(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102883325 B
(45)授权公告日 2015.09.30

(21)申请号 201210421349.3

(22)申请日 2012.10.29

(73)专利权人 东莞宇龙通信科技有限公司
地址 523500 广东省东莞市松山湖科技产业园区北部工业城C区
专利权人 宇龙计算机通信科技(深圳)有限公司

(72)发明人 钟焰涛

(74)专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343
代理人 尚志峰 汪海屏

(51)Int.Cl.
H04W 12/06(2009.01)
H04W 12/02(2009.01)
H04W 88/02(2009.01)

(56)对比文件
CN 101183938 A,2008.05.21,
CN 101183938 A,2008.05.21,
CN 101527905 A,2009.09.09,
WO 2010/031600 A1,2010.03.25,

审查员 刘露玲

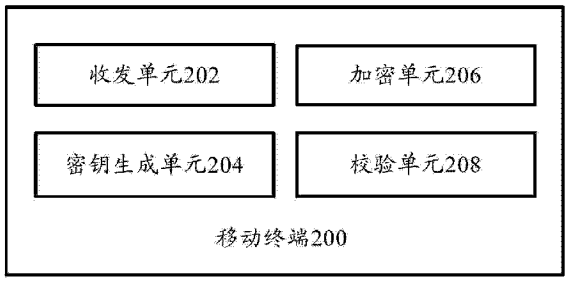
权利要求书2页 说明书7页 附图3页

(54)发明名称

验证服务器、移动终端和端到端认证通信信道建立方法

(57)摘要

本发明提供了一种验证服务器,位于核心网,包括:验证单元,在主叫方呼叫被叫方时,验证主叫方的身份并生成第一消息验证码以及验证被叫方的身份并生成第二消息验证码;公共参数确定单元,根据第一消息验证码和第二消息验证码确定公共参数,并将公共参数分配给主叫方和所述呼叫方。相应地,本发明还提供了一种移动终端和一种端到端认证通信信道建立方法。根据本发明的技术方案,能够实现手机终端之间的端到端加密通信,加密密钥仅由参与通信的两个手机终端掌握,有效提高加密密钥的安全性。



CN 102883325 B

1. 一种验证服务器，其特征在于，位于核心网，包括：

验证单元，在主叫方呼叫被叫方时，验证所述主叫方的身份并生成第一消息验证码以及验证所述被叫方的身份并生成第二消息验证码；

公共参数确定单元，根据所述第一消息验证码和所述第二消息验证码确定公共参数，并将所述公共参数分配给所述主叫方和所述被叫方；

所述公共参数确定单元按照以下公式确定所述公共参数：

$g = h(MAC_a, MAC_b)$，其中，g 表示所述公共参数，h 表示哈希函数，MAC_a表示所述第一消息验证码，MAC_b表示所述第二消息验证码。

2. 一种移动终端，其特征在于，包括：

收发单元，接收来自验证服务器的公共参数，以及将密钥生成单元生成的第一消息发送至与所述移动终端通信的其他终端；

所述密钥生成单元，根据所述公共参数生成所述第一消息，以及根据所述其他终端发送过来的第二消息生成加密密钥；

加密单元，根据所述加密密钥对待发送的数据进行加密，并将加密后的数据经由所述收发单元发送至所述其他终端，其中，所述公共参数由所述验证服务器根据所述终端的身份和所述其他终端的身份生成；

其中，所述验证服务器按照以下公式确定所述公共参数：

$g = h(MAC_a, MAC_b)$，其中，g 表示所述公共参数，h 表示哈希函数，MAC_a表示所述第一消息的第一消息验证码，MAC_b表示所述第二消息的第二消息验证码。

3. 根据权利要求 2 所述的移动终端，其特征在于，还包括：校验单元，验证所述移动终端与所述其他终端是否使用同一所述公共参数，在判断出使用同一所述公共参数时，命令所述收发单元将所述第一消息发送至所述其他终端。

4. 根据权利要求 3 所述的移动终端，其特征在于，所述收发单元还用于将所述验证单元计算出的第一验证值 L_a发送至所述其他终端，以及接收来自所述其他终端的第二验证值 L_b，所述第二验证值 L_b基于公式 $L_b = g^{n_a} \bmod q$ 计算得到；

所述校验单元还用于基于公式$L_a = g^{n_b} \bmod q$ 计算出所述第一验证值 L_a，以及验证所述第二验证值 L_b是否正确，在验证结果为正确时，确定所述移动终端和所述其他终端使用同一所述公共参数，其中，n_b是所述其他终端的识别码，n_a是所述移动终端的识别码，q 是预存在所述移动终端和所述其他终端中的模数。

