[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 03823827.6

[43] 公开日 2005 年 10 月 26 日

[11] 公开号 CN 1689367A

[22] 申请日 2003.9.17 [21] 申请号 03823827.6
[30] 优先权
[32] 2002.10.7 [33] US [31] 60/416,272
[86] 国际申请 PCT/SE2003/001461 2003.9.17
[87] 国际公布 WO2004/032557 英 2004.4.15
[85] 进入国家阶段日期 2005.4.5
[71] 申请人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72] 发明人 M·奈斯伦德 K·诺尔曼
T·戈德贝克-勒维

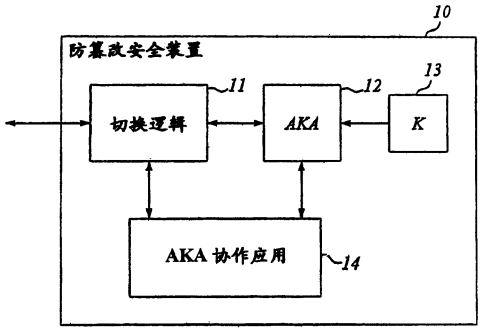
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 杨 凯 刘 杰

权利要求书 5 页 说明书 26 页 附图 8 页

[54] 发明名称 安全装置的安全和保密性增强

[57] 摘要

本发明一般地涉及防篡改安全装置，如用户身份模块或等同物，该装置具有利用存储在装置中的安全密钥执行 AKA(认证和密钥协议)过程的 AKA 模块以及用于外部通信的部件。根据本发明的思想是为防篡改安全装置配备适合与 AKA 模块协作的应用及用于与 AKA 模块和该应用接口的部件。与 AKA 模块协作的应用最好是安全和/或保密增强应用。该应用最好是在安全装置的应用环境中实现的软件应用。为了提高安全性，安全装置也可适于检测它是在其正常的安全环境中工作还是在较不安全的外部环境中工作，并相应地设置对可能暴露 AKA 过程或对应参数的常驻文件或命令的访问权。



ISSN1008-4274

1. 一种防篡改安全装置，具有用于存储至少包括一个安全密钥的用户证书的部件、用于利用所述安全密钥执行认证和密钥协议（AKA）过程的 AKA 模块及用于外部通信的部件，

其中，所述防篡改安全装置还包括:

- 适于与所述 AKA 模块协作的应用；以及
- 与所述 AKA 模块和所述协作应用接口的部件。

2. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用至少包括安全增强应用与保密增强应用之一。

3. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用配置为对与所述 AKA 过程相关联的至少一个参数执行增强安全处理。

4. 如权利要求 3 所述的防篡改安全装置，其特征在于：所述增强安全处理至少包括以下之一:

- 对至少一个 AKA 输入参数进行预处理；以及
- 对至少一个 AKA 输出参数进行后处理。

5. 如权利要求 3 所述的防篡改安全装置，其特征在于：所述增强安全处理包括封装所述至少一个 AKA 参数。

6. 如权利要求 3 所述的防篡改安全装置，其特征在于：所述协作应用配置为从所述 AKA 过程接收至少一个 AKA 参数，以生成比所述接收 AKA 参数具有更高安全性的又一 AKA 参数。

7. 如权利要求 3 所述的防篡改安全装置，其特征在于：所述增强安全处理包括评估预定数量个连续的 AKA 输入参数，以验证所述 AKA 输入参数可安全地使用。

8. 如权利要求 7 所述的防篡改安全装置，其特征在于：所述增强应用处理包括比较预定数量个连续的 AKA 输入参数，以验证所有所述 AKA 输入参数是唯一的。

9. 如权利要求 8 所述的防篡改安全装置，其特征在于：所述增强安全处理还包括对响应多个对应的唯一 AKA 输入参数而生成的预定数量个连续 AKA 输出参数进行组合。

10. 如权利要求 1 所述的防篡改安全装置，其特征在于还包括：基于表示所述防篡改安全装置的相关安全条件的信息，执行安全策略处理的部件。

11. 如权利要求 10 所述的防篡改安全装置，其特征在于：所述安全条件反映所述安全装置工作的环境和借以发起 AKA 处理请求的网络接口中的至少一项。

12. 如权利要求 10 所述的防篡改安全装置，其特征在于：所述安全策略处理至少包括安全策略决定过程和安全策略执行过程之一。

13. 如权利要求 10 所述的防篡改安全装置，其特征在于：用于执行安全策略处理的所述部件包括选择性地禁止直接访问所述 AKA 模块的部件。

14. 如权利要求 10 所述的防篡改安全装置，其特征在于：所述防篡改安全装置包括用于检测所述防篡改安全装置的相关安全条件的部件。

15. 如权利要求 14 所述的防篡改安全装置，其特征在于：用于检测安全条件的所述部件包括用于检测所述防篡改安全装置是在其正常环境中工作还是在视为不安全的环境中工作的部件，并且用于执行安全策略处理的所述部件包括当所述防篡改安全装置在所述不安全环境中工作时用于禁止直接访问所述 AKA 模块的部件。

16. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用包括安全增强应用，并且所述安全装置还包括在所述安全装置工作于视为安全的环境中时用于将 AKA 处理请求直接传送到所述 AKA 模块的部件，以及在所述安全装置工作于视为不安全的环境时用于将所述请求传送到所述安全增强应用的部件。

17. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用配置为执行与用户之间端对端密钥协议相关的至少部分计算。

18. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用配置为屏蔽所述 AKA 模块生成的密钥信息。

19. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用是安装在所述防篡改安全装置的应用环境中的软件应用。

20. 如权利要求 19 所述的防篡改安全装置，其特征在于：输入数据通过用于访问所述应用环境的现有命令传送到所述协作软件应用。

21. 如权利要求 19 所述的防篡改安全装置，其特征在于：所述应用从可信方安全地下载到所述防篡改安全装置。

22. 如权利要求 1 所述的防篡改安全装置，其特征在于：所述协作应用是参与管理用户假名的保密增强应用。

23. 如权利要求 22 所述的防篡改安全装置，其特征在于：所述保密增强应用配置为基于旧用户假名请求所述 AKA 模块的 AKA 响应，并基于所述接收的 AKA 响应生成新的用户假名。

24. 一种防篡改安全装置，具有用于存储至少包括一个安全密钥的用户证书的部件、用于利用所述安全密钥执行认证和密钥协议（AKA）过程的 AKA 模块及用于外部通信的部件，

其中：所述防篡改安全装置还包括在所述防篡改安全装置的应用环境中实现并适合与所述 AKA 模块协作的软件应用，并且所述 AKA 模块也至少部分作为所述应用环境中的软件应用实现。

25. 如权利要求 24 所述的防篡改装置，其特征在于：所述 AKA 软件应用与所述 AKA 协作软件应用至少部分集成。

26. 一种配备有防篡改安全装置的用户终端；所述防篡改安全装置具有用于存储至少包括一个安全密钥的用户证书的部件、用于利用所述安全密钥执行认证和密钥协议（AKA）过程的 AKA 模块及

用于与所述用户终端通信的部件，

其中：所述防篡改安全装置还包括：

- 适用于与所述 AKA 模块协作的应用；以及

- 用于与所述 AKA 模块和所述协作应用接口的部件。

27. 如权利要求 26 所述的用户终端，其特征在于：所述协作应用至少是安全增强应用和保密增强应用之一。

28. 使用如权利要求 26 所述的用户终端，其特征在于：所述协作应用配置为对与所述 AKA 过程相关联的至少一个参数执行增强安全处理。

29. 如权利要求 28 所述的用户终端，其特征在于：所述增强安全处理包括封装所述至少一个 AKA 参数，以产生比所述至少一个 AKA 参数具有更高安全性的输出参数。

30. 如权利要求 26 所述的用户终端，其特征在于还包括：基于表示所述防篡改安全装置的相关安全条件的信息，执行安全策略处理的部件。

31. 如权利要求 30 所述的用户终端，其特征在于：所述安全条件反映所述安全装置工作的环境、借以发起 AKA 处理请求的网络接口和所述用户终端用于网络通信的网络中的至少一项。

32. 如权利要求 30 所述的用户终端，其特征在于：所述安全策略处理至少包括安全策略决定过程和安全策略执行过程之一。

33. 如权利要求 30 所述的用户终端，其特征在于：用于执行安全策略处理的所述部件在所述防篡改安全装置中实现并配置为选择性地禁止直接访问所述 AKA 模块。

34. 如权利要求 30 所述的用户终端，其特征在于：所述防篡改安全装置包括用于检测所述防篡改安全装置的相关安全条件的部件。

35. 如权利要求 30 所述的用户终端，其特征在于：所述用户终端包括用于检测所述防篡改安全装置的相关安全条件的部件。

36. 如权利要求 26 所述的用户终端，其特征在于：所述协作应用是安全增强应用，并且所述安全装置还包括在所述安全装置工作于视为安全的环境中时用于将 AKA 处理请求直接传送到所述 AKA 模块的部件，以及在所述安全装置工作于视为不安全的环境时用于将所述请求传送到所述安全增强应用的部件。

37. 如权利要求 26 所述的用户终端，其特征在于：所述协作应用包括安全增强应用，并且所述用户终端还包括在所述请求通过的接口视为安全时用于将 AKA 处理请求直接传送到所述 AKA 模块的部件，以及在所述请求通过的接口视为不安全时用于将所述请求传送到所述安全增强应用的部件。

38. 如权利要求 37 所述的用户终端，其特征在于：所述安全增强应用包括多个不同的安全增强模块，并且所述安全增强应用配置为依赖接口类型在所述安全增强模块中进行选择。

39. 如权利要求 26 所述的用户终端，其特征在于：所述协作应用是安装在所述防篡改安全装置的应用环境中的软件应用。

40. 如权利要求 26 所述的用户终端，其特征在于：所述协作应用包括配置为对所述用户终端要借以通信的网络进行认证的安全增强应用。

41. 一种网络服务器，由与用户终端中实现的防篡改安全装置共享安全密钥的可信方管理；所述防篡改安全装置具有利用所述安全密钥执行 AKA 过程的认证和密钥协议（AKA）模块，

其中：所述网络服务器包括用于将适合与所述 AKA 模块接口并与其协作的软件应用下载到所述防篡改安全装置的应用环境中的部件。

42. 如权利要求 41 所述的网络服务器，其特征在于：所述下载应用至少是安全增强应用和保密增强应用之一。

43. 如权利要求 42 所述的网络服务器，其特征在于：所述下载应用包括与至少一个安全策略结合的安全增强应用。

安全装置的安全和保密性增强

发明技术领域

本发明一般涉及通信系统中的认证和密钥协议（AKA）过程，更具体地说，涉及在此类过程中使用和配置防篡改安全装置。

发明背景

通常，认证和密钥协议（AKA）包括相互认证，这意味着通信各方如用户和关联操作员可确定另一方是声称方，但也可以包括保留的隐私，这例如意味着通常为用户的发起方可使用假名作为其身份。操作员随后将能够确定用户的真正身份，而其它第三方却不能。当然，通常无需执行认证，除非随后执行涉及被认证方的一些操作和/或过程。因此，一般情况下认证最终将导致密钥协议，由此获得一个或多个密钥以用于保护各方之间的进一步通信，并确保每个随后的消息源于另一方。

许多网络服务基于在例如 GSM SIM(用户身份模块)、UMTS SIM 或 ISIM（IP 多媒体 SIM）卡等防篡改“安全装置”上存储用户证书（一般是保密密钥 k，也可能包括用户身份和假名），并让网络以询问-响应协议通过用户终端与此装置交互以执行（用户）认证和密钥协议（AKA）。以下将此类协议简单地称为 AKA 协议。例如，这包括 GSM 和 UMTS AKA 协议。

