(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 12 月 7 日 (07.12.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/206247 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/087543

(22) 国际申请日: 2016 年 6 月 29 日 (29.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610378602.X 2016年5月31日 (31.05.2016) CN

(71) 申请人: 宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(72) 发明人: 钟焰涛(ZHONG, Yantao); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 傅文治(FU, Wenzhi); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 蒋罗(JIANG, Luo); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 北京友联知识产权代理事务所（普通合伙）(YOULINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路8号科技财富中心A座506室尚志峰, Beijing 100192 (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,

(54) **Title:** VOICE ENCRYPTION METHOD AND APPARATUS, TERMINAL, AND KEY MANAGEMENT PLATFORM AND SYSTEM

(54) **发明名称:** 语音加密方法、装置、终端、密钥管理平台和系统

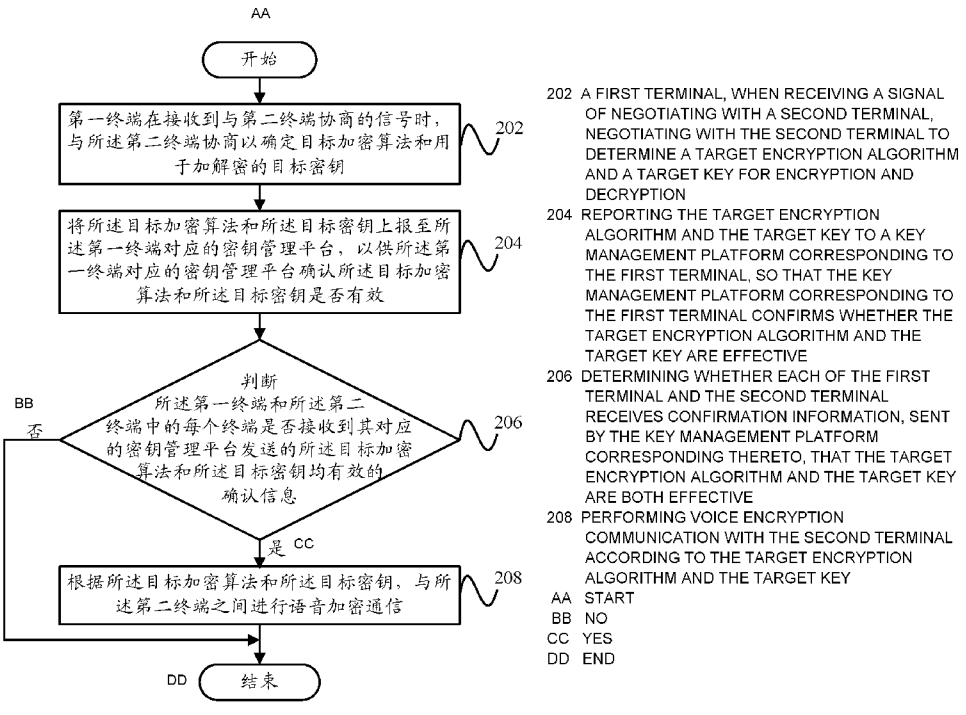


图 2

(57) **Abstract:** Proposed are a voice encryption method and apparatus, a terminal, and a key management platform and system. The voice encryption method comprises: a first terminal, when receiving a signal of negotiating with a second terminal, negotiating with the second terminal to determine a target encryption algorithm and a target key for encryption and decryption; reporting the target encryption algorithm and the target key to a key management platform corresponding to the first terminal; determining whether each of the first terminal and the second terminal receives confirmation information, sent by the key management platform corresponding thereto, that

WO 2017/206247 A1

[见续页]

GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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))。

the target encryption algorithm and the target key are both effective; and if each terminal receives the confirmation information sent by the key management platform corresponding thereto, performing voice encryption communication with the second terminal according to the target encryption algorithm and the target key. By means of the technical solution of the present invention, voice encryption communication can be performed between terminals of different operators, at the same time, avoiding a key management platform bearing tasks of negotiating and issuing a key.

(57) 摘要：本发明提出了一种语音加密方法、装置、终端、密钥管理平台和系统，其中，该语音加密方法包括：第一终端在接收到与第二终端协商的信号时，与第二终端协商以确定目标加密算法和用于加解密的目标密钥；将目标加密算法和目标密钥上报至第一终端对应的密钥管理平台；判断第一终端和第二终端中的每个终端是否接收到其对应的密钥管理平台发送的目标加密算法和目标密钥均有效的确认信息；若每个终端均接收到其对应的密钥管理平台发送的确认信息，则根据目标加密算法和目标密钥，与第二终端之间进行语音加密通信。通过本发明的技术方案，使得属于不同运营商的终端之间可以进行语音加密通信，同时避免了密钥管理平台承担协商、分发密钥的任务。

语音加密方法、装置、终端、密钥管理平台和系统

技术领域

本发明涉及通信技术领域，具体而言，涉及一种语音加密方法、一种语音加密装置、一种终端、一种密钥管理平台和一种通信系统。

背景技术

目前，为实现语音加密通信，中国电信通过采用密钥管理平台为终端提供密钥，终端之间使用该密钥、通过预设的语音加解密算法进行语音加密通信。如图 1 所示，终端 1 和终端 2 进行语音加密通信的步骤包括：（1）终端 1 和终端 2 分别向密钥管理平台请求密钥，（2）密钥管理平台分别下发密钥至终端 1 和终端 2，（3）终端 1 和终端 2 根据下发的密钥进行语音加密通信。但是，这种方案的缺陷是，只能在中国电信网络范围内提供语音加密服务，如果终端 1 和终端 2 属于不同的运营商，则这种方案架构无法实施。

中国移动提出一种可以在不同运营商的终端之间实现语音加密通信的方案。该方案所支持的加密算法、参数规格等均由密钥管理平台确定，换句话说，密钥管理平台承担协商、分发密钥的任务，在大规模系统中该平台负荷会很大，一旦平台出错，用户无法进行语音加密通信。

因此，如何使得属于不同运营商的终端之间可以进行语音加密通信，同时可以降低密钥管理平台的负担成为亟待解决的问题。

发明内容

本发明正是基于上述问题，提出了一种新的技术方案，使得属于不同运营商的终端之间可以进行语音加密通信，同时避免了密钥管理平台承担协商、分发密钥的任务，从而降低密钥管理平台的负担。

