameter registered by the called party user. The invention permits to set the different manners of plain and security interacted with the other users based on the requirement for the different situations, the core control device controls the call based on the plain and security level setted by the user.

(57) 摘要: 本发明公开了一种在通信网络中实现不同明密级别通话的方法, 该网络的终端设备具有支持一种或多种密级通信的能力, 该方法包括: 在所述网络的核心控制设备中登记各终端用户的一组或多组对应通话明密级别的安全参数; 终端用户向所述核心控制设备发起呼叫, 其中在呼叫请求中包括与所述用户指定的本次通话明密级别对应的安全参数; 所述核心控制设备根据该呼叫请求中的安全参数及被叫用户所登记的安全参数进行相应明密级别呼叫的控制。本发明允许用户根据不同场合的需求设置不同的与其他用户的明密交互方式, 核心控制设备根据用户设定的明密级别进行呼叫控制。

WO 2006/066455 A1



BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH,

CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, 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。

所引用双字母代码及其它缩写符号, 请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

在通信网络中实现不同明密级别通话的方法

技术领域

本发明涉及通信领域，尤其涉及在基于 IP 通信网络的体系架构下实现终端用户的不同明密级别通话的方法。

背景技术

随着互联网和宽带技术的发展，基于 IP 网络的语音传输（VOIP）技术在企业网和公共网络中得到了越来越多的应用。但由于 IP 网络的开放性，VOIP 技术存在一些安全性问题，如语音数据 IP 包被嗅探监听；用户账号和设备欺骗等等。

针对这些安全问题，VOIP 系统需要对用户的信令和媒体流进行加密处理，以防止非法用户对合法用户的信息窃取。在通话过程中，如果媒体流是经过加密的，则称本次通话为密话，否则称为明话。

目前，在通信系统的安全体系中，通常的做法是用户终端与系统设备事先约定好鉴权算法、鉴权参数和业务加密方式，用户终端与系统设备之间的通信安全方式都以这些事先约定的设置进行。但采用这种方法，一旦设置了用户终端与系统设备之间的通信方式后，用户就不能自行改变通信方式；如果用户需要改变通信的安全方式，则必须通过网络系统设备的网管操作，重新约定用户终端与系统设备的相应参数，修改比较麻烦。

发明内容

本发明的目的在于提供一种在通信网络中实现不同明密级别通话的方法，以允许用户根据不同场合请求进行不同明密级别的通话，核心控制设备根据用户设定的明密级别进行呼叫控制，从而自动实现用户所请求的明密级别的通话。

为实现以上目的，本发明所采取的技术方案为：

一种在通信网络中实现不同明密级别通话的方法，其中该网络的终端设备具有支持一种或多种密级通信的能力，该方法包括：在所述网络的核心控制设备中登记各终端用户的一组或多组对应通话明密级别的安全参数；终端用户向所述核心控制设备发起呼叫，其中在呼叫请求中包括与该终端用户指定的本次通话明密级别对应的安全参数；所述核心控制设备根据该呼叫请求中的安全参数及被叫用户所登记的安全参数进行相应明密级别呼叫的控制。

优选地，所述登记各终端用户的一组或多组安全参数的步骤进一步包括：所述终端用户向所述核心控制设备发起注册请求；所述终端用户将设定的通话明密级别的安全参数添加到在注册过程中发给所述核心控制设备的消息中进行发送；所述核心控制设备根据所述终端用户的签约信息和安全参数中有关鉴权的信息对所述终端用户进行注册鉴权操作；当注册鉴权操作成功时，所述核心控制设备将所述终端用户当前的通话明密级别的安全参数登记到所述终端用户的通话明密级别属性表中。

所述消息是注册请求消息或其它非注册请求消息。优选地，所述登记各终端用户的一组或多组安全参数的步骤进一步包括：所述终端用户将通话明密级别的安全参数添加到注册成功后发给所述核心控制设备的消息中进行发送；所述核心控制设备对所述消息进行相应处理，并将其中携带的安全参数登记到所述终端用户的通话明密级别属性表中。

