(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 12 月 27 日 (27.12.2012)

WIPO | PCT

(10) 国际公布号
WO 2012/174843 A1

(51) 国际专利分类号:
H04W 12/02 (2009.01)

(21) 国际申请号: PCT/CN2011/085193

(22) 国际申请日: 2011 年 12 月 31 日 (31.12.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201110169683.X 2011 年 6 月 22 日 (22.06.2011) 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): **田甜 (TIAN, Tian)** [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: **北京派特恩知识产权代理事务所(普通合伙) (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (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, 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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY,

[见续页]

(54) **Title**: KEY NEGOTIATION METHOD AND SYSTEM FOR ACHIEVING END-TO-END SECURITY

(54) **发明名称** : 一种实现端到端安全的密钥协商方法及系统

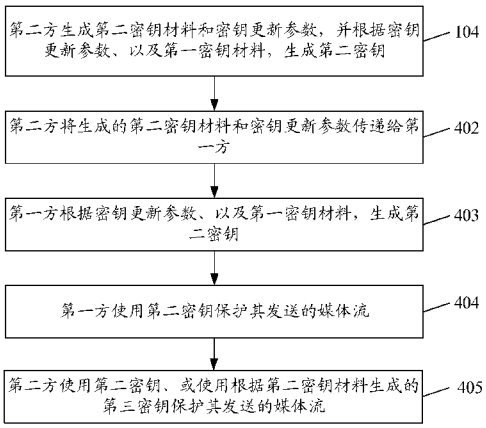

图 4 / Fig. 4

104 A SECOND PARTY GENERATES A SECOND KEY MATERIAL AND A KEY UPDATING PARAMETER, AND GENERATES A SECOND KEY ACCORDING TO THE KEY UPDATING PARAMETER AND A FIRST KEY MATERIAL
402 THE SECOND PARTY SENDS THE GENERATED SECOND KEY MATERIAL AND THE KEY UPDATING PARAMETER TO A FIRST PARTY
403 THE FIRST PARTY GENERATES THE SECOND KEY ACCORDING TO THE KEY UPDATING PARAMETER AND THE FIRST KEY MATERIAL
404 THE FIRST PARTY USES THE SECOND KEY TO PROTECT THE MEDIA STREAM TO BE SENT
405 THE SECOND PARTY USES THE SECOND KEY OR A THIRD KEY GENERATED ACCORDING TO THE SECOND KEY MATERIAL TO PROTECT THE MEDIA STREAM TO BE SENT

(57) **Abstract**: Disclosed are a key negotiation method and system for achieving end-to-end security. The method comprises: a second party generates a second key material and a key updating parameter, and generates a second key according to the key updating parameter and a first key material; the second party sends the generated second key material and the key updating parameter to a first party; the first party generates the second key according to the key updating parameter and the first key material; the first party uses the second key to protect the media stream to be sent; and the second party uses the second key or a third key generated according to the second key material to protect the media stream to be sent. The present invention ensures the end-to-end media stream security, thereby avoiding the risk of disclosure of a key or a session.

(57) **摘要**: 本发明公开了一种实现端到端安全的密钥协商方法和系统，方法包括：第二方生成第二密钥材料和密钥更新参数，并根据密钥更新参数、以及第一密钥材料，生成第二密钥；第二方将生成的第二密钥材料和密钥更新参数传递给第一方；第一方根据密钥更新参数、以及第一密钥材料，生成第二密钥；第一方使用第二密钥保护发送的媒体流；第二方使用第二密钥、或使用根据第二密钥材料导出的第三密钥保护发送的媒体流。通过本发明，能够保证端到端的媒体流安全，避免密钥泄露威胁和会话泄密威胁。

WO 2012/174843 A1

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, 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)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种实现端到端安全的密钥协商方法及系统

技术领域

本发明涉及网络通信安全技术，尤其涉及一种实现端到端安全的密钥协商方法及系统。

背景技术

现有的第三代合作伙伴计划（3GPP，Third Generation Partnership Projects）TS33.328 的 IP 多媒体子系统（IMS，IP Multimedia Subsystem）IMS 媒体面安全中使用 RFC4568 的会话描述协议（SDP，Session Description Protocol）的媒体流安全描述（SDES，SDP Security Descriptions for Media Streams）作为媒体面端到端安全方案。在 SDES 方案中，使用 SDP 协议中的加密属性来传送密钥协商材料，通过通话双方交互 SDP 数据包来导出媒体密钥，并且定义了如何在安全实时传输协议（SRTP，Secure Real-time Transport Protocol）中使用这些媒体密钥。

SDES 本质上不是一个密钥协商协议而是一个密钥分发协议，密钥是直接通过明文在网路上分发，所以 SDES 必须依赖于信令的安全。如图 1 所示，SDES 本质上是这样工作的：当主叫方 UE-A 和被叫方 UE-B 建立了一个 SIP 会话时，他们使用提出/应答（Offer/Response）模式交换提供给 SRTP 进行媒体流保护所需要的密钥及相关参数。

一个使用 SDES 建立端到端安全的呼叫流程如图 2 所示， UE-A 在发起 SIP 会话时，首先生成根密钥 K1，所述根密钥 K1 用来生成保护 UE-A 发给 UE-B 媒体流安全的媒体会话密钥，然后在通过 IMS 网络中间网元以及呼叫服务器发给 UE-B 的一个 SIP 消息中（即 INVITE 消息中）包含所述根密钥 K1，将根密钥 K1 发送给 UE-B; 而 UE-B 在返回给 UE-A 的响应 SIP

消息中（即 200 Ok 消息中）包含根密钥 K2，向 UE-A 返回根密钥 K2，根密钥 K2 用来生成保护 UE-B 发给 UE-A 媒体流安全的媒体会话密钥。

在会话发起协议（SIP，Session Initiation Protocol）系统中，分叉呼叫（forking）和呼叫转移（communication diversion）都是非常常见的实用型业务。现有分叉呼叫业务的场景如图 3 所示，分叉呼叫业务是指，被呼叫方的多个终端可以同时被呼叫，从而提高了呼叫接通的概率。需要注意的是，呼叫方可能并不知道其呼叫被分叉，且当一个终端已经进行了应答，其他终端则不能再对呼叫进行应答。这就要求呼叫方与被呼叫方的任一终端都有唯一的媒体密钥，并且除应答终端之外的所有终端都不能获悉已经在使用的会话密钥，以此来保证会话内容不会从其他终端被监听或泄露出去。呼叫转移业务是指，当呼叫过程中启用呼叫转移服务的被叫方处于不可达、或忙碌、或其他状态时，由被叫方的呼叫转移应用服务器将此呼叫转移到被叫方事先设置的被转呼方的用户设备上，从而提高呼叫的灵活性和可配置性。呼叫转移业务允许用户将其所有来话转接到预先设置的另一个电话号码上或用户的语音信箱中。呼叫转移还包含特殊的多次转移呼叫场景，即用户 A 呼叫用户 B，用户 B 使用呼叫转移业务，呼叫被转移给用户 C，用户 C 也使用了呼叫转移业务，该呼叫被再次转移给用户 D。