有鉴于此，本发明的第一方面提出了一种语音加密方法，包括：第一

终端在接收到与第二终端协商的信号时，与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥；将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效；判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息；若所述每个终端均接收到其对应的密钥管理平台发送的所述确认信息，则根据所述目标加密算法和所述目标密钥，与所述第二终端之间进行语音加密通信。

在该技术方案中，在第一终端与第二终端进行语音通信时，第一终端与第二终端协商确定目标加密算法和目标密钥，将目标加密算法和目标密钥上报至第一终端和第二终端中的每个终端对应的密钥管理平台，即密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。另外，由于是终端各自对应的密钥管理平台确认目标加密算法和目标密钥是否有效，则第一终端和第二终端可以属于同一个运营商，例如，都是使用中国电信网络的终端，也可以属于不同的运营商，例如，一个是使用中国电信网络的终端，另一个是使用中国移动网络的终端。

在上述技术方案中，优选地，所述与所述第二终端协商以确定目标加密算法和目标密钥的步骤，具体包括：在所述第一终端和所述第二终端同时支持的加密算法中选择优先级最高的加密算法作为所述目标加密算法；以及根据密钥协商协议与所述第二终端协商，以确定所述目标密钥。

在该技术方案中，通过选择第一终端和第二终端同时支持的加密算法作为目标加密算法，则在使用该目标加密算法进行加密时，可以保证第一终端与第二终端之间可以正常进行语音加密通信。

在上述任一技术方案中，优选地，还包括：在确定与所述第二终端进行语音加密通信时，若向所述第二终端发送用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号；或者若接收到所述第二终端发送的用于协商加密算法和加密密钥的协商请求，则确定接收

到与所述第二终端协商的信号。

在该技术方案中，与第二终端进行协商的过程可以由第一终端发起，还可以由第二终端发起，在发起协商后就可以与第二终端进行协商。

上述任一项技术方案的执行主体均是第一终端。

本发明的第二方面提出了一种语音加密装置，包括：第一确定单元，用于在第一终端接收到与第二终端协商的信号时，与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥；发送单元，用于将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效；判断单元，用于判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息；语音通信单元，用于若所述每个终端均接收到其对应的密钥管理平台发送的所述确认信息，则根据所述目标加密算法和所述目标密钥，与所述第二终端之间进行语音加密通信。

在该技术方案中，在第一终端与第二终端进行语音通信时，第一终端与第二终端协商确定目标加密算法和目标密钥，将目标加密算法和目标密钥上报至第一终端和第二终端中的每个终端对应的密钥管理平台，即密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。另外，由于是终端各自对应的密钥管理平台确认目标加密算法和目标密钥是否有效，则第一终端和第二终端可以属于同一个运营商，例如，都是使用中国电信网络的终端，也可以属于不同的运营商，例如，一个是使用中国电信网络的终端，另一个是使用中国移动网络的终端。

在上述技术方案中，优选地，所述第一确定单元具体用于，在所述第一终端和所述第二终端同时支持的加密算法中选择优先级最高的加密算法作为所述目标加密算法；以及根据密钥协商协议与所述第二终端协商，以确定所述目标密钥。

在该技术方案中，通过选择第一终端和第二终端同时支持的加密算法

作为目标加密算法，则在使用该目标加密算法进行加密时，可以保证第一终端与第二终端之间可以正常进行语音加密通信。

在上述任一技术方案中，优选地，还包括：第二确定单元，用于在确定与所述第二终端进行语音加密通信时，若向所述第二终端发送用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号；或者第三确定单元，用于若接收到所述第二终端发送的用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号。

在该技术方案中，与第二终端进行协商的过程可以由第一终端发起，还可以由第二终端发起，在发起协商后就可以与第二终端进行协商。

本发明的第三方面提出了一种终端，包括上述技术方案中任一项所述的语音加密装置，因此，该终端具有和上述技术方案中任一项所述的语音加密装置相同的技术效果，在此不再赘述。

本发明的第四方面提出了一种语音加密方法，包括：接收终端发送的目标加密算法和用于加解密的目标密钥；根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效；若所述目标加密算法和所述目标密钥均有效，则向所述终端发送所述目标加密算法和所述目标密钥均有效的确认信息。

在该技术方案中，在目标加密算法和目标密钥都有效的情况下，通过向终端发送目标加密算法和目标密钥均有效的确认信息，以使终端可以正常进行语音加密通信。优选地，语音加密方法用于密钥管理平台，密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。

在上述技术方案中，优选地，在所述语音加密方法用于密钥管理平台的情况下，判断所述目标加密算法和所述目标密钥是否有效的步骤，具体包括：判断所述密钥管理平台是否支持所述目标加密算法；若所述密钥管理平台支持所述目标加密算法，则判定所述目标加密算法有效，若所述密钥管理平台不支持所述目标加密算法，则判定所述目标加密算法无效；以及判断所述目标密钥的属性是否符合预设条件；若所述目标密钥的属性符

合所述预设条件，则判定所述目标密钥有效，若所述目标密钥的属性不符合所述预设条件，则判定所述目标密钥无效。

在该技术方案中，通过判断协商出的目标加密算法是否是密钥管理平台所支持的，以及判断目标密钥的属性是否符合预设条件，例如，目标密钥的长度是否是预设长度，目标密钥的格式是否与预设格式一致，以使终端之间根据目标加密算法和目标密钥可以正常进行语音加密通信，保证了终端之间进行通信的可靠性。

本发明的第五方面提出了一种密钥管理平台，包括：接收单元，用于接收终端发送的目标加密算法和用于加解密的目标密钥；判断单元，用于根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效；发送单元，用于若所述目标加密算法和所述目标密钥均有效，则向所述终端发送所述目标加密算法和所述目标密钥均有效的确认信息。

在该技术方案中，在目标加密算法和目标密钥都有效的情况下，通过向终端发送目标加密算法和目标密钥均有效的确认信息，以使终端可以正常进行语音加密通信。优选地，语音加密方法用于密钥管理平台，密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。

在上述技术方案中，优选地，所述判断单元包括：第一判断子单元，用于判断所述密钥管理平台是否支持所述目标加密算法，若所述密钥管理平台支持所述目标加密算法，则判定所述目标加密算法有效，若所述密钥管理平台不支持所述目标加密算法，则判定所述目标加密算法无效；以及第二判断子单元，用于判断所述目标密钥的属性是否符合预设条件，若所述目标密钥的属性符合所述预设条件，则判定所述目标密钥有效，若所述目标密钥的属性不符合所述预设条件，则判定所述目标密钥无效。