5. 根据权利要求 2 至 4 中任一项所述的移动终端，其特征在于，所述收发单元还用于接收来自所述其他终端的第二消息 K_b，所述第二消息 K_b基于公式 $K_b = g^{r_b} \bmod q$ 生成，以及将所述加密单元生成的第一消息 K_a发送至所述其他终端；

所述加密单元按照公式$K_a = g^{r_a} \bmod q$ 生成第一消息 K_a，以及根据公式 $K = K_b^{r_a} \bmod q$ 和来自所述其他终端的第二消息 K_b计算出所述加密密钥，其中，r_a和 r_b分别是大于等于 1 小于等于预设整数值的整数。

6. 一种端到端认证通信信道建立方法，其特征在于，包括以下步骤：

在主叫方呼叫被叫方时，核心网根据验证所述主叫方的身份生成的第一消息验证码和验证所述被叫方的身份生成的第二消息验证码确定公共参数，并将所述公共参数分配给所述主叫方和所述被叫方；

所述主叫方和所述被叫方根据所述公共参数生成各自的消息，并相互交换所述各自的消息；

所述主叫方和所述被叫方分别根据对方发送过来的消息生成相同的加密密钥，所述主叫方和所述被叫方分别根据所述加密密钥对待发送的数据进行加密，以建立所述主叫方与所述被叫方之间的端到端认证通信信道；

其中，所述核心网按照以下公式确定所述公共参数：

$g = h(MAC_a, MAC_b)$，其中，g 为所述公共参数，h 为哈希函数，MAC_a是所述主叫方的消息验证码，MAC_b为所述被叫方的消息验证码。

7. 根据权利要求 6 所述的端到端认证通信信道建立方法，其特征在于，还包括：

验证所述主叫方与所述被叫方是否使用同一所述公共参数；

若使用同一所述公共参数，则相互交换所述各自的消息。

8. 根据权利要求 7 所述的端到端认证通信信道建立方法，其特征在于，验证过程具体包括：

所述主叫方基于公式$L_a = g^{n_b} \bmod q$计算出第一验证值 L_a，并将所述第一验证值 L_a发送至所述被叫方；

所述被叫方基于公式$L_b = g^{n_a} \bmod q$计算出第二验证值 L_b，并将所述第二验证值 L_b发送至所述主叫方；

所述主叫方验证所述第二验证值L_b是否正确，所述被叫方验证所述第一验证值L_a是否正确，若所述第一验证值 L_a和所述第二验证值 L_b均正确，则确定所述主叫方和所述被叫方使用同一所述公共参数，其中，n_b是所述被叫方的识别码，n_a是所述主叫方的识别码，q 是预存在所述主叫方和所述被叫方中的模数。

9. 根据权利要求 6 至 8 中任一项所述的端到端认证通信信道建立方法，其特征在于，所述加密密钥的生成过程具体包括：

所述主叫方按照公式$K_a = g^{r_a} \bmod q$生成第一消息 K_a，并将第一消息 K_a发送至所述被叫方，所述被叫方按照公式$K_b = g^{r_b} \bmod q$生成第二消息 K_b，并将第二消息 K_b发送至所述主叫方；

所述主叫方根据公式$K = K_b^{r_a} \bmod q$和来自所述被叫方的第二消息 K_b计算出所述加密密钥，所述被叫方根据公式$K = K_a^{r_b} \bmod q$和来自所述主叫方的第一消息 K_a计算出所述加密密钥，其中，r_a和 r_b分别是大于等于 1 小于等于预设整数值的整数。

验证服务器、移动终端和端到端认证通信信道建立方法

技术领域

[0001] 本发明涉及通信技术领域，具体而言，涉及一种验证服务器、一种移动终端和一种端到端认证通信信道建立方法。

背景技术

[0002] 在现有移动通信系统中，移动电话之间的语音通话仅在无线传输时实现了加密处理，而在核心网传输时没有进行加密。这一现状造成了语音通话存在被窃听的可能，而在某些安全性要求更高的场合需要移动语音通信具有更高的安全性，因此需要建立端到端的安全通信信道。

[0003] 相关技术中提出了一种移动通信系统中端到端加密语音通信的方法，该方法中当主叫手机终端发出加密呼叫请求，经过加密资格鉴权后，由密钥分发中心(KDC)生成加密密钥，并将加密密钥分别发送给主叫终端和被叫终端，供双方建立安全的加密语音通信信道。该方案存在一个安全性弱点，即密钥完全由核心网内的密钥分发中(KDC)生成，这有可能导致两方面的安全漏洞。首先，如果 KDC 的数据泄漏，或者密钥由 KDC 发送给移动终端的途中被监听，则该密钥毫无安全性可言；同时，还存在中间人攻击以及攻击者伪装成 KDC 生成密钥的可能。