一般情况下，协议工作方式如下所述，如图 1 所示。在移动通信系统场景中通常称为 AuC 的用户数据库/认证中心内，基于已知的保密密钥和生成的查询 RAND 生成预计的响应 XRES。AKA 协议可以且通常会涉及 AAA（授权、认证和记帐）服务器，该服务器可与 AuC 实体位于同一位置，也可不在同一位置。询问 RAND 和预计的

响应 XRES 通常传送到 AAA 服务器。该询问发送到终端 ME（移动设备），该终端在安全装置帮助下计算响应 RES。响应被送回 AAA 服务器，如果响应与预计响应匹配，则用户通过认证。在图 1 中，只显示了询问响应协议。实际上，还生成例如用于加密的会话密钥。

问题是在一些情况下（同样，例如使用 COMP128 算法的 GSM SIM），AKA 协议中使用的加密算法不是很强大，攻击者通过获得相对少量的询问-响应对便可对安全装置实施反向工程（并找出 k 是什么）。

鉴于如下事实此问题变得更严重：在建议的几种解决方案中，为获得不同类型的访问和服务，安全装置需要拖离其正常的环境（例如，移动电话），并进入外来环境。例如，将安全装置置于经 USB（通用串行总线）端口连接到 PC（个人计算机）的读卡器中。由于与移动电话相比，PC 相对容易感染上病毒和特洛伊木马程序，因此，可能安插了用户不知道的恶意软件，该软件将询问-响应值从装置中“拉出”，并（在以后可能）将它们转发给攻击者进行分析。在没有认证询问的情况下（例如，传统的 GSM 系统），或在询问经过认证，但该认证存在安全缺陷时，这是一个严重的威胁。攻击分析可基于被动监听（在图 1 中由“攻击”和实线表示），或通过主动插入自适应选择的询问（在图 1 中由“攻击”和虚线表示）。

即使安全卡始终保留在终端/电话中，但有时安全仍会受到损害。例如，有人提议通过另一接口如蓝牙或 IRDA 重用 AKA 协议，以便能够使用卡上的证书来对除网络接入之外的其它服务进行认证。例如，电话可与商店中的收银机进行通信以便为购买的货品付款，充当“电子钱包”。由于例如 GSM SIM 无法缺省地对请求认证的装置进行认证（即，认证不是相互的），因此，存在在公共场所放置旨在攻击卡上弱算法的恶意装置。可能更糟的威胁是对手在终端安装恶意代理。这种代理随后可以在攻击者想要通过服务器认证，而又从受感染的终端获得 AKA 参数时从远程激活。这严重限制了可使用

例如基于 SIM 的认证的商业情况。

相关技术

在非常具体的 GSM SIM 情况中，IETF 正在进行工作[1]，以通过将 GSM A3/A8 响应封装在更安全的算法如 MD5 或 SHA1 算法中而增强安全[2]。更具体地说，A3/A8 算法的值不直接返回，而是用作到更强函数的输入，返回该函数结果。这防止了直接分析 A3/A8 的输出。此工作可称为可扩展认证协议的 SIM 子集（EAP-SIM），还为可能需要超过标准 64 位 GSM 加密素材（keying material）的现实提供了部分解决方案。这通过基于不同 RAND 值按顺序查询 A3/A8 算法，并将结果级联成更长的密钥来完成。

图 2 显示了常规的扩展认证协议 EAP-SIM。移动设备（ME）或其它用户终端将询问中继到 SIM，并计算响应 RES 及随后响应的哈希值。此哈希值随后作为新响应 RES'发送到 AAA 服务器。AAA 服务器自然实现相同的哈希函数。在这种情况下探察 AAA 服务器与 ME 之间业务的攻击者将无法直接从 A3/A8 访问输出，而只能访问 A3/A8 输出的哈希值 RES'。要注意的是 UMTS AKA 类似的工作也在进行中[3]。

虽然 EAP SIM 提议解决了与 GSM A3/A8 算法有关的理论问题，或具体为它的 COMP128 实现，但它有几个缺点。首先，该解决方案只将解决与 COMP128/GSM 相关的特定问题。如果在终端如膝上型计算机中实现 EAP 封装，则图 2 中用圆圈“1”所示的 SIM-ME 接口也可能感染病毒和特洛伊木马程序。这表示选择的询问和对应的响应仍可为攻击者所用。最好是如参考[4]中指定的一样，对此特殊问题的任一解决方案不应改变 SIM-ME 接口标准。改变标准需要时间，并且在市场上更强大且不需要额外保护的标准 UMTS USIM 可用前，这甚至是不可能的。同样地，如引言中所述，已建议符合 UMTS 版本 99（R99）的 GSM 电话/网络应支持更强的 UMTS AKA。因此，

此类标准化工作是可疑的。此外，无法排除 EAP SIM 提议本身有一些缺陷且以后可能需要“调整”。实际上，最近发现，按顺序使用几个 RAND 值以导出更长密钥的方案有一些缺陷。例如，通过重复发布同一 RAND 值 n 次，而不是发布 n 个不同的值，获得的有效安全性可能仍只等同于从单个 RAND 值获得的安全性。

发明概述

本发明克服了先有技术安排的这些和其它缺陷。

本发明的总目的是提供与认证和/或密钥协议有关的安全和/或保密增强。

一个目的是提供改进的 SIM 或类似的防篡改安全装置。在此方面，特别需要为增强安全和/或保密而扩展防篡改安全装置的功能。

本发明的另一个目的是，即使防篡改安全装置如 SIM 在不安全的环境中使用，或者在通过较不安全的接口重用 AKA 协议时，也可保持整体安全。

另一个目的是提供适用于增强安全和/或保密的用户终端。

本发明还有一个目的是提供一种网络服务器，它支持安装在用户终端中的防篡改安全装置中的安全和/或保密增强。

如上所述，本发明一般涉及防篡改安全装置，如用户身份模块或等同物，所述装置具有用于存储至少包括一个安全密钥的用户证书的部件、利用该安全密钥执行 AKA 过程的 AKA（认证和密钥协议）模块及用于外部通信的部件。

根据本发明主要方面的基本思想是为防篡改安全装置配备适用于与 AKA 模块协作的应用和将 AKA 模块与此应用接口的部件。

与 AKA 模块协作的应用最好是安全和/或保密增强应用，该应用一般执行与 AKA 模块的认证和/或密钥协议相关的安全和/或保密增强处理。

为增强安全性，应用依据要实现的特殊安全目标，执行有些不

同的安全处理任务。通常，增强安全处理可包括对 AKA 过程的一个或多个输入参数的处理（预处理）和/或对输出参数的处理（后处理）。例如，安全增强应用可配置为将 AKA 响应封装在更安全的算法中，例如，上述 EAP SIM 协议中建议的算法。然而，根据本发明，所有敏感处理在防篡改安全装置中进行，包括安全增强步骤。因此，考虑到 EAP SIM 增加的长度和类似的安全增强算法，旨在检索保密密钥或其它敏感数据的攻击成功的可能性将大大降低。因此，即使防篡改安全装置在较不安全的环境如个人计算机（PC）中使用，或者通过诸如蓝牙等较不安全的接口重用 AKA 协议时，也可保持整体安全。

本发明的安全应用可执行的安全增强处理的其它示例包括：i）扩展基本安全功能以生成额外的加密素材，例如，基于一个或多个询问-响应查询的一个或多个（可能更长的）密钥；ii）执行为两个用户之间端对端加密生成共享密钥所需的至少部分计算（基于 SIM 或类似安全装置中的密钥）；以及 iii）屏蔽 AKA 模块模块生成的 AKA 密钥信息。例如，额外的加密素材可能从最终用户的角度而言对实现安全性提高的合法拦截的目的有用，或者对与公共访问关联的安全增强有用。

本发明也可用于执行重放检查，确保不以不安全的方式重用相同的输入参数（RAND）。具体地说，将几个 AKA 输出参数组合到安全性更高的响应或密钥中时，确保使用一组独特的 AKA 输入参数（RAND 值）很重要。

为增强保密性，一个重要方面是通过管理（保持或可能生成）适当的用户假名（也称为临时用户身份）来保护用户的身份，这将在下面描述。

在增强安全的场景中，防篡改安全装置和/或对应的用户终端最好配置为执行某种形式的安全策略处理。安全策略处理通常涉及安全策略决定和/或执行，且最好基于表示防篡改安全装置的相关安全

条件的信息。例如，重要的是整体安全不受对防篡改安全装置的常驻应用文件和命令的未经授权访问的损害，所述未经授权访问通过例如病毒和特洛伊木马程序进行，可能暴露 AKA 过程和对应的 AKA 参数。因此，防篡改装置有利地适用于仅在给定环境下允许访问此类常驻文件和命令。更具体地说，在安全装置离开其正常环境如移动电话，并插入更敌意的环境如 PC 或诸如此类中时，最好禁用防篡改装置的某些常驻文件和命令。作为替代，可将任何 AKA 处理请求方便地发送到安全增强应用。这可以如下方式进行管理：例如通过利用检测防篡改安全装置安全条件的内部或外部模块，和/或让用户根据安全装置的装置类型输入不同的 PIN 代码或等同物来设置访问权限。类似地，在通过较不安全的接口如蓝牙重用 AKA 协议时，用户终端可将 AKA 请求重新路由到安全增强应用。

人们已认识到，将安全增强和/或保密增强应用作为软件应用（最好是小程序）实现特别有利，此类应用可在制造期间预先安装，或作为通过认证的应用提供，下载到防篡改安全装置的应用环境中。例如，应用环境可通过普通 GSM SIM 卡的 GSM SAT（SIM 应用工具包）或 UMTS SIM 卡的 UMTS SAT 提供。通常，应用安全地（最好是经认证和加密）从可信方如与 GSM/UMTS SIM 关联的网络操作员管理的网络服务器下载到应用环境中。

可轻松地将应用连同一个或多个安全策略替换或升级（甚至通过空中接口），以便终端/安全装置具有最新的小程序“版本”。另外，由于小程序通常在网络操作员或其它可信方的控制下，并由操作员“签名”，因此，它们受恶意软件感染的可能性远远低于普通 PC 上的小程序。

在敌意环境中，通常在外部装置中，对 AKA 过程的询问是作为应用环境中的应用的输入数据发送的，而不是使用普通命令（例如，GSM SIM 的 RUN_GSM_ALGORITHMS 命令）来调用 AKA 算法。

如果应用文件/输入数据通过使用现有命令如 GSM SAT 的

ENVELOPE 命令传送到应用环境，防篡改安全装置的输入/输出接口不需要任何改变。这很重要，因为本发明由此不会违反现有标准规范。

在本发明的替代实施例中，AKA 算法也至少部分作为防篡改装置应用环境中的应用实现，且最好与安全和/或保密增强处理一起实现。显然，此方法不需要在常驻 AKA 模块与应用环境之间使用特殊接口，这是因为增强的安全和/或保密处理与 AKA 算法均位于应用环境中。自然，在 AKA 算法与安全增强功能之间仍将存在程序代码接口。