使用 SDES 方案保证端到端安全时，主叫方会在生成根密钥 K1 后，将根密钥 K1 包含在 INVITE 消息中通过 IMS 网络传到被叫方，当被叫方为 forking 场景时，K1 会被发给被叫方的所有终端；而当被叫方签约了呼叫转移服务时，呼叫转移业务被触发，呼叫转移应用服务器将该呼叫转移到被叫方所设置的被转呼方，将根密钥 K1 包含在 INVITE 消息中转到被转呼方；之后，被转呼方再将根密钥 K2 通过 IMS 网络传到主叫方，主叫方和被转呼方使用根密钥 K1、根密钥 K2 进行安全通信。

现有技术的缺陷在于：在上述分叉呼叫场景下，可能多个被叫终端都

获知了主叫方所使用的根密钥 K1，被叫终端也有能力解密主叫方所发送的加密媒体流，而用户设备的物理安全问题并不能保证使用者的合法性，使用一个合法设备的人可能是一个恶意攻击者，例如用户设备被偷盗后的使用者，这样，就会存在密钥泄露及单方会话泄密的威胁；而在一次会话多次呼叫转移的场景下，所有被转呼方的设备都有能力获知主叫方所使用的根密钥 K1，也就都有能力解密主叫方所发送的加密媒体流。这样，在分叉呼叫及呼叫转移场景下，会存在严重的安全会话泄密威胁，无法实现端到端安全。

发明内容

有鉴于此，本发明的主要目的在于提供一种实现端到端安全的密钥协商方法及系统，以解决现有端到端安全技术存在密钥泄露威胁和会话泄密威胁的问题。

为达到上述目的，本发明的技术方案是这样实现的：

本发明提供了一种实现端到端安全的密钥协商方法，该方法包括：

第二方生成第二密钥材料和密钥更新参数，并根据所述密钥更新参数、以及第一密钥材料，生成第二密钥；

第二方将生成的第二密钥材料和密钥更新参数传递给所述第一方；

所述第一方根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥；

所述第一方使用所述第二密钥保护发送的媒体流。

该方法进一步包括：

选择生成的第二密钥材料作为所述密钥更新参数，且当选择生成的第二密钥材料作为密钥更新参数时，所述第二方只将生成的第二密钥材料传递给所述第一方。

该方法进一步包括：

所述第二方将密钥生成函数发送给所述第一方，所述第一方和第二方使用所述密钥生成函数生成第二密钥。

该方法进一步包括:

所述第一方和第二方分别使用各自预先配置的相同的密钥生成函数，根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥。

该方法进一步包括:

所述第一密钥材料预先配置到所述第一方与所述第二方中，或者所述第一方生成第一密钥材料后传递给所述第二方。

该方法进一步包括:

所述第二方使用所述第二密钥、或使用根据所述第二密钥材料导出的第三密钥保护发送的媒体流。

本发明还提供了一种实现端到端安全的密钥协商系统，该系统包括:第一方和第二方，

所述第二方，用于生成第二密钥材料和密钥更新参数，并根据所述密钥更新参数、以及第一密钥材料，生成第二密钥；将生成的第二密钥材料和密钥更新参数传递给所述第一方；

所述第一方，用于根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥；使用所述第二密钥保护发送的媒体流。

所述第二方进一步用于，选择生成的第二密钥材料作为所述密钥更新参数，且当选择生成的第二密钥材料作为密钥更新参数时，所述第二方只将生成的第二密钥材料传递给所述第一方。

所述第二方进一步用于，将密钥生成函数发送给所述第一方，

相应的，所述第一方和第二方使用所述密钥生成函数生成第二密钥。

所述第一方和第二方分别使用各自预先配置的相同的密钥生成函数，

根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥。

所述第一密钥材料预先配置到所述第一方与所述第二方中，或者所述第一方生成第一密钥材料后传递给所述第二方。

所述第二方进一步用于，使用所述第二密钥、或使用根据所述第二密钥材料导出的第三密钥保护发送的媒体流。

通过本发明的实现端到端安全的密钥协商方法及系统，能够保证端到端的媒体流安全，避免密钥泄露威胁和会话泄密威胁。

附图说明

图 1 为现有技术中 SDES 的工作模型示意图;

图 2 为现有技术中基于 SDES 的端到端安全呼叫过程的流程图;

图 3 为现有技术中 IMS 分叉呼叫的场景示意图;

图 4 为本发明一种实现端到端安全的密钥协商的方法流程图;

图 5 为本发明实施例一的单次呼叫转移中实现端到端安全的方法流程图;

图 6 为本发明实施例二的多次呼叫转移中实现端到端安全的方法流程图;

图 7 为本发明实施例三的分叉呼叫中实现端到端安全的方法流程图。

具体实施方式

下面结合附图和具体实施例对本发明的技术方案进一步详细阐述。

本发明所提供的一种实现端到端安全的密钥协商的方法，如图 4 所示，主要包括:

步骤 401，第二方生成第二密钥材料和密钥更新参数，并根据密钥更新参数、以及第一密钥材料，生成第二密钥。

其中，第一密钥材料可以在第二方预先配置，也可以由第一方生成

后传递给第二方。无论采用哪种方式，需要保证第一方和第二方所使用的第一密钥材料相同。

在实际应用中，可以直接选择生成的第二密钥材料作为密钥更新参数，且当选择生成的第二密钥材料作为密钥更新参数时，第二方只将生成的第二密钥材料传递给第一方即可。当然，也可以选择一随机数作为密钥更新参数、或者选择第二密钥材料和随机数的组合作为密钥更新参数。无论采用哪种方式，需要保证第一方和第二方所使用的密钥更新参数相同。

步骤 402，第二方将生成的第二密钥材料和密钥更新参数传递给第一方。

需要说明的是，如果第二方没有预先配置密钥生成函数，那么第一方还需要将密钥生成函数传递给第二方；如果第二方预先配置有密钥生成函数，那么第一方可以不向第二方发送密钥生成函数。优选的，为了避免第二方没有配置密钥生成函数、或第二方与第一方配置的密钥生成函数不匹配的情况发生，第一方可以始终将密钥生成函数与第二密钥材料和密钥更新参数一起传递给第二方。无论采用哪种方式，需要保证第一方和第二方所使用的密钥生成函数相同。

步骤 403，第一方根据密钥更新参数、以及第一密钥材料，生成第二密钥。

如果是第二方将密钥生成函数发送给第一方，那么第一方和第二方使用所述密钥生成函数生成第二密钥；

如果是在第一方和第二方分别预先配置相同的密钥生成函数，那么第一方和第二方分别使用各自预先配置的相同的密钥生成函数，根据密钥更新参数、以及所述第一密钥材料，生成第二密钥。

步骤 404，第一方使用第二密钥保护其发送的媒体流。

较佳的，本发明还可以进一步包括步骤405，即第二方使用第二密钥保护其发送的媒体流；或者，根据第二密钥材料导出第三密钥，并使用所述第三密钥保护其发送的媒体流。

对应上述实现端到端安全的密钥协商方法，本发明还提供了一种实现端到端安全的密钥协商系统，包括：第一方和第二方。其中，第二方，用于生成第二密钥材料和密钥更新参数，并根据密钥更新参数、以及第一密钥材料，生成第二密钥；将生成的第二密钥材料和密钥更新参数传递给第一方。第一方，用于根据密钥更新参数、以及第一密钥材料，生成第二密钥；使用第二密钥保护发送的媒体流。