在该技术方案中，通过判断协商出的目标加密算法是否是密钥管理平台所支持的，以及判断目标密钥的属性是否符合预设条件，例如，目标密钥的长度是否是预设长度，目标密钥的格式是否与预设格式一致，以使终

端之间根据目标加密算法和目标密钥可以正常进行语音加密通信，保证了终端之间进行通信的可靠性。

本发明的第六方面提出了一种通信系统，包括：多个如上述技术方案中所述的终端；至少一个如上述技术方案中所述的密钥管理平台，因此，该通信系统具有和上述技术方案中所述的终端、密钥管理平台相同的技术效果，在此不再赘述。

通过本发明的技术方案，使得属于不同运营商的终端之间可以进行语音加密通信，同时避免了密钥管理平台承担协商、分发密钥的任务，从而降低密钥管理平台的负担。

附图说明

图 1 示出了相关技术中的通信系统的原理示意图；

图 2 示出了根据本发明的一个实施例的语音加密方法的流程示意图；

图 3 示出了根据本发明的另一个实施例的语音加密方法的流程示意图；

图 4 示出了根据本发明的一个实施例的语音加密装置的结构示意图；

图 5 示出了根据本发明的一个实施例的终端的结构示意图；

图 6 示出了根据本发明的又一个实施例的语音加密方法的流程示意图；

图 7 示出了根据本发明的一个实施例的密钥管理平台的结构示意图；

图 8 示出了根据本发明的一个实施例的通信系统的结构示意图；

图 9 示出了根据本发明的一个实施例的通信系统的原理示意图。

具体实施方式

为了可以更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明

的保护范围并不受下面公开的具体实施例的限制。

图 2 示出了根据本发明的一个实施例的语音加密方法的流程示意图。

如图 2 所示，根据本发明的一个实施例的语音加密方法，包括：

步骤 202，第一终端在接收到与第二终端协商的信号时，与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥。

优选地，还包括：在确定与所述第二终端进行语音加密通信时，若向所述第二终端发送用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号；或者若接收到所述第二终端发送的用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号。与第二终端进行协商的过程可以由第一终端发起，还可以由第二终端发起，在发起协商后就可以与第二终端进行协商。

优选地，所述与所述第二终端协商以确定目标加密算法和目标密钥的步骤，具体包括：在所述第一终端和所述第二终端同时支持的加密算法中选择优先级最高的加密算法作为所述目标加密算法；以及根据密钥协商协议与所述第二终端协商，以确定所述目标密钥。

通过选择第一终端和第二终端同时支持的加密算法作为目标加密算法，则在使用该目标加密算法进行加密时，可以保证第一终端与第二终端之间可以正常进行语音加密通信。另外，与第二终端协商时的密钥协商协议包括但不限于 Diffie-Hellman 密钥协商协议。

步骤 204，将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效。

步骤 206，判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息，在判定所述每个终端均接收到其对应的密钥管理平台发送的所述确认信息时，进入步骤 208，否则结束本次流程。

步骤 208，根据所述目标加密算法和所述目标密钥，与所述第二终端之间进行语音加密通信。

在上述技术方案中，执行主体均是第一终端。在第一终端与第二终端

进行语音通信时，第一终端与第二终端协商确定目标加密算法和目标密钥，将目标加密算法和目标密钥上报至第一终端和第二终端中的每个终端对应的密钥管理平台，即密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。另外，由于是终端各自对应的密钥管理平台确认目标加密算法和目标密钥是否有效，则第一终端和第二终端可以属于同一个运营商，例如，都是使用中国电信网络的终端，也可以属于不同的运营商，例如，一个是使用中国电信网络的终端，另一个是使用中国移动网络的终端。

图 3 示出了根据本发明的另一个实施例的语音加密方法的流程示意图。

如图 3 所示，根据本发明的另一个实施例的语音加密方法，包括:

步骤 302，终端 1 和终端 2 确认进行语音加密通信。

步骤 304，终端 1 和终端 2 进行加密算法和密钥的协商。

步骤 306，协商是否成功？在协商成功时，进入步骤 308，否则进入步骤 310。

步骤 308，终端 1 和终端 2 各自将协商结果上报给自己的密钥管理平台。其中，协商结果包括：协商最终确定的加密算法和密钥。例如，终端 1 对应密钥管理平台 1，终端 2 对应密钥管理平台 2，终端 1 将协商结果上报至密钥管理平台 1，终端 2 将协商结果上报至密钥管理平台 2。

步骤 310，失败退出。协商失败的情况可能由以下几种情况导致：(1)协商超时；(2)双方没有共同支持的算法；(3)密钥协商协议执行失败等情况。

步骤 312，密钥管理平台 1 和密钥管理平台 2 分别对协商结果进行确认。例如，密钥管理平台 1 判断协商的加密算法是否密钥管理平台 1 所支持的，并判断协商的密钥的长度和格式等属性是否符合要求，在密钥管理平台 1 判定加密算法是密钥管理平台 1 所支持的，且判定密钥的长度和格式等属性符合要求的情况下，密钥管理平台 1 向终端 1 发送确认信息，以确认加密算法和密钥是有效的。密钥管理平台 2 发送确认信息的方案和密

钥管理平台 1 的方案相同，在此不再赘述。

步骤 314，终端 1 和终端 2 使用所协商的加密算法和密钥进行语音加密通信。具体地，终端 1 接收到其对应的密钥管理平台 1 发送的确认信息，且终端 2 接收到其对应的密钥管理平台 2 发送的确认信息，终端 1 和终端 2 使用所协商的加密算法和密钥进行语音加密通信。

图 4 示出了根据本发明的一个实施例的语音加密装置的结构示意图。

如图 4 所示，根据本发明的一个实施例的语音加密装置 400，包括：第一确定单元 402、发送单元 404、判断单元 406 和语音通信单元 408。

第一确定单元 402，用于在第一终端接收到与第二终端协商的信号时，与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥。

优选地，所述第一确定单元 402 具体用于，在所述第一终端和所述第二终端同时支持的加密算法中选择优先级最高的加密算法作为所述目标加密算法；以及根据密钥协商协议与所述第二终端协商，以确定所述目标密钥。其中，与第二终端协商时的密钥协商协议包括但不限于 Diffie-Hellman 密钥协商协议。