[0004] 相关技术中还提出了一种建立安全认证信道的方法，该方法中，相当于语音通话双方的两个对等实体均持有数字证书，两个对等实体分别要选取一个暂时私钥，并计算出一个暂时公钥，然后将暂时公钥、数字证书、身份标识发送给对方；双方均通过对方的暂时公钥和己方的暂时私钥计算出暂时共享密钥，并通过数字证书、哈希运算认证对方身份；最后双方均通过对暂时共享密钥进行哈希运算得到最终的会话密钥；最终使用会话密钥对通信进行加密，实现通信的安全性。但是该方案中通信双方的认证性是通过数字证书来实现的，每次建立密钥之前，通信双方都必须到证书中心 CA 处验证对方数字证书的真实性，这带来很大的通信开销，也意味着应用在移动通信系统中时，建立通话之前要经历较大的延迟，这在实时性要求较高的语音通话场合是不可接受的。同时这种依赖于公钥基础设施 PKI 验证移动终端的模式目前在移动通信系统中还无法实现。实际上，在移动通信系统中，核心网对接入的移动终端已经做了身份认证，该认证过程是通过使用核心网的鉴权中心 AUC 存储的鉴权参数实现的。另一个问题是该方案中的公开参数如何选取没有做说明，公开参数在建立密钥前通信双方应该协商一致。

[0005] 因此，需要一种容易实现的可建立端到端的安全认证通信信道，可提高密钥的安全性。

发明内容

[0006] 考虑到上述背景技术，本发明提供了一种端到端安全认证通信信道建立技术，可提高密钥的安全性。

[0007] 根据本发明的一个方面，提供了一种验证服务器，位于核心网，包括：验证单元，在

主叫方呼叫被叫方时，验证所述主叫方的身份并生成第一消息验证码以及验证所述被叫方的身份并生成第二消息验证码；公共参数确定单元，根据所述第一消息验证码和所述第二消息验证码确定公共参数，并将所述公共参数分配给所述主叫方和所述呼叫方。

[0008] 该验证服务器能够利用验证呼叫双方的身份而产生的消息验证码来生成公共参数，并将公共参数发送给呼叫双方，从而完成了对通话双方的身份认证，且无需依赖 PKI 和数字证书。

[0009] 在上述技术方案中，优选的，所述公共参数确定单元按照以下公式确定所述公共参数：$g=h(MAC_a, MAC_b)$，其中，g 表示所述公共参数，h 表示哈希函数，MAC_a表示所述第一消息验证码，MAC_b表示所述第二消息验证码。

[0010] 根据本发明的另一方面，还提供了一种移动终端，包括：收发单元，接收来自验证服务器的公共参数，以及将密钥生成单元生成的第一消息发送至与所述移动终端通信的其他终端；所述密钥生成单元，根据所述公共参数生成所述第一消息，以及根据所述其他终端发送过来的第二消息生成加密密钥；加密单元，根据所述加密密钥对待发送的数据进行加密，并将加密后的数据经由所述收发单元发送至所述其他终端。

[0011] 两个手机终端之间通过一次消息交换过程生成一个加密密钥，从而完成安全认证通信信道的建立，只有参与的这两个手机终端才知道该加密密钥，保证了加密的安全性。

[0012] 在上述技术方案中，优选的，还可以包括：校验单元，验证所述移动终端与所述其他终端是否使用同一所述公共参数，在判断出使用同一所述公共参数时，命令所述收发单元将所述第一消息发送至所述其他终端。只有在保证通话双方使用同一公共参数的基础之上，才能保证通话双方生成相同的加密密钥。

[0013] 在上述技术方案中，优选的，所述收发单元还用于将所述验证单元计算出的第一验证值 L_a发送至所述其他终端，以及接收来自所述其他终端的第二验证值 L_b，所述第二验证值 L_b基于公式 $L_b = g^{n_a} \bmod q$ 计算得到；所述校验单元还用于基于公式 $L_a = g^{n_b} \bmod q$ 计算出所述第一验证值 L_a，以及验证所述第二验证值 L_b是否正确，在验证结果为正确时，确定所述移动终端和所述其他终端使用同一所述公共参数，其中，n_b是所述其他终端的识别码，n_a是所述移动终端的识别码，q 是预存在所述移动终端和所述其他终端中的模数。

[0014] 在上述任一技术方案中，优选的，所述收发单元还用于接收来自所述其他终端的第二消息 K_b，所述第二消息 K_b基于公式 $K_b = g^{r_b} \bmod q$ 生成，以及将所述加密单元生成的第一消息 K_a发送至所述其他终端；所述加密单元按照公式 $K_a = g^{r_a} \bmod q$ 生成第一消息 K_a，以及根据公式 $K = K_b^{r_a} \bmod q$ 和来自所述其他终端的第二消息 K_b计算出所述加密密钥，其中，r_a和 r_b分别是大于等于 1 小于等于预设整数值的整数。该预设整数值与哈希函数输出的最大消息值有关。

