(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 104038340 A
(43)申请公布日 2014.09.10

(21)申请号 201410075945.X

(22)申请日 2014.03.04

(30)优先权数据
13305245.6 2013.03.04 EP

(71)申请人 汤姆逊许可公司
地址 法国伊西莱穆利诺

(72)发明人 E. 德斯米切特 O. 考泰 R. 里加尔

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 叶齐峰

(51)Int.Cl.
H04L 9/14(2006.01)
H04L 9/08(2006.01)

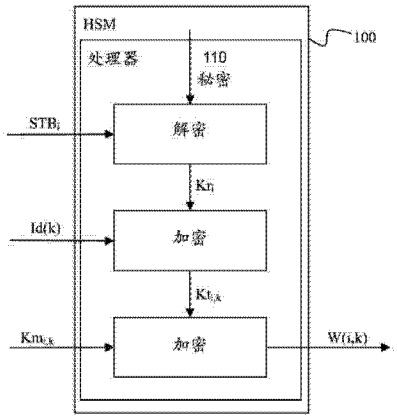
权利要求书1页 说明书4页 附图3页

(54)发明名称

生成加密密钥的设备和向接收器提供加密密钥的方法

(57)摘要

一种用于生成加密的主密钥的设备(100)。该设备(100)包括至少一个输入接口，被配置成接收接收器标识符(STB_i)、服务提供商标识符(Id(k))和用于服务提供商的主密钥($Km_{j,k}$)；存储器，被配置为存储该设备的机密；处理器，被配置为：使用该机密处理接收器标识符以获取根密钥(Kr_i)，使用该根密钥处理服务提供商标识符以获取顶部密钥($Kt_{i,k}$)，并使用该顶部密钥处理主密钥以获取加密的主密钥(W(i,k))；以及输出接口，被配置为输出加密的主密钥。还提供了一种向接收器提供加密的主密钥的方法。一个优点是该设备可以使新服务提供商能够使用已部署的智能卡向接收器提供服务。



CN 104038340 A

1. 一种用于生成加密的主密钥的设备(100),该设备(100)包括:

- 至少一个输入接口,被配置成接收接收器标识符(STB_i)、服务提供商标识符(Id(k))和用于服务提供商的主密钥($Km_{j,k}$);

- 存储器,被配置为存储该设备的机密;

- 处理器,被配置为:

- 使用该机密处理接收器标识符以获取根密钥(Kr_i);

- 使用该根密钥处理服务提供商标识符以获取顶部密钥($Kt_{i,k}$);以及

- 使用该顶部密钥处理主密钥以获取加密的主密钥(W(i,k));以及

- 输出接口,被配置为输出加密的主密钥。

2. 根据权利要求 1 所述的设备,其中,该设备是以硬件安全模块实现的。

3. 根据权利要求 1 所述的设备,其中,该设备是以智能卡实现的。

4. 根据权利要求 1 所述的设备,其中,该处理器被配置为使用所述机密作为解密密钥来解密接收器标识符。

5. 根据权利要求 1 所述的设备,其中,该处理器被配置为使用所述根密钥作为加密密钥来加密服务提供商标识符。

6. 根据权利要求 1 所述的设备,其中,该处理器被配置为使用所述顶部密钥作为加密密钥来加密主密钥。

7. 一种向接收器提供加密的主密钥的方法,该方法包括以下步骤:

- 由根据权利要求 1 的用于生成加密的主密钥的设备接收接收器标识符(STB_i)、服务提供商标识符(Id(k))及用于服务提供商的主密钥($Km_{j,k}$),用于从第一设备生成加密的主密钥;

- 由用于生成加密的主密钥的该设备生成加密的主密钥;

