(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 102057617 B
(45)授权公告日 2013.12.25

(21)申请号 200880129636.9
(22)申请日 2008.07.21
(30)优先权数据
61/059,386 2008.06.06 US
(85)PCT申请进入国家阶段日
2010.12.03
(86)PCT申请的申请数据
PCT/EP2008/005960 2008.07.21
(87)PCT申请的公布数据
WO2009/146729 EN 2009.12.10
(73)专利权人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
(72)发明人 卡尔·诺曼 马茨·内斯隆德
(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 赵伟
(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/02(2006.01)
(56)对比文件
WO 2007/085779 A1,2007.08.02,
US 2008/0032669 A1,2008.02.07,
CN 101160779 A,2008.04.09,
审查员 李锦玲

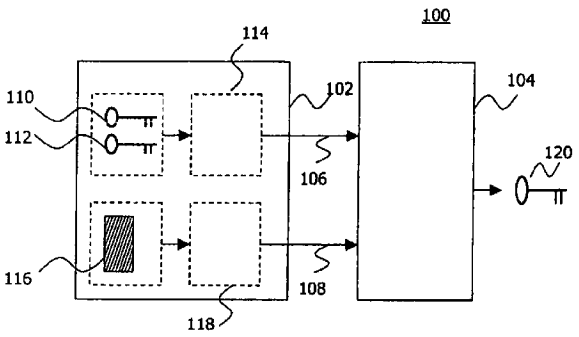
权利要求书2页 说明书10页 附图4页

(54)发明名称

加密密钥生成

(57)摘要

本发明提供了一种用于生成加密密钥(120)的技术。该技术尤其适用于保护协作运行分布式安全操作的两个实体(202、302;204、304)之间的通信。该技术包括:提供至少两个参数(106、108),第一参数(106)包括第一实体(202、302)通过运行该安全操作而计算的一些加密密钥(110、112),或者第一参数(106)是根据所述加密密钥(110、112)导出的;以及第二参数(108)包括令牌(116)或者是根据所述令牌(116)导出的,每次第二实体(204、304)针对所述第一实体(202、302)发起安全(114)操作时,所述令牌(116)具有不同的值。对所提供的参数(106、108)应用密钥导出函数,以生成所需的加密密钥(120)。



CN 102057617 B

1. 一种用于生成加密密钥 (120) 的方法，所述加密密钥用于保护两个实体 (202、204) 之间的通信，其中所述方法由第一实体 (202、302) 执行，作为由第二实体 (204、304) 发起的分布式安全操作的一部分，所述方法包括以下步骤：

- 提供 (306) 至少两个参数 (106、108)，其中，第一参数 (106) 包括所述第一实体 (202) 通过运行所述安全操作而计算的加密密钥集合 (110、112)，或者所述第一参数 (106) 是根据所述加密密钥集合导出的；以及第二参数包括令牌 (116) 或者是根据令牌 (116) 导出的，每次所述第二实体 (204、304) 针对所述第一实体 (202、302) 发起所述安全操作时，所述令牌 (116) 具有不同的值；以及

- 应用 (308) 密钥导出函数，以基于所提供的参数 (106、108) 来生成加密密钥 (120)；

其中所述令牌 (116) 包括序号 SQN 和匿名密钥 AK 的异或。

2. 根据权利要求 1 所述的方法，其中，所述 SQN 指示所述第二实体 (204、304) 已经针对所述第一实体 (202、302) 发起的所述安全操作的次数。

3. 根据权利要求 1 或 2 所述的方法，其中，所述令牌是以下各项的连接：所述 SQN 与所述匿名密钥 AK 的异或、认证和密钥管理字段 AMF 以及消息认证码 MAC。

4. 根据权利要求 1 或 2 所述的方法，其中，所述第一参数 (106) 中包括的所述加密密钥集合 (110、112) 或者用于导出所述第一参数 (106) 的所述加密密钥集合 (110、112) 包括密码密钥 CK(110) 和完整性密钥 IK(112)，或者是根据所述 CK 和所述 IK 导出的。

5. 根据权利要求 1 或 2 所述的方法，还包括以下步骤：

- 应用一个或更多其他密钥导出函数，以基于所生成的加密密钥 (120) 来生成更多加密密钥。

6. 根据权利要求 5 所述的方法，其中，所述更多加密密钥包括以下至少一项：

- 用于保护非接入层 NAS 业务的加密密钥集合；

- 用于保护无线资源控制 RRC 业务的加密密钥集合；

- 用于保护用户平面 UP 业务的加密密钥集合；以及

- 用于导出保护 RRC 业务的加密密钥和 / 或保护 UP 业务的加密密钥的中间加密密钥 K_{eNB}。

7. 根据权利要求 1 或 2 所述的方法，其中，所述第一实体 (202、302) 是用户设备。

8. 根据权利要求 1 或 2 所述的方法，其中，所述第二实体 (204、304) 是网络实体。

9. 根据权利要求 8 所述的方法，其中，所述第二实体 (204、304) 位于系统架构演进 SAE/ 长期演进 LTE 网络中。

10. 根据权利要求 8 所述的方法，其中，所述第二实体 (204、304) 包括认证中心 AuC/ 归属地订户服务器 HSS 和移动性管理实体 MME。

11. 根据权利要求 1 或 2 所述的方法，其中，所述安全操作是由所述第一实体 (202、302) 和第二实体 (204、304) 协作执行的。

12. 根据权利要求 1 或 2 所述的方法，其中，所述安全操作基于 UMTS 认证和密钥协商 AKA 协议。

13. 一种适于生成用于通信实体 (202、302) 的加密密钥的设备 (100)，所述通信实体适于运行安全操作，所述设备 (100) 包括：

- 第一组件 (102)，适于提供至少两个参数 (106、108)，其中，第一参数 (106) 包括所

述通信实体 (202、302) 通过运行所述安全操作而计算的加密密钥集合 (110、112)，或者所述第一参数是根据所述加密密钥集合 (110、112) 导出的；以及第二参数 (108) 包括令牌 (116) 或者是根据令牌 (116) 导出的，每次针对所述通信实体 (202、302) 发起所述安全操作时，所述令牌 (116) 具有不同的值；以及

- 第二组件 (104)，适于运行密钥导出函数，以基于所提供的参数 (106、108) 来生成加密密钥 (120)；

其中所述令牌 (116) 包括序号 SQN 和匿名密钥 AK 的异或。

14. 根据权利要求 13 所述的设备，其中，所述 SQN 指示已经针对所述通信实体 (202、302) 发起所述安全操作的次数。

15. 根据权利要求 13 或 14 所述的设备 (100)，其中，所述第一参数 (106) 中包括的所述加密密钥集合 (110、112) 或者用于导出所述第一参数 (106) 的所述加密密钥集合 (110、112) 包括密码密钥 CK(110) 和完整性密钥 IK(112)，或者是根据 CK 和 IK 导出的，所述 CK 和所述 IK 是所述通信实体 (202、302) 作为所述安全操作的一部分来计算的。