[0015] 根据本发明的又一方面，还提供了一种端到端认证通信信道建立方法，包括以下步骤：在主叫方呼叫被叫方时，核心网根据验证所述主叫方的身份生成的第一消息验证码和验证所述被叫方的身份生成的第二消息验证码确定公共参数，并将所述公共参数分配给所述主叫方和所述呼叫方；所述主叫方和所述被叫方根据所述公共参数生成各自的消息，

并相互交换所述各自的消息；所述主叫方和所述被叫方分别根据对方发送过来的消息生成相同的加密密钥，所述主叫方和所述被叫方分别根据所述加密密钥对待发送的数据进行加密，以建立所述主叫方与所述被叫方之间的端到端认证通信信道。

[0016] 核心网能够利用验证呼叫双方的身份而产生的消息验证码来生成公共参数，并将公共参数发送给呼叫双方，从而完成了对通话双方的身份认证，且无需依赖 PKI 和数字证书。两个手机终端之间通过一次消息交换过程生成一个加密密钥，从而完成安全认证通信信道的建立，只有参与密钥交换的这两个手机终端才知道该加密密钥，保证了加密的安全性。

[0017] 在上述技术方案中，优选的，所述核心网按照以下公式确定所述公共参数：$g=h(MAC_a, MAC_b)$，其中，g 为所述公共参数，h 为哈希函数，MAC_a是所述主叫方的消息验证码，MAC_b为所述被叫方的消息验证码。

[0018] 在上述技术方案中，优选的，还可以包括以下步骤：验证所述主叫方与所述被叫方是否使用同一所述公共参数；若使用同一所述公共参数，则相互交换所述各自的消息。

[0019] 在上述技术方案中，优选的，验证过程具体包括：所述主叫方基于公式$L_a=g^{n_b} \bmod q$计算出第一验证值L_a，并将所述第一验证值L_a发送至所述被叫方；所述被叫方基于公式$L_b=g^{n_a} \bmod q$计算出第二验证值L_b，并将所述第二验证值L_b发送至所述主叫方；所述主叫方验证所述第二验证值L_b是否正确，所述被叫方验证所述第一验证值L_a是否正确，若所述第一验证值L_a和所述第二验证值L_b均正确，则确定所述主叫方和所述被叫方使用同一所述公共参数，其中，n_b是所述被叫方的识别码，n_a是所述主叫方的识别码，q 是预存在所述主叫方和所述被叫方中的模数。

[0020] 在上述技术方案中，优选的，所述加密密钥的生成过程具体包括：所述主叫方按照公式$K_a=g^{r_a} \bmod q$生成第一消息K_a，并将第一消息K_a发送至所述被叫方，所述被叫方按照公式$K_b=g^{r_b} \bmod q$生成第二消息K_b，并将第二消息K_b发送至所述主叫方；所述主叫方根据公式$K=K_b{}^{r_a} \bmod q$和来自所述被叫方的第二消息K_b计算出所述加密密钥，所述被叫方根据公式$K=K_a{}^{r_b} \bmod q$和来自所述主叫方的第一消息K_a计算出所述加密密钥，其中，r_a和r_b分别是大于等于 1 小于等于预设整数值的整数。该预设整数值与哈希函数输出的最大消息值有关。

附图说明

[0021] 图 1 示出了根据本发明的实施例的验证服务器的框图；

[0022] 图 2 示出了根据本发明的实施例的移动终端的框图；

[0023] 图 3 示出了根据本发明的实施例的端到端安全认证信道建立系统的框图；

[0024] 图 4 示出了根据本发明的一个实施例的端到端认证通信信道建立方法的流程图；

[0025] 图 5 示出了根据本发明的又一实施例的端到端认证通信信道建立方法的流程图。

具体实施方式

[0026] 为了能够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。

[0027] 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，本发明的保护范围不受下面公开的具体实施例的限制。

[0028] 下面结合附图和实施例对本发明做进一步说明。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。

[0029] 图 1 示出了根据本发明的实施例的验证服务器的框图。

[0030] 如图 1 所示，根据本发明的实施例的验证服务器 100，位于核心网，包括：验证单元 102，在主叫方呼叫被叫方时，验证主叫方的身份并生成第一消息验证码以及验证被叫方的身份并生成第二消息验证码；公共参数确定单元 104，根据第一消息验证码和第二消息验证码确定公共参数，并将公共参数分配给主叫方和呼叫方。