- 由用于生成加密的主密钥的该设备输出所生成的加密的主密钥;以及

- 由第三设备将加密的主密钥发送给接收器。

生成加密密钥的设备和向接收器提供加密密钥的方法

技术领域

[0001] 本发明总地涉及密码系统，具体地涉及以安全的方式使得能够部署由新服务提供商提供的需要密码密钥的服务。

背景技术

[0002] 本节旨在向读者介绍本领域的各个方面，这可能与所描述的和 / 或要求保护的本发明的各个方面相关。相信这种讨论对于为读者提供背景信息是有帮助的，以便于更好地理解本发明的各个方面。因此，应当理解，要从这个角度阅读这些陈述，而不是作为对现有技术的认可。

[0003] 用于电视（及其他媒体）的条件访问系统（其将被用来作为非限制性示例）已经存在了很长一段时间以保护不同类型的内容。简言之，在这种系统中，服务提供商从内容提供商获得内容并在传送给客户之前使用条件访问系统（CAS），特别是使用加密，来保护该内容。客户通常具有某种解码器，其实现条件访问系统的一部分，从而验证用户是否具有访问所述内容的权限，如果有，则解密并呈现该内容。

[0004] 如众所周知的那样，在用户端，CAS 的一部分通常是在可拆卸地插入到解码器中的智能卡（其将在本文中被用作安全模块的非限制性示例）中实现的。智能卡至少间接地由保证系统安全性的 CAS 提供商提供：无论是解码器主密钥 Km_i 还是通过其使用而获取的密钥都不应该能够从智能卡中提取。

[0005] 图 1 图示了用于访问服务的第一现有技术方案。为了允许配备有具有标识符 STBi 的智能卡的解码器访问使用服务密钥 K_j 加密（有利地对于系统中的所有解码器是通用的）的服务 j，服务提供商在传输之前使用对称加密算法（诸如例如高级加密标准 AES）和服务密钥 K_j 加密服务 j。服务提供商还使用与主密钥 Km_i 对应的密钥、以及优选地使用所述对称加密算法来加密对于所有解码器通用的服务密钥 K_j，并将加密的服务 $E\{K_j\}(j)$ 和具有加密的服务密钥的消息 M(i, j) 传输给解码器。

[0006] 该解码器首先使用对称加密算法及其主密钥 Km_i 解密消息 M(i, j) 以获取服务密钥 K_j，服务密钥 K_j 与对称加密算法一起用于解密加密的服务 $E\{K_j\}(j)$ 以获取服务 j。由于主密钥 Kmi 是特定于解码器的，因此它是能够使用消息 M(i, j) 解密该服务的唯一的一个。

[0007] 图 2 图示了用于访问服务的第二现有技术方案。为了使得在系统中能够具有更大的灵活性和更高的安全性，通常优选地使用会话密钥 $Ks_{j,t}$ 用于服务 j，典型地用于一时间段 t。在这种情况下，服务提供商使用会话密钥 $Ks_{j,t}$ 加密服务 j 以获取加密的服务 $E\{Ks_{j,t}\}(j)$，使用服务密钥 K_j 加密会话密钥 $Ks_{j,t}$ 以获取第一消息 T(j, t)，并使用解码器主密钥 Km_i 加密服务密钥 K_j 以获取第二消息 M(i, j)。加密的服务 $E\{Ks_{j,t}\}(j)$、第一消息 T(j, t) 和第二消息 M(i, j) 不一定在同一时间被发送给解码器。

[0008] 如在图 1 中，解码器逆向进行所述操作。它使用解码器主密钥 Km_i 解密第二消息 M(i, j) 以获取服务密钥 K_j，使用服务密钥 K_j 解密第一消息 T(j, t) 以获取会话密钥，该会话密钥被用于解密加密的服务 $E\{Ks_{j,t}\}(j)$ 以获取服务 j。

[0009] 图 1 和图 2 图示的方案在具有单一服务提供商的系统中工作良好。然而，最近，解码器已经开始从“只”提供内容的解密发展到包括新的应用。这种新的应用的示例包括：

[0010] • 以压缩格式传输去往用户家庭网络中其它设备，例如第二解码器、智能手机或平板电脑的增值服务。

[0011] • 从应用程序商店（如 Apple Store、Freebox Revolution）下载和执行诸如游戏的应用程序。

[0012] • 内容提供商可以经由解码器向用户提供增值服务，其中所述增值服务不在服务提供商或 CAS 提供商的控制之下。

[0013] 这意味着 CAS 的职责是不断发展的。作为整个系统的安全性的之前的保证人，它们变为负责服务提供商的增值服务的安全性，而它们同时与其它“次级”服务提供商“共享”解码器。

