[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410030855.5

[45] 授权公告日 2009 年 7 月 8 日

[11] 授权公告号 CN 100512103C

[22] 申请日 2004.4.7
[21] 申请号 200410030855.5
[73] 专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 漆宝剑 赵建国 谢国军
[56] 参考文献
WO02/33884A2 2002.4.25
CN1406005A 2003.3.26
US2002/0087875A1 2002.7.4
WO99/35783A1 1999.7.15
审查员 董振兴

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 张颖玲 王 琦

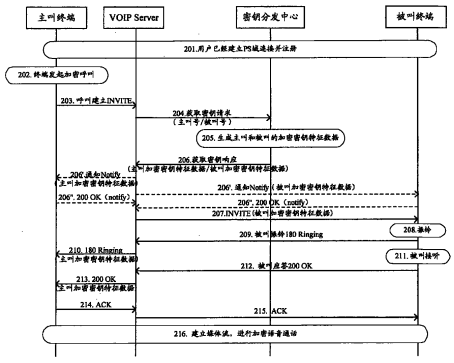
权利要求书 3 页 说明书 9 页 附图 1 页

[54] 发明名称

一种端到端加密通信的密钥分发方法

[57] 摘要

本发明公开了一种端到端加密通信的密钥分发方法，在每个用户终端和密钥分发中心分别存储有对应用户的用户私有数据，该方法包括：VOIP 服务器收到主叫终端的呼叫建立请求后，向密钥分发中心发送获取密钥请求；密钥分发中心收到请求后，分别产生主叫加密密钥特征数据和被叫加密密钥特征数据，并将所产生的加密密钥特征数据返回给 VOIP 服务器；VOIP 服务器将所得到的主叫和被叫加密密钥特征数据分别发送给主叫终端和被叫终端；主叫终端和被叫终端分别通过当前得到的加密密钥特征数据和自身存储的用户私用数据产生本次呼叫的加密通信密钥，并通过所产生的加密通信密钥进行双方的加密语音通话。 该方法能在端到端加密通信系统中实现高安全性的密钥分发。



1、一种端到端加密通信的密钥分发方法，在每个用户终端和密钥分发中心分别存储有对应用户的用户私有数据，其特征在于，该方法包括以下步骤:

a. VOIP 服务器收到主叫终端的呼叫建立请求后，向密钥分发中心发送获取密钥请求;

b. 密钥分发中心收到请求后，分别产生用于主叫终端和被叫终端产生密钥的主叫加密密钥特征数据和被叫加密密钥特征数据，并将所产生的加密密钥特征数据返回给 VOIP 服务器;

c. VOIP 服务器将所得到的用于主叫终端和被叫终端产生密钥的主叫加密密钥特征数据和被叫加密密钥特征数据分别发送给主叫终端和被叫终端。

2、根据权利要求 1 所述的方法，其特征在于，步骤 c 所述 VOIP 服务器将被叫加密密钥特征数据发送给被叫终端具体为: VOIP 服务器将被叫加密密钥特征数据携带于 SIP 信令的呼叫建立消息中发送给被叫终端。

3、根据权利要求 1 所述的方法，其特征在于，步骤 c 所述 VOIP 服务器将主叫加密密钥特征数据发送给主叫终端具体为: VOIP 服务器在收到被叫终端发来的振铃消息后，将主叫加密密钥特征数据携带于 SIP 信令的被叫振铃消息中发送给主叫终端。

4、根据权利要求 3 所述的方法，其特征在于，在将主叫加密密钥特征数据携带于 SIP 信令的被叫振铃消息中发送给主叫终端之后，进一步包括: VOIP 服务器在收到被叫终端发来的被叫应答消息后，将主叫加密密钥特征数据携带于 SIP 信令的被叫应答消息中发送给主叫终端。

5、根据权利要求 1 所述的方法，其特征在于，步骤 c 所述 VOIP 服务器将主叫和被叫加密密钥特征数据分别发送给主叫和被叫终端具体为: VOIP 服务器将主叫加密密钥特征数据和被叫加密密钥特征数据携带于 SIP 信令的通知消息中分别发送给主叫终端和被叫终端。