[0031] 该验证服务器 100 能够利用验证呼叫双方的身份而产生的消息验证码来生成公共参数，并将公共参数发送给呼叫双方，从而完成了对通话双方的身份认证，且无需依赖 PKI 和数字证书。

[0032] 优选的，公共参数确定单元 104 按照以下公式确定公共参数：$g=h(MAC_a, MAC_b)$，其中，g 表示公共参数，h 表示哈希函数，MAC_a表示第一消息验证码，MAC_b表示第二消息验证码。

[0033] 图 2 示出了根据本发明的实施例的移动终端的框图。

[0034] 如图 2 所示，根据本发明的实施例的移动终端 200，包括：收发单元 202，接收来自验证服务器的公共参数，以及将密钥生成单元生成的第一消息发送至与移动终端通信的其他终端；密钥生成单元 204，根据公共参数生成第一消息，以及根据其他终端发送过来的第二消息生成加密密钥；加密单元 206，根据加密密钥对待发送的数据进行加密，并将加密后的数据经由收发单元发送至其他终端。

[0035] 两个手机终端之间通过一次消息交换过程生成一个加密密钥，从而完成安全认证通信信道的建立，只有参与的这两个手机终端才知道该加密密钥，保证了加密的安全性。

[0036] 优选的，移动终端 200 还可以包括：校验单元 208，验证移动终端与其他终端是否使用同一公共参数，在判断出使用同一公共参数时，命令收发单元将第一消息发送至其他终端。只有在保证通话双方使用同一公共参数的基础之上，才能保证通话双方生成相同的加密密钥。

[0037] 优选的，收发单元 202 还用于将验证单元计算出的第一验证值 L_a发送至其他终端，以及接收来自其他终端的第二验证值 L_b，第二验证值 L_b基于公式 $L_b = g^{n_a} \bmod q$ 计算得到；校验单元 208 还用于基于公式 $L_a = g^{n_b} \bmod q$ 计算出所述第一验证值 L_a，以及验证所述第二验证值 L_b是否正确，在验证结果为正确时，确定所述移动终端和所述其他终端使用同一所述公共参数，其中，n_b是所述其他终端的识别码，n_a是所述移动终端的识别码，q 是预存在所述移动终端和所述其他终端中的模数。

[0038] 在上述任一技术方案中，优选的，所述收发单元 202 还用于接收来自所述其他终端的第二消息 K_b所述第二消息 K_b基于公式 $K_b = g^{r_b} \bmod q$ 生成，以及将所述加密单元生

成的第一消息K_a发送至所述其他终端；所述加密单元206按照公式$K_a = g^{r_a} \bmod q$生成第一消息K_a，以及根据公式$K = K_b^{r_a} \bmod q$和来自所述其他终端的第二消息K_b计算出所述加密密钥，其中，r_a和r_b分别是大于等于1小于等于预设整数值的整数。该预设整数值与哈希函数输出的最大消息值有关。

[0039] 图3示出了根据本发明的实施例的端到端安全认证信道建立系统的框图。

[0040] 如图3所示，公共参数g由位于核心网侧的验证服务器100选定之后分发给两个移动终端(移动终端A和移动终端B)，然后两个移动终端之间通过一次验证数据交互来确保双方使用同一个参数g。

[0041] 在确保移动终端A和移动终端B使用同一个参数g后，两个移动终端之间通过一次密钥交换过程生成一个加密密钥，从而完成安全认证通信信道的建立，最后利用该加密密钥对待发送的数据进行加密。由于加密密钥的生成过程只有移动终端A和移动终端B参与并且在交换过程中产生，没有第三方知道该加密密钥，因此有效提高了加密密钥的安全性。

[0042] 安全认证通信信道用于两个通信设备之间互相认证对方身份，并且交换会话加密密钥，以便双方实现加密通信。通过该安全认证信道能够实现手机终端之间的端到端加密通信，本发明依托现有移动通信系统机制，容易实现。加密密钥由通信的两个移动终端通过交互建立，避免了核心网实体对加密密钥的掌握，有效提高了加密密钥的安全性，进而提高了加密语音通信的安全性；同时，本发明中的认证性通过核心网对移动终端的鉴权实现，无需通信双方再次进行认证，降低了通信开销。

[0043] 图4示出了根据本发明的实施例的端到端认证通信信道建立方法的流程图。

[0044] 如图4所示，根据本发明的实施例的端到端认证通信信道建立方法，包括以下步骤：步骤402，在主叫方呼叫被叫方时，核心网根据验证主叫方的身份生成的第一消息验证码和验证被叫方的身份生成的第二消息验证码确定公共参数，并将公共参数分配给主叫方和呼叫方；步骤404，主叫方和被叫方根据公共参数生成各自的消息，并相互交换各自的消息；步骤406，主叫方和被叫方分别根据对方发送过来的消息生成相同的加密密钥，主叫方和被叫方分别根据加密密钥对待发送的数据进行加密，以建立主叫方与被叫方之间的端到端认证通信信道。