优选地，语音加密装置 400 还包括：第二确定单元 410，用于在确定与所述第二终端进行语音加密通信时，若向所述第二终端发送用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号；或者第三确定单元 412，用于若接收到所述第二终端发送的用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号。

发送单元 404，用于将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效。

判断单元 406，用于判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息。

语音通信单元 408，用于若所述每个终端均接收到其对应的密钥管理平台发送的所述确认信息，则根据所述目标加密算法和所述目标密钥，与

所述第二终端之间进行语音加密通信。

在该技术方案中，在第一终端与第二终端进行语音通信时，第一终端与第二终端协商确定目标加密算法和目标密钥，将目标加密算法和目标密钥上报至第一终端和第二终端中的每个终端对应的密钥管理平台，即密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。另外，由于是终端各自对应的密钥管理平台确认目标加密算法和目标密钥是否有效，则第一终端和第二终端可以属于同一个运营商，例如，都是使用中国电信网络的终端，也可以属于不同的运营商，例如，一个是使用中国电信网络的终端，另一个是使用中国移动网络的终端。

图 5 示出了根据本发明的一个实施例的终端的结构示意图。

如图 5 所示，根据本发明的一个实施例的终端 500，包括上述技术方案中任一项所述的语音加密装置 400，因此，该终端 500 具有和上述技术方案中任一项所述的语音加密装置 400 相同的技术效果，在此不再赘述。

图 6 示出了根据本发明的又一个实施例的语音加密方法的流程示意图。

如图 6 所示，根据本发明的又一个实施例的语音加密方法，包括：

步骤 602，接收终端发送的目标加密算法和用于加解密的目标密钥。

步骤 604，根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效，在判定所述目标加密算法和所述目标密钥均有效时，进入步骤 606，否则，结束本次流程。

优选地，所述语音加密方法用于密钥管理平台，步骤 604 具体包括：判断所述密钥管理平台是否支持所述目标加密算法；若所述密钥管理平台支持所述目标加密算法，则判定所述目标加密算法有效，若所述密钥管理平台不支持所述目标加密算法，则判定所述目标加密算法无效；以及判断所述目标密钥的属性是否符合预设条件；若所述目标密钥的属性符合所述预设条件，则判定所述目标密钥有效，若所述目标密钥的属性不符合所述预设条件，则判定所述目标密钥无效。

通过判断协商出的目标加密算法是否是密钥管理平台所支持的，以及判断目标密钥的属性是否符合预设条件，例如，目标密钥的长度是否是预设长度，目标密钥的格式是否与预设格式一致，以使终端之间根据目标加密算法和目标密钥可以正常进行语音加密通信，保证了终端之间进行通信的可靠性。

步骤 606，向所述终端发送所述目标加密算法和所述目标密钥均有效的确认信息。

在上述技术方案中，在目标加密算法和目标密钥都有效的情况下，通过向终端发送目标加密算法和目标密钥均有效的确认信息，以使终端可以正常进行语音加密通信。优选地，语音加密方法用于密钥管理平台，密钥管理平台仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台承担协商、分发密钥的任务，特别是在密钥管理平台负荷很大的情况下，大大降低了密钥管理平台的负担。

图 7 示出了根据本发明的一个实施例的密钥管理平台的结构示意图。

如图 7 所示，根据本发明的一个实施例的密钥管理平台 700，包括：接收单元 702、判断单元 704 和发送单元 706。

接收单元 702，用于接收终端发送的目标加密算法和用于加解密的目标密钥。

判断单元 704，用于根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效。

优选地，所述判断单元 704 包括：第一判断子单元 7042，用于判断所述密钥管理平台 700 是否支持所述目标加密算法，若所述密钥管理平台 700 支持所述目标加密算法，则判定所述目标加密算法有效，若所述密钥管理平台 700 不支持所述目标加密算法，则判定所述目标加密算法无效；以及第二判断子单元 7044，用于判断所述目标密钥的属性是否符合预设条件，若所述目标密钥的属性符合所述预设条件，则判定所述目标密钥有效，若所述目标密钥的属性不符合所述预设条件，则判定所述目标密钥无效。

通过判断协商出的目标加密算法是否是密钥管理平台 700 所支持的，

以及判断目标密钥的属性是否符合预设条件，例如，目标密钥的长度是否是预设长度，目标密钥的格式是否与预设格式一致，以使终端之间根据目标加密算法和目标密钥可以正常进行语音加密通信，保证了终端之间进行通信的可靠性。

发送单元 706，用于若所述目标加密算法和所述目标密钥均有效，则向所述终端发送所述目标加密算法和所述目标密钥均有效的确认信息。

在上述技术方案中，在目标加密算法和目标密钥都有效的情况下，通过向终端发送目标加密算法和目标密钥均有效的确认信息，以使终端可以正常进行语音加密通信。优选地，语音加密方法用于密钥管理平台 700，密钥管理平台 700 仅确认目标加密算法和目标密钥是否有效即可，避免了密钥管理平台 700 承担协商、分发密钥的任务，特别是在密钥管理平台 700 负荷很大的情况下，大大降低了密钥管理平台 700 的负担。

图 8 示出了根据本发明的一个实施例的通信系统的结构示意图。

如图 8 所示，根据本发明的一个实施例的通信系统 800，多个如上述技术方案中所述的终端 500；至少一个如上述技术方案中所述的密钥管理平台 700，因此，该通信系统 800 具有和上述技术方案中所述的终端 500、密钥管理平台 700 相同的技术效果，在此不再赘述。

图 9 示出了根据本发明的一个实施例的通信系统的原理示意图。

如图 9 所示，在该实施例中，通信系统包括：终端 1、终端 1 对应的密钥管理平台 1、终端 2、终端 2 对应的密钥管理平台 2。下面详细介绍该通信系统中终端 1 和终端 2 进行语音加密通信的方案。

（1）终端 1 和终端 2 之间确认进行语音加密通信。

（2）终端 1 和终端 2 之间协商加密算法、密钥。

（3）终端 1 将协商的加密算法和密钥上报至密钥管理平台 1，密钥管理平台 1 对加密算法和密钥进行确认，以确认加密算法是否是密钥管理平台 1 所支持的，并确认密钥的长度和格式等属性是否符合要求。终端 2 将协商的加密算法和密钥上报至密钥管理平台 2，密钥管理平台 2 对加密算法和密钥进行确认，以确认加密算法是否是密钥管理平台 2 所支持的，并确认密钥的长度和格式等属性是否符合要求。