优选地，所述登记各终端用户的一组或多组安全参数的步骤还包括：在所述核心控制设备中预先登记缺省的通话明密级别的安全参数。

优选地，所述核心控制设备进行相应明密级别呼叫的控制的步骤进一步包括：所述核心控制设备根据所述呼叫请求中的主被叫用户标识确定主被叫用户是否合法；当所述呼叫请求的主被叫用户均合法时：所述核心控制设备根据被叫用户标识获得所述被叫用户在所述核心控制设备中登记的各组安全参数；根据所述呼叫请求中的安全参数及被叫用户所登记的各组安全参数，确定主被叫用户之间的通话明密级别是否兼容；当所述主被叫用户之间的通话明密级别兼容时，在所述主被叫用户之间建立相应明密级

别的通话；当所述主被叫用户之间的通话明密级别不兼容时，所述核心控制设备判断主被叫用户的安全参数是否包含允许与对方通过中介资源建立密话，若包含，则主被叫用户之间通过中介资源建立密话；若没有包含，则所述核心控制设备判断主被叫用户的安全参数是否包含允许与对方建立明话，若包含，则主被叫用户之间建立明话；若没有包含，则此次呼叫失败。

优选地，所述核心控制设备确定主被叫用户是否合法的步骤进一步包括：所述核心控制设备根据被叫用户标识，判断被叫用户是否注册，若被叫用户未注册，则确定被叫用户不合法；若被叫用户已注册，则所述核心控制设备根据主被叫用户的业务信息，判断是否允许主被叫用户建立呼叫，若不允许建立呼叫，则主被叫用户不合法。

优选地，当所述主被叫用户之间的通话明密级别兼容时，在所述主被叫用户之间建立相应明密级别的通话的步骤进一步包括：所述核心控制设备向被叫用户发起呼叫请求；所述核心控制设备收到所述被叫用户的应答后，控制主被叫用户之间进行加密参数的协商；所述核心控制设备控制主被叫用户之间建立媒体连接，主被叫用户进入密话通话。

优选地，所述主被叫用户之间通过中介资源建立密话的步骤进一步包括：所述核心控制设备向被叫用户发起呼叫请求；所述核心控制设备收到所述被叫用户的应答后，分配中介资源，并获得中介资源所对应的加密参数；所述核心控制设备分别控制主叫用户与中介资源之间、被叫用户与中介资源之间进行加密参数的协商；所述核心控制设备控制主被叫用户之间建立通过中介资源的媒体连接，主被叫用户进入密话通话。

优选地，所述主被叫用户之间建立明话的步骤进一步包括：所述核心控制设备向被叫用户发起呼叫请求；所述核心控制设备收到所述被叫用户的应答后，控制主被叫用户终端之间建立媒体连接，主被叫用户进入通话。

采用本发明，用户可以根据需要灵活采取各种加密方式（包括不加密）进行通信，具体来说，本发明有如下的优点：

- 1.核心控制设备允许终端用户有一组以上的对应明密级别的安全参

数;

2.核心控制设备允许用户根据不同环境需要,自行通过终端设备设定其明密状态;

3.用户可自行决定与其他用户的明密交互方式,核心控制设备根据用户设定的明密级别进行呼叫控制;

4.核心控制设备为采用不同加密方式的用户终端之间提供呼叫控制服务;

5.运营商可以向用户提供分级的安全通信服务。

附图说明

图1是根据本发明一个实施例的在通信网络中实现不同明密级别通话的方法的流程图;

图2是根据本发明一个实施例的图1方法中终端用户注册过程的流程图;

图3是根据本发明一个实施例的图1方法中核心控制设备进行相应明密级别呼叫的控制过程的流程图。

具体实施方式

相信通过下面结合附图对本发明的优选实施例的详细说明,可以更清楚地了解本发明的上述和其它目的、特征和优点。

本发明是在以软交换技术为基础的IP网络系统体系架构中提出的,其中,两个终端之间的会话是通过软交换建立的,如果两个终端之间通话的媒体流是经过加密的,则称本次通话为密话,否则称为明话。对于带有加密功能的终端来说,可以改变过去单一的通信方式,而根据不同场合与另一个终端建立明话,或是不同级别的密话。

本发明中允许终端用户根据不同场合或需要与另一终端建立明话或不同密级的密话的思想是通过允许用户在发起呼叫时指出本次呼叫的明密级别来实现的。而呼叫的明密级别,这里称为密级,是由一组安全参数设定