6、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括: 用户终

端预先订阅加密呼叫事件，则步骤 c 所述 VOIP 服务器将主叫和被叫加密密钥特征数据发送给主叫和被叫终端具体为：VOIP 服务器收到主叫和被叫加密密钥特征数据后，判断当前主叫终端和被叫终端是否订阅加密呼叫事件，如果是，则将相应的加密密钥特征数据携带于 SIP 信令的通知消息中发送给订阅加密呼叫事件的用户终端；否则，通过 SIP 信令的呼叫建立消息将被叫加密密钥特征数据发送给被叫终端，通过 SIP 信令的被叫振铃消息或/和被叫应答消息将主叫加密密钥特征数据发送给主叫终端。

7、根据权利要求 5 或 6 所述的方法，其特征在于，该方法进一步包括：主叫终端或被叫终端收到通过 SIP 信令的通知消息发来的加密密钥特征数据后，向 VOIP 服务器返回应答消息。

8、根据权利要求 1、2、3、5 或 6 所述的方法，其特征在于，所述主叫加密密钥特征数据至少包括主叫密钥掩码，所述被叫加密密钥特征数据至少包括被叫密钥掩码。

9、根据权利要求 8 所述的方法，其特征在于，步骤 b 中密钥分发中心随机产生分别用于主叫计算本次通信密钥和用于被叫计算本次通信密钥的随机数，再分别通过主叫终端和被叫终端各自的随机数、各自的用户私有数据以及本次呼叫的加密通信密钥产生主叫密钥掩码和被叫密钥掩码，则 VOIP 服务器向主叫终端和被叫终端发送携带有加密密钥特征数据的消息时，所述加密密钥特征数据进一步包括用于主叫或用于被叫计算本次通信密钥的随机数。

10、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：

d. 主叫终端和被叫终端分别通过当前得到的加密密钥特征数据和自身存储的用户私有数据产生本次呼叫的加密通信密钥，并通过所产生的加密通信密钥进行双方的加密语音通话。

11、根据权利要求 10 所述的方法，其特征在于，所述加密密钥特征数据至少包括密钥掩码。

12、根据权利要求 11 所述的方法，其特征在于，步骤 b 中密钥分发中心随

机产生分别用于主叫计算本次通信密钥和用于被叫计算本次通信密钥的随机数，则发送给主叫终端和被叫终端的加密密钥特征数据中分别进一步包括所产生的随机数；

则步骤 d 中主叫终端和被叫终端分别通过当前得到的密钥掩码、随机数和自身存储的用户私用数据产生本次呼叫的加密通信密钥。

13、根据权利要求 1 或 10 所述的方法，其特征在于，每次呼叫所采用的加密通信密钥均不同。

一种端到端加密通信的密钥分发方法

技术领域

本发明涉及保密通信技术，特别是指一种在基于移动分组交换网端到端加密通信系统中实现端到端加密通信的密钥分发方法。

背景技术

目前，移动通信技术已被广泛应用，但在现有的移动通信系统中，对普通民用移动电话的语音流传输大都没有经过加密处理，虽然有的运营商为了提高安全性增加了加密功能，也仅仅是在无线传输部分进行了加密处理。而对于一些特殊的行业应用，需要移动通信有更高的安全性能，不仅要防止通话在无线传输部分被监听，还要避免通话在陆地网络中传送时被截获、监听，换句话说就是，需要对移动电话的呼叫和通信进行端到端的加密处理。

由于现有的移动通信网络，如：GSM、CDMA、WCDMA、CDMA2000 等等，其电路交换网络都是为非加密电话设计的，这些移动网络中的移动交换中心（MSC）设备负责通信控制和语音交换；由于无线传输与 MSC 间的传输网络使用不同的码率和语音编码类型，所以 MSC 还要对语音进行编解码及码率转换。故此，如果在现有的电路交换网络上实现加密移动通信，就需要改造移动网络的 MSC，使 MSC 不进行编解码和码率转换，而直接透传加密后的语音数据。但是，在现有的移动网络中，MSC 数量众多且具有重要的地位，这种通过对 MSC 进行改造来实现端到端加密传输，成本非常昂贵。