[0045] 核心网能够利用验证呼叫双方的身份而产生的消息验证码来生成公共参数，并将公共参数发送给呼叫双方，从而完成了对通话双方的身份认证，且无需依赖PKI和数字证书。两个手机终端之间通过一次消息交换过程生成一个加密密钥，从而完成安全认证通信信道的建立，只有参与密钥交换的这两个手机终端才知道该加密密钥，保证了加密的安全性。

[0046] 在上述技术方案中，优选的，核心网按照以下公式确定公共参数：$g=h(MAC_a, MAC_b)$，其中，g为公共参数，h为哈希函数，MAC_a是主叫方的消息验证码，MAC_b为被叫方的消息验证码。

[0047] 在上述技术方案中，优选的，还可以包括以下步骤：验证主叫方与被叫方是否使用同一公共参数；若使用同一公共参数，则相互交换各自的消息。

[0048] 在上述技术方案中，优选的，验证过程具体包括：主叫方基于公式

$L_a=g^{n_b} \bmod q$计算出第一验证值L_a，并将第一验证值L_a发送至被叫方；被叫方基于公式$L_b=g^{n_a} \bmod q$计算出第二验证值L_b，并将第二验证值L_b发送至主叫方；主叫方验证第二验证值L_b是否正确，被叫方验证第一验证值L_a是否正确，若第一验证值L_a和第二验证值L_b均正确，则确定主叫方和被叫方使用同一公共参数，其中，n_b是被叫方的识别码，n_a是主叫方的识别码，q 是预存在主叫方和被叫方中的模数。

[0049] 在上述技术方案中，优选的，加密密钥的生成过程具体包括：主叫方按照公式$K_a=g^{r_a} \bmod q$生成第一消息K_a，并将第一消息K_a发送至被叫方，被叫方按照公式$K_b=g^{r_b} \bmod q$生成第二消息K_b，并将第二消息K_b发送至主叫方；主叫方根据公式$K=K_b^{r_a} \bmod q$和来自被叫方的第二消息K_b计算出加密密钥，被叫方根据公式$K=K_a^{r_b} \bmod q$和来自主叫方的第一消息K_a计算出加密密钥，其中，r_a和r_b分别是大于等于 1 小于等于预设整数值的整数。该预设整数值与哈希函数输出的最大消息值有关。

[0050] 下面结合图 5 进一步说明根据本发明的实施例的端到端认证通信信道建立方法。本方法中的认证性通过核心网对移动终端的鉴权实现，核心网对手机终端进行的鉴权能够确保手机终端的实体认证性。本方法中的密钥交换过程由一个密钥交换协议实现，其中，密钥交换协议的公开参数包括一个模数 q 和一个模幂运算底数 g，模数 q 是一个大素数且预装在手机终端存储器内，而底数 g 则动态生成。为了叙述方便，下面叙述中将核心网抽象成一个实体，不再区分核心网内的各个网元。

[0051] 在步骤 502，手机终端之间进行正常呼叫流程。此处的呼叫流程即移动通信系统中的呼叫流程，用于在手机终端之间建立呼叫链路。

[0052] 在步骤 504，确定公共参数 g。在正常呼叫流程的鉴权过程中，核心网络为了验证终端身份会生成消息验证码 MAC。参与建立安全认证信道的两个手机终端的对应消息验证码分别记为 MACa 和 MACb。

[0053] 令哈希函数 h 为 $\{0,1\}^* \rightarrow Zp$，其中，$\{0,1\}^*$表示输入的任意长度的消息，Zp 表示 1 到 p-1 之间的任意一个整数，例如Z_{100}表示 1 到 99 之间的任意一个整数，核心网根据哈希算法和两个手机终端的消息验证码计算出公共参数 g=h(MACa, MACb)。

[0054] 假设参与建立安全认证信道的两个手机终端分别记为终端 A 和终端 B，核心网将计算出的公共参数 g 分别发送给终端 A 和终端 B。

[0055] 其中，为了确保两个手机终端使用同一公共参数，需要进行验证。假设终端 A 的手机号为 na，终端 B 的手机号为 nb。为了验证双方是否使用同一个参数 g，终端 A 基于公式$L_a=g^{n_b} \bmod q$计算出L_a并将L_a发送给终端 B，而终端 B 基于公式$L_b=g^{n_a} \bmod q$计算出L_b并将L_b发送给终端 A。