的，这组安全参数设定了终端设备所使用的加密通信方式，至少包括媒体加密方式信息。此外，安全参数中还可以包括鉴权算法、鉴权参数等信息。

图 1 是根据本发明一个实施例的在通信网络中实现不同明密级别通话的方法的流程图。

本实施例中，以软交换技术为基础的 IP 网络体系架构中至少存在核心控制设备，可以是媒体网关控制器 S；主叫用户终端设备 O；被叫用户终端设备 T；网关 G；其中用户终端设备 O 和 T 具备本地加密和解密通信内容的能力。

如图 1 所示，在步骤 105，各终端用户在媒体网关控制器 S 中登记各自的通话明密级别对应的安全参数。

本实施例中，由于允许终端用户设定多个通话明密级别，因此存在与这多个明密级别对应的多组安全参数，所以在核心控制设备 S 中，为每位终端用户都建立了相应的通话明密级别属性表，将终端用户设定的所有通话明密级别对应的安全参数都记录在该通话明密级别属性表中。各终端用户在需要登记或添加新的明密级别时，可以随时将新的明密级别的安全参数添加到既定的消息中，发送给媒体网关控制器 S 进行登记。在本实施例中，通过终端设备向媒体网关控制器 S 注册的过程来实现明密级别的安全参数的登记。

图 2 是根据本发明一个实施例的图 1 方法中终端用户进行注册的流程图。现在以某一用户终端设备 U 为例，参照图 2 所示的用户终端注册过程来详细说明图 1 中的登记明密级别的安全参数的步骤 105。

如图 2 所示，首先在步骤 201，用户在终端设备 U 上设置在以后的通话中终端设备 U 所遵从的明密级别的安全参数。在用户终端 U 发起注册请求时，用户设置的明密级别的安全参数包含在注册消息中。这些安全参数包括媒体加密方式、鉴权算法、鉴权参数以及当主被叫终端设备明密级别不兼容时是否允许明话呼叫或利用中介资源进行呼叫等信息。需要说明的是，本实施例未对注册消息的格式进行规定，因为本实施例只是示例性的说明，而且终端设备发送安全参数所使用的注册消息的消息格式和消息内

容是与具体的核心控制设备（如媒体网关控制器）的要求和终端设备用户支持的协议有关的。

在步骤 202，终端设备 U 向媒体网关控制器 S 发起注册请求，将包含了安全参数的注册消息发送到媒体网关控制器 S。

在步骤 203，媒体网关控制器 S 对终端设备 U 进行鉴权。在这一步骤中，媒体网关控制器 S 从注册消息中获取用户标识和其中的安全参数，从而查找对应的用户签约业务信息，并依此向终端设备 U 发送鉴权消息。媒体网关控制器 S 对终端设备 U 进行鉴权的依据是用户的签约信息以及安全参数中对应的加密方式的鉴权要求。需要说明的是，在图 2 中对鉴权消息交互仅进行了示意性的表示，真正的鉴权消息交互流程需要视实际鉴权算法而定。

在步骤 204，当鉴权通过之后，媒体网关控制器 S 根据注册消息中携带的安全参数设置终端设备 U 的当前明密级别注册状态，并将这些安全参数记录在终端设备 U 的通话明密级别属性表中，并向终端设备 U 发送注册成功消息。反之，如果鉴权失败，则媒体网关控制器 S 将向终端设备 U 发送注册失败信息，并在注册失败消息中包含具体的失败原因。

一旦终端设备注册成功，媒体网关控制器 S 就可以为其提供服务了。

返回图 1，在步骤 110，终端用户发起呼叫请求，同时指出此次呼叫的明密级别。本步骤中，终端用户在呼叫请求时可以指定所期望的通话明密级别，而与该明密级别对应的安全参数便自动作为呼叫请求消息的参数随呼叫请求一起发送。在这些安全参数中，可以包括采用何种密级方式发起呼叫；当被叫终端设备不支持该密级呼叫时，是采取呼叫失败方式，还是采用明话呼叫方式等等。具体的参数形式与具体的媒体网关控制器 S 和终端的呼叫协议有关。用户拨号时，带有安全参数的呼叫请求被发送到媒体网关控制器 S。