为了能满足高安全性的通信需求，实现移动通信网中的端到端加密通信，本申请人在另一专利申请中提出了一种基于移动分组网的端到端加密通信系统，该端到端加密通信系统的组成结构如图 1 所示，主要包括：移动分组接入网络、加密通信移动终端、VOIP 服务器（VOIP Server）和密钥分发中心（KDC，

Key Distribution Center)。

其中，移动分组接入网络是指提供分组接入能力的现有移动通信网络，包括：GPRS、CDMA、WCDMA、CDMA2000 无线分组域接入网络以及这些移动网络的电路域数据业务接入网络，由运营商负责提供和运营。在不同的网络中，提供有不同的服务支持节点，用以实现 IP 网络的接入。

加密通信移动终端是指所有适用于当前所使用移动通信网络的终端，比如：在 GPRS、CDMA、WCDMA、CDMA2000 无线网络中，分别是 GPRS 终端、CDMA 终端、WCDMA 终端、CDMA2000 终端。加密通信移动终端必须具有移动分组接入能力和语音加密能力，并且能将采样得到的语音帧加密，并将加密后的语音帧封装为 IP 数据进行传送。这里，语音帧可以是单帧或多帧，可使用 IP/UDP/RTP 协议来封装语音数据。

VOIP Server 和 KDC 共同组成 VOIP 呼叫控制单元，位于 IP 网络侧，用来进行 VOIP 呼叫控制和密钥的生成、管理和分发，并负责 VOIP 用户的注册和鉴权，该 VOIP 呼叫控制单元还包括用户数据库。这里，VOIP Server 负责 VOIP 的呼叫控制，叠加在移动网络的分组域之上，移动分组接入网络只需配置 IP 路由数据，让加密移动通信的用户能够正常访问 VOIP 呼叫控制网络的边缘入口设备。KDC 用于根据用户私有信息生成加密密钥特征数据，加密通信移动终端可以根据加密密钥特征数据生成真正的密钥，并使用真正加密密钥对语音进行加解密操作。

在进行呼叫控制过程中，VOIP Server 收集通信双方的加密相关信息，并通过用户数据库发送给 KDC; KDC 根据 VOIP Server 收集的通信双方的加密相关信息，产生加密通信所用的密钥，并通过用户数据库返回给 VOIP Server; 用户数据库用来存储用户的签约信息，即注册信息，以及存有与用户的加密模块相同的私有信息。

在保密通信中，产生加密密钥后的密钥分发方式是非常关键的，虽然已提出了上述基于移动分组交换网的端到端加密通信系统，但如何在该系统中进行

密钥分发尚未提出具体的实现方案。

发明内容

有鉴于此，本发明的主要目的在于提供一种端到端加密通信的密钥分发方法，使得在基于移动分组交换网的端到端加密通信系统中能实现高安全性的密钥分发。

为达到上述目的，本发明的技术方案是这样实现的：

一种端到端加密通信的密钥分发方法，在每个用户终端和密钥分发中心分别存储有对应用户的用户私有数据，该方法包括以下步骤：

a. VOIP 服务器收到主叫终端的呼叫建立请求后，向密钥分发中心发送获取密钥请求；

b. 密钥分发中心收到请求后，分别产生用于主叫终端和被叫终端产生密钥的主叫加密密钥特征数据和被叫加密密钥特征数据，并将所产生的加密密钥特征数据返回给 VOIP 服务器；

c. VOIP 服务器将所得到的用于主叫终端和被叫终端产生密钥的主叫加密密钥特征数据和被叫加密密钥特征数据分别发送给主叫终端和被叫终端。其中，步骤 c 所述 VOIP 服务器将被叫加密密钥特征数据发送给被叫终端具体为：VOIP 服务器将被叫加密密钥特征数据携带于 SIP 信令的呼叫建立消息中发送给被叫终端。

步骤 c 所述 VOIP 服务器将主叫加密密钥特征数据发送给主叫终端具体为：VOIP 服务器在收到被叫终端发来的振铃消息后，将主叫加密密钥特征数据携带于 SIP 信令的被叫振铃消息中发送给主叫终端。在将主叫加密密钥特征数据携带于 SIP 信令的被叫振铃消息中发送给主叫终端之后，进一步包括：VOIP 服务器在收到被叫终端发来的被叫应答消息后，将主叫加密密钥特征数据携带于 SIP 信令的被叫应答消息中发送给主叫终端。