16. 根据权利要求 13 或 14 所述的设备 (100)，还适于：应用一个或更多其他密钥导出函数，以基于所生成的加密密钥 (120) 来生成更多加密密钥。

17. 一种用户设备 (202)，包括根据权利要求 13 至 16 中任一项所述的设备 (100)。

18. 一种系统，包括根据权利要求 17 所述的用户设备 (202、302) 和网络实体 (304)。

19. 根据权利要求 18 所述的系统，其中，所述网络实体 (304) 用于 SAE/LTE 网络。

加密密钥生成

技术领域

[0001] 本发明总体涉及用于生成加密密钥的技术。具体地，本发明涉及提供高等级安全性的加密密钥生成技术。

背景技术

[0002] 认证和密钥协商协议 (AKA) 是一种基于质询 - 响应的、使用对称加密的协议。AKA 的主要目的包括两个彼此通信的实体进行互相认证以及建立用于保护其间交换的通信的加密密钥。AKA 的一个变型是 UMTS AKA，包括在技术规范 3G TS 33.102 中由 3GPP 针对 3G 移动通信网络而标准化的安全架构中。

[0003] UMTS AKA 的基本概念如图 1 所示。参照该图，UMTS AKA 协议在用户设备 (UE) 与网络实体 (NE) 之间运行。网络实体通过向 UE 发送用户认证请求来发起 AKA。将随机质询或随机码 (RAND) 和认证令牌 (AUTN) 与该请求一起发送至 UE。在接收到 RAND 和 AUTN 时，UE 计算密码密钥 (CK) 和完整性密钥 (IK) 等等，然后使用 CK 和 IK 用于密码处理和完整性功能。

[0004] 3GPP 还在进行所谓“超 3G”通信网络的标准化。系统架构演进 (SAE) 和长期演进 (LTE) 是超 3G 网络的两个密切相关的方面。与传统 3G 网络相比，基于 SAE/LTE 的网络可以施加更高和 / 或更多安全要求。例如，可能需要以不同等级来保护通信的更多加密密钥。在另一标准相关文献 3GPP TR 33.821 中，3GPP 推荐了一种密钥层级，用于导出在 SAE/LTE 中使用的更多加密密钥。

[0005] 图 2 示出了这种密钥层级。在该层级的最顶部是密钥 K，密钥 K 是在 UE 的全球订户标识模块 (USIM) 与位于网络中的认证中心 (AuC) 之间共享的长期加密密钥。向下一级是一对加密密钥 CK 和 IK，CK 和 IK 是由 UE (具体由 UE 的 USIM) 以与上述 UMTS AKA 操作相同或相似的方式导出的。该层级中的再下一级是密钥 K_{ASME}，密钥 K_{ASME} 是由 UE 从 CK、IK 以及 (如果需要) 一些其他参数导出的。一旦导出，就将 K_{ASME} 从 AuC 传送至接入网，具体而言传送至 SAE/LTE 网络的接入安全管理实体 (ASME)，然后在 UE 与网络之间共享。当接入网是基于 LTE 技术时，ASME 的功能由移动性管理实体 (MME) 来处理。

[0006] 可以通过应用特定加密函数来导出密钥 K_{ASME} 以及该层级中位于其“下层”的密钥。例如，

[0007] K_{ASME} = KDF(CK ‖ IK, 0x02 ‖ PLMN_ID ‖ <other_parameter>)

[0008] 其中 KDF 基于通用自举架构 (GBA) 密钥导出函数 (KDF)。在 3G TS33.220 中规定了一个 GBA KDF。

[0009] GBA KDF 可以利用加密散列函数，如安全散列算法 (SHA) 散列函数。在许多 SHA 散列函数中，SHA-256 是一种高度安全的变型，因为它被认为能够防冲突并且如伪随机函数一样工作。顾名思义，SHA-256 是具有 256 比特摘要 (输出) 长度的安全散列算法散列函数。PLMN_ID 是向 UE 提供服务的网络的标识符。

[0010] 已经认识到，为了实现高等级安全性，GBA KDF 函数仅仅主要基于 CK 和 IK 是不够

的。其原因在于以下风险：给定 UE 可能两次得到相同 CK，或者两个不同 UE 可能得到相同 CK。在这种情况下，破坏了对 KDF 的输入的“唯一性”，不同 UE（使用相同 K_{ASME}）之间可能发生冲突。

[0011] 总而言之，尽管如果 x = y，则 KDF(x) 肯定产生与 KDF(y) 相同的密钥，但是反之则可能不一定成立。即，即使 x ≠ y，仍可能发生 KDF(x) = KDF(y)。然而，由于建议 KDF 基于 SHA-256，如上所述，SHA-256 被设计为能够防冲突，因此这是不太可能发生的事件。因此，对于本文描述的技术，可以安全的假定：当且仅当 x = y，KDF(x) = KDF(y)。这种假定允许本文描述的技术集中关注确保对 KDF 的输入的“唯一性”。

[0012] GBA KDF 规范的标准化团体 (ETSI/SAGE，特别算法专家组）已经注意到上述问题，并建议将 UE 的私有用户标识 (IMPI) 包括在 <other_parameter> 中，以避免不同 UE 之间的冲突。作为另一建议，还可以将随机码（如 RAND) 包括在 <other_parameter> 中。这在从 ETSI/SAGE 至 3GPP SA3 的联络函（在 3GPP 文献中编号 S3-030219) 中进行描述。

[0013] 然而，已经发现，上述建议仍不能保证对 KDF 的输入的“唯一性”。从以下对 GBA KDF 函数的安全属性及其在 SAE/LTE 中针对同一 UE（例如同一 IMPI) 的使用的分析中可以看出这一点。

[0014] 首先，考虑以下基本构造：

[0015] KDF(CK，IMPI)

[0016] 由于已经假定 IMPI = IMPI’（当 UE 固定时），当且仅当 CK = CK’时，该基本构造将导致两个输入 (CK，IMPI)、(CK’，IMPI’) 的冲突。

[0017] 其次，考虑另一构造，该构造更接近实际 GBA KDF：

[0018] KDF(CK ‖ IK，IMPI)

[0019] 然而，与起初可能认为的不同，将 IK 包括在输入中不改变上述冲突属性。即，当且仅当 CK = CK’时，KDF(CK ‖ IK，IMPI) 将等于 KDF(CK’ ‖ IK’，IMPI)。为了理解包括 IK 为何无用，需要考虑在 UE 上执行的加密算法如何生成 CK 和 IK。

[0020] 典型的 UE 侧加密算法是如图 9 所示的 Milenage 算法。在图 9 中，Ek 表示高级加密标准 (AES) 算法，也称为 Rijndael 算法，使用密钥 K（存储在 AuC 和 UE 的 USIM 中）。现在考虑如果 CK = CK’将发生何种情况。由于 AES 是一种置换 (permutation，一对一映射），这意味着，中间值（在宽箭头处出现）由 f3 的结果（正巧为 CK) 唯一确定。但是，这意味着，在产生 CK 时，宽箭头处的值必须与产生 CK’时在相同位置出现的值相同。这继而意味着，作为对 f4 的输入而出现的值必须相同，因此，相同的 f4 值必须出现。恰好 f4 是 IK。因此，已经示出，当且仅当 IK = IK’时，CK = CK’。