接着，在步骤 115，媒体网关控制器 S 进行相应明密级别呼叫的控制。

图 3 是根据本发明一个实施例的图 1 方法中媒体网关控制器 S 进行相应明密级别呼叫的控制的流程图。现在，参照图 3，以主叫用户终端设备

O 和被叫用户终端设备 T 之间的呼叫请求为例, 来说明媒体网关控制器 S 进行相应明密级别呼叫的控制的详细过程。

图 3 中, 步骤 301 和步骤 302 已在图 1 的步骤 110 中进行了介绍, 但为了图 3 中流程的连贯性, 在此进行简单地描述。主叫用户终端 O 向被叫用户终端 T 发起呼叫, 其中在呼叫请求中指出了此次呼叫的期望明密级别, 并将带有对应安全参数的呼叫请求发送给媒体网关控制器 S。

在步骤 303, 媒体网关控制器 S 接收到该呼叫请求后, 分析呼叫请求消息中的通话明密级别的安全参数和主被叫用户标识。

在步骤 304, 媒体网关控制器 S 根据被叫用户标识判断被叫用户是否注册。如果被叫用户没有注册, 则呼叫失败, 退出呼叫处理。

在步骤 305, 媒体网关控制器 S 根据主被叫用户标识, 获得主被叫用户的业务信息, 判断主被叫用户的业务信息是否允许在主叫用户 O 和被叫用户 T 之间建立呼叫。例如, 在主叫用户 O 因欠费而禁止呼出, 或主叫用户 O 在被叫用户 T 的黑名单中等情况下, 该呼叫就不允许建立。如果主被叫用户之间不允许建立呼叫, 则呼叫失败, 退出呼叫处理。

在步骤 306, 媒体网关控制器 S 根据主叫用户 O 和被叫用户 T 的业务信息及其在媒体网关控制器 S 中登记的通话明密级别对应的安全参数, 判断主叫用户 O 和被叫用户 T 的明密级别是否兼容, 从而对呼叫进行相应的明密级别的控制。其中明密级别兼容是指主叫用户 O 和被叫用户 T 当前的明密级别所对应的媒体加密方式相同, 或在被叫用户 T 的通话明密级别属性表中存在与主叫用户 O 当前的明密级别的媒体加密方式相同的明密级别。媒体网关控制器 S 根据判断结果, 按照如下原则进行处理:

(1) 如果明密级别兼容, 则执行步骤 30610 - 30613:

在步骤 30610, 媒体网关控制器 S 向被叫用户终端 T 发起呼叫请求消息。在此呼叫请求消息中包含着主叫用户 O 的安全参数;

在步骤 30611, 被叫终端 T 向媒体网关控制器 S 发送摘机应答消息;

在步骤 30612, 媒体网关控制器 S 控制主叫用户终端设备 O 与被叫用户终端设备 T 之间进行加密参数的协商;

在步骤 30613, 加密参数协商成功后, 媒体网关控制器 S 控制主叫用户终端设备 O 与被叫用户终端设备 T 之间建立通过网关 G 的媒体连接, 进入通话状态。

(2) 如果明密级别不兼容, 但主叫用户终端 O 与被叫用户终端 T 允许通过中介资源建立密话, 则执行步骤 30620 - 30625:

需要说明的是, “中介资源”是为了满足不同明密级别的用户之间的通话而引进的。在本发明中, 中介资源的作用有两个: 一是中介资源参与呼叫密钥的协商, 对主叫方来说, 中介资源将模拟与主叫方相同密级的被叫方, 而对被叫方来说, 中介资源则模拟与被叫方相同密级的主叫方。第二个作用是对主叫方和被叫方之间的通信内容进行适配转换。

在步骤 30620, 媒体网关控制器 S 向被叫用户终端 T 发起呼叫请求消息, 在此呼叫请求消息中包含着主叫用户 O 的安全参数;

在步骤 30621, 被叫用户终端 T 向媒体网关控制器 S 发送摘机应答消息;

在步骤 30622, 媒体网关控制器 S 为此次呼叫分配中介资源;

在步骤 30623, 媒体网关控制器 S 获得所分配的中介资源对应的加密参数, 并在步骤 30624, 分别控制主叫用户终端 O 与中介资源、被叫用户终端 T 与中介资源进行加密参数的协商;

在步骤 30625, 加密参数协商成功后, 媒体网关控制器 S 控制主叫用户终端 O 与被叫用户终端 T 之间建立通过网关 G 和中介资源的媒体连接, 进入通话状态。中介资源可以从网关中分配也可独立于网关。