步骤 c 所述 VOIP 服务器将主叫和被叫加密密钥特征数据发送给主叫和被叫终端具体为：VOIP 服务器将主叫加密密钥特征数据和被叫加密密钥特征数据

携带于 SIP 信令的通知消息中分别发送给主叫终端和被叫终端。

该方法进一步包括：用户终端预先订阅加密呼叫事件，则步骤 c 所述 VOIP 服务器将主叫和被叫加密密钥特征数据发送给主叫和被叫终端具体为：VOIP 服务器收到主叫和被叫加密密钥特征数据后，判断当前主叫终端和被叫终端是否订阅加密呼叫事件，如果是，则将相应的加密密钥特征数据携带于 SIP 信令的通知消息中发送给订阅加密呼叫事件的用户终端；否则，通过 SIP 信令的呼叫建立消息将被叫加密密钥特征数据发送给被叫终端，通过 SIP 信令的被叫振铃消息或/和被叫应答消息将主叫加密密钥特征数据发送给主叫终端。

该方法进一步包括：主叫终端或被叫终端收到通过 SIP 信令的通知消息发来的加密密钥特征数据后，向 VOIP 服务器返回应答消息。

上述方案中，所述主叫加密密钥特征数据至少包括主叫密钥掩码，所述被叫加密密钥特征数据至少包括被叫密钥掩码。其中，步骤 b 中密钥分发中心随机产生分别用于主叫计算本次通信密钥和用于被叫计算本次通信密钥的随机数，再分别通过主叫终端和被叫终端各自的随机数、各自的用户私有数据以及本次呼叫的加密通信密钥产生主叫密钥掩码和被叫密钥掩码，则 VOIP 服务器向主叫终端和被叫终端发送携带有加密密钥特征数据的消息时，所述加密密钥特征数据进一步包括用于主叫或用于被叫计算本次通信密钥的随机数。

该方法进一步包括：d. 主叫终端和被叫终端分别通过当前得到的加密密钥特征数据和自身存储的用户私有数据产生本次呼叫的加密通信密钥，并通过所产生的加密通信密钥进行双方的加密语音通话。其中，所述加密密钥特征数据至少包括密钥掩码。步骤 b 中密钥分发中心随机产生分别用于主叫计算本次通信密钥和用于被叫计算本次通信密钥的随机数，则发送给主叫终端和被叫终端的加密密钥特征数据中分别进一步包括所产生的随机数；

则步骤 d 中主叫终端和被叫终端分别通过当前得到的密钥掩码、随机数和自身存储的用户私用数据产生本次呼叫的加密通信密钥。

上述方案中，每次呼叫所采用的加密通信密钥均不同。

本发明所提供的端到端加密通信的密钥分发方法，在基于移动分组交换网

络端到端加密通信系统中，完成加密密钥的分发。由于对于每次呼叫，密钥分发中心都会产生不同的主叫和被叫加密密钥特征数据，使每次加密通信中使用不同的加密密钥对语音进行加密处理，具有非常高的安全可靠性。并且，本发明的密钥分发方式不涉及在信令网络传输中传递未加密的密钥，保证了密钥的安全性。

本发明的密钥分发方式具有高兼容性和扩展性，能够适应于不同的加密算法，而且能满足移动加密通信网络与其他网络的互通时的加密密钥分发需求。

本发明可基于已有的呼叫流程发起获取密钥请求，并完成密钥分发，实现简单方便。本发明的方法对已有处理流程改动很小，基本不会影响正常的通信处理过程。另外，本发明进行密钥分发时，可利用正常传输的信令消息携带所需的参数或增加传输信令发送所需参数，实现方式灵活多样。