[0056] 终端 A 和终端 B 分别验证对方发送值的正确性，如果正确，则继续执行步骤 506 的密钥交换；如果不正确，则终止该流程。

[0057] 在步骤 506，密钥交换。

[0058] 终端 A 选择随机数$r_a \in Zp$，计算$K_a=g^{r_a} \bmod q$，并将第一消息 Ka 发送给终端 B。

[0059] 终端 B 选择随机数 $r_b \in Zp$，计算 $K_b = g^{r_b} \bmod q$，并将第二消息 Kb 发送给终端 A。

[0060] 终端 A 计算加密密钥为 $K = K_b^{r_a} \bmod q$；终端 B 计算加密密钥为 $K = K_a^{r_b} \bmod q$。最终双方生成同一个用于会话的加密密钥，至此建立了端到端安全认证通信信道。双方利用该加密密钥对待发送的数据进行加密，实现了加密通信。

[0061] 以上结合附图详细说明了根据本发明的技术方案，提出了一种在手机终端之间建立端到端安全认证信道的技术，只需在现有移动通信系统基础上增加几条交互消息，容易实现。其次，本技术方案中的加密密钥仅由参与通信的两个手机终端掌握，有效提高了密钥的安全性；同时本方案中手机终端的认证由核心网的鉴权机制完成，无需依赖于公钥基础设施和数字证书，使用本技术方案实现的加密通信，在建立通信信道阶段延迟较小，可应用于实时性要求较高的语音通话场合，能很好满足用户的实时需求，提高用户的体验感受。