(3) 如果明密级别不兼容且不允许通过中介资源建立通话, 但主叫用户终端 O 与被叫用户终端 T 允许建立明话, 则执行步骤 30630 - 30632:

在步骤 30630, 媒体网关控制器 S 向被叫用户终端 T 发起呼叫请求消息, 在此呼叫请求消息中包含着主叫用户 O 的安全参数;

在步骤 30631, 被叫用户终端 T 向媒体网关控制器 S 发送摘机应答消息;

在步骤 30632, 媒体网关控制器 S 控制主叫用户终端 O 与被叫用户终

端 T 建立通过网关 G 的媒体连接，进入通话状态。

(4) 如果以上情况皆不满足，则此次呼叫失败，退出呼叫控制流程。

以上对本发明的优选实施例进行了详细描述，需要说明的是，在密级兼容的情况下，媒体网关控制器也可为主被叫用户分配相应的中介资源，建立呼叫；此外，中介资源分配操作的时机可以选在用户愿意接听的情况下再进行，如在被叫用户终端设备上显示一个来话信息后，用户按下接听键之后，也可以选在此之前进行；而且，无论明/密话呼叫建立成功与否，媒体网关控制器都需将呼叫状态通知主叫终端设备用户；无论是明话呼叫建立成功的情况下，还是在密话建立成功的情况下，媒体网关控制器都可根据策略设置决定是否将呼叫状态通知被叫终端设备用户；在密话呼叫建立失败的情况下，根据相应的策略设置决定是否将呼叫状态通知被叫终端设备用户。

权利要求

1. 一种在通信网络中实现不同明密级别通话的方法，该网络的终端设备具有支持一种或多种密级通信的能力，其特征在于，该方法包括：

在所述网络的核心控制设备中登记各终端用户的一组或多组对应通话明密级别的安全参数；

终端用户向所述核心控制设备发起呼叫，其中在呼叫请求中包括与所述终端用户指定的本次通话明密级别对应的安全参数；

所述核心控制设备根据所述呼叫请求中的安全参数及被叫用户所登记的安全参数进行相应明密级别呼叫的控制。

2. 如权利要求 1 所述的方法，其特征在于，所述安全参数包括媒体加密方式、鉴权算法、鉴权参数以及当主被叫终端设备明密级别不兼容时是否允许明话呼叫或利用中介资源进行呼叫。

3. 如权利要求 2 所述的方法，其特征在于，所述登记各终端用户的一组或多组安全参数的步骤进一步包括：

所述终端用户向所述核心控制设备发起注册请求；

所述终端用户将设定的通话明密级别的安全参数添加到在注册过程中发给所述核心控制设备的消息中进行发送；

所述核心控制设备根据所述终端用户的签约信息和安全参数中有关鉴权的信息对所述终端用户进行注册鉴权操作；

当注册鉴权操作成功时，所述核心控制设备将所述终端用户的通话明密级别的安全参数登记到所述终端用户的通话明密级别属性表中。

4. 如权利要求 3 所述的方法，其特征在于，所述消息是注册请求消息或其它非注册请求消息。

5. 如权利要求 2 所述的方法，其特征在于，所述登记各终端用户的一组或多组安全参数的步骤进一步包括：

所述终端用户将通话明密级别的安全参数添加到注册成功后发给所述核心控制设备的消息中进行发送；

所述核心控制设备对所述消息进行相应处理，并将其中携带的安全参数登记到所述终端用户的通话明密级别属性表中。

6. 如权利要求 3 或 5 所述的方法，其特征在于，所述登记各终端用户的一组或多组安全参数的步骤还包括：在所述核心控制设备中预先登记缺省的通话明密级别的安全参数。

7. 如权利要求 2、3 或 5 所述的方法，其特征在于，所述核心控制设备进行相应明密级别的呼叫控制的步骤进一步包括：

所述核心控制设备根据所述呼叫请求中的主被叫用户标识确定主被叫用户是否合法；

当所述呼叫请求的主被叫用户均合法时：

所述核心控制设备根据被叫用户标识获得所述被叫用户在所述核心控制设备中登记的各组安全参数；

根据所述呼叫请求中的安全参数及被叫用户所登记的各组安全参数，确定主被叫用户之间的通话明密级别是否兼容；

当所述主被叫用户之间的通话明密级别兼容时，在所述主被叫用户之间建立相应明密级别的通话；

当所述主被叫用户之间的通话明密级别不兼容时，所述核心控制设备判断主被叫用户的安全参数是否包含允许与对方通过中介资源建立密话，若包含，则主被叫用户之间通过中介资源建立密话，若没有包含，则所述核心控制设备判断主被叫用户的安全参数是否包含允许与对方建立明话，若包含，则主被叫用户之间建立明话；若没有包含，则此次呼叫失败。