附图说明

图 1 为实现本发明方法的系统组成结构示意图；

图 2 为本发明方法具体实现的处理流程图。

具体实施方式

本发明的核心思想是：利用已有的端到端呼叫流程，VOIP 服务器在收到主叫终端的呼叫建立请求后，向密钥分发中心发起获取密钥的请求，由密钥分发中心产生主叫和被叫加密密钥特征数据，所产生的加密密钥特征数据再由 VOIP 服务器通过 SIP 信令消息分别下发给主叫终端或被叫终端，主叫和被叫终端通过得到的加密密钥特征数据产生本次呼叫的真正的加密通信密钥，双方进行加密语音通信。这里，所述的加密密钥特征数据可以是一组数据，至少包括用户终端的密钥掩码。

基于图 1 所示的端到端加密通信系统，本发明提出了一种加密密钥的发送方式，分发过程涉及加密通信移动终端、VOIP Server 和密钥分发中心。其中，加密通信移动终端中保存有用户私有加密信息，加密通信移动终端根据私有加

密信息和加密密钥特征数据生成真正的加密密钥，VOIP Server 在密钥分发过程中承担密钥转发功能，密钥分发中心负责加密密钥特征数据的生成。

假定主叫用户和被叫用户均为移动分组网络的普通用户，都签约了移动网络的相关数据业务，并且都签约了 VOIP 加密通信业务。那么，主叫用户和被叫用户在签约 VOIP 加密通信业务时，在 VOIP Server 和密钥分发中心同时保存了每个用户的私有数据，即指定的用户个人信息，如用户加密标识、用户密码、其它特定数据等；并且在用户使用的加密通信移动终端中也保存了加密相关私有数据，比如：用户开户时，在加密通信移动终端的加密模块中写入一些特定数据。

以两个加密通信移动终端之间进行端到端加密通信为例，这里，主叫加密通信移动终端简称为主叫终端，被叫加密通信移动终端简称为被叫终端。本发明中，密钥分发过程是在加密通信的呼叫流程基础上实现的。

具体的密钥分发过程如图 2 所示，包括以下步骤：

步骤 201：移动用户成功附着移动分组交换网络，并在 VOIP Server 上登记，也就是说，用户已建立分组域（PS）连接并注册，在登记过程中 VOIP Server 和密钥分发中心都会对当前附着的用户进行鉴权。

步骤 202~203：当主叫终端要发起加密呼叫时，主叫终端向 VOIP Server 发出起始会话协议（SIP）信令的呼叫建立消息 INVITE，发起呼叫建立过程。

步骤 204：VOIP Server 收到 INVITE 消息后，向密钥分发中心发送获取密钥请求，请求密钥分发中心生成本次呼叫的主叫加密密钥特征数据和被叫加密密钥特征数据，该获取密钥请求中携带有主叫用户号码和被叫用户号码。

步骤 205：密钥分发中心根据所收到请求中的主叫用户号码和被叫用户号码以及用户私有数据，分别产生主叫加密密钥特征数据和被叫加密密钥特征数据。这里，加密密钥特征数据是指与加密通信所用真正密钥 Key 相关的数据，主叫或被叫终端能够根据所得到的特征数据和自身保存的用户私有数据生成当前加密通信所用的真正密钥 Key，该加密密钥特征数据至少包括主叫或被叫的

密钥掩码，还可以包括用于计算本次通信密钥的随机数。当然，也可以携带其它与本次呼叫所用的加密通信密钥相关的信息参数。

其中，密钥掩码的具体产生过程可以是这样：密钥分发中心根据主叫用户号码和被叫用户号码，到用户数据库中查找主叫和被叫所对应的用户私有数据；同时，分别随机产生两个随机数，采用一个随机数、主叫用户私有数据和本次呼叫的加密通信密钥 Key 通过预先设定的已有标准加密算法，如 MD5 算法等，生成主叫密钥掩码，同样，再利用另一随机数、被叫用户私有数据和本次呼叫的加密通信密钥 Key 通过预先设定的已有标准加密算法，生成被叫密钥掩码。当然，密钥掩码的生成过程并不仅限于此。

由于加密密钥特征数据是每次呼叫时随机产生的，所以能够保证每次加密通话所采用的加密通信密钥均不一致。

步骤 206：生成主叫密钥掩码和被叫密钥掩码后，密钥分发中心将主叫加密密钥特征数据和被叫加密密钥特征数据，通过获取密钥响应传送给 VOIP Server，该响应的加密密钥特征数据中还包括有密钥分发中心随机产生的、用于计算本次通信密钥的随机数。