[0021] 接下来，考虑根据标准化团体 (SAGE) 的建议的一种“改进”构造，即将 RAND 包括在输入中：

[0022] KDF(CK ‖ IK，RAND ‖ IMPI)

[0023] 假定 CK = CK’（从而 IK = IK’)。希望使用 RAND 将保证唯一性。然而并非如此。再次考虑 Milenage 算法中根据 RAND 来产生 CK 和 IK 的“相关”部分：如图 9 所示，存在以下情形，在宽箭头处与 RAND 相对应的值与对应于 RAND’的值相同。但是再次，AES(Ek) 是一种置换，使得输入必须也相等，即 RAND = RAND’。（因为假定固定 UE，并且因此在两种情况下都将出现相同的 K，因此 AES 依赖于 K 的事实无济于事。）

[0024] 换言之，已经示出，当且仅当 RAND = RAND' 时，(CK‖IK，RAND‖IMPI) = (CK'‖IK'，RAND'‖IMPI)。在 SAE/LTE 的情况下，输入中也可以包括 PLMN_ID，但是由于 UE 很可能保持在相同网络中多次，因此不能依赖于该参数 PLMN_ID 来实现保证唯一性的目的。

[0025] 尝试避免冲突的一种备选方式可以是使用不同于 AES 的另一算法来进行 f3 和 f4 算法的加密处理。具体地，上述分析基于 AES 是置换的事实。因此可以使用非置换（多对一映射）来取代 AES。由于两个原因，这是有问题的。首先，必须将现有 USIM 调整为适合 3GPP SAE 架构。其次，通过选择非置换函数，实际上增大了例如 f3 的两个输出相冲突的概率。

[0026] 缺乏输入唯一性可能是一个严重的安全问题。由于当且仅当 RAND = RAND'时，将出现冲突，并且由于 RAND 是 128 比特，预期该冲突将在约 2^(128/2) = 2^64 次认证之后出现（这是所谓的“生日悖论”）。显然，这低于 GBA(128 比特）的目标安全等级。对于 LTE，情况甚至更糟，因为需要 LTE 提供 256 比特的安全等级。因此，高冲突概率是在 SAE/LTE 中提供所需安全等级的重大障碍。

发明内容

[0027] 相应地，需要一种避免上述冲突的方案。该方案还应当理想地与已经部署的 USIM 一起工作，并且不需要替换所有 USIM。

[0028] 根据第一方面，提供了一种用于生成加密密钥的方法。加密密钥用于保护两个实体之间的通信等等。该方法由第一实体执行。该方法形成由第二实体发起的分布式安全操作的一部分。该方法包括：提供至少两个参数，其中，第一参数包括第一实体通过运行该安全操作而计算的加密密钥集合，或者第一参数是根据所述加密密钥集合导出的；以及第二参数包括令牌或者是根据令牌导出的，每次第二实体针对第一实体发起安全操作时，所述令牌具有不同的值（换言之，对于任何两次安全操作，该令牌的值永不相同）；以及应用密钥导出函数，以基于所提供的参数来生成加密密钥。

[0029] 表述“参数包括 X”可以意味着具有字符串格式的变量 X 形成该参数或该参数的一部分。表述“参数是根据 X 导出的”可以意味着该参数是将特定函数（如数学函数）至少应用至变量 X 的结果。函数的示例包括但不限于：算术运算、逻辑运算、字符串运算、及其任何组合。算术运算可以是加法、减法、乘法等等，及其任何有意义的组合。逻辑运算可以是与 (AND)、或 (OR)、异或 (xOR)、非 (NOT) 等等，及其任何有意义的组合。字符串运算可以是连接、反转、替换等等，及其任何有意义的组合。此外，可以将算术运算、逻辑运算和字符串运算进行组合。

[0030] 具体地，上述令牌可以包括序号 (SQN) 或根据 SQN 导出，所述 SQN 指示第二实体已经针对第一实体发起安全操作的次数。对于每次发起，第二实体可以增大 SQN。这种机制确保针对所发起的每次安全操作，令牌具有不同的值。

[0031] 令牌可以具有许多形式。在一种情况下，SQN 本身可以是令牌。备选地，可以使用涉及特定数学运算（如算术运算、逻辑运算和字符串运算中的至少一个）的算法从所述 SQN 导出令牌。例如，令牌可以包括由第二实体基于 SQN 来构造并传送给第一实体的认证令牌 (AUTN)，或者根据该 AUTN 导出。这种构造和传送可以是安全操作的一部分。

[0032] 具体地，令牌可以包括 SQN 与匿名密钥 (AK) 的异或。更具体地，令牌可以是以下各项的连接 :SQN 与匿名密钥 (AK) 的异或、认证和密钥管理字段 (AMF) 以及消息认证码 (MAC)。可以将该连接表示为 :

[0033] 令牌＝ AUTN ＝ (SQN xOR AK) ‖ AMF ‖ MAC

[0034] 或者

[0035] 令牌＝函数 (AUTN) ＝函数 ((SQN xOR AK) ‖ AMF ‖ MAC)

[0036] 第二参数还可以包括随机质询或随机码 (RAND)，或者根据随机质询或随机码 (RAND) 导出。RAND 可以由第二实体生成，并传送至第一实体，作为安全操作的一部分。第二参数还可以包括第一实体的标识符，或根据第一实体的标识符导出。该标识符可以是私有用户标识 (IMPI) 或者国际移动订户标识 (IMSI)。此外，第二参数可以包括通信网络 (具体为第一实体的服务网络) 的标识符，或者根据通信网络的标识符导出。例如，该标识符可以是公共陆地移动网络标识符 (PLMN_ID)。

[0037] 具体地，第二参数可以包括 0x02、PLMN_ID、RAND、IMPI 或 IMSI 以及令牌的连接，或根据该连接导出。可以将其表示为 :

[0038] 0x02 ‖ PLMN_ID ‖ RAND ‖ IMPI ‖ 令牌

[0039] 当令牌是 SQN 自身时，以上变为 :

[0040] 0x02 ‖ PLMN_ID ‖ RAND ‖ IMPI ‖ SQN

[0041] 当令牌是 AUTN 时，以上变为 :

[0042] 0x02 ‖ PLMN_ID ‖ RAND ‖ IMPI ‖ AUTN

[0043] 关于方法中使用的第一参数，该参数包括第一实体通过运行安全操作而获得的加密密钥集合，或根据该加密密钥集合导出。该加密密钥集合可以包括密码密钥 (CK) 和完整性密钥 (IK)，或者根据所述 CK 和所述 IK 导出。

[0044] CK 和 IK 可以是第一实体基于 AUTN 和 RAND 计算的密码密钥和完整性密钥。可以从第二实体传送 AUTN 和 RAND。该计算以及 AUTN 和 RAND 的传送可以形成安全操作的一部分。

