(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105379175 A
(43)申请公布日 2016.03.02

(21)申请号 201480036064.5
(22)申请日 2014.06.24
(30)优先权数据
13/925,299 2013.06.24 US
(85)PCT国际申请进入国家阶段日
2015.12.24
(86)PCT国际申请的申请数据
PCT/IB2014/002161 2014.06.24
(87)PCT国际申请的公布数据
WO2015/008158 EN 2015.01.22
(71)申请人 黑莓有限公司
地址 加拿大安大略省沃特卢市
申请人 塞尔蒂卡姆公司
(72)发明人 迈克尔·约恩·巴克利
迈克尔·查尔斯·霍拉茨
罗伯特·约翰·兰伯特
内文·莫里斯·纳斯夫·艾贝德
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 苏志莲
(51)Int.Cl.
H04L 9/30(2006.01)
H04W 12/04(2006.01)

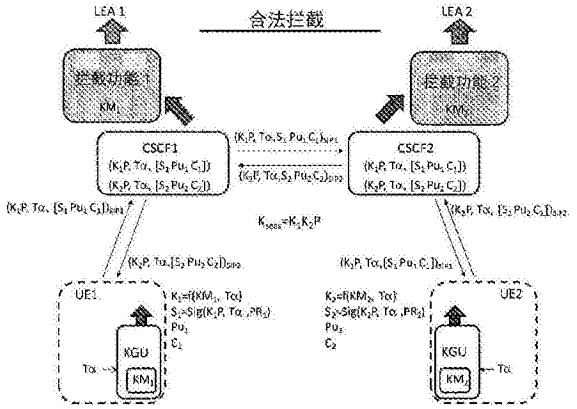
权利要求书2页 说明书7页 附图8页

(54)发明名称

用于合法拦截的安全方法

(57)摘要

提出了一种用于安全通信的方法，该方法包括：使用私钥、一次性数以及标识符和密钥分量两者中的至少一个，生成签名；以及发送所述签名、所述一次性数、安全参数以及所述标识符和所述密钥分量两者中的至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。



CN 105379175 A

1. 一种用于安全通信的方法，包括：

使用私钥、一次性数、以及标识符和密钥分量两者中的至少一个，生成签名；以及

发送所述签名、所述一次性数、安全参数、以及所述标识符和所述密钥分量两者中的至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。

2. 根据权利要求 1 所述的方法，其中，所述标识符是以下之一：国际移动台设备标识 (IMEI)、全球可路由用户代理 URI(GRUU)、国际移动订户标识 (IMSI) 和临时国际移动订户标识 (TIMSI)。

3. 根据权利要求 1 所述的方法，其中，所述一次性数是时间戳、随机数和序列号之一。

4. 根据权利要求 1 所述的方法，其中，所述安全参数是证书。

5. 根据权利要求 1 所述的方法，还包括：

使用主密钥、所述一次性数和已知的椭圆曲线点来生成所述密钥分量。

6. 根据权利要求 1 所述的方法，其中，发送步骤还包括：

发送所述签名和所述公钥。

7. 根据权利要求 1 所述的方法，还包括：

接收第二一次性数、第二标识符和第二密钥分量两者中的至少一个、第二安全参数和第二签名，所述第二签名是使用第二私钥、所述第二一次性数、以及所述第二标识符和所述第二密钥分量两者中的至少一个来生成的；

使用接收到的第二签名和第二安全参数，验证所述第二一次性数以及所述第二标识符和所述第二密钥分量两者中的至少一个，其中，所述第二安全参数将第二用户标识与第二公钥相关联，所述第二公钥与所述第二私钥相关联；以及

当在验证步骤中验证成功时，使用所述第二标识符和所述第二密钥分量中的至少一个来生成会话密钥。

8. 一种用于安全通信的方法，包括：

接收一次性数、标识符和密钥分量两者中的至少一个、安全参数和签名，所述签名是使用私钥、所述一次性数、以及所述标识符和所述密钥分量两者中的至少一个来生成的；以及

使用接收到的签名和安全参数，验证所述一次性数以及所述标识符和所述密钥分量中的两者至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。

9. 根据权利要求 8 所述的方法，还包括：当在验证步骤中验证成功时，

使用所述标识符和所述密钥分量中的至少一个来生成会话密钥。

10. 根据权利要求 8 所述的方法，还包括：当在验证步骤中验证成功时，

使用第二私钥、第二一次性数、以及第二标识符和第二密钥分量两者中的至少一个，生成第二签名；以及

发送所述第二签名、所述第二一次性数、第二安全参数、以及所述第二标识符和所述第二密钥分量两者中的至少一个，其中，所述第二安全参数将第二用户标识与第二公钥相关联，所述第二公钥与所述第二私钥相关联。

11. 一种用于安全通信的方法，包括：

使用 MAC 密钥、一次性数、以及标识符和密钥分量两者中的至少一个，生成 MAC 标签；以及

发送所述 MAC 标签、所述一次性数、以及所述标识符和所述密钥分量两者中的至少一个。

12. 根据权利要求 11 所述的方法，其中，所述标识符是以下之一：国际移动台设备标识 (IMEI)、全球可路由用户代理 URI(GRUU)、国际移动订户标识 (IMSI) 和临时国际移动订户标识 (TIMSI)。

13. 根据权利要求 11 所述的方法，其中，所述一次性数是时间戳、随机数和序列号之一。

14. 一种用于安全通信的方法，包括：

接收一次性数、标识符和密钥分量两者中的至少一个、以及 MAC 标签，所述 MAC 标签是使用所述一次性数、所述标识符和所述密钥分量两者中的至少一个以及 MAC 密钥生成的；以及

使用接收到的 MAC 标签，验证所述一次性数以及所述标识符和所述密钥分量两者中的至少一个。

15. 一种用于安全通信的装置，包括：

处理电路，被配置为使用私钥、一次性数、以及标识符和密钥分量两者中的至少一个，生成签名；以及

发射机，被配置为发送所述签名、所述一次性数、安全参数、以及所述标识符和所述密钥分量两者中的至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。

16. 一种用于安全通信的装置，包括：

接收机，被配置为接收一次性数、标识符和密钥分量两者中的至少一个、安全参数和签名，所述签名是使用私钥、所述一次性数、以及所述标识符和所述密钥分量两者中的至少一个来生成的；以及

处理单元，被配置为使用接收到的签名和安全参数，验证所述一次性数以及所述标识符和所述密钥分量中的两者至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。

17. 一种用于安全通信的装置，包括：

处理单元，被配置为使用 MAC 密钥、一次性数、以及标识符和密钥分量两者中的至少一个，生成 MAC 标签；以及

发射机，被配置为发送所述 MAC 标签、所述一次性数、以及所述标识符和所述密钥分量两者中的至少一个。

18. 一种用于安全通信的装置，包括：

接收机，被配置为接收一次性数、标识符和密钥分量两者中的至少一个、以及 MAC 标签，所述 MAC 标签是使用所述一次性数、所述标识符、和所述密钥分量两者中的至少一个以及 MAC 密钥生成的；以及

处理电路，被配置为使用接收到的 MAC 标签，验证所述一次性数以及所述标识符和所述密钥分量两者中的至少一个。

用于合法拦截的安全方法

技术领域

[0001] 本公开涉及合法拦截的安全方法。

背景技术

[0002] 第三代伙伴项目 (3GPP) 目前正考虑用于 IP 多媒体子系统 (IMS) 媒体安全的多种合法拦截和密钥生成方法。一种这样的密钥生成方法是多媒体互联网密钥 - 基于身份的认证密钥交换 (MIKEY-IBAKE),其是公知的 Diffie-Hellman 密钥交换的示例。这样的密钥生成协议的目标是在两个 UE 间关于会话密钥 K_{sess} 达成一致,其中,UE 代表用户设备。