8. 如权利要求 7 所述的方法，其特征在于，所述核心控制设备确定主被叫用户是否合法的步骤进一步包括：

所述核心控制设备根据被叫用户标识，判断被叫用户是否注册，若被叫用户未注册，则确定被叫用户不合法；

若被叫用户已注册，则所述核心控制设备根据主被叫用户的业务信息，判断是否允许主被叫用户建立呼叫，若不允许建立呼叫，则主被叫用户不合法。

9. 如权利要求 7 所述的方法，其特征在于，当所述主被叫用户之间的通话明密级别兼容时，在所述主被叫用户之间建立相应明密级别的通话的步骤进一步包括：

所述核心控制设备向被叫用户发起呼叫请求；

所述核心控制设备收到所述被叫用户的应答后，控制主被叫用户之间进行加密参数的协商；

所述核心控制设备控制主被叫用户之间建立媒体连接，主被叫用户进入密话通话。

10. 如权利要求 7 所述的方法，其特征在于，所述主被叫用户之间通过中介资源建立密话的步骤进一步包括：

所述核心控制设备向被叫用户发起呼叫请求；

所述核心控制设备收到所述被叫用户的应答后，分配中介资源，并获得中介资源所对应的加密参数；

所述核心控制设备分别控制主叫用户与中介资源之间、被叫用户与中介资源之间进行加密参数的协商；

所述核心控制设备控制主被叫用户之间建立通过中介资源的媒体连接，主被叫用户进入密话通话。

11. 如权利要求 7 所述的方法，其特征在于，所述主被叫用户之间建立明话的步骤进一步包括：

所述核心控制设备向被叫用户发起呼叫请求；

所述核心控制设备收到所述被叫用户的应答后，控制主被叫用户终端之间建立媒体连接，主被叫用户进入通话。

12. 如权利要求 7 或 9 所述的方法，其特征在于，所述明密级别兼容是指主被叫用户当前的明密级别所对应的媒体加密方式相同，或在被叫用户的通话明密级别属性表中存在与主叫用户当