（4）密钥管理平台 1 确认加密算法是密钥管理平台 1 所支持的，且确认密钥符合要求时，向终端 1 发送加密算法和密钥均有效的确认信息。密钥管理平台 2 确认加密算法是密钥管理平台 2 所支持的，且确认密钥符合要求时，向终端 2 发送加密算法和密钥均有效的确认信息。

（5）在终端 1 接收到加密算法和密钥均有效的确认信息，且终端 2 接收到加密算法和密钥均有效的确认信息时，终端 1 和终端 2 根据协商的加密算法和密钥进行语音加密通信。

以上结合附图详细说明了本发明的技术方案，通过本发明的技术方案，使得属于不同运营商的终端之间可以进行语音加密通信，同时避免了密钥管理平台承担协商、分发密钥的任务，从而降低密钥管理平台的负担。

在本发明中，术语“第一”、“第二”仅用于描述的目的，而不能理解为指示或暗示相对重要性；术语“多个”表示两个或两个以上。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种语音加密方法，其特征在于，包括:

第一终端在接收到与第二终端协商的信号时，与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥;

将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效;

判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息;

若所述每个终端均接收到其对应的密钥管理平台发送的所述确认信息，则根据所述目标加密算法和所述目标密钥，与所述第二终端之间进行语音加密通信。

2. 根据权利要求 1 所述的语音加密方法，其特征在于，所述与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥的步骤，具体包括:

在所述第一终端和所述第二终端同时支持的加密算法中选择优先级最高的加密算法作为所述目标加密算法; 以及

根据密钥协商协议与所述第二终端协商，以确定所述目标密钥。

3. 根据权利要求 1 或 2 所述的语音加密方法，其特征在于，还包括:

在确定与所述第二终端进行语音加密通信时，若向所述第二终端发送用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号; 或者

若接收到所述第二终端发送的用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号。

4. 一种语音加密装置，其特征在于，包括:

第一确定单元，用于在第一终端接收到与第二终端协商的信号时，与

所述第二终端协商以确定目标加密算法和用于加解密的目标密钥;

发送单元，用于将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效;

判断单元，用于判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息;

语音通信单元，用于若所述每个终端均接收到其对应的密钥管理平台发送的所述确认信息，则根据所述目标加密算法和所述目标密钥，与所述第二终端之间进行语音加密通信。

5. 根据权利要求 4 所述的语音加密装置，其特征在于，所述第一确定单元具体用于，

在所述第一终端和所述第二终端同时支持的加密算法中选择优先级最高的加密算法作为所述目标加密算法，以及根据密钥协商协议与所述第二终端协商，以确定所述目标密钥。

6. 根据权利要求 4 或 5 所述的语音加密装置，其特征在于，还包括:

第二确定单元，用于在确定与所述第二终端进行语音加密通信时，若向所述第二终端发送用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号; 或者

第三确定单元，用于若接收到所述第二终端发送的用于协商加密算法和加密密钥的协商请求，则确定接收到与所述第二终端协商的信号。

7. 一种终端，其特征在于，包括: 如权利要求 4 至 6 中任一项所述的语音加密装置。

8. 一种语音加密方法，其特征在于，包括:

接收终端发送的目标加密算法和用于加解密的目标密钥;

根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效;

若所述目标加密算法和所述目标密钥均有效，则向所述终端发送所述

目标加密算法和所述目标密钥均有效的确认信息。

9. 根据权利要求 8 所述的语音加密方法，其特征在于，所述语音加密方法用于密钥管理平台，其中，判断所述目标加密算法和所述目标密钥是否有效的步骤，具体包括:

判断所述密钥管理平台是否支持所述目标加密算法;

若所述密钥管理平台支持所述目标加密算法，则判定所述目标加密算法有效，若所述密钥管理平台不支持所述目标加密算法，则判定所述目标加密算法无效；以及

判断所述目标密钥的属性是否符合预设条件;

若所述目标密钥的属性符合所述预设条件，则判定所述目标密钥有效，若所述目标密钥的属性不符合所述预设条件，则判定所述目标密钥无效。

10. 一种密钥管理平台，其特征在于，包括:

接收单元，用于接收终端发送的目标加密算法和用于加解密的目标密钥;

判断单元，用于根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效;

发送单元，用于若所述目标加密算法和所述目标密钥均有效，则向所述终端发送所述目标加密算法和所述目标密钥均有效的确认信息。

11. 根据权利要求 10 所述的密钥管理平台，其特征在于，所述判断单元包括:

第一判断子单元，用于判断所述密钥管理平台是否支持所述目标加密算法，若所述密钥管理平台支持所述目标加密算法，则判定所述目标加密算法有效，若所述密钥管理平台不支持所述目标加密算法，则判定所述目标加密算法无效；以及

第二判断子单元，用于判断所述目标密钥的属性是否符合预设条件，若所述目标密钥的属性符合所述预设条件，则判定所述目标密钥有效，若所述目标密钥的属性不符合所述预设条件，则判定所述目标密钥无效。

12. 一种通信系统，其特征在于，包括:

多个如权利要求 7 所述的终端;