应理解，虽然软件实现特别有利，但也可将 AKA 协作应用预制成防篡改安全装置中的硬件，且硬件应用与 AKA 模块之间存在大致直接的接口。

本发明提供了以下优点：

- 从终端角度而言，本发明显示了如何通过在易受病毒和特洛伊木马程序影响的敌意环境中保护装置的额外安全层，扩展和提高传统 SIM 和类似的防篡改安全装置。
- 它也显示了一种基于传统技术实现新的安全/保密目标的简单方法。
- 主要的优点在于该解决方案适应未来发展，且易于通过经认证的下载以安全的方式进行管理。
- 在某种意义上，该解决方案对于防篡改安全装置插入的装置是透明的。另外，在安全装置仍在原（移动）终端中，通过例如蓝牙进行通信时，它允许对安全装置如 SIM 直接进行安全的远程访问。这意味着移动终端可用作“通用”认证装置，而不会影响 SIM 的安全。
- 从网络的角度而言，应注意的是，AuC（或类似）节点可保持完全不变，如果使用 AAA 服务器，则只有 AAA 服务器需要实现额外的安全处理。

- 最后，许多建议的实施例没有标准影响，但可能要求朝正常的 SIM 功能稍微改变内部 SAT 环境的 API。

通过阅读针对本发明实施例的以下说明，可理解本发明提供的其它优点。

附图简述

结合附图参照以下说明，可最好地理解本发明及其其它目的和优点，附图中：

图 1 是说明相关各方之间的信息传输的典型先有技术询问-响应认证过程的示意图；

图 2 是用 EAP-SIM 协议扩展的先有技术询问-响应认证的示意图；

图 3 显示了根据本发明的防篡改安全装置的示范实施例；

图 4 是根据本发明示范实施例，配有防篡改安全装置的用户终端示意图；

图 5 是作为用户身份模块实现的根据本发明的防篡改装置的示范实施例方框图；

图 6 是根据本发明示范实施例，支持防篡改安全装置中的安全和/或保密增强的网络服务器的示意图；

图 7 是防篡改装置替代实施例的方框图，其中，一个或多个安全策略与对应的安全策略处理在安全装置的应用环境中实现；

图 8 是作为用户身份模块实现的根据本发明的防篡改装置的另一示范实施例的方框图；

图 9 是作为用户身份模块实现的根据本发明的防篡改装置的又一示范实施例的方框图；

图 10 是防篡改安全装置的示意方框图，说明了根据本发明示范实施例的安全增强应用操作；

图 11 是防篡改安全装置的示意方框图，说明根据本发明示范实施例，采用封装和比较预处理的安全增强应用；

图 12 说明通过根据本发明的防篡改用户身份模块增强了保密性的认证过程；以及

图 13 是作为用户身份模块实现的根据本发明的防篡改装置另一示范实施例的方框图。

本发明实施例详细说明

在附图中，将使用相同的标号表示相同或类似的单元。

如下面将要叙述的一样，可以一种不考虑安全装置上当前实现的算法的方式，实现上述和其它安全目标。

根据本发明主要方面的基本思想是如图 3 所示，在 AKA 模块与应用之间提供适用于与 AKA 模块协作的应用及接口，例如 API 或类似接口。

图 3 显示了根据本发明的防篡改安全装置的示范实施例。安全装置 10 基本上包括切换逻辑 11、AKA 模块 12、至少包括安全密钥 K（也可能包括用户身份和密码）的安全存储的用户证书 13、适用于与 AKA 模块协作的应用 14 及 AKA 模块 12 与 AKA 协作应用 14 之间大致直接的接口。切换逻辑 11 解析发送到安全装置的命令，并处理与内部功能之间的通信。AKA 模块 12 包括至少部分基于安全密钥 K 进行认证和/或密钥协议的算法。

防篡改安全装置最适用于在网络装置如用户终端或等同物中实现。图 4 显示了用户终端 20，例如移动电话或个人计算机，该终端一般具有某种形式的网络通信功能 25，还显示了类似图 3 所示的防篡改安全装置 10。

与 AKA 模块协作的应用通常是与认证和/或密钥协议相关的应用，且最好是安全和/或保密增强应用。

为提高安全性，应用将根据特定的安全目标执行稍微不同的安

全处理任务。增强的安全处理通常与 AKA 模块的认证和/或密钥协议相关，并且与 AKA 过程的输入参数和/或输出参数关联。

在增强安全的场景中，防篡改安全装置和/或对应的用户终端最好配置为执行某种形式的安全策略处理。安全策略处理通常涉及安全策略决定和/或执行，且最好基于表示防篡改安全装置的相关安全条件的信息，下面将对此作更详细的描述。

为提高保密性，应用管理例如用户假名。

下面将主要在 GSM SIM 的场景中描述本发明，但其思想也适用于 UMTS SIM 或实际上具有 AKA 功能的任何防篡改安全装置以及如下所述的类似应用和接口。其它示例包括用于 3GPP IP 多媒体的 ISIM，或更一般地包括可同时包含几个 SIM 的 UICC 卡。

应用最好作为软件应用实现，其可在制造期间预安装在作为通过认证的应用提供，下载到防篡改安全装置的应用环境中。

图 5 所示的 SIM 10 包括切换逻辑 11、AKA 模块 12、安全密钥 K 13、应用环境 15 且最好还包括模块 16，模块 16 用于检测 SIM 相关安全条件，例如，检测 SIM 10 是在其正常安全环境中工作还是在较不安全的环境中工作。切换逻辑 11 解析发送到 SIM 的命令，处理与内部模块的通信，并且还将出站数据转发到 SIM 所处的用户终端。AKA 模块 12 使用安全密钥，例如客户-操作员预约关联的预约密钥或从中导出的密钥执行 AKA 过程。在 GSM SIM 中，此功能通常为 A3/A8 AKA 算法。

应用环境

有利的是，应用环境 15 由用户身份模块的应用工具包提供，且通常是能够执行代码的环境。对于 GSM SIM，应用环境可由 SIM 应用工具包（SAT）提供 [5]，而 UMTS SIM（USIM）的类似应用环境由 UMTS SAT（USAT）提供 [6]。

对于 GSM SIM，SIM-ME（SIM-移动设备）接口指定可发送到

SIM/ME 或从 SIM/ME 发送的“命令”和数据。例如，为运行 GSM A3/A8 AKA 算法，存在 RUN_GSM_ALGORITHMS 命令，该命令将输入参数路由到常驻 AKA 算法，或从常驻 AKA 算法发送输出结果。AKA 算法依据询问 RAND（和存储的安全密钥）计算响应和/或一个或多个密钥。在 SIM-ME 上的可能命令列表中，需要特别注意 ENVELOPE 命令。此命令用于向 SIM 发送或多或少的任意数据，以用于 SIM 应用工具包（SAT）。SIM 的输入/输出格式已明确指定，但就应用究竟可以或不可以执行什么操作而言，存在高度自由。例如，应用可以是很普通的 Java 小程序，参见文献[7]。小程序可获得不同程度的授权以访问常驻的 GSM 相关文件，一种可能性是给予它“完全的 GSM 访问权”。

在本发明的优选实施例中，AKA 协作应用 14 在 SIM 应用工具包提供的应用环境中利用 ENVELOPE 命令或类似命令实现。应用的输入/输出数据随后最好也通过 ENVELOPE 传送到 SAT。

对于 SAT 环境 15 中的软件应用 14 与 AKA 模块 12 之间的通信，最好在 AKA 模块 12 与 SAT 应用环境 15 之间采用特殊的接口，如专用的 API。

SIM 应用工具包（SAT）允许操作员将 AKA 协作应用“硬编码”或经空中下载到 SIM 中。在后一种下载情况下，也可以（并强烈建议）对来源于可信方如正确的操作员的应用进行认证。这很重要，因为这样避免了从恶意服务器下载“病毒”。下载的应用也可以加密，这样，应用内容在 SIM 外便不可用。对于涉及 GSM SAT 的安全方面，请参考文献[8]。通过在 SIM 的应用环境中实现所述应用，也可以将 SIM 的功能升级。升级版本只需使用 ENVELOPE 命令下载。

图 6 是支持将安全和/或保密增强应用或小程序下载到防篡改安全装置的网络服务器的示意图。网络服务器 30 一般由诸如网络操作员等可信方管理，且基本上包括小程序源 31、用于加密/认证用途的模块 32 及下载模块 33。

安全策略处理

如上所述，某种形式的安全策略处理一般在防篡改安全装置和/或用户终端中实施，并且安全策略处理最好基于表示防篡改安全装置安全条件的信息。相关安全条件的示例可包括安全装置工作的环境、AKA 处理请求经过的接口、用户终端进行网络通信所用的网络等等。

为增加安全控制，SIM 或更一般的安全装置最好仅在某些安全条件下或环境中授权访问可暴露 AKA 过程和对应的 AKA 参数的常驻应用文件和命令。例如，可以在防篡改安全装置内部检测安全条件，或者例如通过用户终端在外部检测安全条件。

再次参照图 5，可以看到，SIM 包括用于检测安全条件，例如放置 SIM 的环境的模块 16。例如，SIM 或更一般的安全装置最好只在 SIM 在其正常环境（例如，移动电话）中工作时才授权访问可能暴露 AKA 过程和对应的 AKA 参数的常驻应用文件和命令。如果 SIM 位于或暴露于外部较不安全的环境中，则最好禁止访问此类常驻文件和命令。作为替代，可将任何 AKA 处理请求方便地发送到安全和/或保密增强应用。这是防篡改安全装置中实施并执行的安全策略的完美示例。

应理解，安全装置使用用户终端的普通网络接口在其正常环境中工作时，可能不需要安全和/或保密增强处理。另一方面，对于不安全的环境，依据 SIM 所处的特定的不安全环境定制安全处理可能会有利。实际上，这可通过提供若干种不同的定制安全增强模块或子应用，并根据环境在这些模块中进行选择来达此目的。

当例如 GSM SIM 在其正常环境外部使用时，推荐停用正常的 RUN_GSM_ALGORITHMS 命令/接口（否则病毒可能仍会使用该命令）。下面将描述实现这种停用操作的多种可能性。

如果 SIM 只是要在正常终端外使用（即，我们有特殊用途的

SIM），则可以简单地制造 SIM 以便其不接受 RUN_GSM_ALGORITHMS 命令，或者，使得此命令始终在内部“重新路由到” SAT 环境和其中运行的软件应用。当然，在这种情况下，似乎简单地从头开始构建特殊用途的 SIM 会更好。然而，如果可重用大多数现有 SIM 体系结构，这当然有益。

如图 5 所示，安全装置或 SIM 最好配备有检查使用其的终端或手持装置的身份/类型。这可在开机时执行，并且由配置为检测 SIM 10 是在其正常安全环境（通常为移动终端）中工作还是在诸如 PC 或诸如此类较不安全环境中工作的模块 16 完成。检测模块 16 最好控制切换逻辑 11，以便根据具体环境将 AKA 请求直接传送到 AKA 模块，或者重新路由到应用环境。因此，可以利用此功能，以便在 SIM 发现或怀疑其不在（正确）的终端/手持装置中时，SIM 假定它在外部（在不安全环境中）并进入只接受 SAT 命令的模式，并且拒绝通过常驻文件或命令的所有 AKA 访问请求。

也可能将不止一个 PIN 码与 SIM 相关联。这种情况下，特定 PIN 代码可通知 SIM 它在外部装置中使用，并且相应地设置访问权限以便只接受“无害的” SAT 命令。这里，可能必须再次确认用于正常 SIM 访问的 PIN 代码以防止错误地激活正常访问。

如图所示，还可能在防篡改安全装置的应用环境中实施一个或多个安全策略与对应的安全策略处理。在此示例中，应用环境 15 包括诸如安全增强应用之类的 AKA 协作应用 14A 和安全策略应用 14B。安全策略应用 14B 可以部分或全部与安全增强应用 14A 集成，或作为单独的应用提供。在实际情况中，可在开机时缺省地禁用正常的 AKA 命令（例如，通过控制切换逻辑 11 或以其它方式），并且最初将有关 SIM 安全条件的信息传送到安全策略应用 14B，该应用随后作出安全策略决定以确定适当的进一步操作。例如，如果安全策略应用 14B 获悉 SIM 位于其正常工作环境（例如，移动终端）中，安全策略应用 14B 会启用正常的 AKA 命令。如果安全策略应用