步骤 207~209：VOIP Server 收到获取密钥响应后，将主叫终端发送的 INVITE 消息发送给被叫终端，该消息中携带有包括被叫密钥掩码、用于被叫计算本次通信密钥的随机数的被叫加密密钥特征数据。被叫终端根据所得到的加密密钥特征数据和自身存储的用户私有数据，通过预先设定的加密算法计算本次呼叫真正的加密通信密钥，比如：被叫终端将被叫密钥掩码、随机数和用户私有数据按照设定的加密算法计算得到本次呼叫的加密通信密钥；之后，利用所产生的密钥对语音数据进行加密和解密操作。

同时，被叫终端收到 INVITE 请求消息后，如果自身空闲，就会产生振铃，并向 VOIP Server 返回 SIP 信令的被叫振铃消息 180 Ringing，表示被叫振铃。

步骤 210：VOIP Server 收到 180 Ringing 消息后，获知被叫振铃，则将 180 Ringing 消息转发给主叫终端，通知主叫终端被叫振铃；并在转发 180 Ringing

消息时，在消息中携带有包括主叫密钥掩码和用于主叫计算本次通信密钥的随机数的主叫加密密钥特征数据。

主叫终端收到主叫密钥掩码和随机数后，结合自身存储的用户私有数据，通过预先设定的加密算法产生本次呼叫的加密通信密钥 Key，比如：主叫终端将主叫密钥掩码、随机数和用户私有数据按照设定的加密算法计算得到本次呼叫的加密通信密钥；之后，利用所产生的密钥对语音数据进行加密和解密操作。

这里，选择在 180 Ringing 消息中下发主叫加密密钥特征数据，能够避免因终端计算真正加密密钥过程的时间对会话的影响。

步骤 211~213：此时，如果被叫摘机接听电话，则被叫终端向 VOIP Server 发送 SIP 信令的被叫应答消息 200 OK，表示被叫已摘机应答。

VOIP Server 收到后，会将 200 OK 消息转发给主叫终端。由于 180 Ringing 为不可靠消息，故在 VOIP Server 向主叫终端前转 200 OK 消息中，可再次携带主叫加密密钥特征数据，以避免因 180 Ringing 消息丢失，导致主叫终端不能获取本次呼叫的加密密钥特征数据。

步骤 214~215：主叫终端收到主叫密钥特征数据后，如果因 180 Ringing 消息丢失导致没有获得本次呼叫的加密密钥特征数据，那么，就根据 200 OK 消息中的加密密钥特征数据，结合自身存储的用户私有数据，通过预先设定的加密算法产生本次呼叫的加密通信密钥 Key，并使用密钥对语音进行加密和解密操作；同时，通过 VOIP Server 向被叫终端发送 SIP 信令的确认消息 ACK。

如果主叫终端已从 180 Ringing 消息获取本次呼叫的加密密钥特征数据并产生本次呼叫的加密通信密钥，则在这里可以不作任何处理，直接向被叫终端返回 ACK 消息。

如果主叫终端已从 180 Ringing 消息获取本次呼叫的加密密钥特征数据并产生本次呼叫的加密通信密钥，在这里也可以再次核对上一次所获得加密密钥特征数据的准确性，选择重新产生本次呼叫的加密通信密钥 Key 或不作处理；同时向被叫终端返回 ACK 消息。

如果主叫终端已从 180 Ringing 消息获取本次呼叫的加密密钥特征数据但并未产生本次呼叫的加密通信密钥，则在这里结合自身存储的用户私有数据，通过预先设定的加密算法产生本次呼叫的加密通信密钥 Key，并使用密钥对语音进行加密和解密操作；同时向被叫终端返回 ACK 消息。