至少一个如权利要求 10 或 11 所述的密钥管理平台。

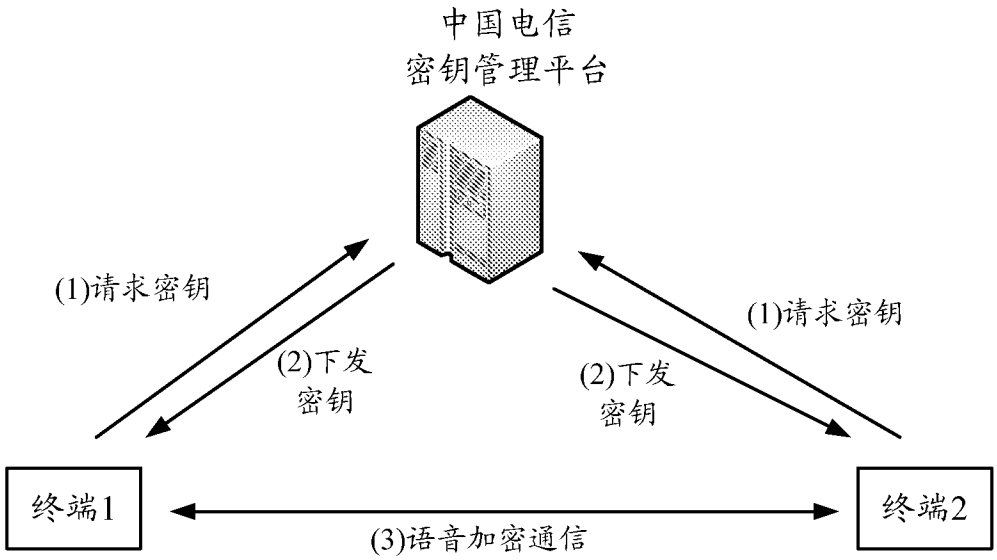


图 1

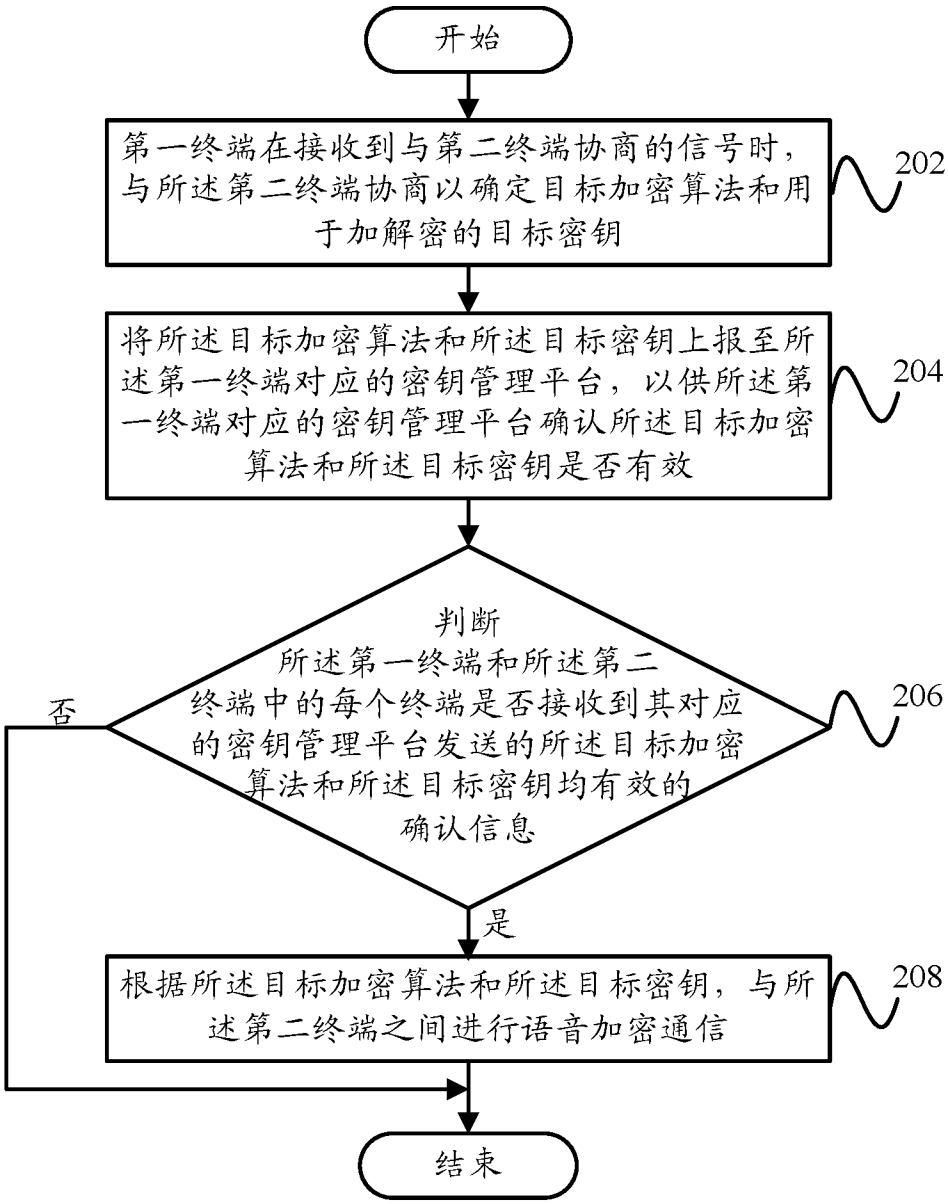

开始
第一终端在接收到与第二终端协商的信号时，与所述第二终端协商以确定目标加密算法和用于加解密的目标密钥
202
将所述目标加密算法和所述目标密钥上报至所述第一终端对应的密钥管理平台，以供所述第一终端对应的密钥管理平台确认所述目标加密算法和所述目标密钥是否有效
204
判断所述第一终端和所述第二终端中的每个终端是否接收到其对应的密钥管理平台发送的所述目标加密算法和所述目标密钥均有效的确认信息
206
否
是
根据所述目标加密算法和所述目标密钥，与所述第二终端之间进行语音加密通信
208
结束