14B 获悉 SIM 位于另一较不安全的环境中，则将继续禁用正常的 AKA 命令，并将所有 AKA 处理请求传送到安全增强应用 14A，该应用根据适用的安全策略处理 AKA 请求。SIM 的安全条件可在 SIM 内部或外部检测，但在 SIM 本身配备有用于检测相关安全条件的功能时，可提供更高程度的自治权和安全性。安全策略和对应的安全策略处理可由诸如归属操作员等可信方进行“硬编码”，或下载（经加密/认证）到 SIM 的应用环境中。SAT 环境和 ENVELOPE 命令（或等同物）使下载发布的安全策略及策略改变实际可行。

即使 SIM 在普通终端（移动装置）中工作，也可能希望在不同于正常（GSM/UMTS）网络接口的其它接口上重用 AKA 协议。不同的解决方案可用于处理这种情况下的安全问题。

例如在典型的支付情形中，用户将只需启动遵循某种标准化协议的支付应用，其中，通过使用例如 ENVELOPE 或等效命令，将 AKA 请求重新路由到安全增强应用。这种情况下，问题在应用层次得到解决。

另外，在上述支付情形中，用户也可能希望对第三方保持匿名。因此，在经适当和安全的认证后，可调用生成用户假名的保密增强应用，这将在后面详细地描述。

此外，终端（移动终端）可配置为判断 AKA 请求最初经由正常网络接口而来还是经由另一接口如蓝牙或 IRDA（红外数据联盟）接口而来。例如，这意味着移动终端本身能够检测 SIM 访问请求何经由较不安全的接口而来，并相应地采取适当的措施。例如，终端可基于端口标识（IR 端口、蓝牙端口、普通无线电接口端口等）确定请求源。一般情况下，在请求经由蓝牙或 IRDA 接口而来时，AKA 处理请求不是使用正常的常驻命令直接传送到 AKA 模块，而是由终端使用 SAT 应用环境命令将其重新路由到安全增强应用。这是适合本发明实施的安全策略的另一示例。此处，通过提供若干不同子应用并根据终端使用的接口的特定类型在子应用中进行选择，同样可

能有利于定制安全处理。

适合在本发明的防篡改安全装置中实施的安全策略的另一示例与用于增强 3GPP Gb 接口安全的现有提议有关[13]。安全就绪时，还需要控制如何/何时使用安全的策略。有时，低的安全/无安全可接受，有时却无法接受。具体地说，在协商使用哪种安全算法期间，可能存在中间人执行所谓“压低攻击（bidding-down attack）”的问题。假设移动终端向网络发信号表示它能够使用安全算法“A”和“B”，其中，“A”比“B”更强。如果攻击者现简单地从支持的算法列表中删除“A”，则即使移动终端和网络都支持“A”，网络也将相信移动装置只支持“B”，并且移动终端/网络将以使用次优安全结束。为此，建议添加某种形式的协商完整性保护。然而，有时会存在支持增强安全协商的网络与一些尚未升级的网络并存的情况。因此，操作员可能希望向其用户发布策略，指示移动终端是否应该接受外部受访网络中不安全的协商。很明显，此策略控制最好设置在诸如 SIM 等防篡改安全装置的应用环境中。有关是否应该接受不安全协商的决定最好基于通过 AKA 得到完整性保护的信息。

安全策略处理的另一变型是例如通过检查输入的 AKA 参数来识别网络/操作员，并且根据网络/操作员身份定制随后的安全处理。这假定可依据例如输入的 AKA 参数来区分不同的操作员。

为便于说明，下面显示了用于在根据本发明的防篡改安全装置中实施的安全策略表的示例。

表 I

安全条件			安全模式	
环境	网络/操作员	接口	正常的 AKA	安全增强子应用
移动终端	归属	普通	启用	-

PC	归属	普通	禁用	01
移动终端	归属	蓝牙	禁用	02
移动终端	归属	IR	禁用	03
移动终端	归属	WLAN	禁用	04
移动终端	受访	普通	-	05（协商）
移动终端	操作员 A	普通	禁用	06
移动终端	操作员 B	普通	禁用	07
…				…
PC	受访	WLAN	禁用	01、04、05

对用户终端的修改

非常希望保持 SIM/ME 接口完整，不影响标准（至少即便是可能需要添加新命令，SIM 仍可与标准后向兼容）。当然，考虑终端/手持装置是否不受本发明影响的问题也很重要。SIM 要在终端/手持装置外部使用时，显然无需改变手持装置，因为甚至不会涉及手持装置。如果手持装置要用作如上所述的“认证令牌”，通常需要修改。然而，应该可能仅通过 IRDA 或蓝牙运行 GSM AKA 命令的简单事实使得必需进行修改（将 SIM 连接到蓝牙/IRDA），就 SIM 功能而言，本发明不会使得引入这些改变更困难。

实现 AKA 算法的替代位置

如图 8 和图 9 所示，也可以将 AKA 算法或至少部分该算法实现为防篡改装置应用环境中可以对安全密钥（或可能从中导出的密钥）进行读访问的应用，不过这种做法并非首选。在图 8 中，AKA 协作应用 14 和 AKA 算法 12 作为彼此协作的单独应用实现。或者，如图 9 所示，将两个功能 12、14 集成或至少部分集成到同一软件应用中。

以下将主要参照在 SIM 的 SAT 环境中作为软件实现的增强安全处理和保密处理的多种非限制性示例来描述本发明。

有关 GSM SIM 规范的基本细节的其它信息，请参考文献[9]。

增强安全处理的示例

例如，为提高 GSM SIM 的安全性，为了正常 GSM AKA 的目的，可执行以下步骤。

制造的 SIM 卡遵循文献[4、5 和 9]，但另外具有从 SAT 环境到 A3/A8 算法的内部 API 或类似接口。请注意，这对现有 SIM 标准规范并无影响。

另外，如果 SIM 要在电话外部使用，插入某一其它装置，则高度推荐制定规定，以便可以禁用正常的 RUN_GSM_ALGORITHMS 命令。为此，如上所述的几种不同的解决方案是可行的。

操作员为 SIM 配备（在制造期间，或在以后作为经认证的应用下载时）配置用于在 SAT 环境中执行增强安全处理的应用。例如，安全增强应用可配置为以更安全的算法，例如 EAP SIM 协议中建议的算法封装 AKA 响应。询问（RAND）通过 ENVELOPE 命令作为输入数据发送到 SAT 应用，而不是使用 SIM-ME 接口上的 RUN_GSM_ALGORITHMS 命令。或者，为每次认证下载整个小程序。其优点在于使对网络进行认证（因为小程序已进行了认证）并确保终端始终具有最新“版本”的小程序成为可能。当然，在未下载整个小程序时，通常无论如何要实现这种认证，例如，通过运行对“RAND”值进行认证并可能还检查重放的协议，每次在 SAT 小程序本身中验证认证/新鲜度（authentication/freshness）。

无论 SIM 连接到的终端的类型及访问 SIM 的方式（通过蓝牙、IRDA、在读卡器中等），所有 AKA 相关处理均在 SIM 上进行，包括安全增强步骤。增强安全处理可能涉及操作 AKA 过程的输出参数和/或输入参数，图 10 中针对一般的防篡改安全装置作了示意。

例如，EAP SIM 协议基于通过操作 AKA 输出参数对敏感参数进行封装。假定存在从初始的 RAND 值：RAND(1)、…、RAND(n)

得到的多个 AKA 响应：RES（1）、…、RES(n)，则可用以下方式封装 AKA 响应以得到相应的具有更高安全性的响应 RES'：

h(key, RES(1), …, RES(n))

其中，h 是密钥函数，例如，基于 SAH-1。换而言之，n 个响应通过密钥函数组合成一个响应。类似地，更长的密钥 K_c'可通过将从上述 RAND 值集得到的密钥 $K_c(1)$、…、$K_c(n)$级联以及可能随后的其它处理生成。

最近发现，按顺序使用几个 RAND 值以导出更长密钥的方法有一些缺陷[11]。例如，通过重复发布同一 RAND 值 n 次，而不是发布 n 个不同的 RAND 值，所获得的有效安全性可能仍只等效于从单个 RAND 值获得的安全性。通常，通过就新鲜度和/或唯一性比较相关的 AKA 输入参数集，可解决此特殊问题。根据本发明的特定实施例，在防篡改安全装置 10（例如 SIM）上实现的安全增强应用 14 因此包括比较器及封装模块 18，如图 11 所示。例如，封装模块 18 可通过对响应若干对应 AKA 输入参数（RAND）而生成的预定数量个连续 AKA 输出参数（K_c，RES）进行组合来执行封装。比较器 17 比较相关的连续 AKA 输入参数（RAND）集，以验证所有这些 AKA 输入参数是唯一的。一般情况下，比较器 17 期望接收包含给定数量个连续输入参数（RAND 值）的集合以便整体封装，并将每个输入的输入参数与该集合中每个以前的输入参数进行比较。这样，可确保结果“屏蔽”的 AKA 输出参数（K_c'，RES）是为响应唯一 AKA 输入参数（RAND 值）集而生成的参数。如果需要，AKA 输入参数还可以作为用于封装的额外输入馈入封装模块 18，如图 11 虚线所示。或者，可以其它方式确定 AKA 输入参数的新鲜度/唯一性，例如，通过使用加时戳的 AKA 输入参数并检查给定参数集的时戳是否在预定时间间隔内来完成。

从 EAP-SIM 协议中可以归纳并实现于 AKA 协作应用中的另一

特性是对用户终端借以通信的网络进行认证。在正常的 GSM AKA 中，网络发送认证请求连同 RAND，而 SIM 只以响应 RES 应答。通过让 SIM 或等效的防篡改安全装置响应认证请求而向网络端发送新随机值 RAND'，可扩展这种认证。网络随后基于收到的 RAND'和从 RAND 导出的会话密钥及 SIM 密钥 k 计算 MAC（消息认证码）或类似代码，并将该 MAC 发送回 SIM 以验证网络的可靠性。这种扩展协议的相关步骤可以如下方式设计：

1. 网络向 SIM 发送认证请求。
2. SIM 向网络发送 RAND'。
3. 网络生成 RAND，计算 MAC（密钥、RAND、RAND'...）并向 SIM 发送 RAND 和 MAC。
4. SIM 检查 MAC，并在可用时计算密钥/响应。

EAP SIM 协议中建议的 AKA 密钥/响应封装一般指对 AKA 输出参数的处理。然而，也可能处理 AKA 过程的输入参数。例如，新的经过处理的输入可计算为：

h (key, RAND),

因此，输出响应等于：

A8 (key, h (key, RAND)),

其中，h 是密钥函数，例如，基于 SHA-1。处理输入参数和输出参数的示例是生成如下最终结果输出响应：

g (key, A8 (key, h (key, RAND))),

其中，g 和 h 是密钥函数，例如，基于 SHA-1。

SIM 外无敏感数据可用，并且安全功能也可扩展为提供不止一个密钥等等。

对于使用 USIM 的 UMTS，可执行对应的处理/封装。同样，对于用于 3GPP IP 多媒体的 ISIM，有人建议在 HTTP 摘要协议中“封装”认证消息[12]。此封装可通过本发明实现。

对 AKA 输入参数进行预处理的示例包括：

- 验证 AKA 输入参数的新鲜度；
- 验证 AKA 输入参数的完整性；
- 将 AKA 输入参数解密；
- 组合 AKA 输入参数；以及
- 基于 AKA 输入参数决定安全策略。