[0003] 如图 1 所示,MIKEY-IBAKE 过程中的步骤可概括如下 :(1)UE_1 通过使用其密钥生成单元 (KGU),生成私钥信息 K_1;UE_1 使用 K1 和公知的椭圆曲线点 P,计算 K_1P ;(3)UE_1 使用会话发起协议 (SIP) 信令经由设备 $CSCF_1$ 和设备 $CSCF_2$ 向 UE_2 发送 K_1P,$CSCF_1$ 和 $CSCF_2$ 中的每一个实现呼叫会话控制功能 (CSCF) ;(4)UE_2 通过使用其 KGU,生成私钥信息 K_2;(5)UE_2 使用 K_2 和公知的椭圆曲线点 P,计算 K_2P ;(6)UE_2 使用 SIP 信令向 UE_1 发送 K_2P ;以及 (7)UE_1 和 UE_2 分别使用 $[K_1, K_2P]$ 和 $[K_1P, K_2]$ 来生成 $K_{sess} = K_1K_2P$。

[0004] 在图 1 中,仅 UE_1 和 UE_2 是知道会话密钥的实体。然而,除了在 UE 间提供安全通信,政府规章还要求支持合法拦截。

[0005] 图 2 示出了允许合法拦截的传统密钥生成过程。如图 2 所示,相应 UE_i 中的每个 KGU 以所定义的方法由相应的主密钥 KM_i 和时间戳 Tα 来生成对应的密钥信息 K_i。主密钥仅对相应的 UE_i 和被配置为在相应的执法机构 (LEA) 的控制下执行网络拦截功能的相应的网络设备已知,如图 2 所示。例如,$CSCF_1$ 和 LEA_1 的相应拦截设备是第一网络的一部分,而 $CSCF_2$ 和 LEA_2 的相应拦截设备是与第一网络通信的第二网络的一部分。

[0006] 此外,用于生成相应密钥信息 K_i 的时间戳 Tα 由每个相应 UE_i 以 SIP 与 K_iP 一起发送。K_iP 和 Tα 可以存储在相应网络中的 CSCF 设备 ($CSCF_1$ 和 $CSCF_2$) 中的一个或多个中,如图 2 所示。具体地,注意图 2 示出了 UE 位于不同网络中的一般情形,因此需要分离的 CSCF 设备。当 UE 位于单个网络中时,仅需使用一个 CSCF 设备。

[0007] LEA_2 的拦截设备在为了合法拦截而生成会话密钥 K_{sess} 时所采取的步骤如下 :(1) 从内部存储取得 KM_2 (由 UE_2 使用),从设备 $CSCF_2$ 取得 K_1P 和 Tα ;(2) 生成密钥信息 $K_2 = f(KM_2, T\alpha)$;以及 (3) 生成 $K_{sess} = K_1K_2P$。LEA_2 的拦截设备此时可以解密 UE_1 和 UE_2 间的业务,并将其转发至 LEA_2。LEA_1 的拦截设备的拦截过程是类似的,但使用 KM_1、Tα 和 K_2P。

[0008] 此外,注意上述合法拦截过程可以推广,使得 UE_1 和 UE_2 将不同时间戳用于密钥生成和 / 或信令 (例如 $T\alpha_1$ 和 $T\alpha_2$)。

附图说明

[0009] 由于在结合附图考虑时此处公开的实施例通过参照以下描述被更好的理解,将易于获得对实施例及其许多伴随优点的更完全的理解,在附图中 :

[0010] 图 1 示出了 MIKEY-IBAKE 过程 ;

[0011] 图 2 示出了传统的合法拦截过程；

[0012] 图 3 示出了避免合法拦截的过程；

[0013] 图 4 示出了根据一个实施例的用于安全合法拦截的新颖方法；

[0014] 图 5 示出了根据一个实施例的安全合法拦截的新颖方法的步骤的流程图；

[0015] 图 6 示出了根据一个实施例的使用 IMEI 的安全合法拦截的新颖方法；

[0016] 图 7 示出了根据一个实施例的使用 MAC 标签的安全合法拦截的新颖方法；以及

[0017] 图 8 示出了可在公开的实施例中使用的硬件。

具体实施方式

[0018] MIKEY-IBAKE 过程的合法拦截依赖于用于生成密钥信息的时间戳 Tα 的网络知识。然而，危险用户可以改变运行在 UE 上的软件，以通过在生成密钥信息时使用与以 SIP 发信号通知的时间戳不同的时间戳，从而生成不同的密钥分量 ($K_{2\beta}P$)，但发送未用于生成密钥分量 $K_{2\beta}P$ 的时间戳 Tα，来避免合法拦截。

[0019] 例如，如图 3 所示，假设 UE_2 的用户是恶意的并且希望在他的网络中避免合法拦截。他因而重构了运行在他的设备上的内核软件，修改了 SIP 栈，使得用于在 SIP 上发信号通知的时间戳 Tα 不同于用于生成密钥信息的时间戳 Tβ。作为结果，网络不能重新生成 UE_2 的必要密钥信息 $K_{2\beta}$，从而避免了合法拦截。

[0020] 在该示例中，第二网络存储 $K_{2\beta}P$，并且因此具有确定 UE_2 在生成 $K_{2\beta}$ 时未使用 Tα 的必要信息。

[0021] 如果第二网络中的设备 $CSCF_2$ 在呼叫建立时检测到滥用，网络可以不允许通信。然而，为了有效，将要求网络在至少一部分呼叫建立中验证 $K_{2\beta}P$，这从运营商的角度看是非常不希望的。如有必要，运营商强烈希望任何这样的检查在 UE 处执行。

[0022] 备选地，作为合法拦截过程的一部分，第二网络中的设备 $CSCF_2$ 可以验证 $K_{2\beta}P$。然而，任何诸如禁用电话或简单地切断通信的动作将破坏现有要求：除了请求的执法机构和拦截网络，合法拦截不可被任何实体检测。

[0023] 该要求的附加结果是第二网络不能与第一网络一起工作以进行合法拦截。例如，在以上示例中，第一网络具有合法拦截所需的所有信息，即，$K_{2\beta}P$、Tα 和 KM_1。然而，由于 LEA_2 不一定希望披露发生合法连接，任何最终密钥交换协议必须使第二网络能够执行合法拦截，而无需联系任何附加实体。

[0024] 因此，虽然第二网络能够检测到当前 MIKEY-IBAKE 过程中变形的密钥信息，该过程需要进一步修改以成为满足所有当前要求的可行方案。

[0025] 此外，应理解：如果 UE_1 和 UE_2 有修改它们内核的自由，它们也自由地实现任何密钥协商方案，潜在地甚至不同于标准化密钥协商方案的方案，但信令是兼容的。随着开源操作系统（如 Android）的出现，不幸地修改内核的能力目前是可接受的事实。事实上，该能力通常被吹捧为是希望的。由于在这样的情形下合法拦截变得极不可能，此处解决的问题是保护防止两个 UE 之一恶意修改其内核以避免合法拦截。

[0026] 相关问题是国际移动台设备标识 (IMEI) 的 SIP 信令，IMEI 是移动设备 (ME) 的（即不包括订户标识模块 (SIM) 卡的 UE 的）标识符。在一些法律中，IMEI 被用作合法拦截根据其发生的标识符。然而，由于伪造，多于一个电话可以共享相同的 IMEI。虽然在世界的西

方地区这不是太大的问题，但在其他地区这是很有问题的。如果多个 ME 共享相同的 IMEI，则指定目标 ME 变为更复杂的过程，使得合法拦截更加困难。此外，如果 UE 修改其内核，存在以下危险：UE 还可以发信号通知假 IMEI，可能通过 IMEI 瞄准避免合法拦截。因此，还需要用于 IMEI 的安全信令的方案。

[0027] 在传统系统中，由于对每个 KGU 使用的时间戳 Tα 的安全保护不足，危险用户将通常成功。所需的是确保 KGU 所使用的时间戳也以 SIP 发信号通知的方法。