步骤 216：主叫终端和被叫终端建立媒体流，进行加密语音通信。

为了保证主叫终端和被叫终端能够准确获得密钥分发中心生成主叫和被叫加密密钥特征数据，VOIP Server 可以在收到密钥分发中心发来的主叫和被叫加密密钥特征数据后，主动通过 SIP 信令中的通知消息 Notify，分别将主叫加密密钥特征数据和被叫加密密钥特征数据发送给主叫终端和被叫终端，如步骤 206'所示。这种情况下，就不需要再通过 INVITE 消息将被叫加密密钥特征数据送给被叫终端，也不用通过 180 Ringing 消息和 200 OK 消息将主叫加密密钥特征数据送给主叫终端。

VOIP Server 这种通过通知消息向主叫和被叫终端分发加密密钥特征数据的方式，也可以是由用户终端事先订阅的加密呼叫事件触发的。比如：某个用户终端事先订阅了加密呼叫事件，也就是说，该用户终端要求 VOIP Server 在获得给自己的加密密钥特征数据后，就通过通知消息发给自己。那么，在实际应用中，VOIP Server 收到密钥分发中心发来的加密密钥特征数据后，判断一下该加密密钥特征数据对应的用户终端是否订阅了加密呼叫事件，如果订阅了，就通过通知消息将当前得到的加密密钥特征数据发给相应用户终端，如果未订阅，VOIP Server 可以选择主动通过通知消息发送，也可以选用 180 Ringing 以及 200 OK 消息发送给主叫终端或通过 INVITE 消息发送给被叫终端。

对于 VOIP Server 通过通知消息向主叫或被叫终端发送加密密钥特征数据的情况，主叫终端或被叫终端在收到加密密钥特征数据后，可以向 VOIP Server 返回针对通知消息的应答消息 200 OK，表示成功接收加密密钥特征数据，如步骤 206"所示。

以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

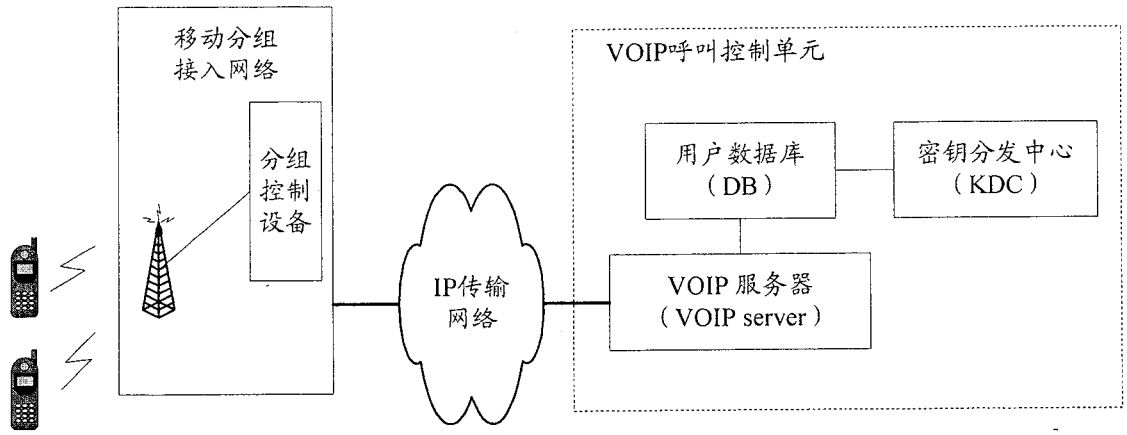

移动分组
接入网络
分组
控制
设备
IP传输
网络
VOIP呼叫控制单元
用户数据库
（DB）
密钥分发中心
（KDC）
VOIP 服务器
（VOIP server）