较佳的，第二方可进一步用于，选择生成的第二密钥材料作为密钥更新参数，且当选择生成的第二密钥材料作为密钥更新参数时，第二方只将生成的第二密钥材料传递给第一方。

较佳的，第二方还可进一步用于，将密钥生成函数发送给第一方，

相应的，第一方和第二方使用所述密钥生成函数生成第二密钥。

较佳的，第一方和第二方分别使用各自预先配置的相同的密钥生成函数，根据密钥更新参数、以及第一密钥材料，生成所第二密钥。

第二方还进一步用于，使用第二密钥、或使用根据第二密钥材料导出的第三密钥保护发送的媒体流。

当上述密钥协商方法和系统应用于呼叫转移场景时，端到端安全通信的主叫方可以作为第一方，执行第一方的功能操作；被叫方或被转呼方可以作为第二方，执行第二方的功能操作。

当上述密钥协商方法和系统应用于分叉呼叫场景时，端到端安全通信的主叫方可以作为第一方，执行第一方的功能操作；被叫方或被分叉方可以作为第二方，执行第二方的功能操作。

较佳的，本发明的密钥协商系统还可以包括应用服务器，如分叉呼叫

服务器、呼叫转移应用服务器等。当应用服务器作为第二方所属的呼叫服务器时，用于在收到第一方的呼叫后向第二方发送呼叫请求消息。

下面结合具体实施例对上述端到端安全的密钥协商方法和系统进一步详细说明。以下实施例分别列举呼叫转移场景和分叉呼叫场景下的端到端安全实现，其中实施例一和实施例二针对呼叫转移场景，实施例三针对分叉呼叫场景。

呼叫转移场景下被叫方将被转呼方设定为呼叫转移目标，触发被叫方签约的呼叫转移业务的情况，可以是以下情况之一：遇忙呼叫转移（CFB，Communication Forwarding Busy）、无应答呼叫转移（CFNR，Communication Forwarding No Reply）、无条件呼叫转移（CFU，Communication Forwarding Unconditional）、寻呼不可及转移（CFNRc，Communication Forwarding on Subscriber Not Reachable）、未注册时呼叫转移（CFNL，Communication Forwarding on Not Logged in）和会话转移（CD，Communication Deflection）业务。

图 5 所示为本发明实施例一的单次呼叫转移中实现端到端安全呼叫转移的方法，即用户 A 想呼叫用户 B，用户 B 签约了呼叫转移业务，预设用户 C 为呼叫转移对象，在呼叫建立过程中，用户 B 签约的呼叫转移业务被触发。在本实施例中，UE-A 作为第一方，UE-C 作为第二方，实现端到端安全呼叫转移具体包括以下步骤：

步骤 501，UE-A 生成主叫密钥 K1（作为第一密钥材料）。

步骤 502，UE-A 向 IMS 网络发送对 UE-B 的呼叫请求（INVITE）消息，且此呼叫请求消息中携带主叫密钥 K1。

步骤 503，IMS 网络将收到的 INVITE 消息转发到 UE-B 所属的呼叫转移应用服务器。

步骤 504，呼叫转移应用服务器将 INVITE 消息发送到 UE-B。该步骤

为可选的，例如：当用户 B 签约的为无条件呼叫转移时，步骤 504 省略。

步骤 505，UE-B 签约的呼叫转移业务被触发。

步骤 506，呼叫转移应用服务器将包含主叫密钥 K1 的 INVITE 消息通过 IMS 网络转发给用户 B 设定的呼叫转移号码，在本实施例中即 UE-C。

步骤 507，UE-C 收到 INVITE 消息后，获知此为一个呼叫转移，并由消息中包含的主叫密钥 K1 获知该呼叫是一个 SDES 端到端安全的安全呼叫；UE-C 生成被叫密钥 K2（作为第二密钥材料）和密钥更新参数 P1，且 UE-C 基于 P1 和收到的 K1 生成新的主叫密钥 K1′=KDF（K1，P1），其中 KDF 为密钥生成函数（Key Derivation Function），K1′作为第二密钥。

步骤 508，UE-C 将被叫密钥 K2 和密钥更新参数 P1，以及 KDF 包含在 200 OK 消息（或其他含有 SDP Answer 的 SIP 消息）中通过 IMS 网络返回给呼叫转移应用服务器。其中，如果 P1 选择为 K2，则消息中只包含 K2 和 KDF。

步骤 509~510，呼叫转移应用服务器将 200 OK 消息通过 IMS 网络返回给 UE-A。

步骤 511，UE-A 在收到该消息后基于主叫密钥 K1 和收到的密钥更新参数 P1，使用 KDF 生成新的主叫密钥 K1′=KDF（K1，P1）。

步骤 512，UE-A 和 UE-C 建立起端到端安全的加密媒体流通信，UE-A 使用 K1′保护从 UE-A 发给 UE-C 的媒体流，UE-C 可以使用 K1′对 UE-A 发送的媒体流进行解密；UE-C 使用 K2（即直接将第二密钥材料作为第三密钥导出）保护从 UE-C 发给 UE-A 的媒体流，UE-A 可以使用 K2 对 UE-C 发送的媒体流进行解密。

UE-A 和 UE-C 也可以均使用 K1′保护其之间交互的媒体流，UE-C 可以使用 K1′对 UE-A 发送的媒体流进行解密，UE-A 可以使用 K1′对 UE-C 发送的媒体流进行解密。

图 6 所示为本发明实施例二的多次呼叫转移中实现端到端安全呼叫转移的方法，即用户 B 签约呼叫转移业务，预设将通话转移到用户 C，用户 C 也签约了呼叫转移业务，预设将通话转移到用户 D，且在 UE-A 呼叫 UE-B 的会话中，UE-B 和 UE-C 均触发签约的呼叫转移业务，最终会话被转移到 UE-D。在本实施例中，UE-A 作为第一方，UE-D 作为第二方，实现端到端安全呼叫转移具体包括以下步骤:

步骤 601~606 的操作与步骤 501~506 的操作相同。其中，步骤 606 也为可选，这与用户签约的呼叫转移业务相关，如果是无条件呼叫转移业务，则步骤 606 省略。

步骤 607，UE-C 的呼叫转移业务被触发。

步骤 608，呼叫转移应用服务器将包含主叫密钥 K1 的 INVITE 消息通过 IMS 网络转发给用户 C 设定的呼叫转移号码，在本实施例中即 UE-D。

步骤 609，UE-D 收到 INVITE 消息后，由消息中包含的主叫密钥 K1（作为第一密钥材料）获知该呼叫是一个 SDES 端到端安全的安全呼叫；UE-D 生成被叫密钥 K2（作为第二密钥材料）和密钥更新参数 P1，且 UE-D 基于 P1 和收到的 K1 生成新的主叫密钥 K1′=KDF（K1，P1），K1′作为第二密钥。