[0028] 相应地，提供了一种用于安全通信的方法，包括：(1) 使用私钥、一次性数以及标识符和密钥分量两者中的至少一个，生成签名；以及 (2) 发送所述签名、所述一次性数、安全参数、以及所述标识符和所述密钥分量两者中的至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。所述标识符是以下之一：国际移动台设备标识 (IMEI)、全球可路由用户代理 URI(GRUU)、国际移动订户标识 (IMSI) 和临时国际移动订户标识 (TIMSI)。此外，所述一次性数是时间戳、随机数和序列号之一，并且所述安全参数是证书。

[0029] 在另一实施例中，提供了一种用于安全通信的方法，包括：(1) 接收一次性数、标识符和密钥分量两者中的至少一个、安全参数和签名，所述签名是使用私钥、所述一次性数、以及所述标识符和所述密钥分量两者中的至少一个来生成的；以及 (2) 使用接收到的签名和安全参数，验证所述一次性数以及所述标识符和所述密钥分量中的两者至少一个，其中，所述安全参数将用户标识与公钥相关联，所述公钥与所述私钥相关联。当在验证步骤中验证成功时，所述方法还包括 (1) 使用所述标识符和所述密钥分量中的至少一个来生成会话密钥；(2) 使用第二私钥、第二一次性数、以及第二标识符和第二密钥分量两者中的至少一个，生成第二签名；以及 (3) 发送所述第二签名、所述第二一次性数、第二安全参数、以及所述第二标识符和所述第二密钥分量两者中的至少一个，其中，所述第二安全参数将第二用户标识与第二公钥相关联，所述第二公钥与所述第二私钥相关联。

[0030] 在另一实施例中，提供了一种用于安全通信的方法，包括：(1) 使用 MAC 密钥、一次性数、以及标识符和密钥分量两者中的至少一个，生成 MAC 标签；以及 (2) 发送所述 MAC 标签、所述一次性数、以及所述标识符和所述密钥分量两者中的至少一个。

[0031] 在另一实施例中，提供了一种用于安全通信的方法，包括：(1) 接收一次性数、标识符和密钥分量两者中的至少一个、以及 MAC 标签，所述 MAC 标签是使用所述一次性数、所述标识符和所述密钥分量两者中的至少一个以及 MAC 密钥生成的；以及 (2) 使用接收到的 MAC 标签，验证所述一次性数以及所述标识符和所述密钥分量两者中的至少一个。

[0032] 特别地，在一个实施例中，UE_j的 KGU 使用在制造时获得的私钥 PR_j对时间戳 Tα 和密钥分量 K_jP 签名。与私钥 PR_j相关联的公钥 Pu_j由证书 C_j保证，证书也可在制造时提供给 KGU。注意虽然公钥被描述为与证书分离，但通常公钥可以形成证书的一部分。

[0033] 图 4 提供了根据一个实施例的密钥分量保护方法的示意图。

[0034] 如图 4 所示，在使用函数 $S_j = Sig(K_jP, T\alpha, PR_j)$ 对 Tα 和 K_jP 签名后，每个 KGU 向软件不仅传递密钥分量 K_jP 和时间戳 Tα 还传递签名 S_j、公钥 Pu_j和证书 C_j，以在 SIP 上发送。注意，由于 KGU 通常以硬件实现，预期 KGU 对恶意用户的篡改显著地更加鲁棒。此外，通过向 SIP 传递 S_j、Pu_j和 C_j以发信号通知，进行接收的 UE 和网络都能够确信在生成时 K_{sess} 使用的时间戳 Tα。

[0035] 虽然必须在密钥生成过程期间验证UE_1和UE_2所发送的密钥分量和时间戳，验证实体优选是KGU或UE的某个其他实体。此外，网络CSCF设备也可执行该验证。然而，运营商可能优选不验证每个密钥交换，并且取而代之地将这样的检查推送至UE而不在网络内执行该任务（除了对于合法拦截保证），以减轻网络负载。当时间戳验证失败时，连接尝试可由失败发生的验证实体终止。如果UE由于失败的验证拒绝连接，可以向网络发信号通知警报，例如，作为将违反UE列入黑名单的第一步。

[0036] 图5示出了根据一个实施例的密钥分量保护方法中的步骤。

[0037] 在步骤501中，UE_1的KGU生成密钥分量K_1和签名S_1。

[0038] 在步骤502中，UE_1在SIP首部向设备$CSCF_1$发送$(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$。

[0039] 在步骤503中，除了向设备$CSCF_2$转发$(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$，设备$CSCF_1$还存储$(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$的拷贝。

[0040] 在步骤504中，在合法拦截需要的情况下，设备$CSCF_2$存储$(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$的拷贝。设备$CSCF_2$还向$UE_2$转发$(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$。

[0041] 在步骤505a中，UE_2接收$(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$并检查签名$S_1$。如果签名得到验证，$UE_2$在步骤505b中计算会话密钥$K_{sess}=K_1K_2P$。接着，前进至步骤506。否则，连接被拒绝，并且密钥协商协议被终止。

[0042] 在步骤506中，UE_2的KGU生成密钥分量K_2和签名S_2。

[0043] 在步骤507中，UE_2在SIP首部中向设备$CSCF_2$发送$(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$。

[0044] 在步骤508中，除了向设备$CSCF_1$转发$(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$，设备$CSCF_2$还存储$(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$的拷贝。

[0045] 在步骤509中，在合法拦截需要的情况下，设备$CSCF_1$存储$(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$的拷贝。设备$CSCF_1$还向$UE_1$转发$(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$。

[0046] 在步骤510a中，UE_1接收$(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$并检查签名$S_2$。如果签名得到验证，$UE_1$在步骤510b中计算会话密钥$K_{sess}=K_1K_2P$，并且受保护的通信开始。否则，连接被拒绝，并且密钥协商协议被终止。

[0047] 注意，该实施例包括对在密钥生成中使用的参数进行签名，因此不限于以上讨论的MIKEY-IBAKE密钥协商协议的示例情形。该实施例可扩展至当前针对IMS媒体安全考虑的其他密钥协商协议，如MIKEY-TICKET和会话描述协议安全描述(SDES)。

[0048] 类似地，签名的参数无需是时间戳并且无需在两个UE中相同。例如，每个UE在生成密钥信息K_j时可以使用其自身特定的一次性数值，一次性数值由UE签名并以某种形式通过网络向目标UE发信号通知。一次性数值上的签名将使其能够得到验证，类似于以上讨论的时间戳。一次性数可以是例如时间戳、随机数或序列号。

[0049] 在另一实施例中，为了保护IMEI的完整性，UE的硬件部分对一次性数和IMEI签名。一次性数N_i可以是例如随机生成的或者是以SIP发信号通知的时间戳$T\alpha$。如图6所示，取代单独发信号通知IMEI，协议包含元素$IMEI_i$、N_i和$[S_i\ Pu_i\ C_i]$，其中，在扩展字段中携带附加信息N_i和$[S_i\ Pu_i\ C_i]$。

[0050] 类似于密钥生成中的情形，$IMEI_i$的完整性保护可由多个实体（如LEA_1、LEA_2、UE_2或任意网络（包括任一CSCF设备））中的任一个验证。如上讨论的，优选地，这样的检查是由UE执行的，并且在验证失败的情况下拒绝连接。

[0051] 如果UE由于失败的验证拒绝连接，可以向网络发信号通知警报，例如，作为将可能假冒的UE列入黑名单的第一步。由于验证信息（$IMEI_i$、N_i和$[S_i\ Pu_i\ C_i]$）存储在CSCF设备中，网络还具有再次确认这样的警报的手段，作为确定假冒UE的另一步骤。

[0052] 在另一实施例中，取代使用签名机制，每个KGU从MAC密钥计算消息认证码（MAC）标签。如图7所示，图4的实施例中使用的签名、公钥和证书被所计算的MAC标签代替。

[0053] 注意，由于使用MAC标签实质上相当于对称密钥签名方案，与给定UE网络相关联的拦截设备和UE的对应KGU必须首先对用以计算MAC标签的MAC密钥（$KMAC_i$）达成一致，如图7所示。注意，该实施例在复杂度上优于图4所示的实施例，这是由于生成MAC标签比生成数字签名便宜。