对 AKA 输出参数进行后处理的示例包括：

- 将若干生成的 AKA 输出参数（K_c 和/或 RES）组合成一个或多个（可能更长）的修改过的 AKA 输出参数（K_c' 和/或 RES'）；
- 对生成的 AKA 输出参数进行完整性保护；
- 将生成的 AKA 输出参数加密；以及
- 基于对 AKA 输入参数的检查结果决定策略和/或执行 AKA 输出参数。

用于合法拦截的增强安全处理

对合法拦截有法律要求。也就是说，网络操作员必须根据法院指令，能够向执法机构提供明文会话。在经典的 GSM 情况中，由于只对 ME 与 RBS（无线电基站）之间的链路进行加密（使用操作员知道的密钥），因此，这可轻松实现。

预计我们很快将看到用户之间的端对端（e2e）加密。也就是说，在会话开始前，执行两个用户之间的 e2e 密钥协议，例如，使用如文献[10]中指定的协议 MIKEY。这使得合法拦截变得更困难，因为操作员必须能够以某种方式推导出与用户获得的在用户之间共享的相同密钥。本发明建议将与 e2e 密钥协议相关的至少部分所需操作和计

算作为类似 SAT 的环境中的一个应用来实现，方法是利用一个应用将 SIM 升级，该应用也基于操作员-用户共享密钥 k 导出用户 A 与 B 之间的端对端密钥，这些密钥也“自动地”为操作员所知。

例如，假设 g^x 表示某一合适（安全）组 G 中的取幂，例如，整数模素数 p，或有限域上椭圆曲线上的点。对于用户 A，GSM（或 UMTS）AKA 的结果是密钥 kA。同样地，用户 B 获得密钥 kB。现在执行 Diffie-Hellman 协议[14]，其中 A 向 B 发送 g^{kA}，并且 B 向 A 发送 g^{kB}。共享的密钥是 g^{kA*kB}。任一操作员（A 或 B 的归属操作员）可通过知道 kA（或 kB）并观察 g^{kB}（或 g^{kA}）而计算出完全相同的密钥。

注意，如果终端要扩展为具有此额外的功能，同样需要在 SIM 本身中执行 g^{kA}（和 g^{kB}）计算，因为否则 kA（和 kB）需要离开受保护的 SIM 环境。通过本发明，全部计算实际上可在 SIM 中完成，最好在可通过新的密钥交换方法轻松升级的 SAT 应用中完成。

有关 e2e 加密和全法拦截的信息，请参阅我们以前的专利申请[15]，该专利通过引用结合于本文中。

另一个在[15]中讨论的问题是，不仅归属操作员能够“窃听”A 和 B 之间的通信，而且 A 与 B 当时所在受访网络的操作员也将能够“窃听”A 与 B 之间的通信。如果受访网络的操作员不是 100％值得信任的，这可能是一个威胁。这是将 ka（和 kB）发送到受访网络的影响。为解决此问题，可采用[15]中建议的方法或类似的方法。假设 k 为用户与家庭网络之间共享的密钥（存储在 SIM 中）。我们不向受访网络发送 kA=kdf(k, RAND)，其中，kdf 是密钥导出函数，而向受访网络发送 kA' = f(kA)（对于 kB，这是类似的），其中 f 是某种单向函数。单向属性确保只知道 kA'的某个人可能仍然不知道 kA 是什么。密钥 kA'现在（透明地）用于正常的 GSM/UMTS 安全，而仍然将 kA（和 kB）用作例如使用 Diffie-Hellman 协议的 A 与 B 之间 e2e 密钥协议的基础。现在，只有归属操作员可执行合法拦截。根据本

发明的思想是在类 SAT 应用中实现函数 f 的屏蔽功能。

用于公共访问的增强安全处理

涉及上述最后一个问题的问题如下。存在有计划要提供公共“热点”，其中，移动用户通过另一种访问技术，例如 IEEE 802.11 WLAN（无线 LAN）暂时获得较高的比特率。此处的问题是“基站”或 AP（接入点）处于不可信的环境中。这可能意味着可在物理上“搭接”AP 以获得敏感数据，例如用于业务完整性保护的密钥、操作员对业务正确计费所必需的密钥。因此，存在一些想法，其中，完整性保护在称为 ASN（接入服务节点）的某一另外节点中终止，再进入网络，则得到更多的保护。在终端与 AP 之间某处可能仍存在常规 802.11 或类似的完整性保护，因而需要两个密钥：

- 保护 ME-AP 链路的密钥 k1；以及
- 保护 ME-ASN 链路的密钥 k2，该密钥在 AP 中必须不可用。

这意味着，必须基于存储在 SIM 中的用户密钥导出两个密钥，而不只是一个密钥。此外，k2 不得从 k1 中导出。这可以如下方式实现：利用正常的 AKA 协议导出 k2，然后，用合适的单向函数导出 k1=f(k2)，然后只将后一 k1 发送到 AP。同样地，使用本发明，至少可以将另一密钥 k1 的生成以安全的方式实现为 SIM 本身上的 SAT 应用。

保密增强

在本发明的另一方面中，SIM 或类似的安全装置（具体为其中的应用工具包）用于以方便的方式增强对用户的保密，例如，通过管理用户假名。

一般情况下，在连接到网络期间为用户指定了临时标识符或假名以便保护其真正的身份。另外，假名可多次刷新，从而甚至使事

务链接也不可能实现。Id 即 tmpID 最好只是每次用户连接时随机选择的字符串。它可由用户选择（例如，通过用户的通信装置）或由网络指定给用户。后者的优点在于易于确保每个使用的假名的唯一性。

但应理解，用户假名的指定可能同时涉及网络和用户终端。例如，临时 id 可由来自网络的第一部分和来自用户终端的第二部分例如可能是特定于用户归属操作员的第二部分来定义。此类 tmpID 的一个示例可以为“4711@xyz.com”，其中，第一部分“4711”由网络指定，而第二部分“@xyz.com”在用户终端中指定。

考虑在用户不时改变接入的多路接入的情况。在接入改变时，一般为用户指定新身份。然而，新指定值一般必须基于旧的 tmpID，即用于以前网络/装置的 ID，或者用于与同一网络的以前会话中的 ID。这意味着 tmpID 最初需要以某种方式传送到新接入方法或服务提供者。这会造成同步问题。例如，用户可从 GPRS 终端接入改变为膝上计算机上的无线 LAN 接入。

利用本发明，SIM 或类似的安全装置可以存储和管理 tmpID，且最好是在 SAT 应用或等同物中。用户改变接入时，SIM 连接到新终端（例如，通过物理移动它），从而将当前 tmpID（和可能的其它现有安全参数）传送到新装置。新网络现在可以为他指定新的临时 ID 即 tmpID'，此操作最好是在对用户进行认证（涉及 AKA 模块）之后。在使用同一终端，但将其用于新会话的稍微更简单的情况中，SIM 将类似地“记住”以前使用的 ID，并且不需要物理移动。

如图 12 所示，从 SIM 10 中检索出（0）安排在第一用户终端 20-1 中的证书（包括例如认证响应和已经存在的 ID），并且执行（1）SIM 10 与第一接入网 40-1 之间的用户/网络认证协议。此认证可能涉及（2）外部认证服务器 50。用户获得新的假名（3）tmpID，该假名存储（4）在 SIM 10-1 中。可选地每隔一段时间重复步骤（1-4/3-4），导致重新认证和/或新的假名。在一段时间后，第一用户终端 20-1 的

用户想将接入改变到第二用户终端 20-2 和第二接入网 40-2。SIM 10 移动（5）到第二用户终端 20-2。利用现有证书/tmpID（6），用户可能需要向新网络 40-2 重新认证（7），同样可能涉及（8）认证服务器 50。可选地，将用户的假名刷新（9）为新值 tmpID'，然后将该新值存储在 SIM 10 中。同样，可每隔一段时间重复步骤（7-9/8-9）以增强保密和安全。

两个终端 20-1 和 20-2 当然可能是相同的，并且两次接入由同一终端 20 中的不同接入部件实现，在这种情况下，SIM 10 从不离开终端，但仍然管理接入变更 ID。

保密增强应用的执行通常是有条件的，取决于 AKA 认证是否成功。例如，保密增强应用只响应成功的认证而执行。

考虑至少部分由用户终端指定临时标识符时的情况，通过使用 AKA 模块可以生成新的 tmpID'或至少它的一部分，例如，通过将新的 tmpID'计算为：

新 tmpID'= s (key, A8 (key, 旧 tmpID))，

其中，s 是密钥函数，例如，基于 SHA-1。在此特殊示例中，SIM 的 SAT 环境中的保密增强应用将向 AKA 模块发送旧 tmpID，并接收 A8 响应，该响应由保密增强应用用于计算新的 tmpID'。

或者，网络可为用户指定新的假名 tmpID'。指定的假名随后安全地传送（经加密/认证）到 SIM 或等效的防篡改安全装置，其中假名通过 SIM 密钥进行解密和/或认证，并在保密增强应用中记录和管理。在另一实施例中，保密增强应用只是随机选择新的 tmpID'，在 AKA 响应正确时，网络会接受该新的 tmpID'。

硬件实现

应理解，虽然软件实现特别有利，但也可以将 AKA 协作应用预制成防篡改安全装置中的硬件，该硬件具有在硬件应用与 AKA 模块

之间大致直接的接口。

图 13 显示了特别有利的硬件实现方案，该实现方案利用了 SIM 的应用环境以及将输入数据传送到应用环境的现有命令（例如，ENVELOPE 命令），然后将输入数据从应用环境经另外的接口路由到 SIM 上预制的硬件应用模块。硬件应用大致直接地与 AKA 模块接口，最好是通过特殊的接口连接，最后经应用环境将输出数据转发给用户终端。

在另一实现方案中，AKA 模块和协作应用如安全增强应用集成在 SIM 上的同一硬件电路中。然而，在这种集成硬件实现中，最好应仍可以根据 SIM 的工作环境，在正常 AKA 处理与增强 AKA 处理之间进行选择。

硬件实现不排除以后下载软件应用或软件补丁的可能性，所述软件应用可替换硬件应用，而软件补丁可与硬件应用协作。

最后，我们参考以前的专利申请[16]，该申请通过引用结合于本文中。

上述实施例只是作为示例提供，并且应理解，本发明并不限于此。保持本文所公开并要求权利的基本原理的其它修改、变更和改进均在本发明的范围之内。

参考

[1] “EAP SIM 认证”（Haverinen, "EAP SIM Authentication",draft-haverinen-pppext-eap-sim-05. txt, IETF）。

[2] 联邦信息处理标准（Federal Information Processing Standard FIPS PUB 180-1, NIST）。

[3] “EAP AKA 认证”（Arkko and Haverinen:"EAP AKA Authentication", draft-arkko-pppext-eap- aka-04. txt, IETF）。

[4] 3GPP TS 11.11 技术规范，第 3 代合作伙伴项目；技术规范组终端用户身份模块-移动设备（SIM-ME）接口规范。

[5] 3GPP TS 11.14 技术规范，第 3 代合作伙伴项目；用户身份模块-移动设备（SIM-ME）接口的 SIM 应用工具包规范。

[6] 3GPP TS 31.111 技术规范，第 3 代合作伙伴项目；技术规范组终端；USIM 应用工具包（USAT）。

[7] 3GPP TS 03.19 技术规范，第 3 代合作伙伴项目；技术规范组终端；用于 Java Card™的用户身份模块应用编程接口（SIM API）；第 2 级。