步骤 610，UE-D 将被叫密钥 K2 和密钥更新参数 P1，以及 KDF 包含在 200 OK 消息（或其他含有 SDP Answer 的 SIP 消息）中通过 IMS 网络返回给呼叫转移应用服务器。其中，如果 P1 选择为 K2，则消息中只包含 K2 和 KDF。

步骤 611~612，呼叫转移应用服务器将 200 OK 消息通过 IMS 网络返回给 UE-A。

步骤 613，UE-A 在收到该消息后基于主叫密钥 K1 和收到的密钥更新参数 P1，使用 KDF 生成新的主叫密钥 K1′=KDF（K1，P1）。

步骤 614，UE-A 和 UE-D 建立起端到端安全的加密媒体流通信，UE-A 使用 K1′保护从 UE-A 发给 UE-D 的媒体流，UE-D 可以使用 K1′对 UE-A 发送的媒体流进行解密；UE-D 使用 K2（即直接将第二密钥材料作为第三密钥导出）保护从 UE-D 发给 UE-A 的媒体流，UE-A 可以使用 K2 对 UE-D 发送的媒体流进行解密。

UE-A 和 UE-D 也可以均使用 K1′保护其之间交互的媒体流，UE-D 可以使用 K1′对 UE-A 发送的媒体流进行解密，UE-A 可以使用 K1′对 UE-D 发送的媒体流进行解密。

图 7 所示为本发明实施例三的端到端安全的分叉呼叫，即用户 B 签约了分叉呼叫业务，当用户 A 呼叫用户 B 时，用户 B 所拥有的 UE-B1、UE-B2 终端将同时被呼叫，假设该实施例中 UE-B2 终端最终应答。在本实施例中，UE-A 作为第一方，UE-B1、UE-B2 作为第二方，实现端到端安全呼叫转移具体包括以下步骤:

步骤 701，UE-A 生成主叫密钥 K1（作为第一密钥材料）。

步骤 702，UE-A 向 IMS 网络发送对 UE-B 的呼叫请求（INVITE）消息，且此呼叫请求消息中携带主叫密钥 K1。

步骤 703，IMS 网络将收到的 INVITE 消息转发到 UE-B 所属的分叉呼叫应用服务器。

步骤 704，分叉呼叫应用服务器将 INVITE 消息发送到 UE-B1、UE-B2，即在步骤 705a 和 705b 步骤中，分叉呼叫应用服务器发送包含 K1 的 SDP Offer 的 SIP 消息给 UE-B1、UE-B2。

步骤 706a，UE-B1 收到 INVITE 消息后，由消息中包含的主叫密钥 K1 获知该呼叫是一个 SDES 端到端安全的安全呼叫；UE-B1 生成被叫密钥 K2（作为第二密钥材料）和密钥更新参数 P1，且 UE-B1 基于 P1 和收到的 K1 生成新的主叫密钥 K_{a1}=KDF（K1，P1），其中 KDF 为密钥生成函数（Key

Derivation Function），K_{a1}作为 UE-B1 与 UE-A 之间的第二密钥。

步骤 707a，UE-B1 将被叫密钥 K2 和密钥更新参数 P1，以及 KDF 包含在 SDP Answer 消息中通过 IMS 网络返回给呼叫转移应用服务器。其中，如果 P1 选择为 K2，则消息中只包含 K2 和 KDF。

步骤 708a~709a，分叉呼叫应用服务器将该消息通过 IMS 网络返回给 UE-A。

步骤 710a，UE-A 在收到该消息后基于主叫密钥 K1 和收到的密钥更新参数 P1，使用 KDF 生成新的主叫密钥 K_{a1}=KDF（K1，P1）。

步骤 706b-709b，UE-B2 生成 K3（作为第二密钥材料）和 P2，使用 KDF 生成 K_{a2}=KDF（K1，P2），K_{a2}作为 UE-B2 与 UE-A 之间的第二密钥；其他过程与 706a-709a 步骤相同，不再累述。

步骤 710b，UE-A 基于主叫密钥 K1 和收到的密钥更新参数 P2，使用 KDF 生成新的主叫密钥 K_{a2}=KDF（K1，P2）。

步骤 711-713，UE-B2 应答，通过网络向 UE-A 发送 200 Ok 消息。

步骤 714，UE-A 和 UE-B2 建立起端到端安全的加密媒体流通信，UE-A 使用 K_{a2}保护从 UE-A 发给 UE-B2 的媒体流，UE-B2 可以使用 K_{a2}对 UE-A 发送的媒体流进行解密；UE-B2 使用 K3（即直接将第二密钥材料作为第三密钥导出）保护从 UE-B2 发给 UE-A 的媒体流，UE-A 可以使用 K3 对 UE-B2 发送的媒体流进行解密。

UE-A 和 UE-B2 也可以均使用 K_{a2}保护其之间交互的媒体流，UE-B2 可以使用 K_{a2}对 UE-A 发送的媒体流进行解密，UE-A 可以使用 K_{a2}对 UE-B2 发送的媒体流进行解密。

以上所述，仅为本发明的较佳实施例，并非用于限定本发明的保护范围。

权利要求书

1、一种实现端到端安全的密钥协商方法，其特征在于，该方法包括:

第二方生成第二密钥材料和密钥更新参数，并根据所述密钥更新参数、以及第一密钥材料，生成第二密钥;

第二方将生成的第二密钥材料和密钥更新参数传递给所述第一方;

所述第一方根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥;

所述第一方使用所述第二密钥保护发送的媒体流。

2、根据权利要求 1 所述实现端到端安全的密钥协商方法，其特征在于，该方法进一步包括:

选择生成的第二密钥材料作为所述密钥更新参数，且当选择生成的第二密钥材料作为密钥更新参数时，所述第二方只将生成的第二密钥材料传递给所述第一方。

3、根据权利要求 1 所述实现端到端安全的密钥协商方法，其特征在于，该方法进一步包括:

所述第二方将密钥生成函数发送给所述第一方，所述第一方和第二方使用所述密钥生成函数生成第二密钥。

4、根据权利要求 1 所述实现端到端安全的密钥协商方法，其特征在于，该方法进一步包括:

所述第一方和第二方分别使用各自预先配置的相同的密钥生成函数，根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥。

5、根据权利要求 1 所述实现端到端安全的密钥协商方法，其特征在于，该方法进一步包括:

所述第一密钥材料预先配置到所述第一方与所述第二方中，或者所

述第一方生成第一密钥材料后传递给所述第二方。

6、根据权利要求 1 至 5 任一项所述实现端到端安全的密钥协商方法，其特征在于，该方法进一步包括:

所述第二方使用所述第二密钥、或使用根据所述第二密钥材料导出的第三密钥保护发送的媒体流。

7、一种实现端到端安全的密钥协商系统，其特征在于，该系统包括:第一方和第二方，

所述第二方，用于生成第二密钥材料和密钥更新参数，并根据所述密钥更新参数、以及第一密钥材料，生成第二密钥；将生成的第二密钥材料和密钥更新参数传递给所述第一方;

所述第一方，用于根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥；使用所述第二密钥保护发送的媒体流。

8、根据权利要求 7 所述实现端到端安全的密钥协商系统，其特征在于，所述第二方进一步用于，选择生成的第二密钥材料作为所述密钥更新参数，且当选择生成的第二密钥材料作为密钥更新参数时，所述第二方只将生成的第二密钥材料传递给所述第一方。