[0014] 次级服务提供商有可能在解码器中需要其自身的安全功能来保护它们的服务，并且该功能提供至少等于 CAS 的安全级别的安全级别。

[0015] 可以通过例如，在图 1 和图 2 中所示的那些层的顶部添加一层（storey）来添加更多的服务提供商。这种方案被图示于图 3，它扩展了图 1 所示的方案。

[0016] 更多的服务提供商具有他们的主密钥 $Km_{i,k}$，使用 $STBiKr_i$ 的根密钥对其加密以获取加密的主密钥 W(i,k)，其中 i 是 STBi 的索引，k 是服务提供商的索引。可以通过将主密钥 $Km_{i,k}$ 提供给智能卡来使用智能卡而获取该加密的主密钥 W(i,k)，只要特定的熔丝（fuse）并未烧断，该智能卡使用根密钥 Kr_i 加密主密钥 $Km_{i,k}$，并输出加密的主密钥 W(i,k)。加密的主密钥 W(i,k) 然后可被存储在智能卡外部，例如在闪存中。然而，一旦熔丝烧断，智能卡则不加密密钥，它只解密加密的密钥。

[0017] 应当指出，没有必要知道根密钥，但不可能在智能卡的生命周期期间添加服务提供商，因为出于安全原因，熔丝在被传送给最终用户之前被烧断。即使在对称加密中加密与解密是相同的，也不可能提供用于“解密”的密钥，并希望获取“解密的”（与加密的相同）密钥，因为从智能卡只输出解密的服务；中间密钥被保留在内部。

[0018] 解码器 i 接收加密的主密钥 W(i,k)，并使用根密钥 Kr_i 对其解密，并输出主密钥 $Km_{i,k}$，它被用来解密第二消息 (M,i,j,k) 以获取用于服务提供商 k 的服务密钥 $K_{j,k}$。然后，该服务密钥 $K_{j,k}$ 被用于解密加密的服务 $E\{Ks_{j,k}\}$(j,k) 以不受阻碍地获取服务 j,k。

[0019] 可以看出，存在多个所涉及的参与者：智能卡制造商、制造该解码器的集成商、一个或多个服务提供商和将解码器提供给最终用户的客户。虽然现有技术解决方案通过添加其密钥来允许定制智能卡以与多家服务提供商一起工作，但该数量限于在智能卡中的一次性可编程闪存中熔丝的数量（每增加一个密钥就烧断一个熔丝）。此外，由于必须在工厂使用一种特殊的机器添加该密钥，这些服务提供商必须在传送定制的智能卡之前是已知的。

[0020] 因此，应理解，需要一种系统，它允许最终用户访问最初未考虑的服务提供商。出于安全原因，解码器制造商应控制服务提供商的添加，并且服务提供商的密钥不应被其它参与者知道，尤其是其它服务供应商。

[0021] 本发明提供了这种可能性。

发明内容

[0022] 在第一方面，本发明涉及一种用于生成加密的主密钥的设备。该设备包括至少一个输入接口，被配置成接收接收器标识符、服务提供商标识符、和用于服务提供商的主密钥；存储器，被配置为存储该设备的机密（secret）；处理器，被配置为：使用该机密处理接收器标识符以获取根密钥，使用该根密钥处理服务提供商标识符以获取顶部密钥，并使用该顶部密钥处理主密钥以获取加密的主密钥；以及输出接口，被配置为输出加密的主密钥。