[0062] 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。

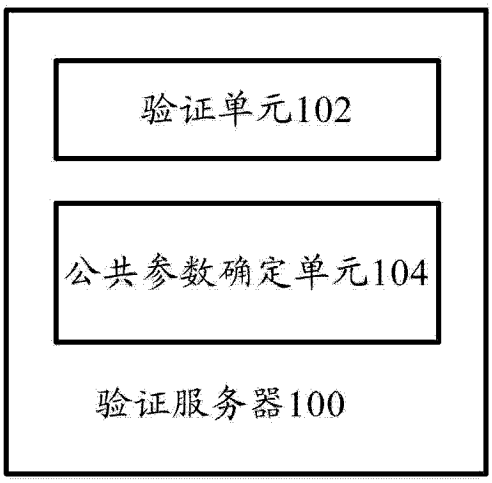

验证单元102
公共参数确定单元104
验证服务器100

图 1

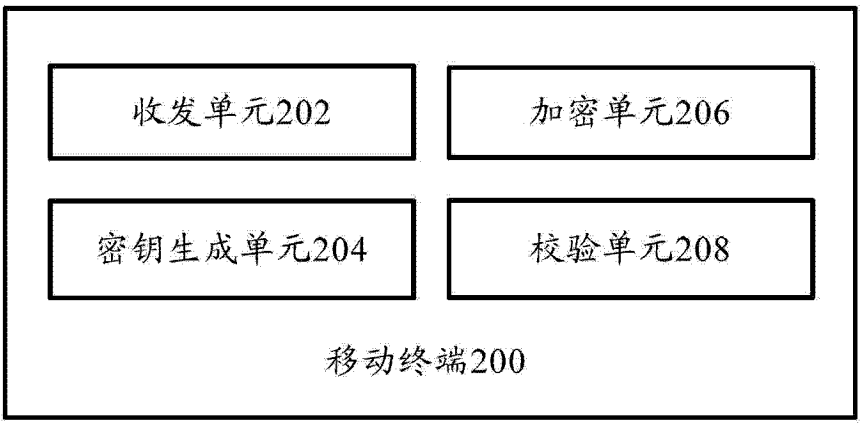

收发单元202
加密单元206
密钥生成单元204
校验单元208
移动终端200

图 2

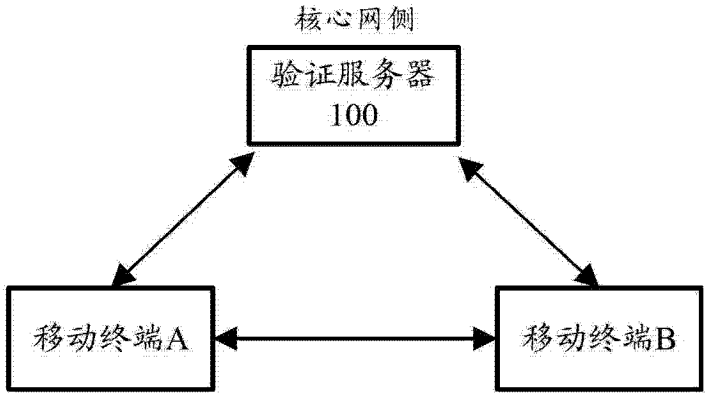

核心网侧
验证服务器
100
移动终端A
移动终端B

图 3

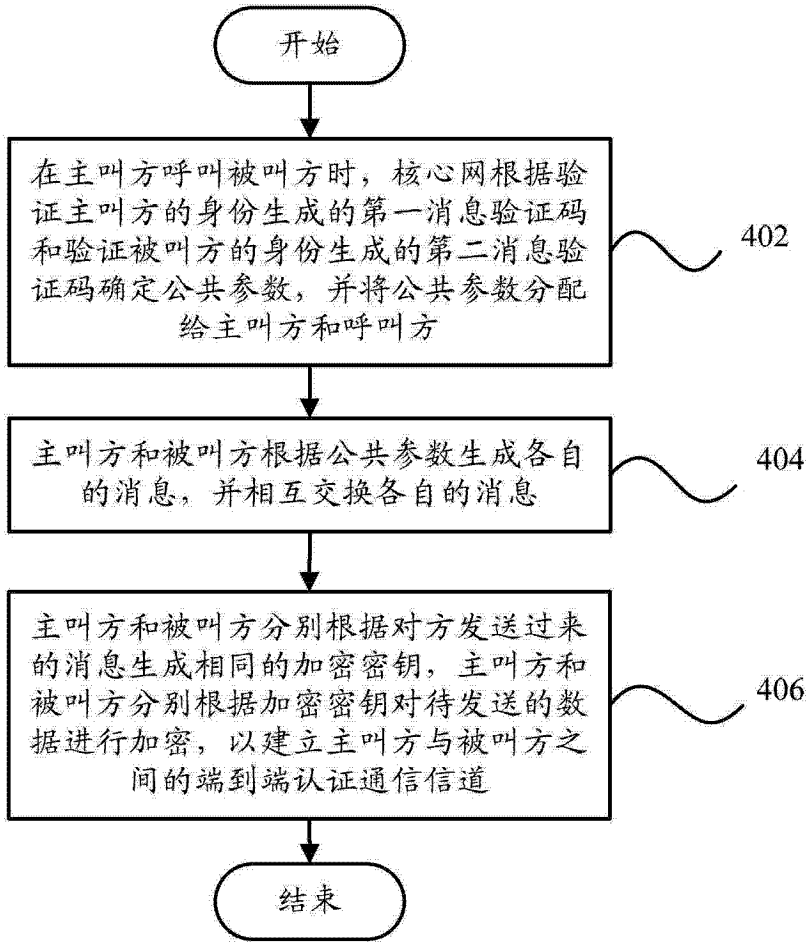

开始
在主叫方呼叫被叫方时，核心网根据验证主叫方的身份生成的第一消息验证码和验证被叫方的身份生成的第二消息验证码确定公共参数，并将公共参数分配给主叫方和呼叫方
402
主叫方和被叫方根据公共参数生成各自的消息，并相互交换各自的消息
404
主叫方和被叫方分别根据对方发送过来的消息生成相同的加密密钥，主叫方和被叫方分别根据加密密钥对待发送的数据进行加密，以建立主叫方与被叫方之间的端到端认证通信信道
406
结束

图 4

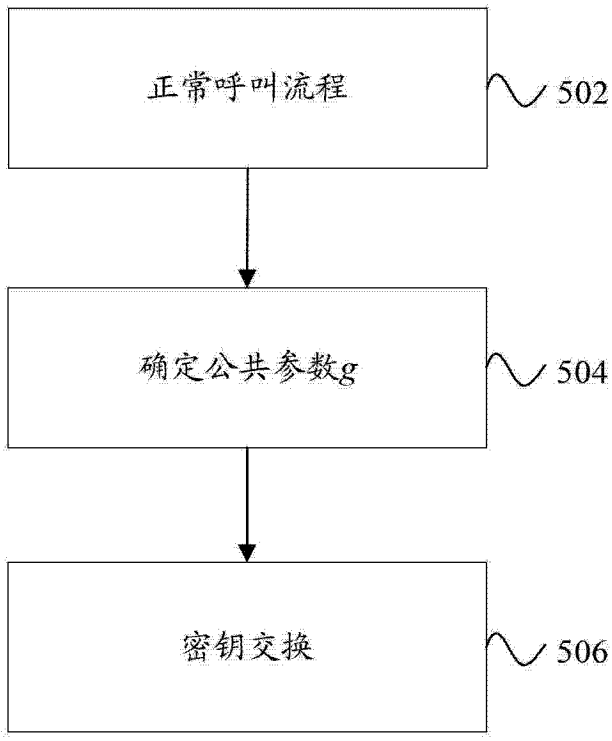


图 5