9、根据权利要求 7 所述实现端到端安全的密钥协商系统，其特征在于，所述第二方进一步用于，将密钥生成函数发送给所述第一方，

相应的，所述第一方和第二方使用所述密钥生成函数生成第二密钥。

10、根据权利要求 7 所述实现端到端安全的密钥协商系统，其特征在于，所述第一方和第二方分别使用各自预先配置的相同的密钥生成函数，根据所述密钥更新参数、以及所述第一密钥材料，生成所述第二密钥。

11、根据权利要求 7 所述实现端到端安全的密钥协商系统，其特征在于，所述第一密钥材料预先配置到所述第一方与所述第二方中，或者

所述第一方生成第一密钥材料后传递给所述第二方。

12、根据权利要求 7 至 11 任一项所述实现端到端安全的密钥协商系统，其特征在于，所述第二方进一步用于，使用所述第二密钥、或使用根据所述第二密钥材料导出的第三密钥保护发送的媒体流。

5


UE-A
提出
UE-B
应答

图 1

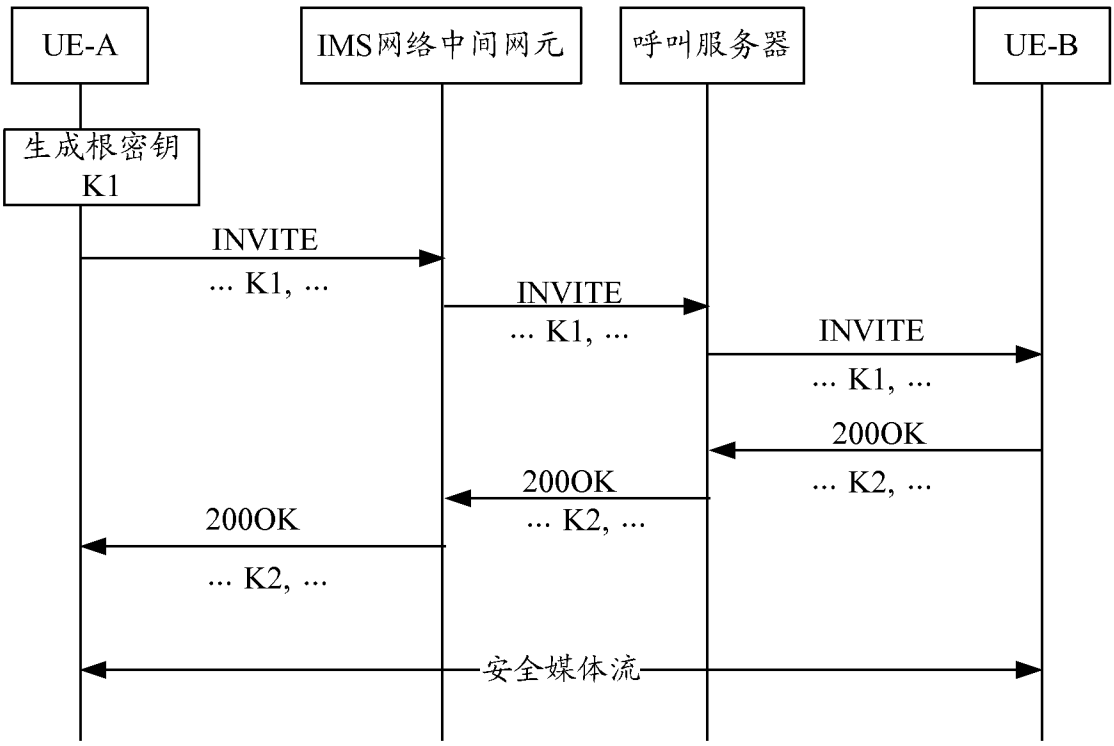
UE-A
IMS网络中间网元
呼叫服务器
UE-B
生成根密钥
K1
INVITE
... K1, ...
INVITE
... K1, ...
INVITE
... K1, ...
200OK
... K2, ...
200OK
... K2, ...
200OK
... K2, ...
安全媒体流