[8] 3GPP TS 03.48 技术规范，第 3 代合作伙伴项目；技术规范组终端；用于 SIM 应用工具包的安全机制；第 2 级。

[9] ETSI TS 100 922 技术规范，数字蜂窝电信系统（2+阶段）；用户身份模块（SIM）；功能特征。

[10] “MIKEY：多媒体因特网密钥”（Arkko, Carrara, Lindholm,Nslund, and Norrman,"MIKEY : Multimedia Internet KEYing", draft-ietf-msec-mikey-04. txt, IETF）。

[11] “EAP-SIM 会话密钥协议分析”（Sarvar Patel, "Analysis of EAP-SIM Session Key Agreement", posted on the Internet on May 29,2003）。

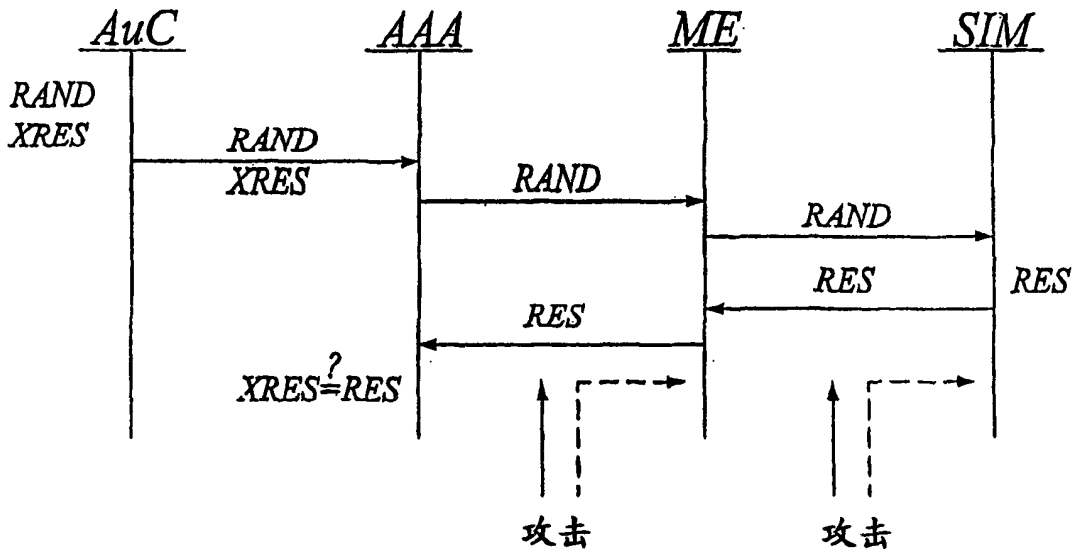
[12] “使用 AKA 的 HTTP 摘要认证”（Niemi, Arkko, Torvinen, IETF RFC 3310, "HTTP Digest Authentication Using September 2002）。

[13] “增强 A/Gb 的安全性”（3GPP TSG WG3 Security, "Enhanced Security for A/Gb", July 15-18 2003）。

[14] “应用加密学手册”（Menezes, van Oorschot, and Vanstone:"Handbook of Applied Cryptography", CRC Press, pp. 489-541）。

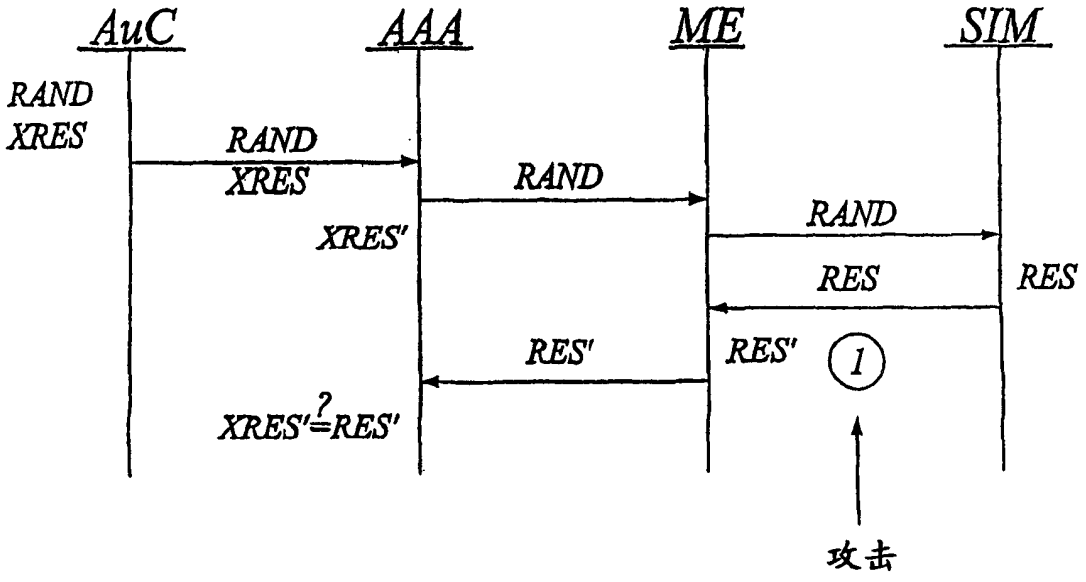
[15] 2001 年 12 月 7 日提交的英国专利申请 No.0129339-8。

[16] 国际专利申请 WO 02/084980，其要求于 2001 年 4 月 10 日提交的瑞典专利申请 No.0101295-4 的优先级。



(先有技术)

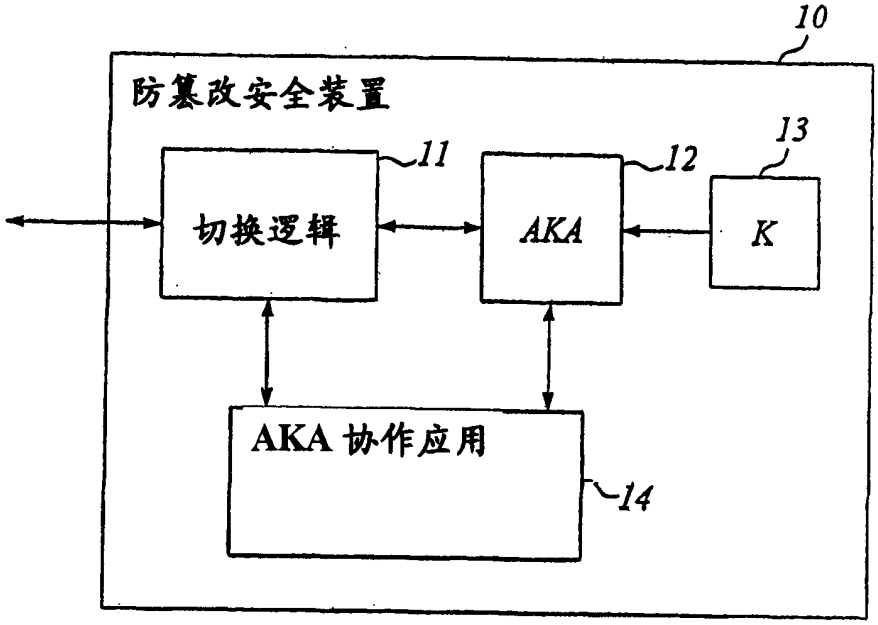
图 1



先有技术

图 2

图 3


10
防篡改安全装置
11
12
13
切换逻辑
AKA
K
AKA 协作应用
14

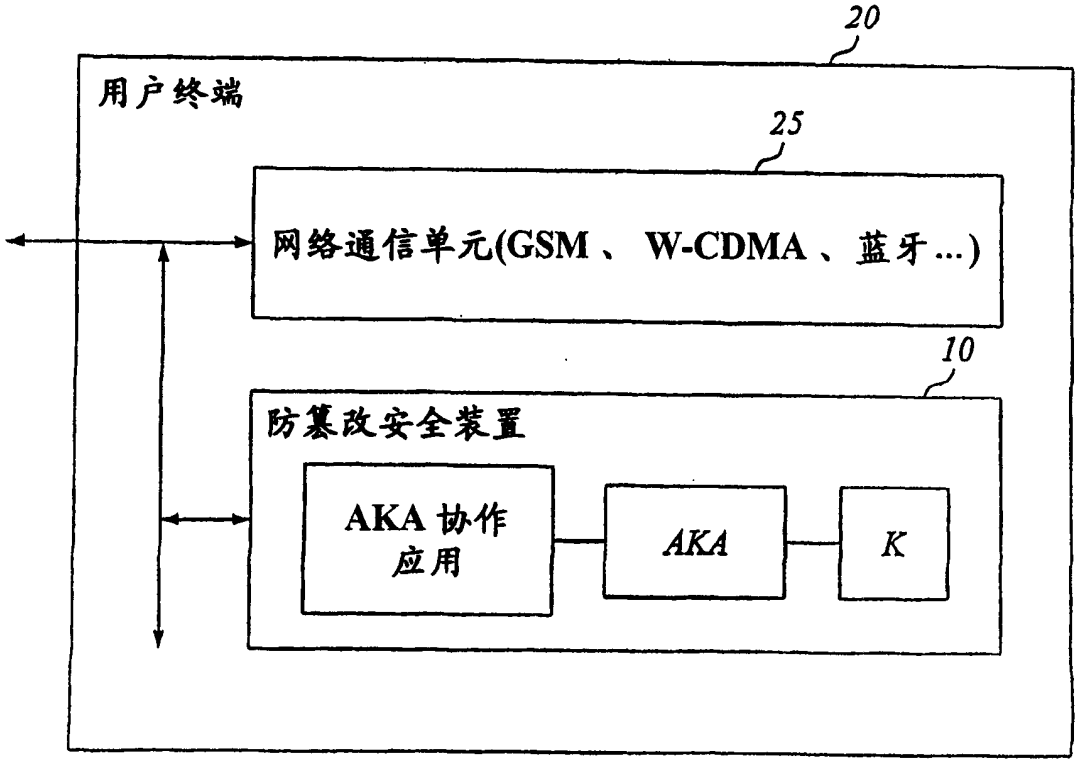
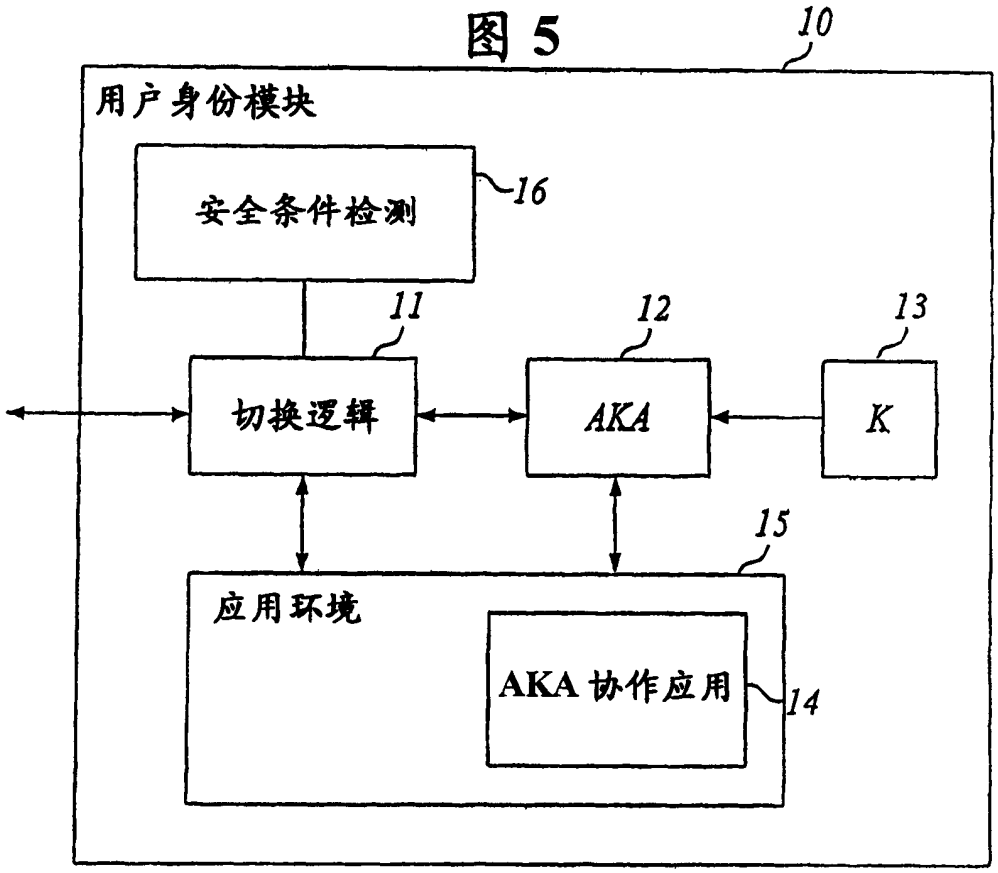