[0045] 在一个实施中，第一参数可以包括 CK 和 IK 的连接，或者根据 CK 和 IK 的连接导出。数学上可以将其表示为 :

[0046] CK ‖ IK

[0047] 本文所述的方法生成加密密钥。该密钥可以至少由第一实体和第二实体在它们之间的任何后续通信中共享。在特定实施中，该密钥可以是图 2 的“密钥层级”中的 K_{ASME}，可以由第一实体和第二实体的接入安全管理实体 (ASME) 共享该密钥。

[0048] 可以将该方法扩展为包括 :应用一个或多个其他密钥导出函数，以生成更多加密密钥。这种生成基于或者利用上述基本的、未扩展的方法中生成的加密密钥，例如 K_{ASME}。

[0049] 由扩展方法生成的加密密钥可以包括以下至少一项 :用于保护非接入层 (NAS) 业务的加密密钥集合 ;用于保护无线资源控制 (RRC) 业务的加密密钥集合 ;用于保护用户平面 (UP) 业务的加密密钥集合 ;以及用于导出保护 RRC 业务的加密密钥和 / 或保护 UP 业务的加密密钥的中间加密密钥，如 K_{eNB}。为了更容易理解这些密钥，参照图 2，图 2 示出了 SAE/LTE 中使用的密钥层级。

[0050] 具体地，用于保护 NAS 业务的加密密钥集合可以包括 :用于使用加密算法来保护

NAS 业务的密钥 (K_{NASenc}) 和 / 或用于使用完整性算法来保护 NAS 业务的另一密钥 (K_{NASint})。类似地，用于保护 RRC 业务的加密密钥集合可以包括 :用于使用加密算法来保护 RRC 业务的密钥 (K_{RRCenc}) 和 / 或用于使用完整性算法来保护 RRC 业务的另一密钥 (K_{RRCint})。此外，用于保护 UP 业务的加密密钥集合可以包括用于使用加密算法来保护 UP 业务的密钥 (K_{UPenc})。

[0051] 对于本文描述的技术，“第一实体”可以是用户设备，如移动台。“第二实体”可以是位于通信网络内的实体，因此是“网络实体”。具体地，第二实体可以位于 SAE/LTE 网络中。

[0052] 第二实体可以包括认证中心 (AuC) / 归属地订户服务器 (HSS) 和移动性管理实体 (MME)。MME 可以负责发起针对第一实体的安全操作。所生成的加密密钥可以由 AuC/HSS 生成，并由第一实体和 MME 共享。AuC/HSS 可以增大 SQN，具体在每次针对第一实体发起安全操作时增大 SQN。此外，AuC/HSS 也可以基于 SQN 来构造 AUTN。

[0053] 可以由第一和第二实体以协作方式来执行本文涉及的安全操作。例如，安全操作可以基于 AKA 过程，如 UMTS AKA 协议。

[0054] 该方法涉及的密钥导出函数可以是通用自举架构 (GBA) 密钥导出函数。通用自举架构密钥导出函数可以采用安全散列算法 (SHA) 散列函数。具体地，可以采用具有 256 比特长度的摘要的安全散列算法散列函数 (SHA-256)。

[0055] 根据另一方面，提供了一种计算机程序产品。所述计算机程序产品包括程序代码部分，当在计算设备的计算机系统上执行计算机程序产品时，所述程序代码部分用于执行本文所述的方法的步骤。可以在计算机可读报告介质上存储所述计算机程序产品。

[0056] 一般而言，可以通过硬件、软件或组合的硬件 / 软件方法来实现该方案。

[0057] 对于硬件实现，提供了一种适于生成用于通信实体的加密密钥的设备。所述设备可以执行安全操作，加密密钥的生成可以是安全操作的一部分。所述设备包括 :第一组件，适于提供至少两个参数，其中，第一参数可以包括通信实体通过运行该安全操作而计算的加密密钥集合，或者第一参数是根据所述加密密钥集合导出的 ;以及第二参数可以包括令牌或者是根据令牌导出的，每次针对通信实体发起安全操作时，所述令牌具有不同的值。所述设备还包括 :第二组件，适于执行密钥导出函数，以基于所提供的参数来生成加密密钥。如上所述，令牌可以采取许多可能形式。

[0058] 令牌可以包括 SQN 或根据 SQN 导出，SQN 指示已经针对通信实体发起安全操作的次数。在一个实施中，SQN 本身是令牌。备选地，可以使用涉及算术运算、逻辑运算和字符串运算中的至少一个的算法基于所述 SQN 构造令牌。例如，令牌可以包括基于 SQN 构造并传送给通信实体的 AUTN，或者根据该 AUTN 导出，其中，这种构造和传送形成安全操作的一部分。例如，令牌可以是以下各项的连接 :SQN 与匿名密钥 (AK) 的异或、认证和密钥管理字段 (AMF) 以及消息认证码 (MAC)。可以将该连接表示为 :

[0059] 令牌 = AUTN = (SQN xOR AK) || AMF || MAC

[0060] 除了令牌之外，第二参数还可以包括 RAND，或者根据 RAND 导出。可以将 RAND 传送至通信实体，作为安全操作的一部分。此外，第二参数可以包括通信实体的标识符，或根据通信实体的标识符导出。该标识符的示例是通信实体的私有用户标识 (IMPI)。此外，第二参数可以包括通信实体的服务网络的标识符，或者根据通信实体的服务网络的标识符导出。该标识符可以是公共陆地移动网络标识符 (PLMN_ID)。

[0061] 第二参数的具体示例可以包括 0x02、PLMN_ID、RAND、IMPI 或 IMSI 以及令牌的连

接，或根据该连接导出。例如，可以将第二参数表示为：

[0062] 0x02 ‖ PLMN_ID ‖ RAND ‖ IMPI ‖ 令牌

[0063] 当令牌是 SQN 时，以上变为：

[0064] 0x02 ‖ PLMN_ID ‖ RAND ‖ IMPI ‖ SQN

[0065] 当令牌是 AUTN 时，以上变为：

[0066] 0x02 ‖ PLMN_ID ‖ RAND ‖ IMPI ‖ AUTN

[0067] 如上所述，第一参数可以包括加密密钥集合，或根据加密密钥集合导出。具体地，该加密密钥集合可以包括由通信实体作为安全操作的一部分而计算的密码密钥 (CK) 和完整性密钥 (IK)。备选地，加密密钥集合可以根据密码密钥和完整性密钥导出。

[0068] 作为一个具体实施，第一参数可以包括 CK 和 IK 的连接，或者根据所述 CK 和所述 IK 的连接导出，可以将该连接表示为：

[0069] CK ‖ IK

[0070] 该设备不仅可以基于所提供的第一和第二参数来生成加密密钥，还可以基于所生成的加密密钥来生成更多加密密钥。因此，该设备可以适于应用一个或多个其他密钥导出函数，以基于已经生成的加密密钥来生成更多加密密钥。