图 2

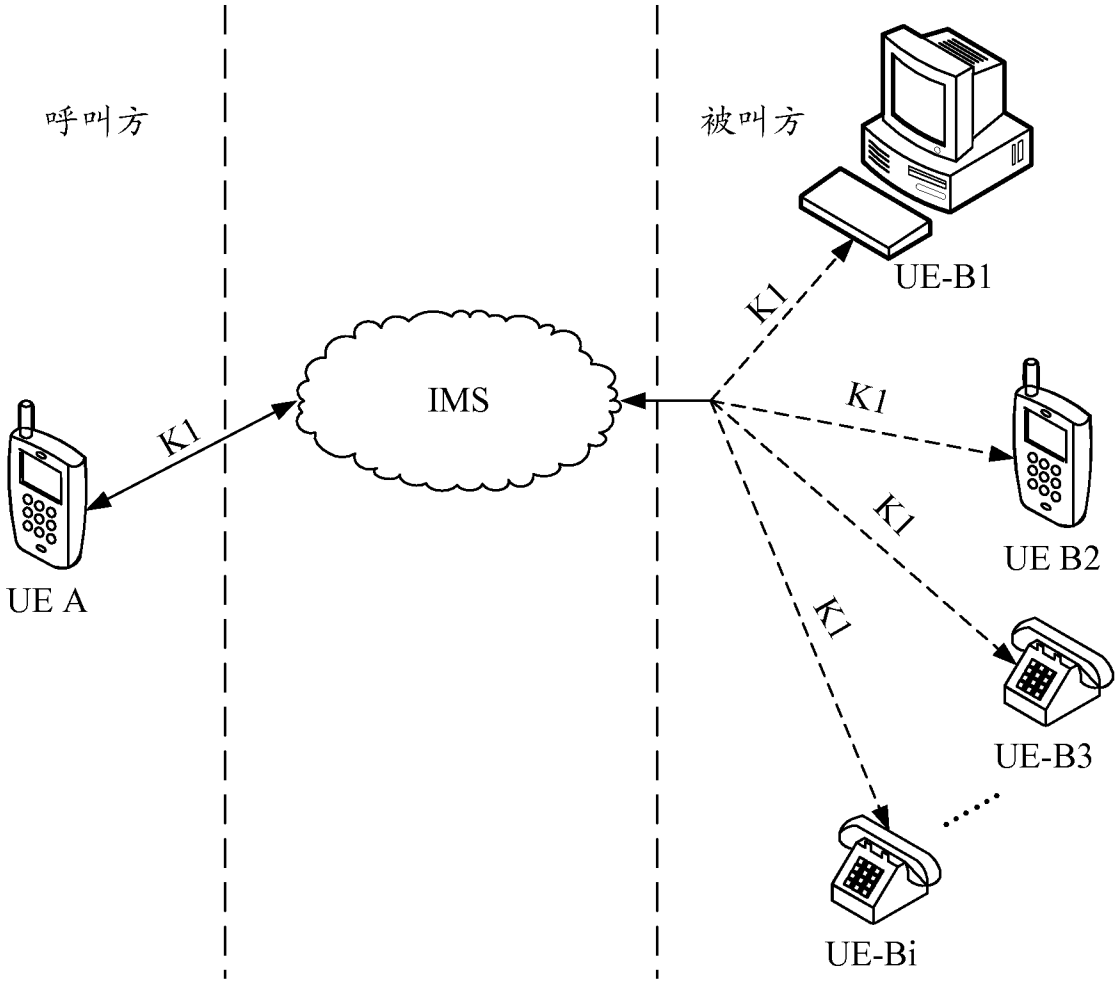

图 3

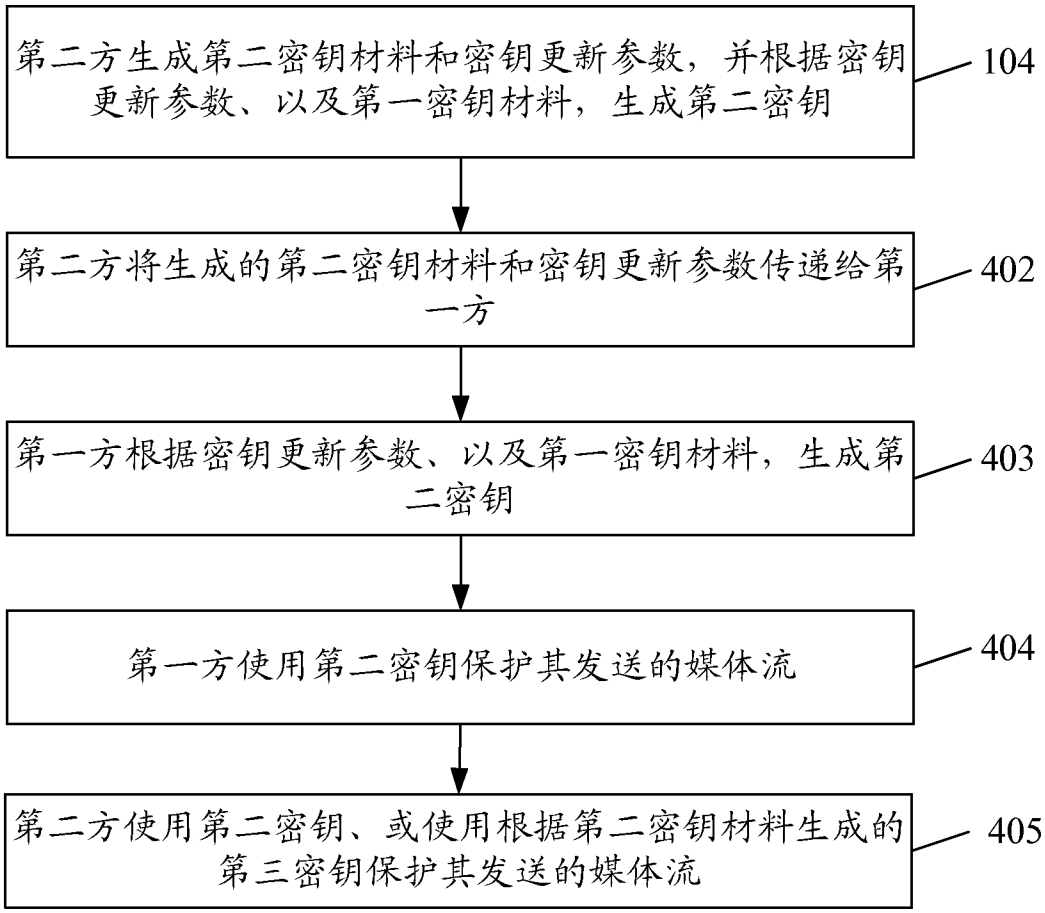
第二方生成第二密钥材料和密钥更新参数，并根据密钥更新参数、以及第一密钥材料，生成第二密钥
104
第二方将生成的第二密钥材料和密钥更新参数传递给第一方
402
第一方根据密钥更新参数、以及第一密钥材料，生成第二密钥
403
第一方使用第二密钥保护其发送的媒体流
404
第二方使用第二密钥、或使用根据第二密钥材料生成的第三密钥保护其发送的媒体流
405

图 4

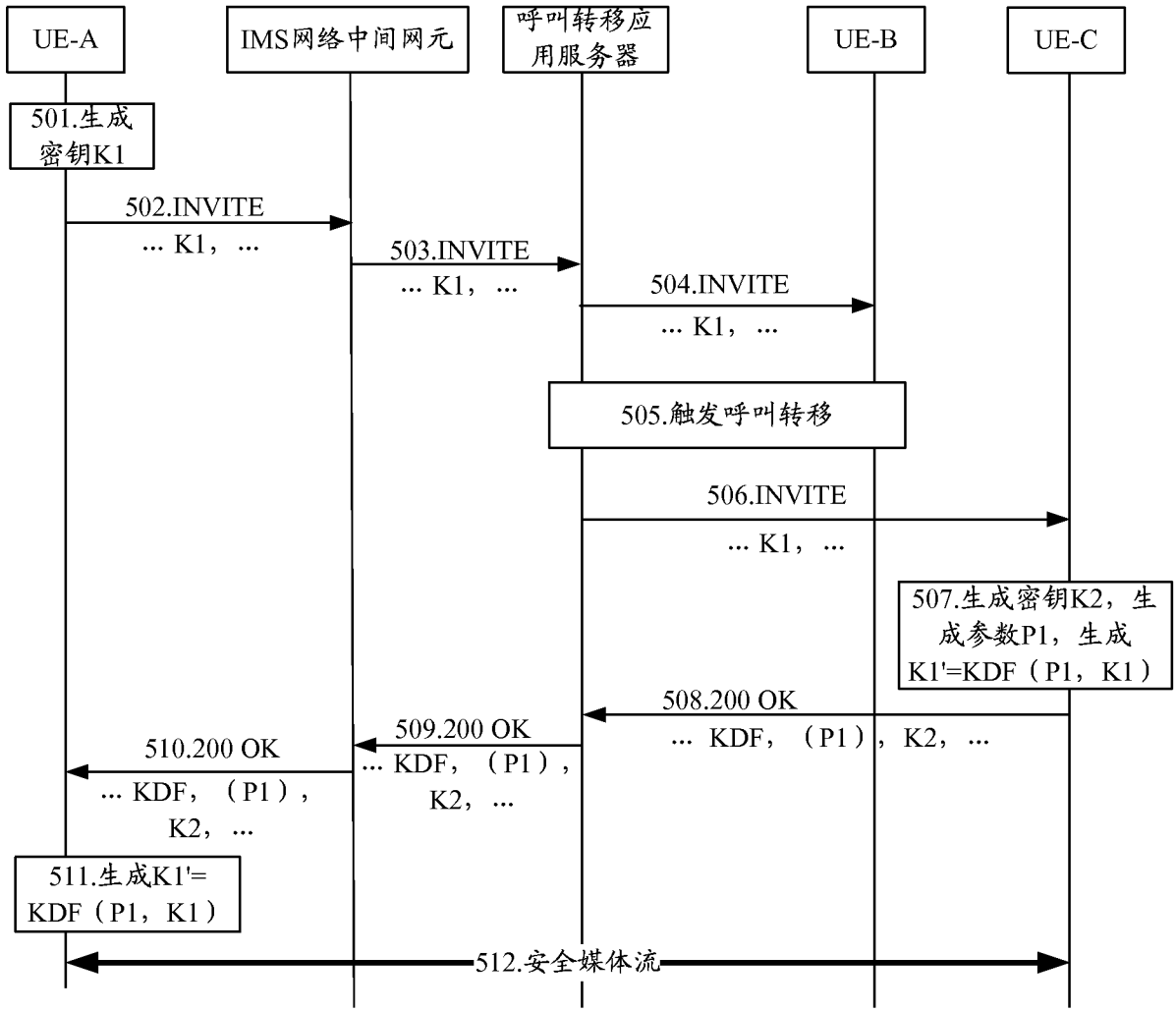
UE-A
IMS网络中间网元
呼叫转移应用服务器
UE-B
UE-C
501.生成密钥K1
502.INVITE
… K1，…
503.INVITE
… K1，…
504.INVITE
… K1，…
505.触发呼叫转移
506.INVITE
… K1，…
507.生成密钥K2，生成参数P1，生成K1'=KDF（P1，K1）
508.200 OK
… KDF，（P1），K2，…
509.200 OK
… KDF，（P1），K2，…
510.200 OK
… KDF，（P1），K2，…
511.生成K1'=KDF（P1，K1）
512.安全媒体流