前的明密级别的媒体加密方式相同的明密级别。

13. 如权利要求 1 所述的方法，其特征在于，所述终端用户在呼叫请求中指定的本次通话的明密级别不同于其在所述核心控制设备中登记的各组安全参数对应的明密级别。

14. 如权利要求 1 所述的方法，其特征在于，所述通信网络采用 IP 网络体系架构，所述核心控制设备采用软交换技术。

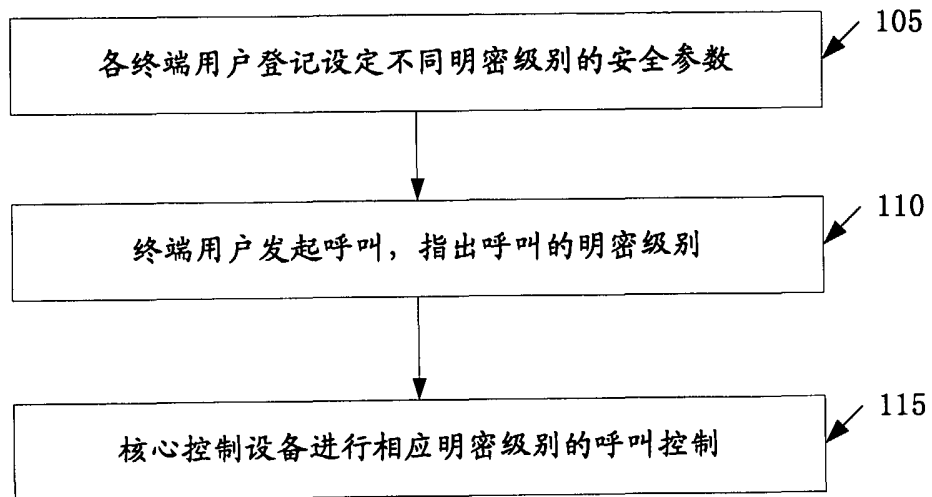


图1

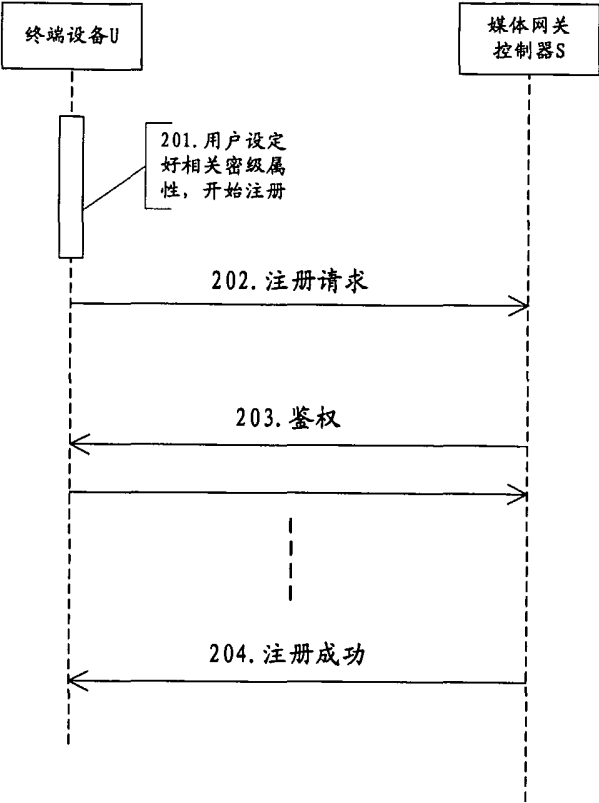


图 2

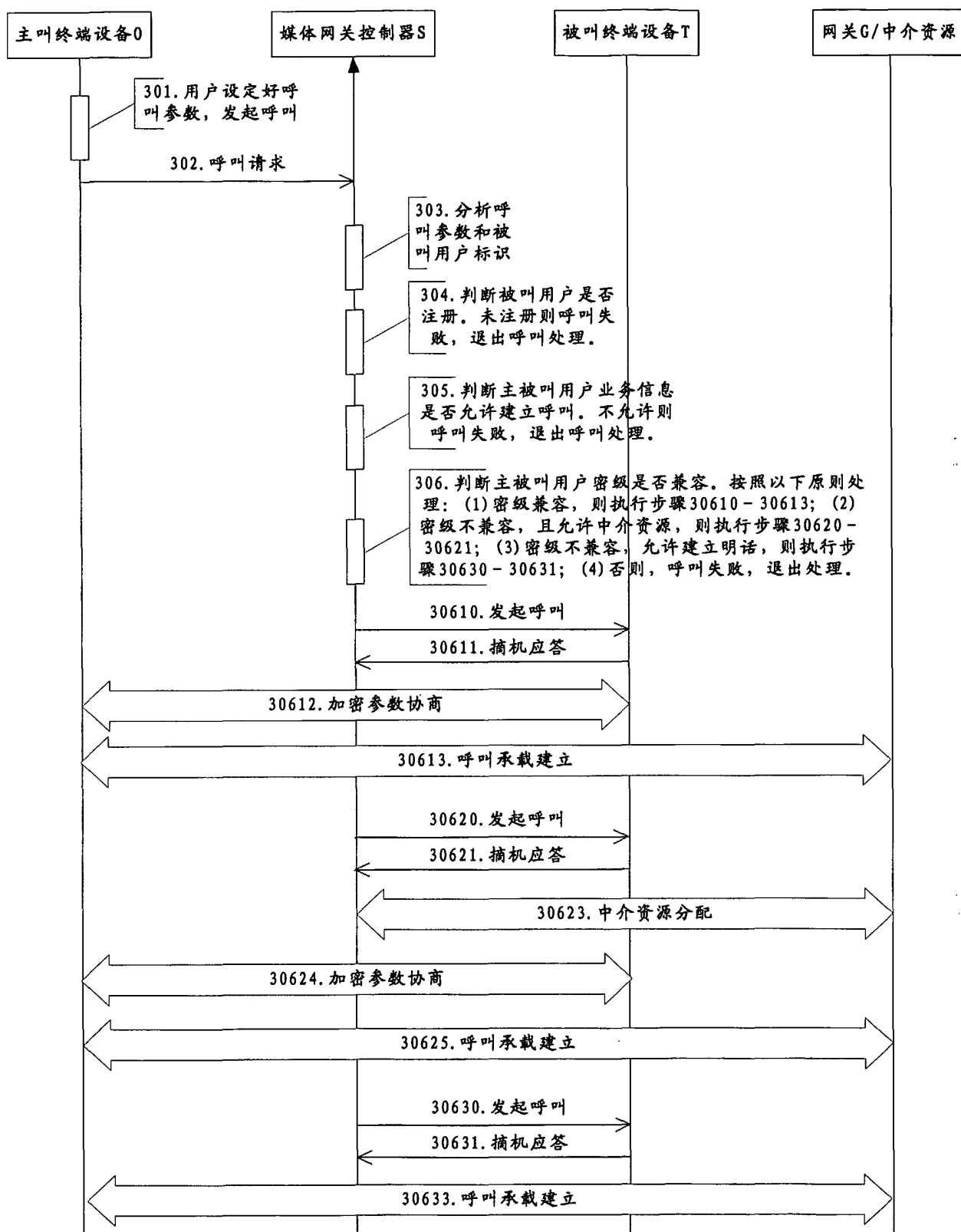


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2004/001497

A. CLASSIFICATION OF SUBJECT MATTER

IPC⁷: H04L9/06

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)

IPC⁷: H04L9/00 H04L9/06 H04L12/34, 29/06 G06F15

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)

WPI, EPODOC, PAJ, CNPAT, CNKI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1365562 A 2002-08-21 ((TELF) TELEFONAKTIEBOLAGET ERICSSON L M) see the whole	1-14
A	WO0064111 A1 2000-10-26 ((UNIF-N) UNIFREE LLC) see the whole	1-14
A	US2002038431 A1 2002-03-28 ((CHES-I) CHESKO J B - (CHES-I) CHESKO J D - (CHES-I) CHESKO J E A) see the whole	1-14
A	JP2001312486 A 2001-11-09 ((HITA) HITACHI LTD) see the whole	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

22005-03-21

Date of mailing of the international search report

07 · APR 2005 (07 · 04 · 2005)

Name and mailing address of the ISA/

6 Xitucheng Rd., Jimen Bridge, Haidian District,
100088 Beijing, China

Facsimile No. 86-01-62019451

Authorized officer

zhuqi

Telephone No. 86-01-62084554



INTERNATIONAL SEARCH REPORT

Information patent family members

Search request No.

PCT/CN2004/001497