[0071] 这些“更多加密密钥”可以包括以下至少一项：用于保护非接入层 (NAS) 业务的加密密钥集合；用于保护无线资源控制 (RRC) 业务的加密密钥集合；用于保护用户平面 (UP) 业务的加密密钥集合；用于导出保护 RRC 业务的加密密钥和 / 或保护 UP 业务的加密密钥的中间加密密钥 K_{eNB}。

[0072] 上述通信实体可以是用户设备，如移动台（例如移动电话或网卡）。

[0073] 根据另一方面，提供了一种包括上述设备的用户设备。该用户设备可以是移动台。

[0074] 根据另一方面，提供了一种包括上述用户设备的系统。所述系统还包括网络实体。该网络实体可以用于 SAE/LTE 网络内。该网络实体可以包括 AuC/HSS 和 MME。MME 可以负责发起针对用户设备的安全操作。AuC/HSS 可以生成加密密钥。可以由用户设备和 MME 共享所生成的加密密钥。AuC/HSS 可以增大 SQN，具体地，在每次针对用户设备发起安全操作时增大 SQN。此外，AuC/HSS 也可以基于 SQN 来构造 AUTN。

附图说明

[0075] 以下参照附图中示出的示例实施例来描述加密密钥生成技术，其中：

[0076] 图 1 是示出了 UMTS AKA 协议的基本概念的图；

[0077] 图 2 是示出了针对 SAE/LTE 系统提出的密钥层级的框图；

[0078] 图 3 是示出了设备实施例的框图；

[0079] 图 4 是示出了系统实施例的框图；

[0080] 图 5 是示出了方法实施例的框图；

[0081] 图 6 是示出了网络实体生成认证向量的 UMTS AKA 操作过程的框图；

[0082] 图 7 是示出了认证和密钥建立的另一 UMTS AKA 操作过程的框图；

[0083] 图 8 是示出了 UE 执行的、作为 UMTS AKA 操作的一部分的一般认证功能的框图；

[0084] 图 9 是示出了在 UE 处执行上述认证功能的特定加密算法的框图；以及

[0085] 图 10 是示出了上述加密算法的特定细节的框图。

具体实施方式

[0086] 在以下描述中，为了解释而非限制的目的，阐述了具体细节，如步骤的特定序列、接口和配置，以提供对加密密钥生成技术的透彻理解。对本领域技术人员而言显而易见地，在脱离这些具体细节的其他实施例中，可以实现该技术。例如，尽管主要在UMTS AKA协议和SAE/LTE网络环境的上下文中描述该技术，但是对本领域技术人员而言显而易见地，可以通过其他安全协议、架构或环境相结合实现该技术。

[0087] 此外，本领域技术人员可以理解，可以使用与编程的微处理器或通用计算机结合工作的软件来实现在下文中解释的功能。还可以理解，尽管主要以方法和设备的形式来描述该技术，但是还可以将该技术嵌入计算机程序产品中以及包括计算机处理器和耦合至处理器的存储器在内的系统中，其中，使用可以执行本文公开的功能的一个或更多程序来对存储器进行编码。

[0088] 图3示出了设备100的实施例，设备100适于生成用于通信实体（图3中未示出）的加密密钥。该通信实体适于运行安全操作。设备100包括第一组件102和第二组件104。第一组件102适于提供至少两个参数，象征性地在箭头106和108处示出。

[0089] 第一参数106包括加密密钥110和112的集合，或根据加密密钥110和112的集合的导出（尽管图中示出了两个密钥，但是加密密钥集合可以包括任何数目的密钥）。已经由通信实体通过运行安全操作来计算加密密钥集合。将加密密钥110和112的集合导出为第一参数106的操作象征性地示出为块114。第二参数108包括令牌116，或根据令牌116导出。每次针对通信实体发起安全操作时，令牌116具有不同的值。将令牌116导出为第二参数108的操作象征性地示出为块118。设备100的第二组件104适于运行密钥导出函数，以基于所提供的参数106和108来生成加密密钥120。

[0090] 参照图4，示出了包括上述设备100的系统200的实施例。通信实体202可以包括设备100，通信实体202可以是UE，如移动台。当然，通信实体202可以是能够容纳设备100的任何合适类型的通信实体。此外，系统包括网络实体204，网络实体204可以位于SAE/LTE网络中。网络实体204可以包括AuC或HSS和MME。它还可以是SAE/LTE网络中的另一通信实体。

[0091] 与图3和4所示的加密密钥生成设备100相对应，图5中示出了图300，图300示出了用于生成加密密钥的方法的实施例。所生成的密钥用于保护两个实体之间的通信。第一实体302可以与图4所示的通信实体202相对应，并且第二实体304可以与图4的网络实体204相对应。第一实体可以是UE。然而，该实施例不限于UE-网络实体场景。而是可以应用与一般的任何两个通信实体。

[0092] MME可以负责发起针对通信实体202的安全操作。所生成的加密密钥可以由MME和通信实体202共享。

[0093] 具体地，该方法实施例可以由第一实体302执行，作为在箭头300’处象征性地示出的安全操作的一部分，该安全操作由第二实体304（具体由其MME）针对第一实体302发起。该实施例本身包括两个步骤：306和308。步骤306提供至少两个参数（图3的106和108）。第一参数包括第一实体302通过运行安全操作300’计算的加密密钥（图3中所示的110和112）的集合，或根据加密密钥集合导出。第二参数包括令牌（图3中所示的116），或

根据令牌导出，每次第二实体 304 针对第一实体 302 发起安全操作 300’时，令牌具有不同的值。在第二步骤 308，应用密钥导出函数，基于所提供的参数（图 3 中所示的 106 和 108）来生成加密密钥（图 3 中所示的 120）。

[0094] 以下给出实质细节，以解释加密密钥生成技术，其中特别强调该技术如何可以成功避免两个 UE 之间的密钥冲突，或者更重要地，如何避免针对同一 UE 的安全操作的两次不同执行之间的密钥冲突。

[0095] 加密密钥生成可以是 UMTS AKA 操作的一部分。UMTS AKA 基于以下实施 :UE（尤其是其 USIM）与 UE 的归属地环境 (HE) 中的 AuC/HSS 共享用户专有密钥 K、特定消息认证函数 f1、f2 和特定加密密钥生成函数 f3、f4、f5。此外，USIM 和 AuC/HSS 跟踪计数器，或分别跟踪序号 SQN_{UE} 和 SQN_{HE}，以支持网络认证。例如，AuC/HSS 可以增大 SQN_{HE}，具体地，每次针对第一实体发起安全操作时增大 SQN_{HE}。UMTS AKA 操作包括多个过程，包括认证向量 (AV) 的生成以及认证和密钥建立。

[0096] AV 过程的目的是向 SN/VLR（或 MME）提供来自 UE 的 HE 的新 AV 的数组，以执行多个用户认证。图 6 示出了 HE 生成认证向量的操作。参照该图，在从 SN/VLR 接收到请求时，AuC/HSS 向 SN/VLR 发送 n 个认证向量 AV(1...n) 的有序数组。每个 AV 包括随机数（或随机质询）RAND、期望响应 XRES、密码密钥 CK、完整性密钥 IK 和认证令牌 AUTN。