[0054] 然而，该实施例的一个缺点在于仅UE的当前网络的拦截功能存储验证UE_i的MAC标签所需的MAC密钥$KMAC_i$。因此，可以仅在直接服务UE的CSCF设备中需要存储MAC标签。此外，UE_2可以不再验证UE_1的时间戳（反之亦然）。换言之，LEA_1的拦截设备是UE_1外部的能够验证MAC_1作为针对$[K_1P, T\alpha]$计算的MAC标签的唯一实体。

[0055] 图4的实施例通过将椭圆曲线Diffie-Hellman(ECDH)密钥分量K_iP绑定至在导出K_i时使用的时间戳来实现合法拦截的目标。在其他备选方法中，该绑定可以不同方式实现。

[0056] 例如，在第一备选方法中，会话密钥可使用以ECDH生成的密钥和两个时间戳（一次性数）作为输入的密钥导出函数（KDF）来导出。

[0057] 在第二备选方法中，两个时间戳作为标量与ECDH生成的密钥相乘。例如，UE_2在检查$T\alpha_1T\alpha_2K_2 \bmod n \neq 1$后计算$K_{sess} = T\alpha_1T\alpha_2K_1K_2P$，其中n是组顺序，即P的顺序。

[0058] 第三备选方法是在会话密钥计算中并入两个时间戳（此处称为$T\alpha_1$和$T\alpha_2$）的椭圆曲线Menezes-Qu-Vanstone(ECMQV)的略微修改的版本。时间戳也被看作一次性数。由于不在SIP上发信号通知签名，该方法带宽效率更高，并且与时间戳签名验证方法相比计算效率更高。

[0059] 在第三备选方法中，UE_2具有长期密钥(d_2, Pu_2)，其中，Pu_2在UE_2的证书C_2中。此处d_2可以通过KDF从KM_2导出，这是由于LEA_2能够计算它。备选地，d_2可以是通过KDF以及k_2导出的另一暂时数。

[0060] 接着，UE_2的KGU中的计算顺序如下：

[0061] (1)$k_2 = f(KM_2, T\alpha_2)$；（与如图2中计算的K_2相同）

[0062] (2)$G_2 = k_2P$；（如前，此处ECMQV开始）

[0063] (3)$s_2 = k_2 + T\alpha_2x(G_2)d_2 \pmod n$；(ECMQV加上了$T\alpha_2$)

[0064] (4)UE_2向UE_1发送$[G_2, T\alpha_2, C_2]$并且UE_2从UE_1接收$[G_1, T\alpha_1, d]$；

[0065] 5)$K_{sess} = hs_2(G_1 + [T\alpha_1x(G_1)]Pu_1)$；(ECMQV加上了$T\alpha_1$)

[0066] 注意，当计算s_2时，UE_2检查$T\alpha_2x(G_2) \bmod n \neq 1$，否则过程返回步骤1。此外，当计算$K_{sess}$时，$UE_2$检查$T\alpha_1x(G_1) \bmod n \neq 1$，否则过程中止。

[0067] 如果UE_2尝试在SIP上发信号通知与$T\alpha_2$不同的$T\alpha_2'$，会话密钥将不会正确建立。这向LEA_2确保了$T\alpha_2$是在KGU_2内的计算中使用的。额外检查由LEA_2执行：(1)$k_2' = f(KM_2, T\alpha_2)$，并且(2)检查$G_2' = k_2'P$等于$G_2$。

[0068] 此外，注意上述第二和第三备选方法均需要对密钥协议本身进行一些修改，因此

可能要求对 3GPP 内在先协定的较大改变。

[0069] 上述实施例具有若干优点：它们 (1) 能够使用 MAC 标签或签名确保密钥信息和 UE 标识符信息的完整性保护；(2) 能被用于拒绝其他 UE 连接和 / 或报告恶意 UE；(3) 能够被网络用作将假冒或危险 UE 列入黑名单的手段；以及 (4) 如果目标 UE 或 KGU 是验证实体，实施例不对网络施加显著负载，从而减少了网络实现忧虑。

[0070] 设备 $CSCF_1$ 和 $CSCF_2$ 以及 LEA_1 和 LEA_2 的拦截设备能由一个或多个计算机和 / 或一个或多个专用电路实现。参照图 8 描述这样的计算机的硬件描述。此外，每个 UE 包括一个或多个处理器 (例如 CPU)、存储器、显示器以及通信接口。处理器被配置为执行软件，以执行上述 UE 的功能。上述 KGU 可实现为专用硬件电路或在一个或多个处理器上执行的软件。

[0071] 如图 8 所示，处理数据和指令可以存储在存储器 302 中。这些过程和指令还可以存储在存储介质盘 304(如硬盘 (HDD) 或便携式存储介质) 或者可以远程存储。此外，要求保护的进步不限于存储了本发明过程的指令的计算机可读介质的形式。例如，指令可以存储在 CD、DVD 上，闪存、RAM、ROM、PROM、EPROM、EEPROM、硬盘或计算机与之通信的任意信息处理设备 (如服务器) 上。

[0072] 此外，要求保护的实施例可以被提供为实用应用、后台守护程序或操作系统组件或其组合，结合 CPU 300 和操作系统 (如 Microsoft Windows 7、UNIX、Solaris、LINUX、Apple MAC-OS 和本领域技术人员已知的其他系统) 执行。

[0073] CPU 301 可以是美国 Intel 的 Xenon 或 Core 处理器，美国 AMD 的 Opteron 处理器，或者可以是本领域技术人员认识的其他处理器类型。备选地，如本领域技术人员将意识到的，CPU 301 可以实现在 FPGA、ASIC、PLD 上或使用分立逻辑电路实现。此外，CPU 301 可以实现为并行协同工作以执行上述本发明过程的指令的多个处理器。

[0074] 图 8 中的计算机还包括网络控制器 306(如，美国 Intel 公司的 Intel Ethernet PRO 网络接口卡)，用于与网络 399 接口。如可理解的，网络 399 可以是公共网络 (互联网) 或私有网络 (LAN 或 WAN 网络) 或其任意组合，并且还可以包括 PSTN 或 ISDN 子网。网络 399 还可以是有线的 (如以太网) 或者可以是无线的 (如蜂窝网络，包括 EDGE、3G 和 4G 无线蜂窝系统)。无线网络还可以是 WiFi、蓝牙或任意其他已知的无线通信形式。网络控制器 306 可用于在两方之间建立通信信道 (可能通过网络 399)。

[0075] 计算机还包括显示控制器 308，如，用于与显示器 310(如 Hewlett Packard HPL2445w LCD 监视器) 接口的显示器控制器 308(如美国 NVIDIA 公司的 NVIDIA GeForce GTX 或 Quadro 图形适配器)。通用 I/O 接口 312 与键盘和 / 或鼠标 514 以及显示器 310 上或与其分离的触摸屏面板 316 接口。通用 I/O 接口还连接至各种外围设备 318，包括打印机和扫描仪，如 Hewlett Packard 的 OfficeJet 或 DeskJet。

[0076] 还在计算机中提供声音控制器 320，如 Creative 的 Sound Blaster X-Fi Titanium，以与扬声器 / 麦克风 322 接口，从而提供声音和 / 或音乐。扬声器 / 麦克风 322 还可用于接受口述单词作为用于控制计算机或用于提供位置和 / 或关于目标属性的属性信息的命令。

[0077] 通用存储控制器 324 将存储介质盘 304 与通信总线 326 连接，其可以是 ISA、EISA、VESA、PCI 等，用于互连计算机的所有组件。此处省略对显示器 310、键盘和 / 或鼠标 314 以及显示控制器 308、存储控制器 324、网络控制器 306、声音控制器 320 和通用 I/O 接口 312

的一般特征和功能的描述，这是由于这些特征是已知的。

[0078] 在以上描述中，流程图中的任何过程、描述或框应理解为代表包括用于实现过程中的特定逻辑功能或部分的代码模块、段或部分，并且备选实施例包括在本进步的示例实施例的范围内，其中，可以不按所示或所讨论的顺序执行功能，根据所涉及的功能，包括基本上同时或按相反顺序，如本领域技术人员将理解的那样。