图 5

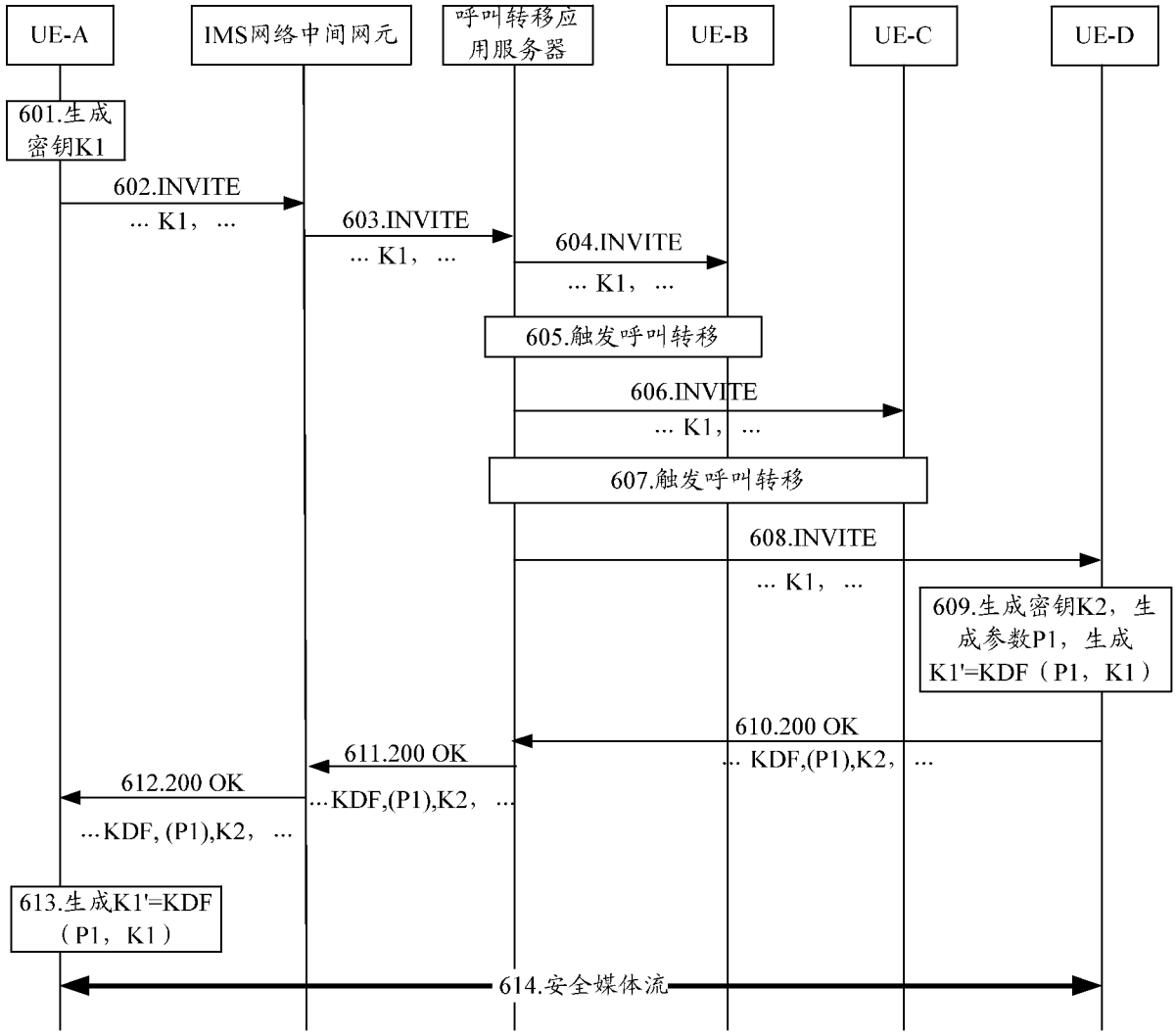
UE-A
IMS网络中间网元
呼叫转移应用服务器
UE-B
UE-C
UE-D
601.生成密钥K1
602.INVITE
... K1，...
603.INVITE
... K1，...
604.INVITE
... K1，...
605.触发呼叫转移
606.INVITE
... K1，...
607.触发呼叫转移
608.INVITE
... K1，...
609.生成密钥K2，生成参数P1，生成K1'=KDF（P1，K1）
610.200 OK
... KDF,(P1),K2，...
611.200 OK
...KDF,(P1),K2，...
612.200 OK
...KDF, (P1),K2，...
613.生成K1'=KDF（P1，K1）
614.安全媒体流