[0023] 在第一实施例中，该设备是在硬件安全模块中实现的。

[0024] 在第二实施例中，该设备是在智能卡中实现的。

[0025] 在第三实施例中，该处理器被配置为使用所述机密作为解密密钥来解密接收器标识符。

[0026] 在第四实施例中，该处理器被配置为使用所述根密钥作为加密密钥来加密服务提供商标识符。

[0027] 在第五实施例中，该处理器被配置为使用所述顶部密钥作为加密密钥来加密主密钥。

[0028] 在第二方面，本发明涉及一种向接收器提供加密的主密钥的方法。根据第一方面的用于生成加密的主密钥的设备接收接收器标识符（STB_i）、服务提供商标识符（Id(k)）及用于服务提供商的主密钥（$Km_{j,k}$），该服务提供商从第一设备生成加密的主密钥；生成加密的主密钥；以及输出所生成的加密的主密钥，该加密的主密钥由第三设备发送给接收器。

附图说明

[0029] 将参照附图，通过非限制性示例的方式描述本发明的优选特征，附图中

[0030] 图 1 图示用于访问服务的第一现有技术方案；

[0031] 图 2 图示用于访问服务的第二现有技术方案；

[0032] 图 3 图示用于访问服务的第三现有技术方案；

[0033] 图 4 图示根据本发明的优选实施例访问服务，以及

[0034] 图 5 图示根据本发明的优选实施例的硬件安全模块。

具体实施方式

[0035] 现有技术解决方案需要解码器制造商在制造解码器之前知道服务提供商。

[0036] 添加其它密钥层使得有可能解决这个问题。此外，如将在下文中进一步描述的，每个服务提供商具有不需要是机密的唯一的标识符 Id(k)，以及生成加密的主密钥的设备。

[0037] 图 4 图示根据本发明的优选实施例访问服务，这是图 3 所图示的方案的扩展。诸如智能卡的处理器或解码器 i 的片上系统中的密码处理器以以下至少两种方式之一访问其根密钥 Kr_i：根密钥可能被写入其存储器中，或者它可以通过使用该处理器的机密以解密加密的根密钥来生成——后一选项示于虚线框中。处理器接收服务提供商 k 的标识符 Id(k)，并使用其根密钥 Kr_i 对其解密以获取该处理器和服务提供商的顶部（top）密钥 $Kt_{i,k}$。使用顶部密钥 $Kt_{i,k}$ 解密加密的主密钥 W(i,k) 以获取主密钥 $Km_{i,k}$，它被用于解密第二消息 (M,i,j,k) 以获取服务提供商 k 的服务密钥 $K_{j,k}$。然后，该服务密钥 $K_{j,k}$ 被用于解密加密的服务 $E\{Ks_{j,k}\}(j,k)$ 以不受阻碍地获取服务 j,k。

[0038] 如图 5 所图示，服务提供商 k 使用由解码器制造商所提供的所谓的硬件安全模块

(HSM)100 以安全的方式为用户 i 获取加密的主密钥 W(i,k)。实施 HSM100 以使得其机密信息对外部保持为隐蔽。HSM100 包括至少一个处理器 110 和其它必要的,但是,为了清楚起见,未图示的特征,诸如输入和输出接口、存储器、内部连接和电源(其能量可以从外部提供)。

[0039] HSM100 从一设备接收接收器的标识符 STBi、服务提供商标识符 Id(k) 和用于服务提供商和接收器的主密钥 $Km_{i,k}$。处理器 110 从内部存储器获取 HSM 的机密并用它解密标识符 STBi 以获取根密钥 Kr_i。然后,处理器使用根密钥 Kr_i 加密服务提供商标识符 Id(k) 以获取顶部密钥 $Kt_{i,k}$,然后该顶部密钥 $Kt_{i,k}$ 被用于加密主密钥 $Km_{i,k}$ 以获取加密的主密钥 W(i,k),然后,该加密的主密钥 W(i,k) 通过 HSM100 输出并被发送到解码器 i,在该处它可以被用来访问服务。因为加密的主密钥 W(i,k) 已被加密,就没有必要将它进一步加密以传输(使用任何合适的传输设备和方法,诸如电子邮件或带内传输)到解码器。但应注意的是,在对称加密中,加密和解密基本上是相同的。