[0079] 虽然描述了特定实施例，这些实施例仅作为示例示出，而不意在限制发明的范围。相反，此处描述的新颖的方法、装置和系统可以各种其他形式实现；此外，可以在不背离本发明精神的前提下做出此处描述的方法、装置和系统的形式的各种省略、替换和改变。所述权利要求及其等效物意在覆盖诸如落入本发明范围和精神范围内的形式或修改。

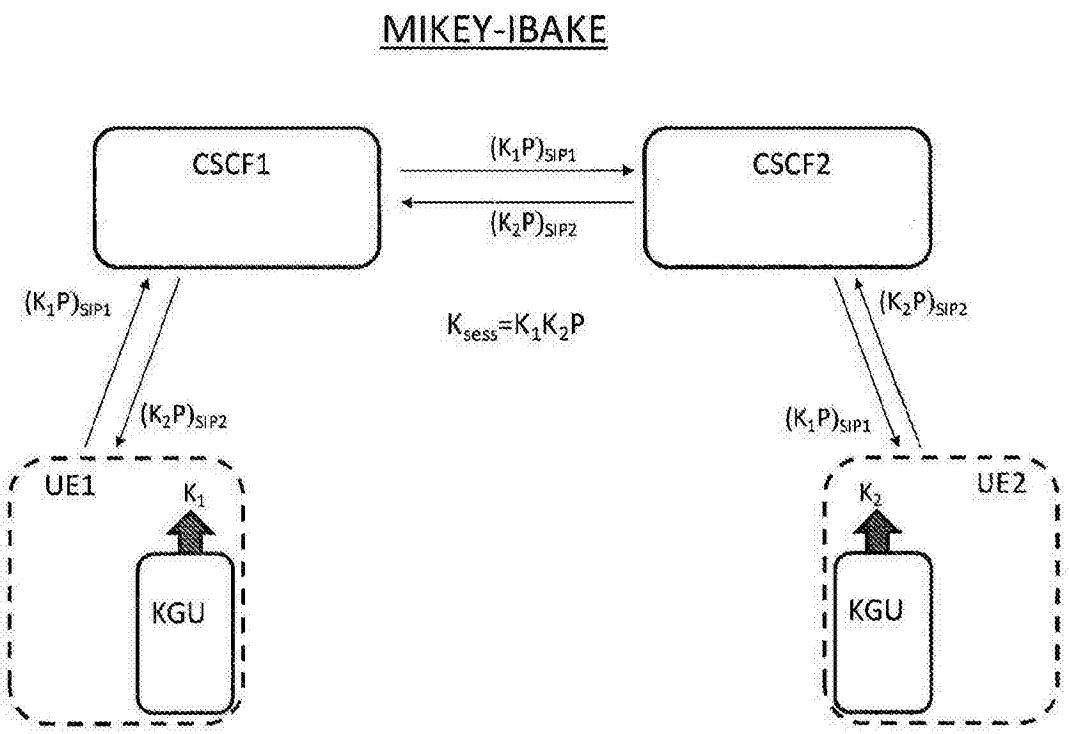

MIKEY-IBAKE
CSCF1
CSCF2
$(K_1P)_{SIP1}$
$(K_2P)_{SIP2}$
$K_{sess}=K_1K_2P$
UE1
UE2
K_1
K_2
KGU
KGU

图 1

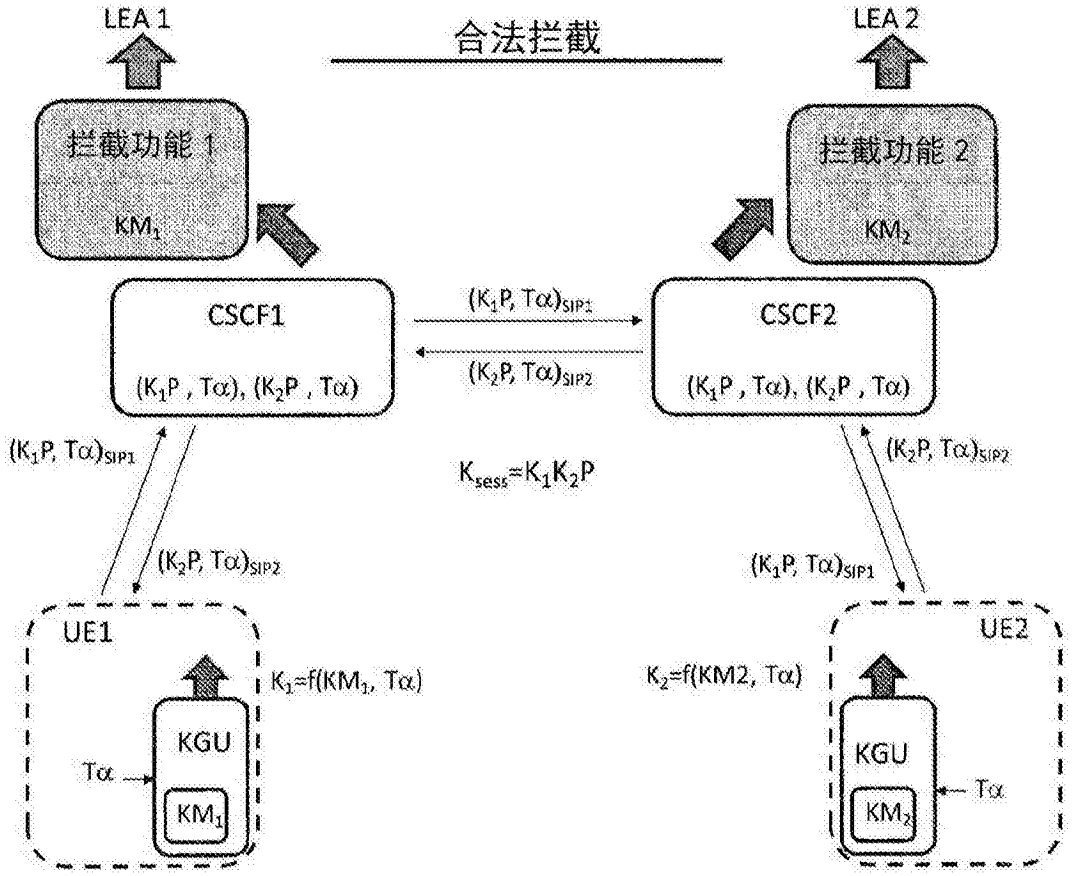

LEA 1
合法拦截
LEA 2
拦截功能 1
KM1
拦截功能 2
KM2
CSCF1
(K1P , Tα), (K2P , Tα)
(K1P, Tα)SIP1
(K2P, Tα)SIP2
CSCF2
(K1P , Tα), (K2P , Tα)
Ksess=K1K2P
(K1P, Tα)SIP1
(K2P, Tα)SIP2
(K2P, Tα)SIP2
(K1P, Tα)SIP1
UE1
K1=f(KM1, Tα)
KGU
Tα
KM1
K2=f(KM2, Tα)
UE2
KGU
KM2
Tα