图 2

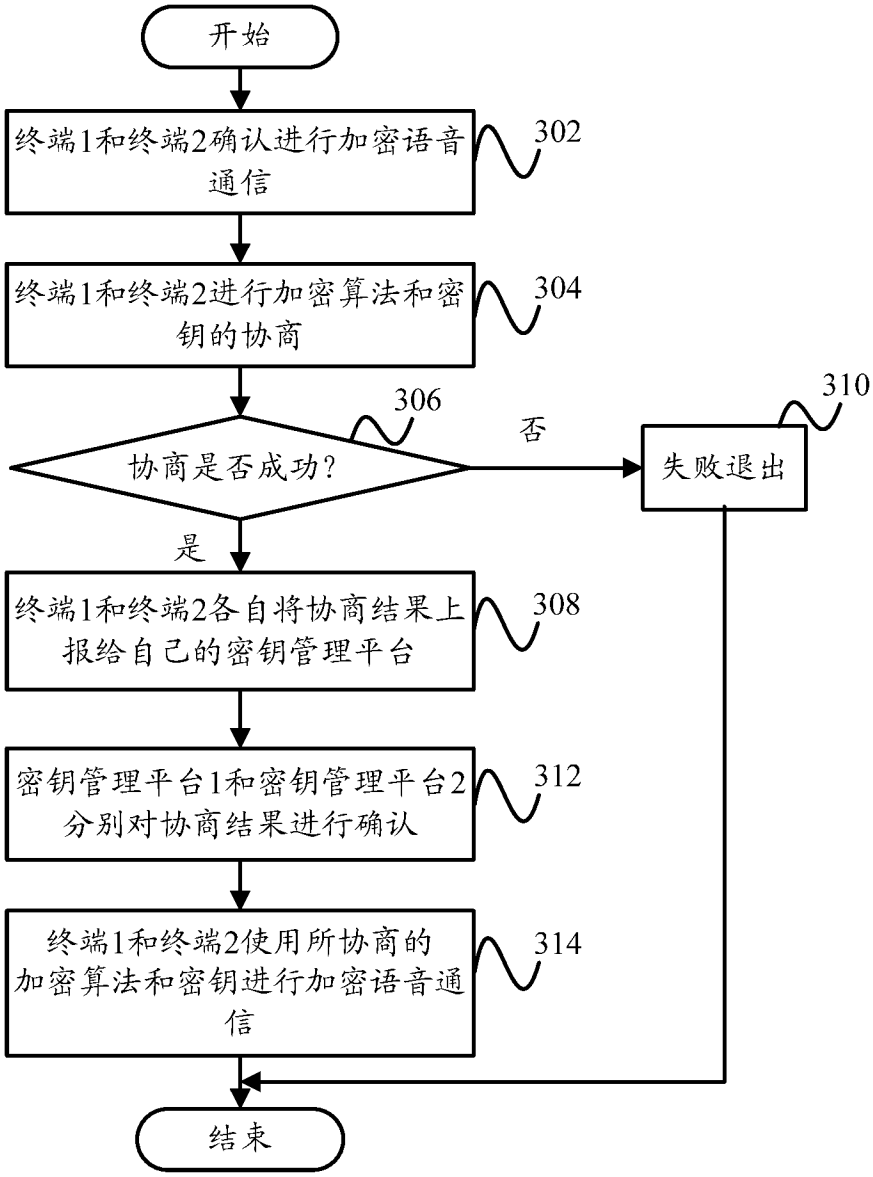

开始
终端1和终端2确认进行加密语音通信
302
终端1和终端2进行加密算法和密钥的协商
304
协商是否成功?
306
否
失败退出
310
是
终端1和终端2各自将协商结果上报给自己的密钥管理平台
308
密钥管理平台1和密钥管理平台2分别对协商结果进行确认
312
终端1和终端2使用所协商的加密算法和密钥进行加密语音通信
314
结束

图 3


第一确定单元402
语音通信单元408
发送单元404
第二确定单元410
判断单元406
第三确定单元412
语音加密装置400

图 4


语音加密装置400
终端500

图 5

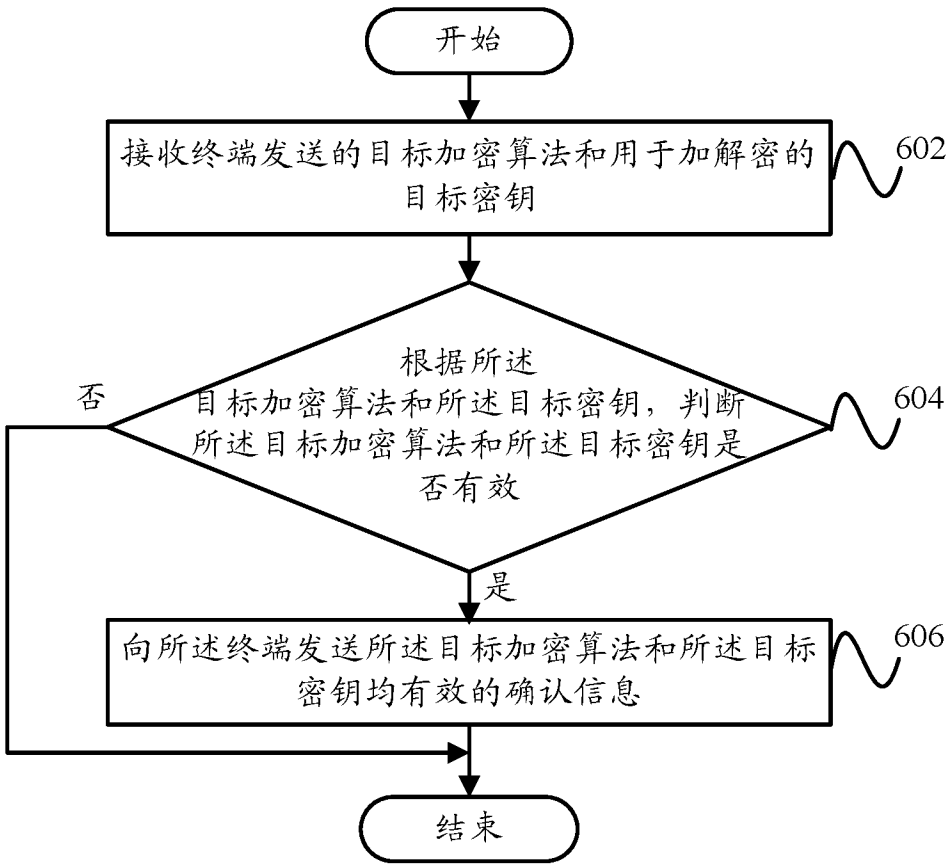

开始
接收终端发送的目标加密算法和用于加解密的目标密钥
602
根据所述目标加密算法和所述目标密钥，判断所述目标加密算法和所述目标密钥是否有效
604
否
是
向所述终端发送所述目标加密算法和所述目标密钥均有效的确认信息
606
结束