[0097] AuC/HSS 从生成新序号 SQN 和不可预测的质询 RAND 开始操作。随后，计算以下值 :

[0098] - 消息认证码 MAC = f1(SQN ‖ RAND ‖ AMF)，其中 f1 是消息认证函数 ;

[0099] - 期望响应 XRES = f2(RAND)，其中 f2 是（可能截断的）消息认证函数 ;

[0100] - 密码密钥 CK = f3(RAND)，其中 f3 是密钥生成函数 ;

[0101] - 完整性密钥 IK = f4(RAND)，其中 f4 是密钥生成函数 ;以及

[0102] - 匿名密钥 AK = f5(RAND)，其中 f5 是密钥生成函数。

[0103] 最终，构造认证令牌 AUTN = (SQN xOR AK) ‖ AMF ‖ MAC。可以由 AuC/HSS 来构造它。这里，AK 是用于隐藏 SQN 的匿名密钥，因为 SQN 可能暴露 UE 的标识和位置。隐藏 SQN 是为了抵御被动攻击。AK 的使用可以是可选的。当不使用 AK 时，可以象征性地代之以值 AK = 000...0。

[0104] 在认证响应中，将 AV 的数组发送回进行请求的 SN/VLR。每个 AV 对 SN/VLR 与 USIM 之间的一个（并且仅有一个）认证和密钥协商有效。

[0105] UMTS AKA 操作的下一过程，认证和密钥建立，是用于在 SN/VLR 与 UE 之间互相认证和建立新的密码密钥和完整性密钥。图 7 中示出了该过程。参照该图，当 SN/VLR 发起认证和密钥协商时，SN/VLR 从数组中选择下一 AV，并将参数 RAND 和 AUTN 发送至 UE。USIM 检查是否可以接受 AUTN，如果是，则产生发送回 SN/VLR 的响应 RES。具体地，在图 8 中示出了 UE 的过程。

[0106] 参照图 8，在接收到 RAND 和 AUTN 时，UE 首先计算匿名密钥 AK = f5(RAND)（或使用 AK = 000...0），并取回序号 SQN = (SQN xOR AK)xOR AK。接下来，UE 计算 XMAC = f1(SQN ‖ RAND ‖ AMF)，并将其与 AUTN 中包括的 MAC 进行比较。如果它们不同，则 UE 将具有原因指示的用户认证拒绝发送回 SN/VLR，UE 放弃该过程。否则，UE 验证接收的 SQN 在正确范围内。

[0107] 如果认为 SQN 在正确范围内，则 UE 计算 RES = f2(RAND)，并将该参数包括在返

回 SN/VLR 的用户认证响应中。最终，UE 计算密码密钥 CK = f3(RAND) 和完整性密钥 IK = f4(RAND)。为了提高效率，也可以在接收 RAND 之后的任何时间，更早地计算 RES、CK 和 IK。UE 可以存储 RAND 用于同步目的。

[0108] 在接收用户认证响应之后，SN/VLR 将 RES 与来自所选认证向量的期望响应 XRES 进行比较。如果 XRES 与 RES 相等，则用户的认证已经被接受。然后，USIM 和 SN/VLR 将新计算的密钥 CK 和 IK 传送至执行密码和完整性功能的实体。

[0109] 从以上内容可以看到，UMTS AKA 操作基于 (RAND，AUTN) 对，AUTN 包括序号 SQN 或根据序号 SQN 导出，如：

[0110] AUTN = (SQN xOR AK) ‖ AMF ‖ MAC

[0111] 其中 AK 是匿名密钥，可以通过 Milenage（见图 9）根据上述输出“f5”来产生。

[0112] 以下函数是对上述冲突问题的第一解决方案：

[0113] KDF(CF ‖ IK，RAND ‖ IMPI ‖ SQN)

[0114] 其中输入已经包括 SQN。现在，即使两个 RAND 相同，即 RAND = RAND’，SQN 始终增大（例如增大 1）的事实将确保输入不同、唯一或独特。

[0115] 备选解决方案使用：

[0116] KDF(CK ‖ IK，RAND ‖ IMPI ‖ AUTN)

[0117] 该方案更容易实现，因为可以“原样”使用来自 AKA 信令的 AUTN。然而，在这种情况下，输入的“唯一性”可能不明显，因为：

[0118] AUTN = (SQN xOR AK) ‖ AMF ‖ MAC

[0119] 即使 SQN ≠ SQN’，可能不能直接看出 (SQN xOR AK)、(SQN’ xOR AK’) 将不同，因为 AK 可能潜在地“消除”了差异。然而，以下，可以证明 (SQN xOR AK) 的独特性。

[0120] 假定：

[0121] (CK ‖ IK，RAND ‖ IMPI ‖ AUTN) = (CK’ ‖ IK’，RAND’ ‖ IMPI ‖ AUTN’)

[0122] 已经表明，这意味着 CK = CK’，IK = IK’以及 RAND = RAND’。因此，仍要检查 AUTN = AUTN’ 是否成立。这种检查可以转换为检查以下是否成立：

[0123] (SQN xOR AK) ‖ AMF ‖ MAC = (SQN’ xOR AK’) ‖ AMF’ ‖ MAC’

[0124] 不失一般性，假定 AMF = AMF’，MAC = MAC’。此时，只要检查以下是否成立：

[0125] SQN xOR AK = SQN’ xOR AK’

[0126] 回想期望 RAND = RAND’。参照图 9 所示的 Milenage 算法，这意味着 AK = AK’（由于它们是由相同的 RAND 产生的）。因此，必须有：

[0127] SQN = SQN’

[0128] 这是一个矛盾，因为如上所述，SQN 始终“逐步增大”，因此 SNQ ≠ SQN’。

[0129] 因此，证明第二方案也保证了对 KDF 函数的输入的唯一性。

[0130] 作为一般方案，取代使用 SQN 或 AUTN 来实现唯一性，每次网络针对 UE 发起 UMTS AKA 操作时具有不同值的任何令牌都是可行的。例如，可以使用 SQN xOR AK（形成 AUTN 的一部分），由于它（通过上述分析）具有所需的唯一性属性。

[0131] 这里，上述加密密钥生成技术表现出许多优点。例如，它保证了 KDF 输入的唯一性。因此，它成功地避免了可能的相同输入所带来的问题。使用这种技术，所生成的加密密钥应当能够满足例如 SAE/LTE 系统中的高等级安全性要求。作为另一优点，该技术可以基

于已经部署的USIM来实现，无需任何USIM替换。使用AUTN而不是SQN的另一具体优点在于，可以在移动终端中（在USIM之外）实施本发明。

[0132] 尽管已经在附图中示出了并在前述描述中描述了加密密钥生成技术的实施例，但是可以理解，该技术不限于本文公开的实施例。在不脱离本发明范围的前提下，能够对该技术进行许多重新配置、修改和替换。