20
用户终端
25
网络通信单元(GSM 、 W-CDMA 、蓝牙...)
10
防篡改安全装置
AKA 协作
应用
AKA
K

图 4

图 5


10
用户身份模块
安全条件检测
16
11
12
13
切换逻辑
AKA
K
15
应用环境
AKA 协作应用
14

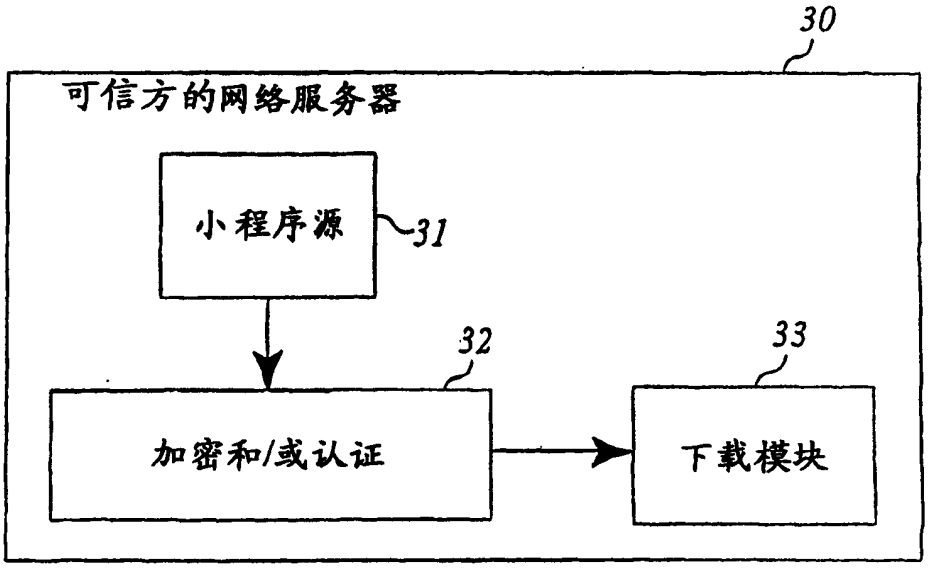

30
可信方的网络服务器
小程序源
31
32
33
加密和/或认证
下载模块

图 6

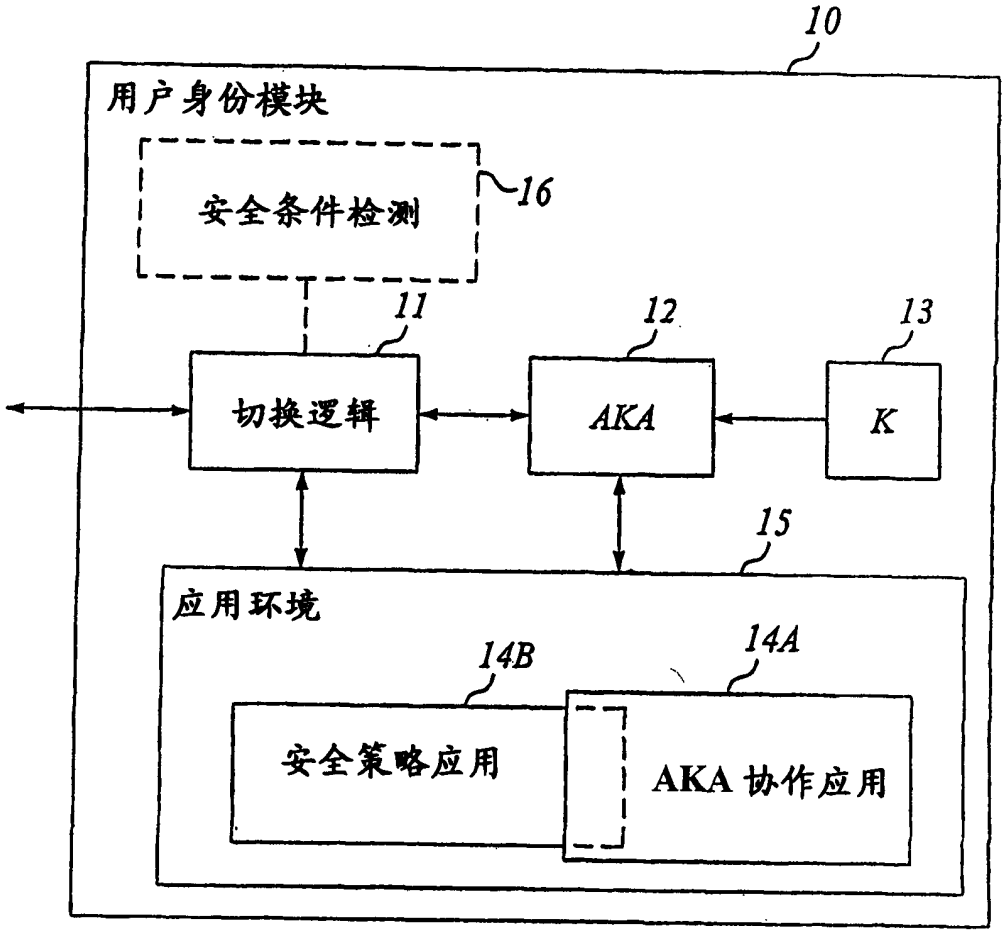

10
用户身份模块
安全条件检测
16
11
12
13
切换逻辑
AKA
K
15
应用环境
14B
14A
安全策略应用
AKA 协作应用

图 7

图 8

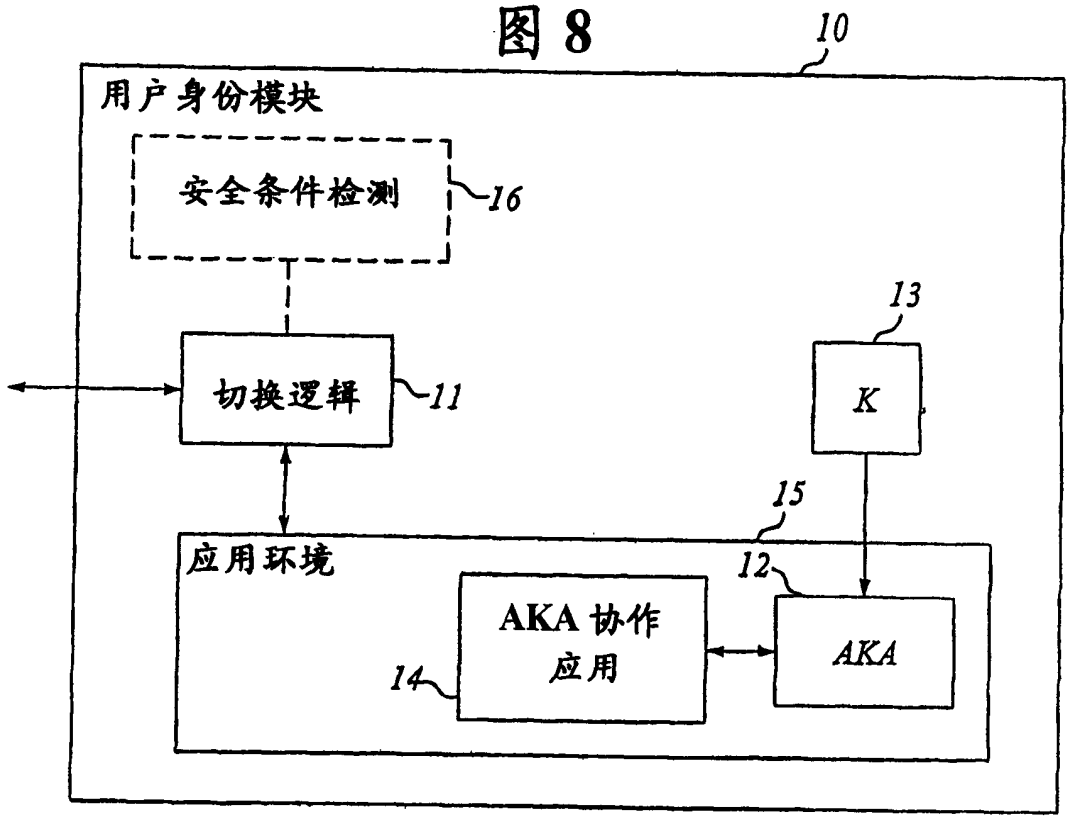

10
用户身份模块
安全条件检测
16
13
切换逻辑
11
K
15
应用环境
12
AKA 协作
应用
AKA
14

图 9

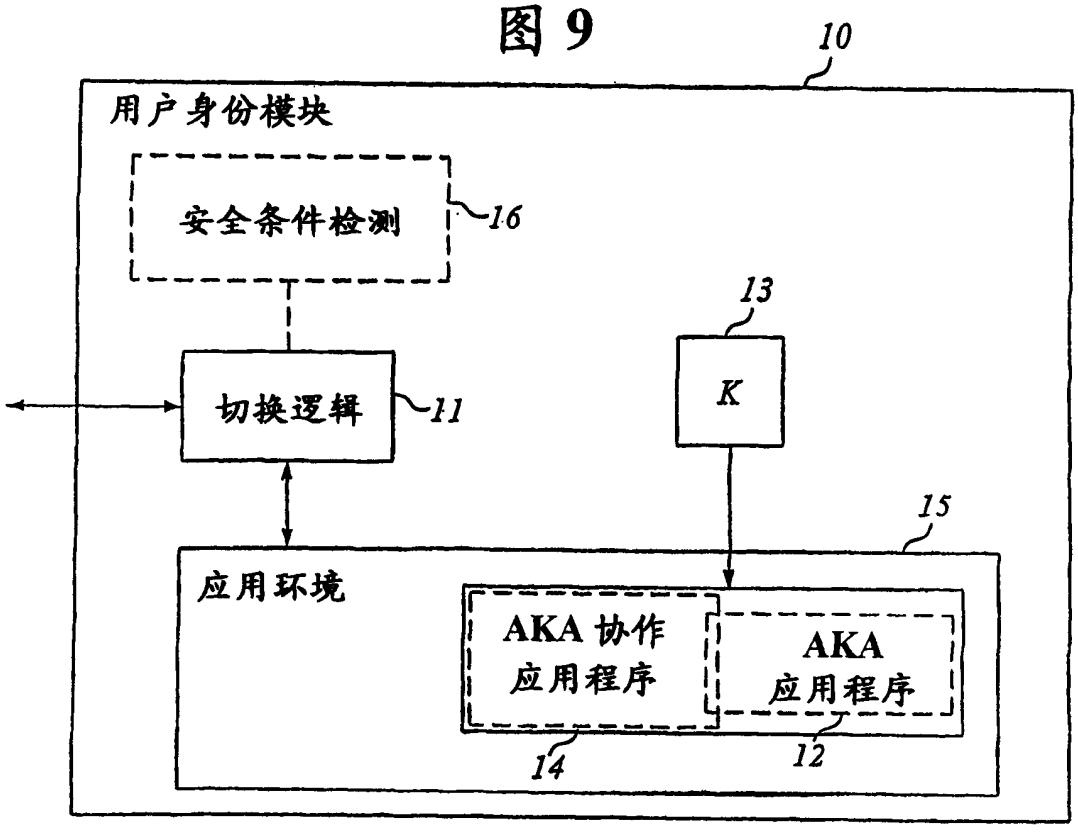