图 6

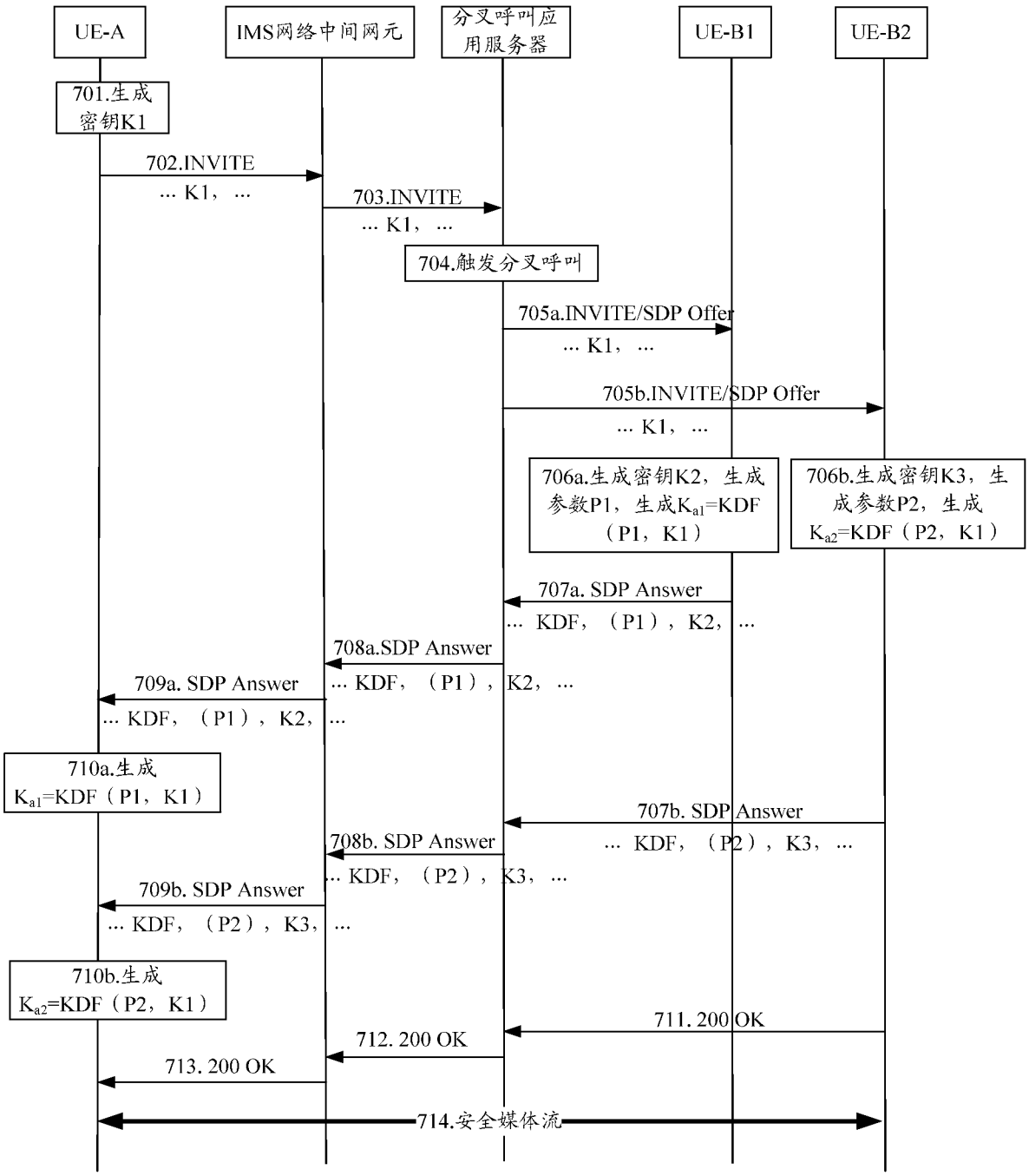
UE-A
IMS网络中间网元
分叉呼叫应用服务器
UE-B1
UE-B2
701.生成密钥K1
702.INVITE
... K1, ...
703.INVITE
... K1, ...
704.触发分叉呼叫
705a.INVITE/SDP Offer
... K1, ...
705b.INVITE/SDP Offer
... K1, ...
706a.生成密钥K2，生成参数P1，生成Ka1=KDF（P1，K1）
706b.生成密钥K3，生成参数P2，生成Ka2=KDF（P2，K1）
707a. SDP Answer
... KDF, （P1）, K2, ...
708a.SDP Answer
... KDF, （P1）, K2, ...
709a. SDP Answer
... KDF, （P1）, K2, ...
710a.生成Ka1=KDF（P1，K1）
707b. SDP Answer
... KDF, （P2）, K3, ...
708b. SDP Answer
... KDF, （P2）, K3, ...
709b. SDP Answer
... KDF, （P2）, K3, ...
710b.生成Ka2=KDF（P2，K1）
711. 200 OK
712. 200 OK
713. 200 OK
714.安全媒体流

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/085193

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/02 (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: H04L, H04Q, H04W, C06F

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, CNKI, CNPAT, IEEE, GOOGLE: cipherkey, key, first, second, parameter, negotiation, agreement, update, end to end, encrypt, SDES, SRTP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101895877 A (HUAWEI TECHNOLOGIES CO., LTD.), 24 November 2010 (24.11.2010), description, paragraphs [0023]-[0038] and [0056]-[0080], and figures 1-2 and 5	1-12
A	CN 101183935 A (HUAWEI TECHNOLOGIES CO., LTD.), 21 May 2008 (21.05.2008), the whole document	1-12
A	WO 2006/106393 A2 (NOKIA CORPORATION), 12 October 2006 (12.10.2006), the whole document	1-12
A	ALCATEL LUCENT et al., 3GPP TSG SA WG3 Security-S3#58 S3-100276: Corrections and clarifications in call set-up, 01-05 February 2010 (01-05.02.2010), pages 4-6, section 7.2.2	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
13 February 2012 (13.02.2012)	**08 March 2012 (08.03.2012)**
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 **HU, Yan** Telephone No.: (86-10) **62413334**

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2011/085193

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101895877 A	24.11.2010	None	
CN 101183935 A	21.05.2008	None	
WO 2006/106393 A2	12.10.2006	US 2006251256 A1	09.11.2006
		EP 1875659 A2	09.01.2008
		INCHENP 200704535 E	25.01.2008
		KR 20070116151 A	06.12.2007
		CN 101167305 A	23.04.2008
		JP 2008537381 A	11.09.2008
		ZA 200708722 A	26.11.2008
		KR 100996872 B1	26.11.2010

国际检索报告

国际申请号
PCT/CN2011/085193

A. 主题的分类

H04W 12/02(2009.01)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)

IPC: H04L, H04Q, H04W, G06F

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, CNKI, CNPAT, IEEE, GOOGLE: 密钥，第一，第二，参数，协商，更新，端到端，加密；cipherkey, key, first, second, parameter, negotiation, agreement, update, end to end, encrypt, SDES, SRTP

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
X	CN 101895877 A (华为技术有限公司) 24.11 月 2010 (24.11.2010) 说明书第[0023]-[0038],[0056]-[0080]段，图 1-2,5	1-12
A	CN 101183935 A (华为技术有限公司) 21.5 月 2008 (21.05.2008) 全文	1-12
A	WO 2006/106393 A2（NOKIA CORPORATION）12.10 月 2006（12.10.2006）全文	1-12
A	ALCATEL LUCENT 等, 3GPP TSG SA WG3 Security - S3#58 S3-100276: Corrections and clarifications in call set-up, 01-05.2 月 2010(01-05.02.2010), 第 4-6 页第 7.2.2 节	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
13.2 月 2012(13.02.2012)	**08.3 月 2012 (08.03.2012)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 **胡延** 电话号码：(86-10) 62413334

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/085193

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 101895877 A	24.11.2010	无	
CN 101183935 A	21.05.2008	无	
WO 2006/106393 A2	12.10.2006	US 2006251256 A1	09.11.2006
		EP 1875659 A2	09.01.2008
		INCHENP 200704535 E	25.01.2008
		KR 20070116151 A	06.12.2007
		CN 101167305 A	23.04.2008
		JP 2008537381 A	11.09.2008
		ZA 200708722 A	26.11.2008
		KR 100996872 B1	26.11.2010