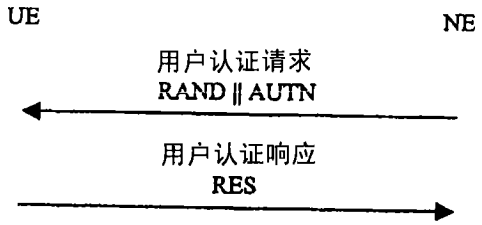

UE
NE
用户认证请求
RAND || AUTN
用户认证响应
RES

图 1

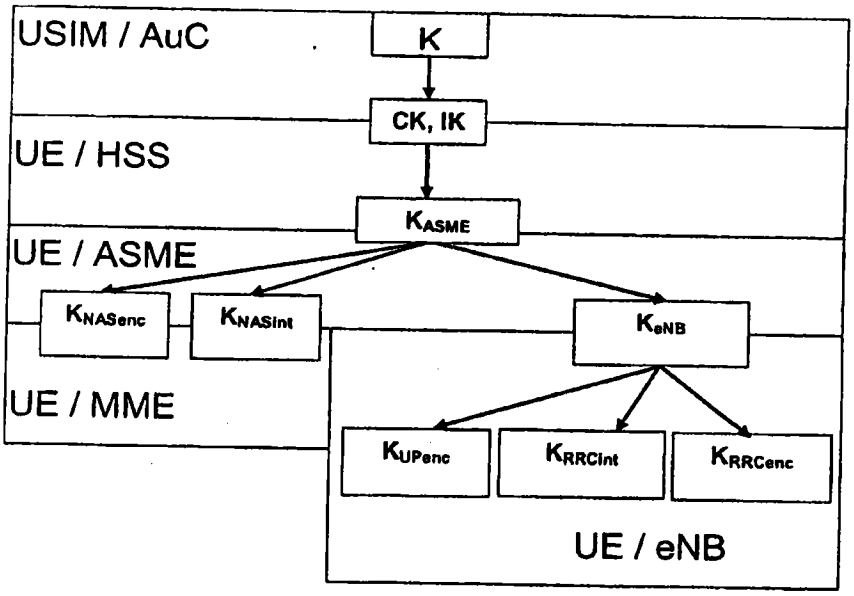

USIM / AuC
K
CK, IK
UE / HSS
KASME
UE / ASME
KNASenc
KNASint
KeNB
UE / MME
KUPenc
KRRCint
KRRCenc
UE / eNB