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN1365562 A	2002-08-21	JP2003501891T	2003-01-14
		WO0074345 A1	2000-12-07
		AU200052637 A	2000-12-18
		EP1180294 A1	2002-02-20
WO0064111 A1	2000-10-26	none	
US2002038431 A1	2002-03-28	CA2319871 A1	2002-03-15
JP2001312486 A	2001-11-09	none	

国际检索报告

国际申请号

PCT/CN2004/001497

A. 主题的分类

IPC⁷: H04L9/06

按照国际专利分类表(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)

IPC⁷: H04L9/00, 9/06, H04L12/34, 29/06 G06F15

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))

WPI, EPODOC, PAJ, CNPAT, 中国期刊全文库

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
A	CN1365562 A (艾利森电话股份有限公司) 2002-08-21 参见全文	1-14
A	WO0064111 A1 ((UNIF-N) UNIFREE LLC) 2000-10-26 参见全文	1-14
A	US2002038431 A1 ((CHES-I) CHESKO J B - (CHES-I) CHESKO J D - (CHES-I) CHESKO J E A) 2002-03-28 参见全文	1-14
A	JP2001312486 A ((HITA) HITACHI LTD) 2001-11-09 参见全文	1-14

☐ 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, 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

“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

2005-03-21

国际检索报告邮寄日期

07. 4月 2005 (07. 04. 2005)

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

朱琦



电话号码: (86-10)-62084554

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2004/001497

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1365562 A	2002-08-21	JP2003501891T	2003-01-14
		WO0074345 A1	2000-12-07
		AU200052637 A	2000-12-18
		EP1180294 A1	2002-02-20
WO0064111 A1	2000-10-26	无	
US2002038431 A1	2002-03-28	CA2319871 A1	2002-03-15
JP2001312486 A	2001-11-09	无	