图 2

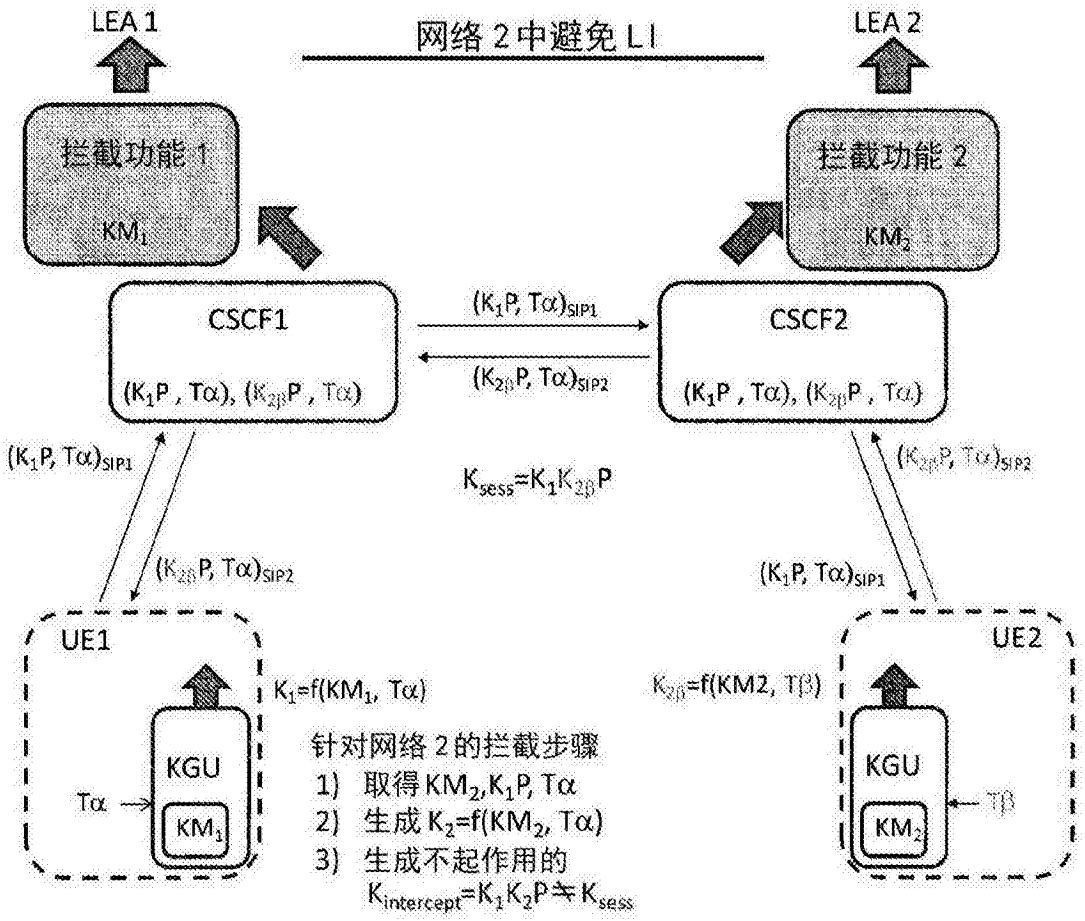

LEA 1
网络 2 中避免 LI
LEA 2
拦截功能 1
KM1
拦截功能 2
KM2
CSCF1
(K1P , Tα), (K2βP , Tα)
(K1P, Tα)SIP1
(K2βP, Tα)SIP2
CSCF2
(K1P , Tα), (K2βP , Tα)
Ksess=K1K2βP
UE1
K1=f(KM1, Tα)
KGU
Tα
KM1
针对网络 2 的拦截步骤
1) 取得 KM2,K1P, Tα
2) 生成 K2=f(KM2, Tα)
3) 生成不起作用的
Kintercept=K1K2P≒Ksess
UE2
K2β=f(KM2, Tβ)
KGU
Tβ
KM2

图 3

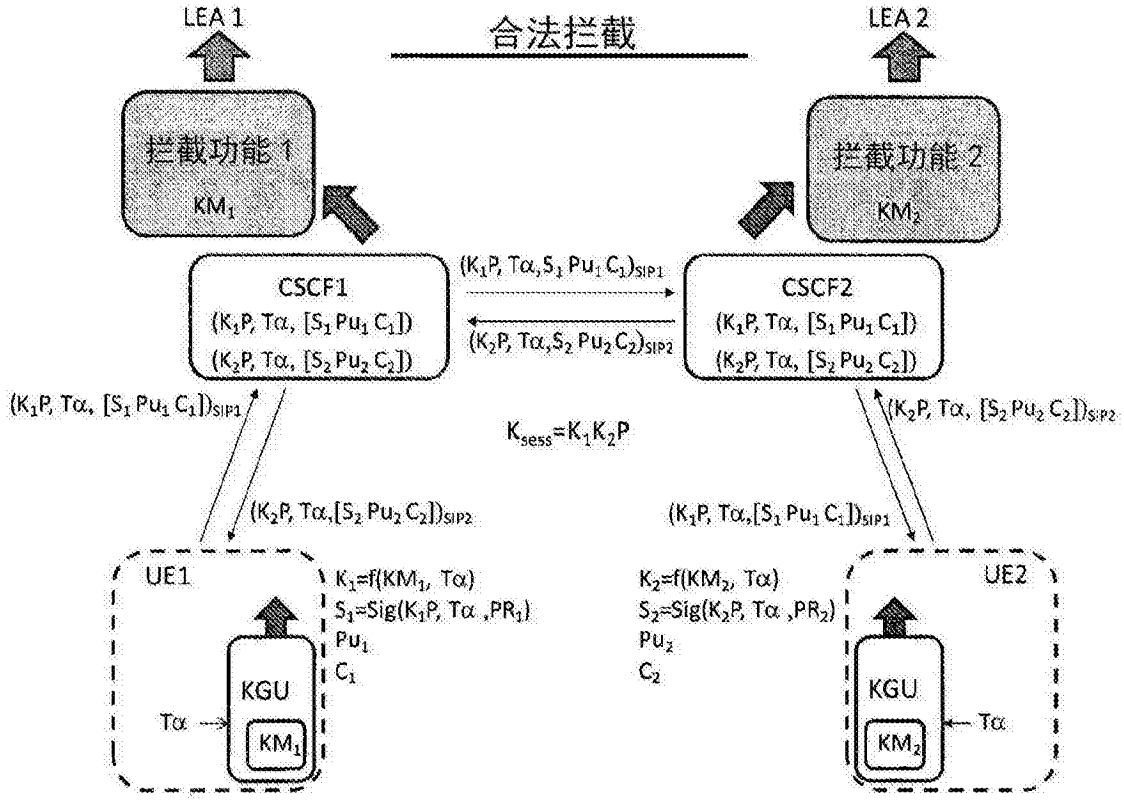

LEA 1
合法拦截
LEA 2
拦截功能 1
KM1
拦截功能 2
KM2
CSCF1
(K1P, Tα, [S1 Pu1 C1])
(K2P, Tα, [S2 Pu2 C2])
(K1P, Tα,S1 Pu1 C1)SIP1
(K2P, Tα,S2 Pu2 C2)SIP2
CSCF2
(K1P, Tα, [S1 Pu1 C1])
(K2P, Tα, [S2 Pu2 C2])
(K1P, Tα, [S1 Pu1 C1])SIP1
(K2P, Tα, [S2 Pu2 C2])SIP2
Ksess=K1K2P
(K2P, Tα,[S2 Pu2 C2])SIP2
(K1P, Tα,[S1 Pu1 C1])SIP1
UE1
K1=f(KM1, Tα)
S1=Sig(K1P, Tα ,PR1)
Pu1
C1
KGU
Tα
KM1
K2=f(KM2, Tα)
S2=Sig(K2P, Tα ,PR2)
Pu2
C2
UE2
KGU
Tα
KM2