图 2

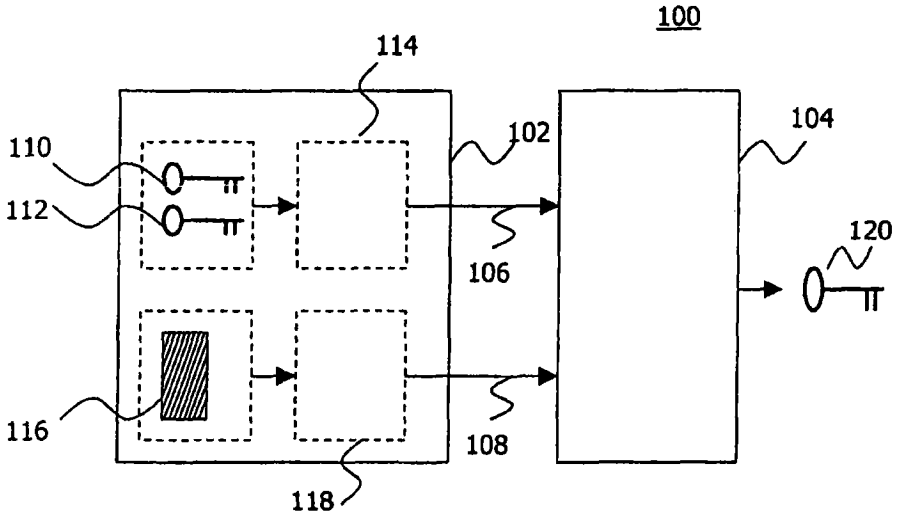

100
114
110
112
102
104
106
120
116
108
118

图 3

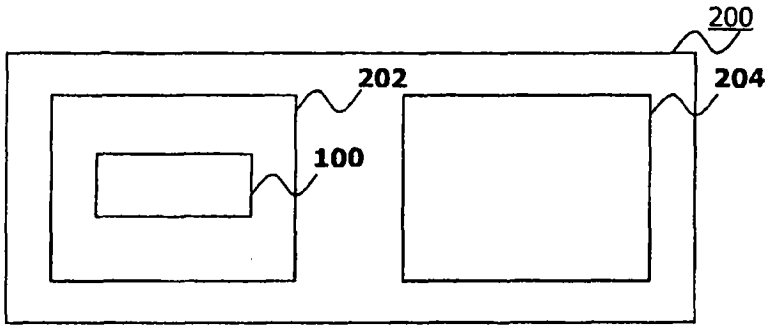

200
202
204
100

图 4

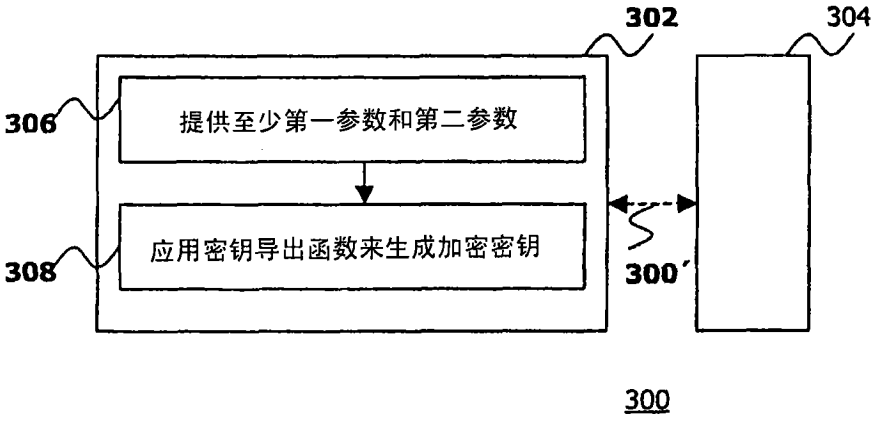

302
304
306
提供至少第一参数和第二参数
应用密钥导出函数来生成加密密钥
308
300'
300

图 5

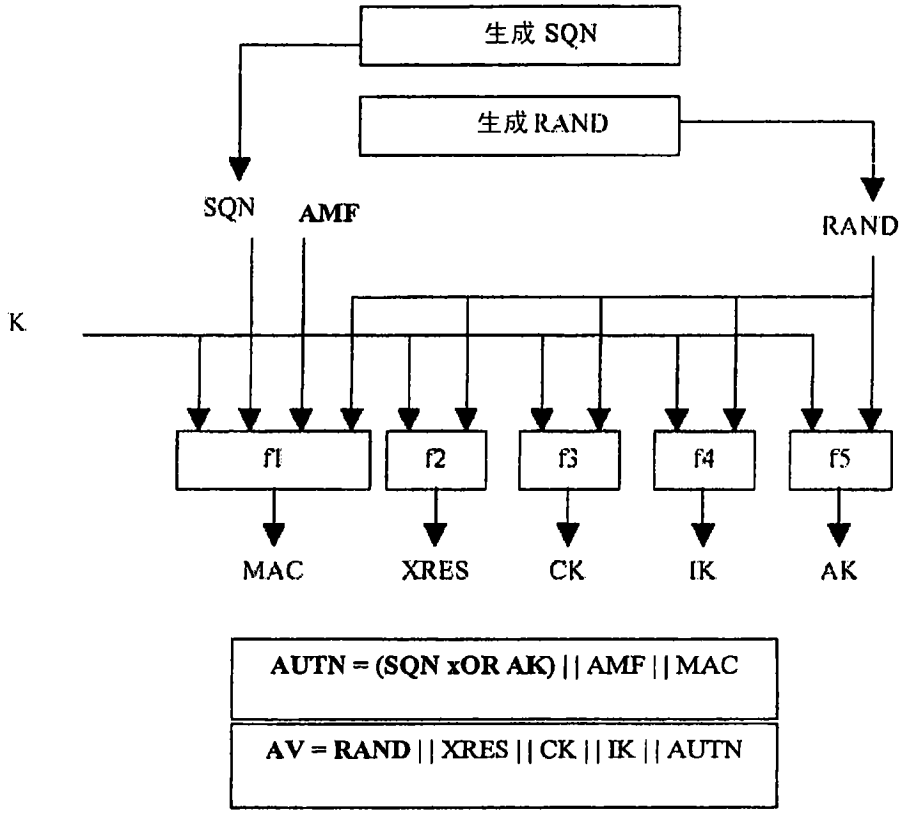

生成 SQN
生成 RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN = (SQN xOR AK) || AMF || MAC
AV = RAND || XRES || CK || IK || AUTN

图 6

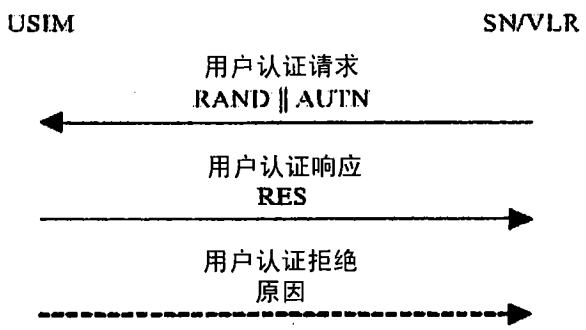

USIM
SN/VLR
用户认证请求
RAND || AUTN
用户认证响应
RES
用户认证拒绝
原因

图 7

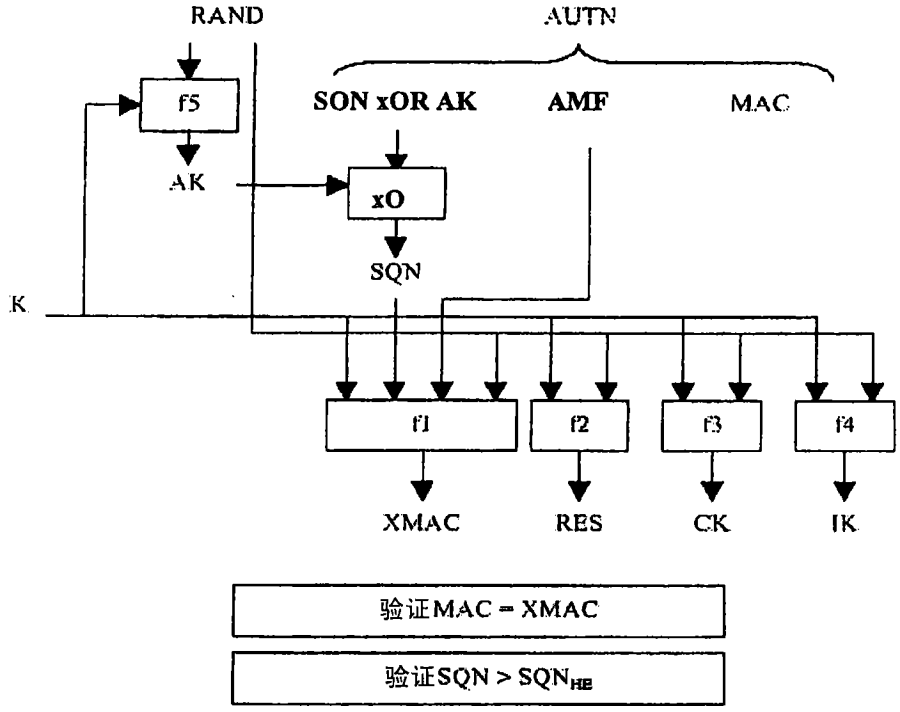

RAND
AUTN
f5
SON xOR AK
AMF
MAC
AK
xO
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
验证MAC = XMAC
验证SQN > SQN

图 8

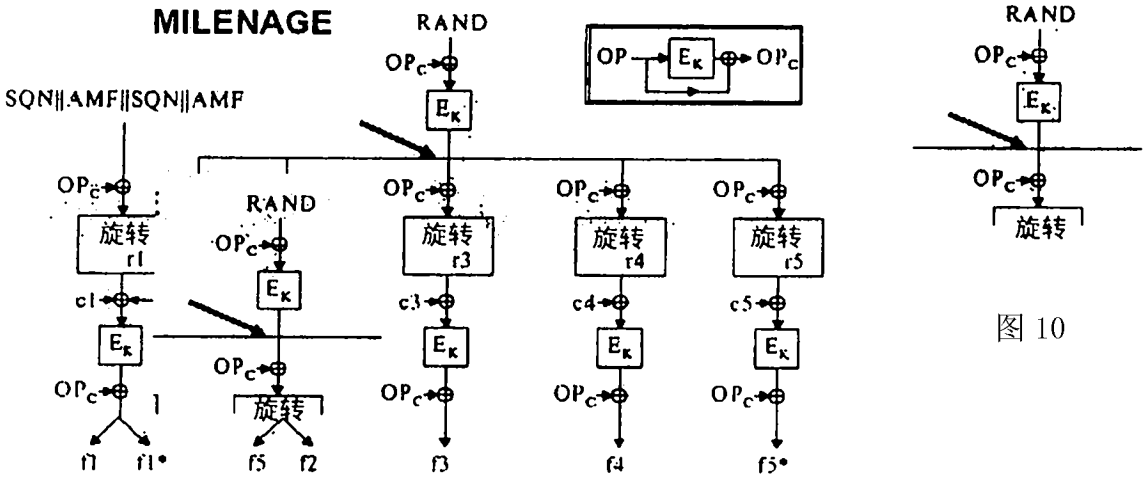

MILENAGE
SQN||AMF||SQN||AMF
RAND
OP
旋转
r1
r3
r4
r5
c1
c3
c4
c5
f1
f1*
f5
f2
f3
f4
f5*

图 9

RAND
旋转

图 10