图 1

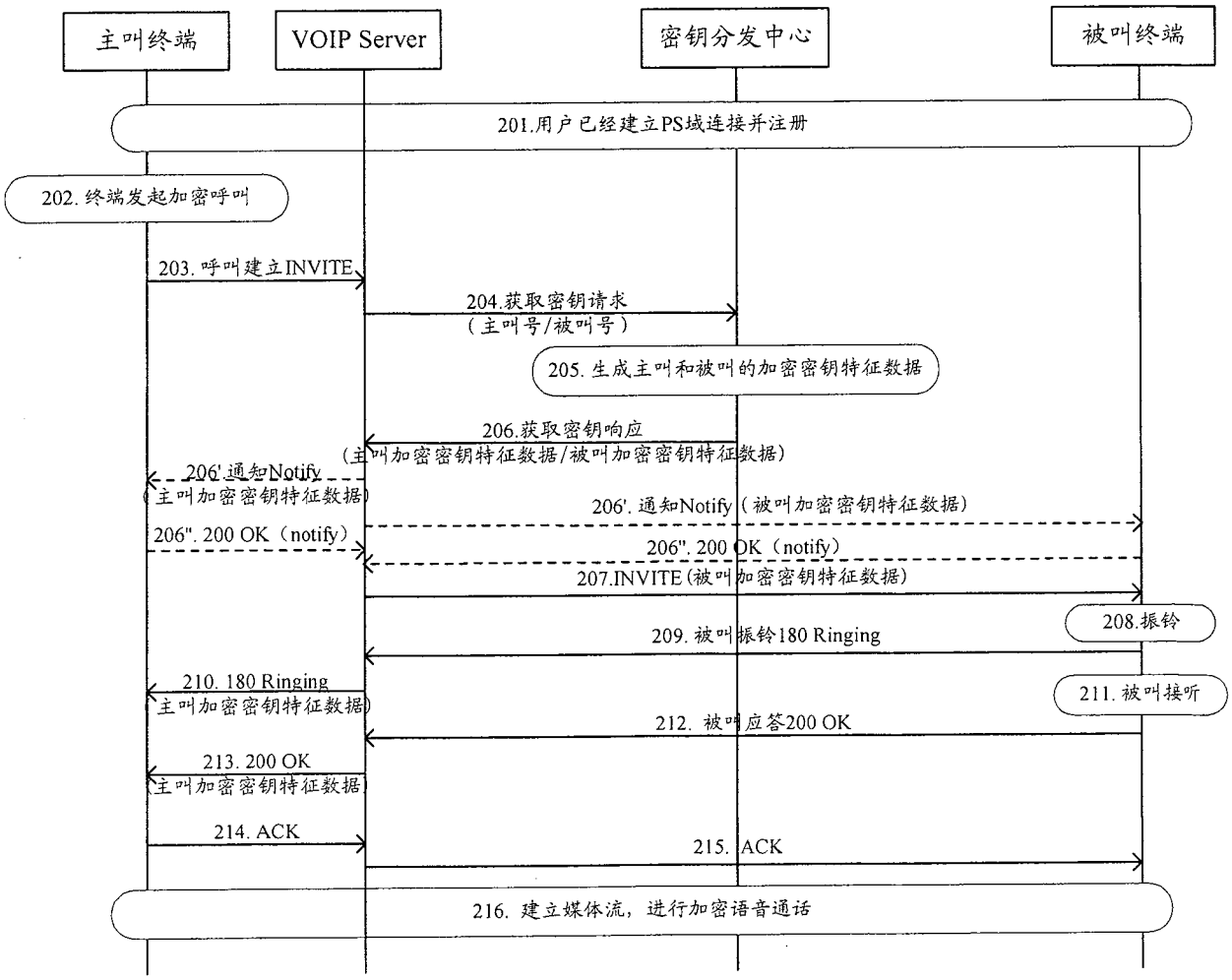

主叫终端
VOIP Server
密钥分发中心
被叫终端
201.用户已经建立PS域连接并注册
202. 终端发起加密呼叫
203. 呼叫建立INVITE
204.获取密钥请求
（主叫号/被叫号）
205. 生成主叫和被叫的加密密钥特征数据
206.获取密钥响应
（主叫加密密钥特征数据/被叫加密密钥特征数据）
206'.通知Notify
（主叫加密密钥特征数据）
206'. 通知Notify（被叫加密密钥特征数据）
206". 200 OK（notify）
206". 200 OK（notify）
207.INVITE（被叫加密密钥特征数据）
208.振铃
209. 被叫振铃180 Ringing
210. 180 Ringing
（主叫加密密钥特征数据）
211. 被叫接听
212. 被叫应答200 OK
213. 200 OK
（主叫加密密钥特征数据）
214. ACK
215. ACK
216. 建立媒体流，进行加密语音通话

图 2