图 4

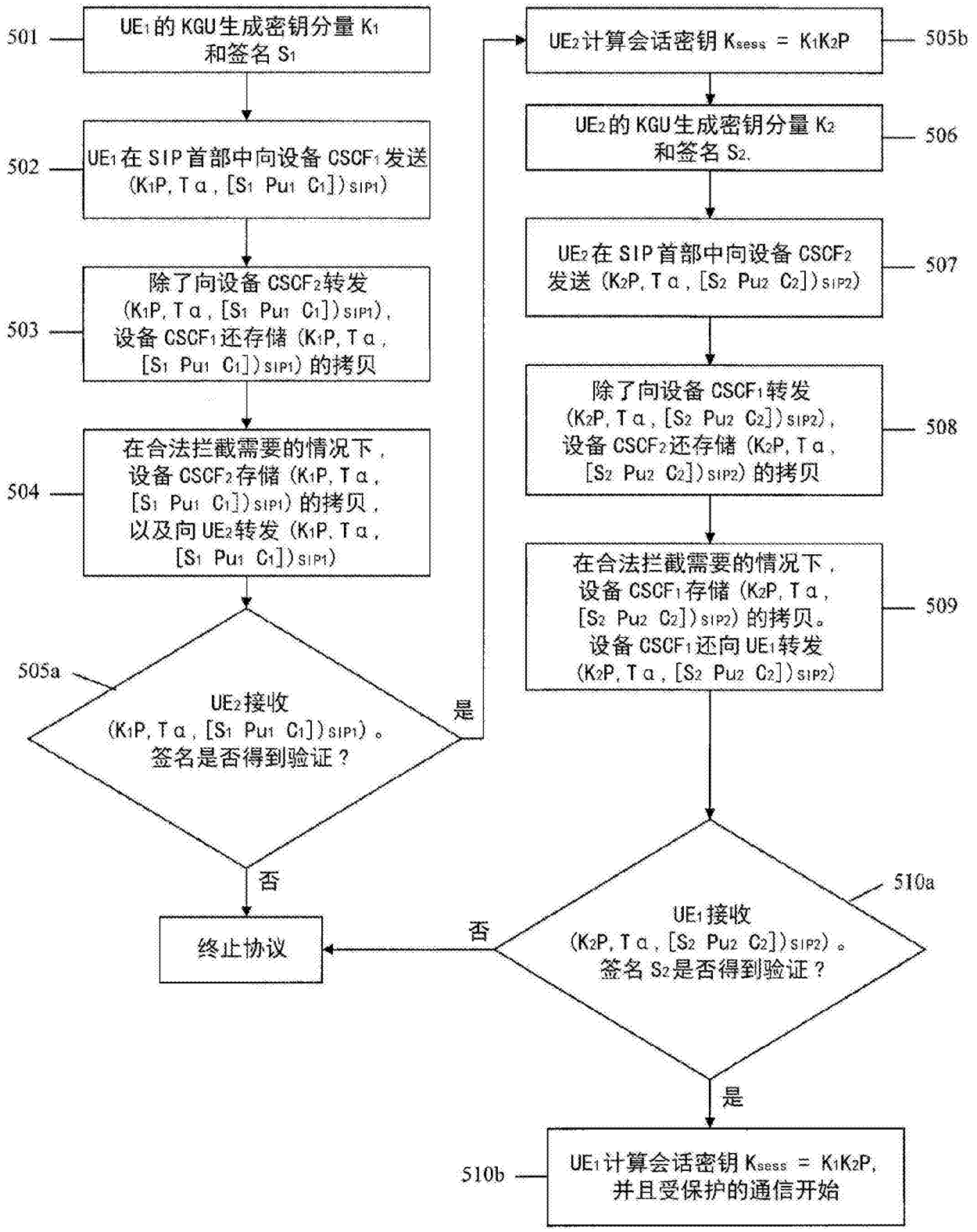

501
UE1的KGU生成密钥分量K1和签名S1
502
UE1在SIP首部中向设备CSCF1发送(K1P, Tα, [S1 Pu1 C1])SIP1)
503
除了向设备CSCF2转发(K1P, Tα, [S1 Pu1 C1])SIP1)，设备CSCF1还存储(K1P, Tα, [S1 Pu1 C1])SIP1)的拷贝
504
在合法拦截需要的情况下，设备CSCF2存储(K1P, Tα, [S1 Pu1 C1])SIP1)的拷贝，以及向UE2转发(K1P, Tα, [S1 Pu1 C1])SIP1)
505a
UE2接收(K1P, Tα, [S1 Pu1 C1])SIP1)。签名是否得到验证？
是
否
终止协议
505b
UE2计算会话密钥Ksess = K1K2P
506
UE2的KGU生成密钥分量K2和签名S2.
507
UE2在SIP首部中向设备CSCF2发送(K2P, Tα, [S2 Pu2 C2])SIP2)
508
除了向设备CSCF1转发(K2P, Tα, [S2 Pu2 C2])SIP2)，设备CSCF2还存储(K2P, Tα, [S2 Pu2 C2])SIP2)的拷贝
509
在合法拦截需要的情况下，设备CSCF1存储(K2P, Tα, [S2 Pu2 C2])SIP2)的拷贝。设备CSCF1还向UE1转发(K2P, Tα, [S2 Pu2 C2])SIP2)
510a
UE1接收(K2P, Tα, [S2 Pu2 C2])SIP2)。签名S2是否得到验证？
否
是
510b
UE1计算会话密钥Ksess = K1K2P，并且受保护的通信开始

图 5

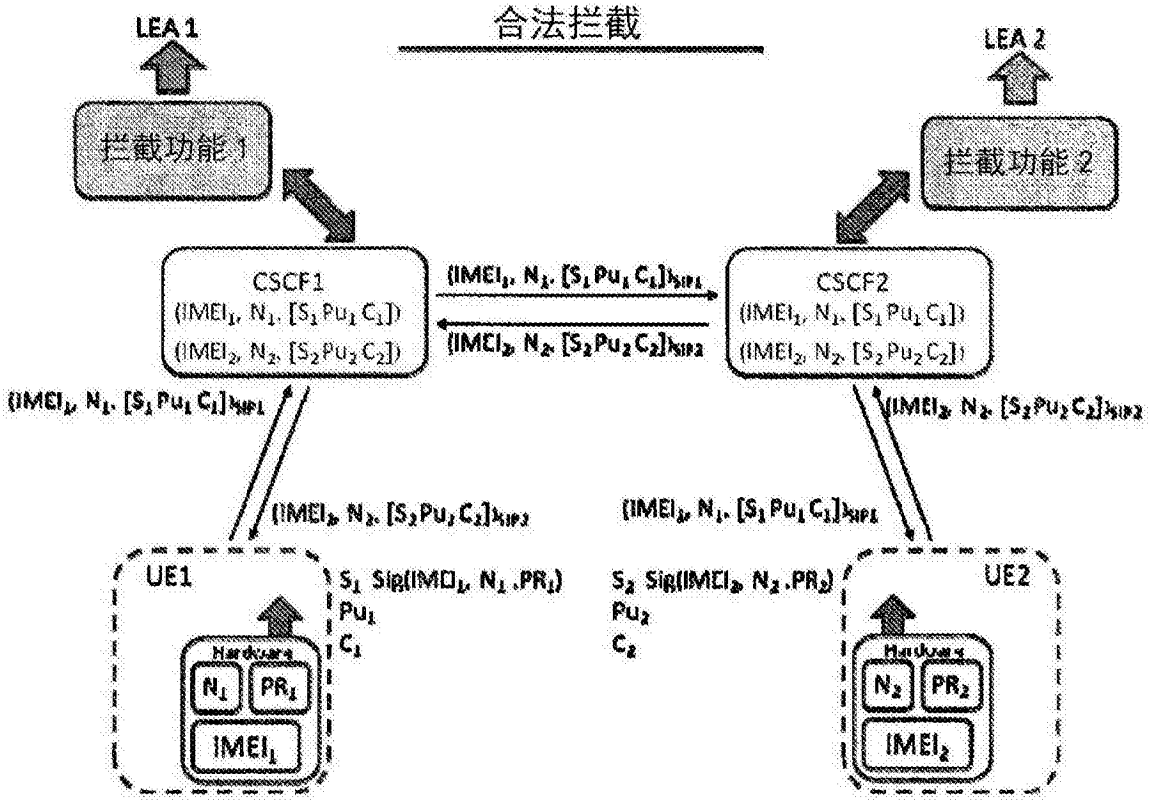

合法拦截
LEA 1
LEA 2
拦截功能 1
拦截功能 2
CSCF1
(IMEI1, N1, [S1 Pu1 C1])
(IMEI2, N2, [S2 Pu2 C2])
CSCF2
(IMEI1, N1, [S1 Pu1 C1])
(IMEI2, N2, [S2 Pu2 C2])
UE1
UE2
Hardware
N1
PR1
IMEI1
N2
PR2
IMEI2
S1 Sig(IMEI1, N1 ,PR1)
Pu1
C1
S2 Sig(IMEI2, N2 ,PR2)
Pu2
C2