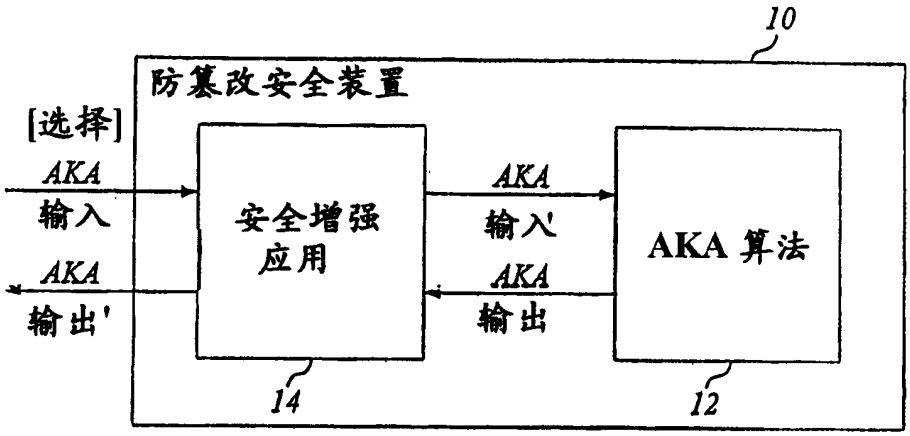

10
用户身份模块
安全条件检测
16
13
切换逻辑
11
K
15
应用环境
AKA 协作
应用程序
AKA
应用程序
14
12

图 10


10
防篡改安全装置
[选择]
AKA
输入
AKA
输出'
安全增强
应用
AKA
输入'
AKA
输出
AKA 算法
14
12

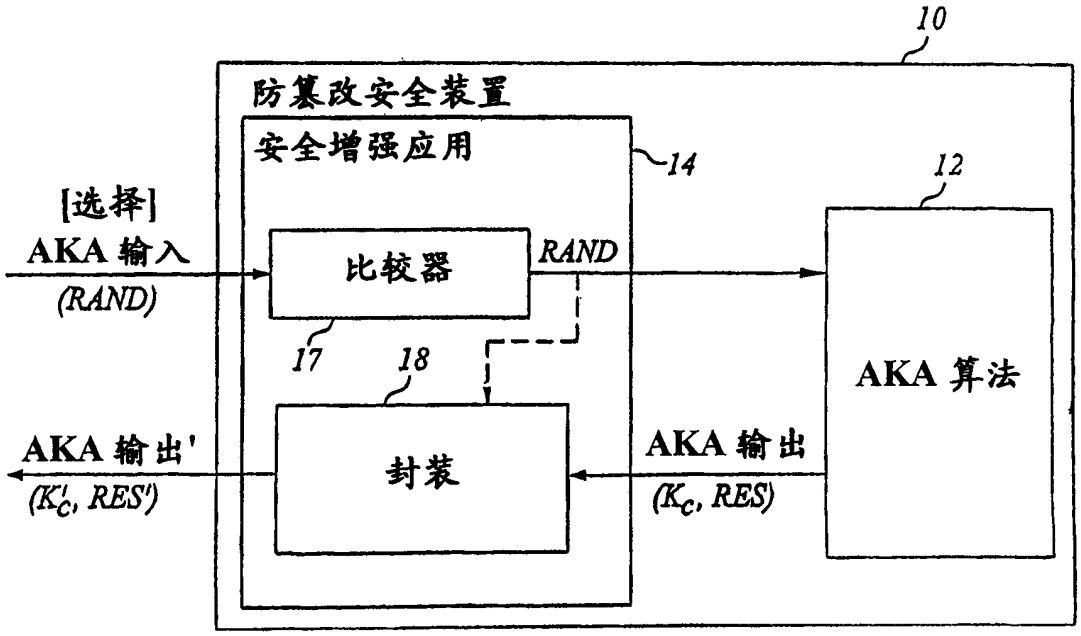

10
防篡改安全装置
安全增强应用
14
12
[选择]
AKA 输入
(RAND)
比较器
RAND
17
18
AKA 算法
AKA 输出'
(K'C, RES')
封装
AKA 输出
(KC, RES)

图 11

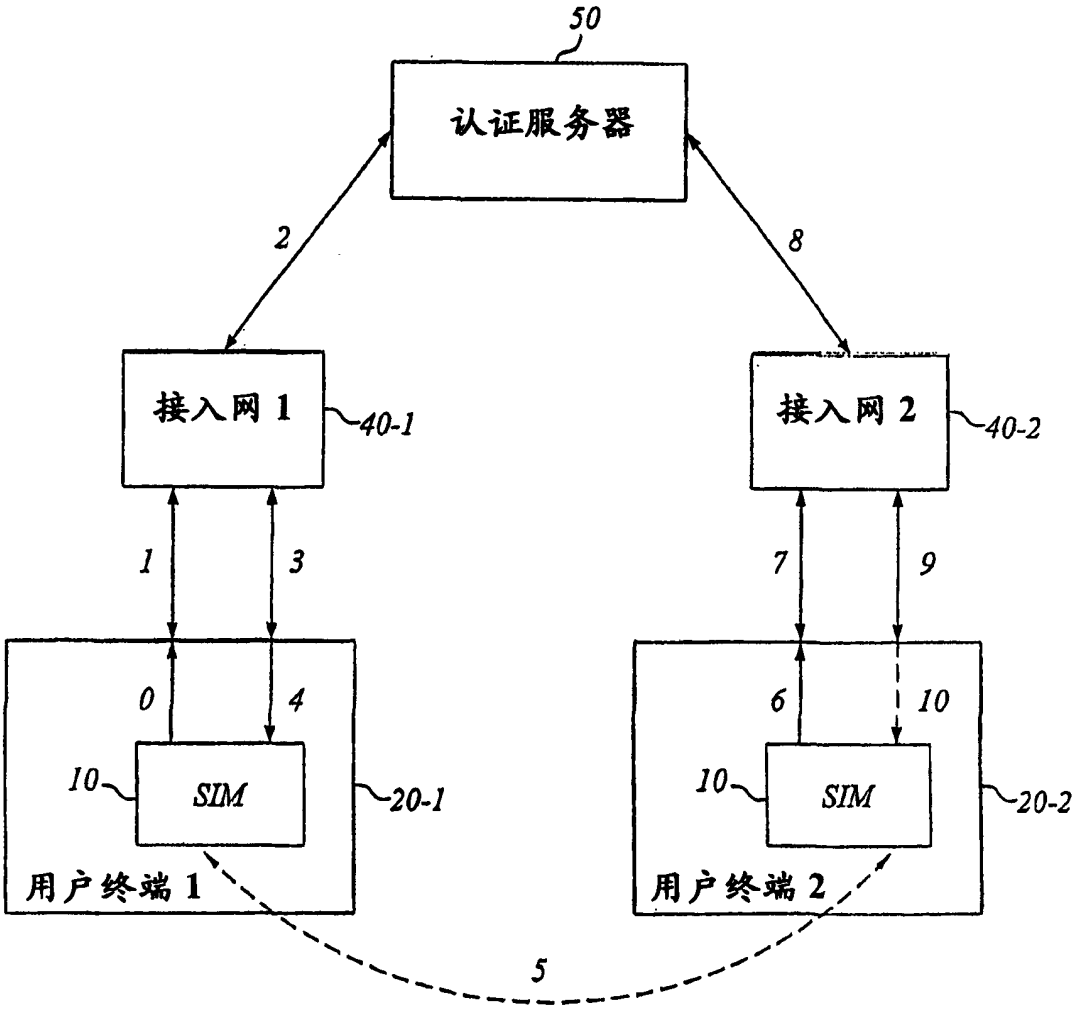

50
认证服务器
2
8
接入网 1
40-1
接入网 2
40-2
1
3
7
9
0
4
6
10
10
SIM
20-1
10
SIM
20-2
用户终端 1
用户终端 2
5

图 12

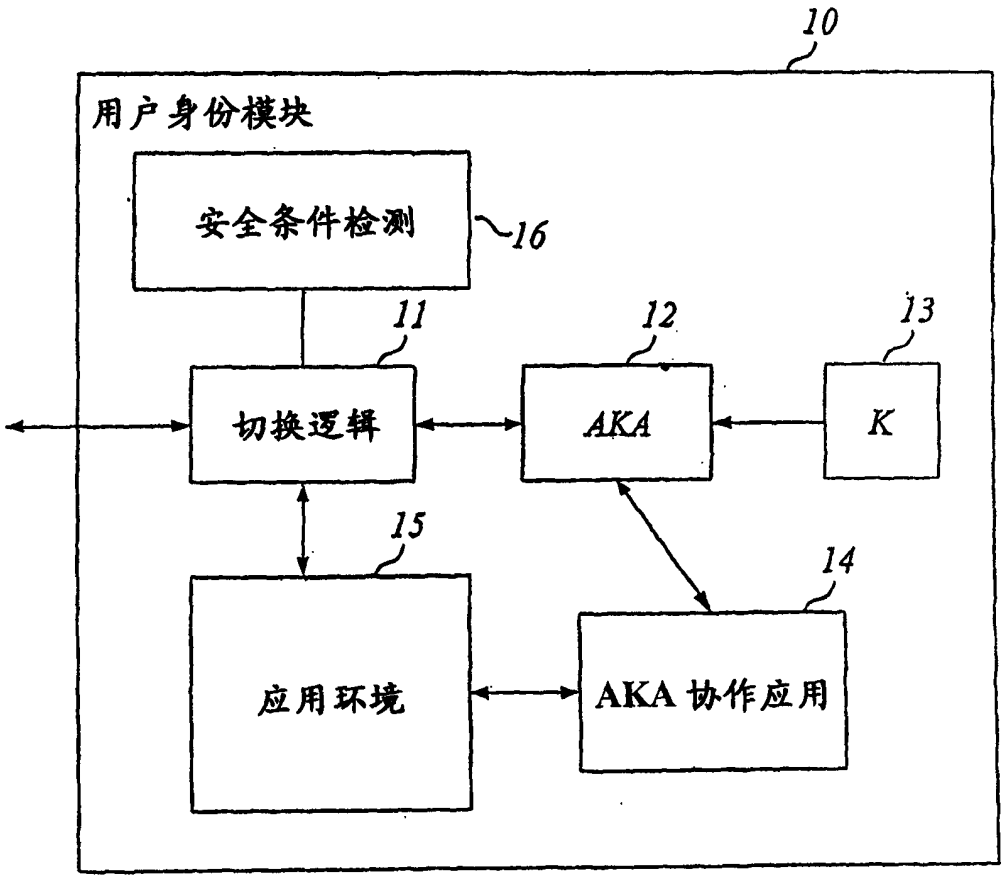


图 13