[0040] 应理解,由于顶部密钥 $Kt_{i,k}$ 不被 HSM100 输出,因此它不能被服务提供商改变,这意味着从安全的角度来看,服务提供商彼此隔离。

[0041] 本领域技术人员将理解,本发明能够提供一种解决方案,它允许智能卡以安全的方式访问新的服务提供商。

[0042] 在说明书和(适当的地方的)权利要求书以及附图中所公开的每个特征可以独立地或以任何适当的组合来提供。被描述为以硬件实现的特征也可以以软件实现,反之亦然。权利要求中出现的参考标号仅仅是图示的方式,并应对权利要求的范围不起到任何限制作用。

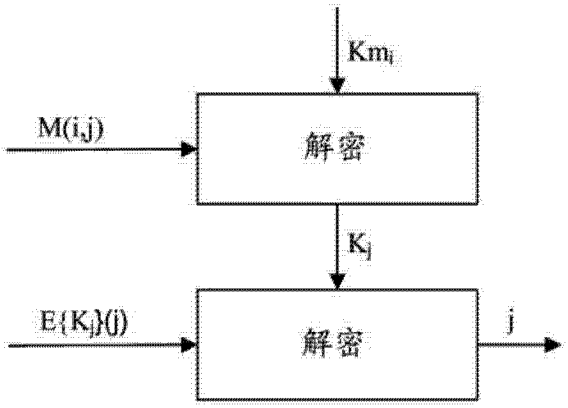

Km_i
M(i,j)
解密
K_j