图 6

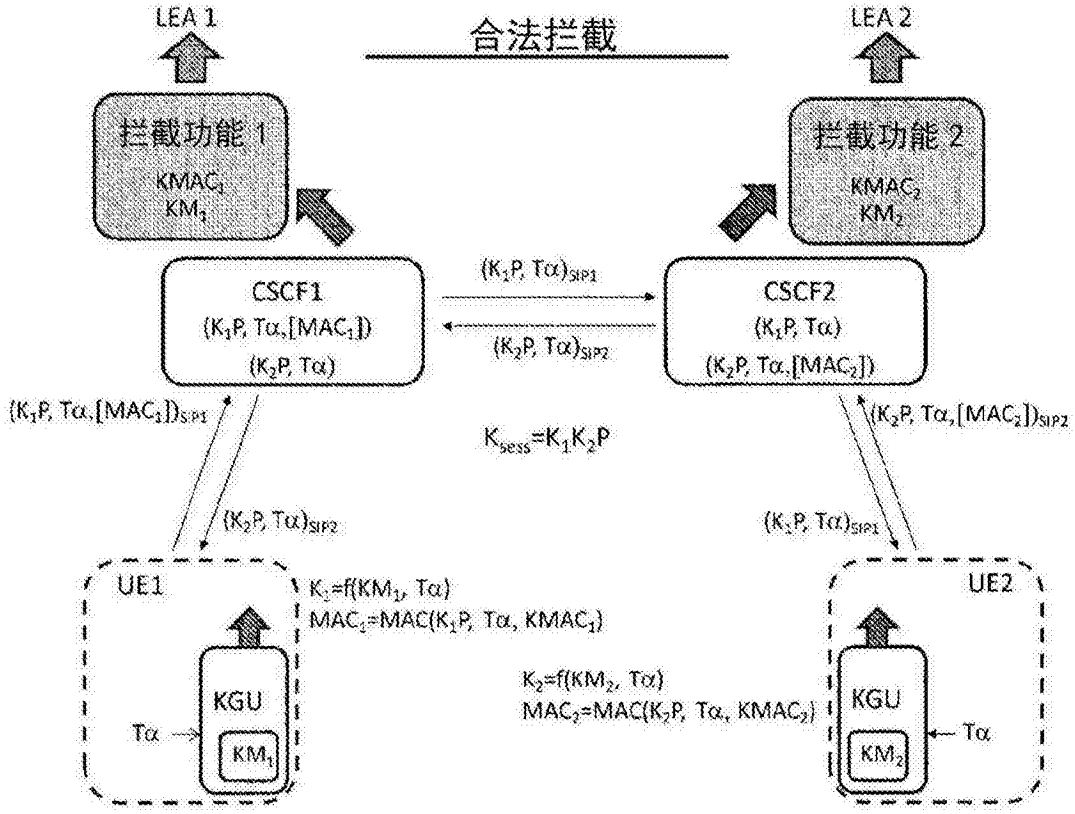

LEA 1
合法拦截
LEA 2
拦截功能 1
KMAC1
KM1
拦截功能 2
KMAC2
KM2
CSCF1
(K1P, Tα,[MAC1])
(K2P, Tα)
(K1P, Tα)SIP1
(K2P, Tα)SIP2
CSCF2
(K1P, Tα)
(K2P, Tα,[MAC2])
(K1P, Tα,[MAC1])SIP1
(K2P, Tα)SIP2
Ksess=K1K2P
(K2P, Tα,[MAC2])SIP2
(K1P, Tα)SIP1
UE1
K1=f(KM1, Tα)
MAC1=MAC(K1P, Tα, KMAC1)
KGU
Tα
KM1
K2=f(KM2, Tα)
MAC2=MAC(K2P, Tα, KMAC2)
UE2
KGU
Tα
KM2

图 7

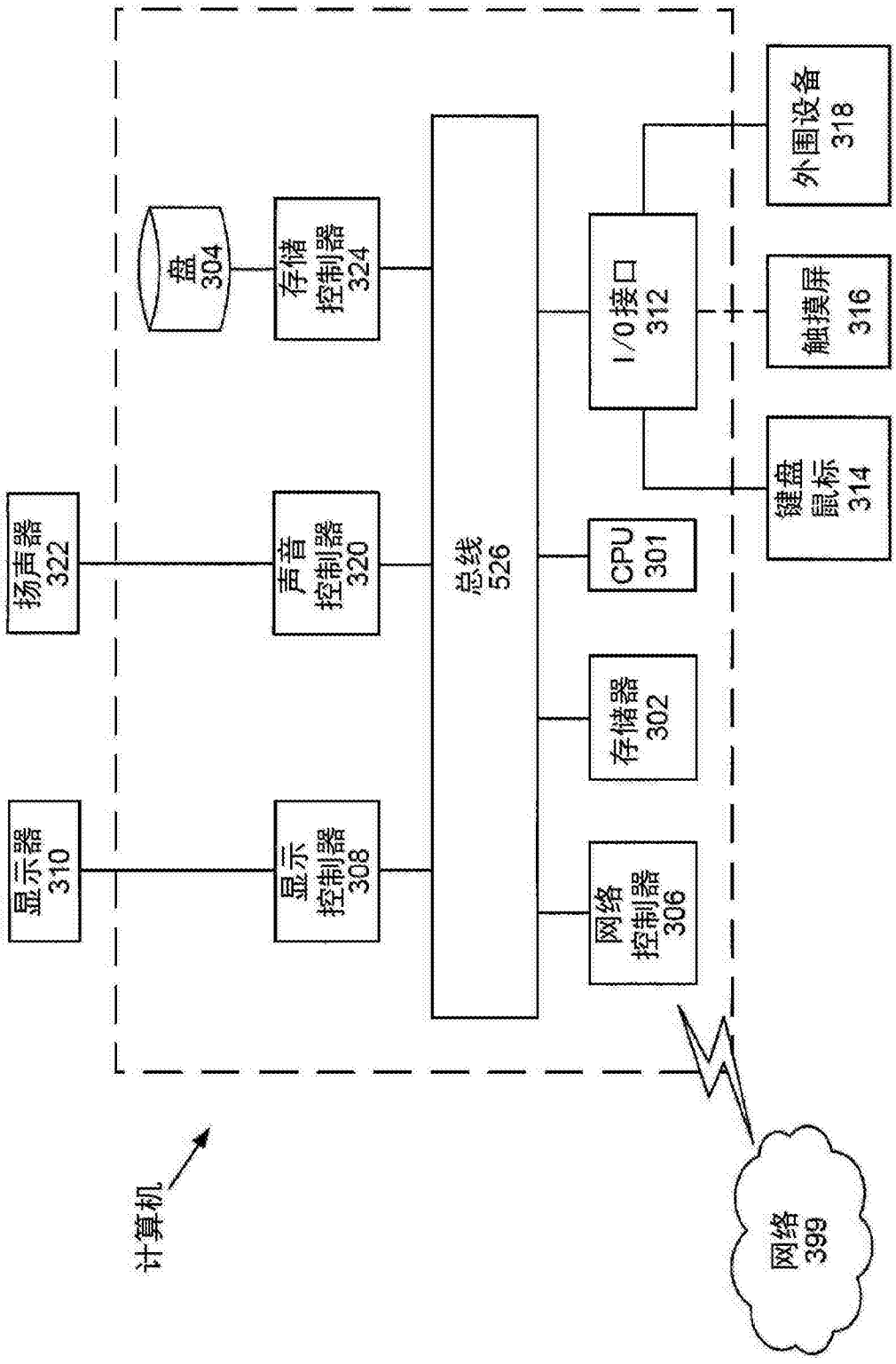

计算机
盘
304
存储
控制器
324
扬声器
322
声音
控制器
320
显示器
310
显示
控制器
308
总线
526
CPU
301
存储器
302
网络
控制器
306
I/O接口
312
外围设备
318
触摸屏
316
键盘
鼠标
314
网络
399

图 8