图 6

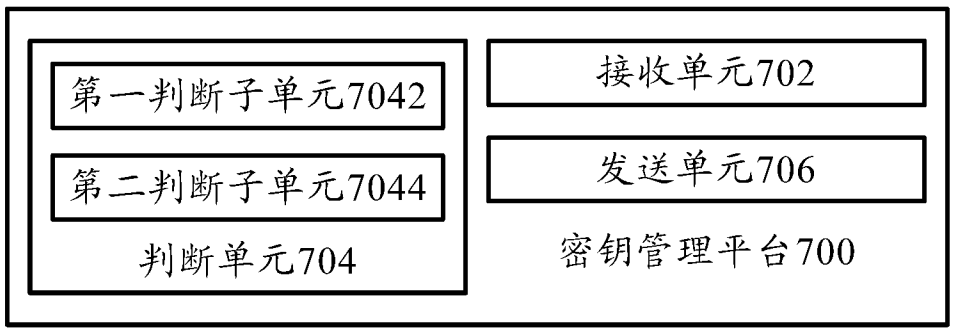

第一判断子单元7042
第二判断子单元7044
判断单元704
接收单元702
发送单元706
密钥管理平台700

图 7


终端500
密钥管理平台700
通信系统800

图 8

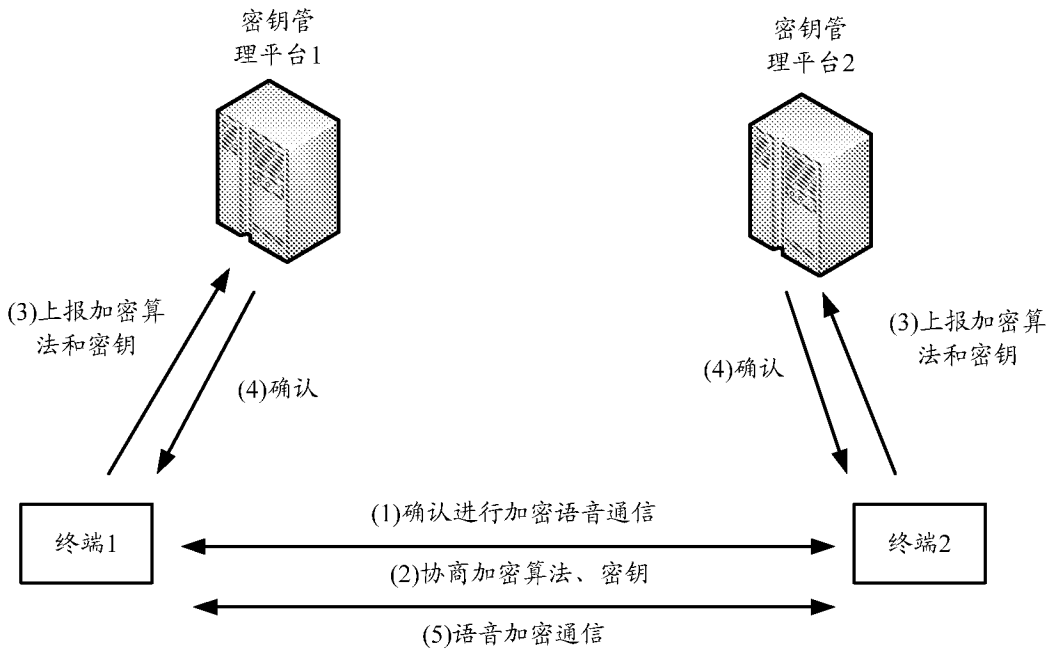

密钥管理平台1
密钥管理平台2
(3)上报加密算法和密钥
(4)确认
(4)确认
(3)上报加密算法和密钥
终端1
终端2
(1)确认进行加密语音通信
(2)协商加密算法、密钥
(5)语音加密通信

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/087543

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; 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)

CNPAT, EPODOC, WPI, CNKI:determine, voice, call, security, secure, encrypt+, key, negotiat+, agreement, platform, center, server, network, verif+, certificat+, affirm+, valid, effective, support+, algorithm, operator

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101931949 A (ZTE CORP.), 29 December 2010 (29.12.2010), the whole document	1-12
A	CN 102685746 A (ZTE CORP.), 19 September 2012 (19.09.2012), the whole document	1-12
A	CN 105282734 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 27 January 2016 (27.01.2016), the whole document	1-12
A	CN 101345965 A (CHINA TELECOM CORPORATION LIMITED), 14 January 2009 (14.01.2009), the whole document	1-12
A	US 2012331298 A1 (HUAWEI TECHNOLOGIES CO., LTD.), 27 December 2012 (27.12.2012), 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
03February 2017 (03.02.2017)	**16February 2017 (16.02.2017)**
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 **ZHANG, Yujie** Telephone No.:(86-10) **62413561**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/087543

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101931949 A	29 December 2010	WO 2012019443 A1	16 February 2012
		EP 2547132 A1	16 January 2013
		US 2013136261 A1	30 May 2013
CN 102685746 A	19 September 2012	WO 2013163846 A1	07 November 2013
		EP 2835999 A1	11 February 2015
		JP 2015517747 A	22 June 2015
		US 2015181421 A1	25 June 2015
CN 105282734 A	27 January 2016	None	
CN 101345965 A	14 January 2009	None	
US 2012331298 A1	27 December 2012	WO 2011110101 A1	15 September 2011
		CN 102196436 A	21 September 2011
		EP 2547050 A1	16 January 2013

国际检索报告

国际申请号
PCT/CN2016/087543

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; H04Q

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,EPODOC,WPI,CNKI:语音，通话，安全，加密，密钥，协商，平台，中心，服务器，网络，验证，确认，确定，有效，支持，算法，运营商，voice，call，security，secure，encrypt+，key，negotiat+，agreement，platform，center，server，network，verif+，certificat+，affirm+，valid，effective，support+，algorithm，operator

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	CN 101931949 A (中兴通讯股份有限公司) 2010年 12月 29日 (2010-12-29) 全文	1-12
A	CN 102685746 A (中兴通讯股份有限公司) 2012年 9月 19日 (2012-09-19) 全文	1-12
A	CN 105282734 A (中国移动通信集团公司) 2016年 1月 27日 (2016-01-27) 全文	1-12
A	CN 101345965 A (中国电信股份有限公司) 2009年 1月 14日 (2009-01-14) 全文	1-12
A	US 2012331298 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2012年 12月 27日 (2012-12-27) 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
2017年 2月 3日	2017年 2月 16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 张玉洁 电话号码 (86-10)62413561

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/087543

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	101931949	A	2010年 12月 29日	WO	2012019443	A1	2012年 2月 16日
				EP	2547132	A1	2013年 1月 16日
				US	2013136261	A1	2013年 5月 30日
CN	102685746	A	2012年 9月 19日	WO	2013163846	A1	2013年 11月 7日
				EP	2835999	A1	2015年 2月 11日
				JP	2015517747	A	2015年 6月 22日
				US	2015181421	A1	2015年 6月 25日
CN	105282734	A	2016年 1月 27日		无		
CN	101345965	A	2009年 1月 14日		无		
US	2012331298	A1	2012年 12月 27日	WO	2011110101	A1	2011年 9月 15日
				CN	102196436	A	2011年 9月 21日
				EP	2547050	A1	2013年 1月 16日