E{K_j}(j)
解密
j

图 1

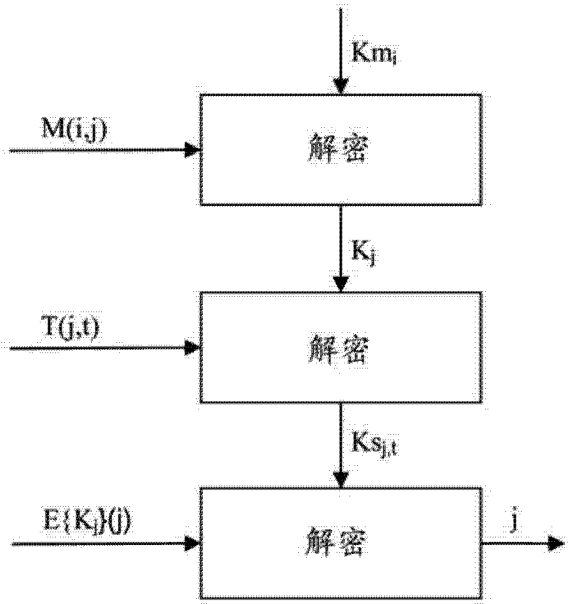

Km_i
M(i,j)
解密
K_j
T(j,t)
解密
Ks_j,t
E{K_j}(j)
解密
j

图 2

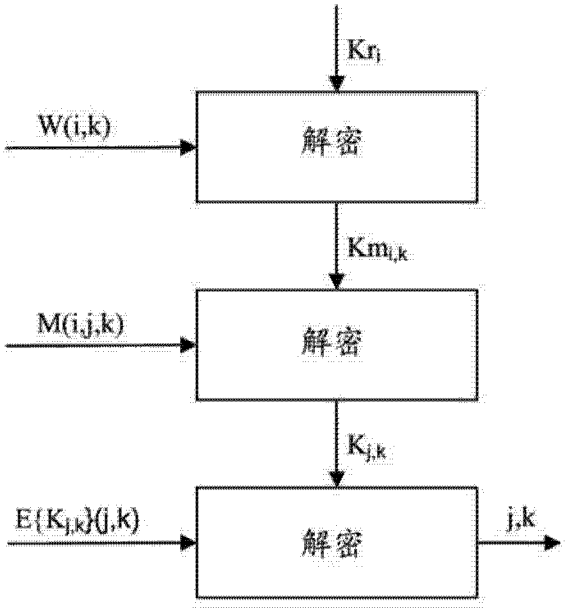

Kr_i
W(i,k)
解密
Km_i,k
M(i,j,k)
解密
K_j,k
E{K_j,k}(j,k)
解密
j,k

图 3

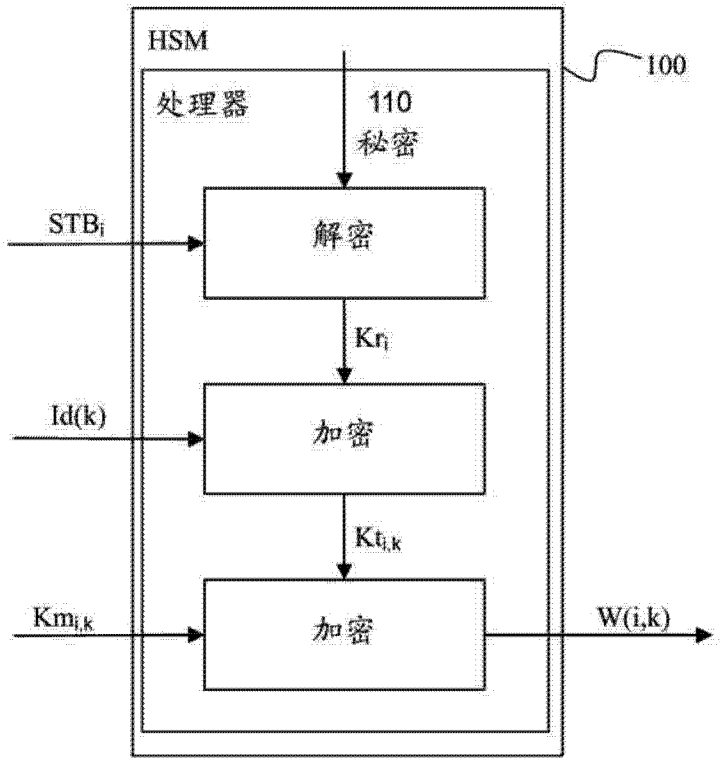


图 5

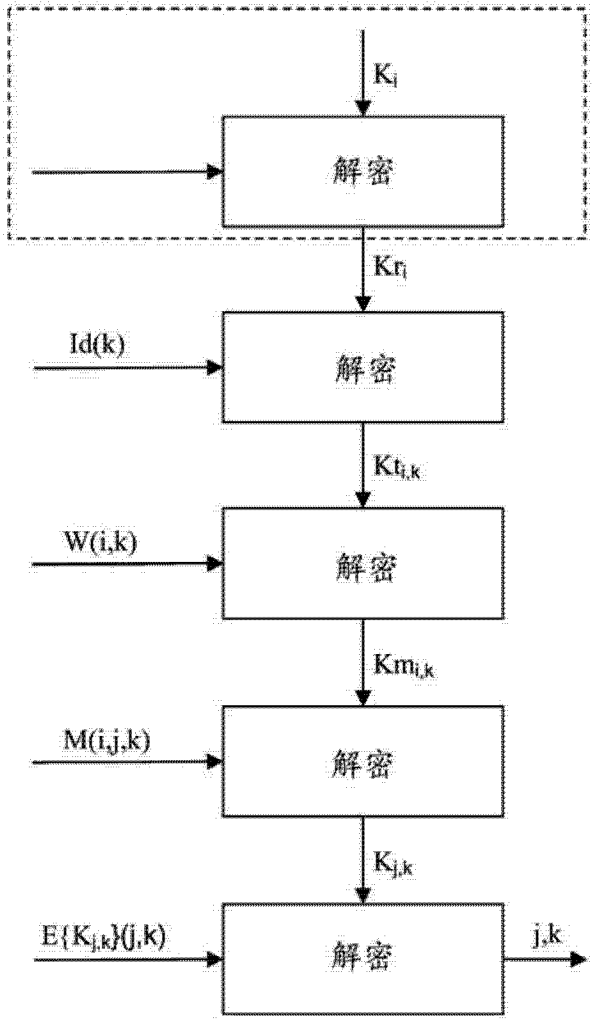


图 4