

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)



[12] 发明专利说明书

专利号 ZL 02816627.2

[45] 授权公告日 2008 年 12 月 3 日

[11] 授权公告号 CN 100440884C

[22] 申请日 2002. 8. 23 [21] 申请号 02816627. 2

[30] 优先权

[32] 2001. 8. 24 [33] FR [31] 01/11078

[86] 国际申请 PCT/FR2002/002928 2002. 8. 23

[87] 国际公布 WO2003/019899 法 2003. 3. 6

[85] 进入国家阶段日期 2004. 2. 24

[73] 专利权人 汤姆森许可贸易公司

地址 法国布洛里

[72] 发明人 让-皮埃尔·安德烈奥斯

埃里克·迪尔 阿兰·迪朗

[56] 参考文献

WO0062505A 2000. 10. 19

CN1282475A 2001. 1. 31

EP0382296A 1990. 8. 16

CN1211363A 1999. 3. 17

CN1167304A 1997. 12. 10

审查员 彭 锐

[74] 专利代理机构 中科专利商标代理有限责任公
司

代理人 戎志敏

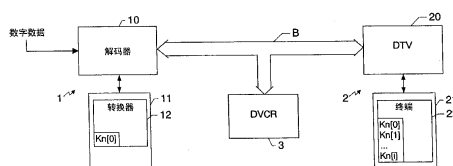
权利要求书 2 页 说明书 12 页 附图 1 页

[54] 发明名称

本地数字网络、安装新设备的方法及数据广播和接收方法

[57] 摘要

本发明涉及一种本地数字网络，包括：至少一个源设备(1)，设计用于通过网络广播数据(60)；以及至少一个接收机设备(2)，设计用于接收所述数据(60)，源设备(1)使用网络有效加密密钥($K_n[0]$)对趋向于要在网络中广播的数据进行加密；以及接收机设备(2)包括：网络有效解密密钥($K_n[0]$)，用于对利用所述有效加密密钥加密过的数据进行解密；以及该网络的至少一个解密密钥($K_n[i]$)，用于对利用先前在网络中所使用的加密密钥加密过的数据进行解密，接收机设备(2)适合于包含自从网络创建以来先前所使用的所有网络解密密钥。本发明还涉及在这样的网络中安装新设备，以及从源设备到接收机设备发送数据。



1. 一种本地数字网络，包括：
 - 至少一个源设备（1），设计用于通过网络广播数据（60）；以及
 - 至少一个接收机设备（2），设计用于接收所述数据（60），其特征在于：源设备（1）使用网络有效加密密钥对趋向于要在网络中广播的数据进行加密；以及接收机设备（2）包括：
 - 网络有效解密密钥，用于对利用所述有效加密密钥加密过的数据进行解密；以及
 - 该网络的至少一个解密密钥，用于对利用先前在网络中所使用的加密密钥加密过的数据进行解密，其特征还在于：接收机设备（2）适合于包含自从网络创建以来先前所使用的所有网络解密密钥。
2. 根据权利要求 1 所述的本地数字网络，其特征在于：源设备（1）和接收机设备（2）使用对称加密处理，并且在网络中所使用的加密密钥和相应的解密密钥是相同的。
3. 一种在已经包括至少一个接收机设备的根据前述权利要求之一所述的本地数字网络中安装新接收机设备（2）的方法，其特征在于网络中的先前存在的接收机设备拥有网络有效解密密钥和在网络中先前使用过的至少一个解密密钥，并且能够以安全的方式来发送这些密钥，所述接收机设备向新接收机设备发送所述解密密钥。
4. 一种在已经包括至少一个接收机设备（2）的根据权利要求 2 所述的本地数字网络中安装新源设备（1）的方法，网络中的先前存在的接收机设备拥有网络有效解密密钥和在网络中先前使用过的至少一个解密密钥，并且能够以安全的方式来发送这些密钥，所述接收机设备向新源设备发送所述网络有效解密密钥。
5. 一种由与根据权利要求 1 或 2 所述的网络链接的源设备（1）

传送数据的方法，其特征在于所述方法在于：

- 利用网络有效加密密钥对数据进行加密；以及
- 传送所述已加密数据（611）以及与网络的网络有效加密密钥相对应的索引。

6. 一种在与根据权利要求 1 或 2 所述的网络链接的接收机设备（2）中接收根据权利要求 5 所述的方法进行广播的数据的方法，其特征在于所述方法在于：

- 从接收到的数据中提取与用于加密所述数据的网络加密密钥相对应的索引；
- 从该索引推算相应的网络解密密钥；以及
- 利用所述解密密钥对数据进行解密。

本地数字网络、安装新设备的方法及数据广播和接收方法

技术领域

本发明通常涉及本地数字网络领域，更具体地，涉及家用数字网络。更为准确地说，本发明涉及针对环流这种网络的数字数据的复制的保护。

背景技术

这种网络是通过如根据IEEE 1394标准的总线等数字总线而链接在一起的设备的集合。该网络特别地包括两种类型的设备：

— 源设备，能够通过网络来发送数据：这些设备可以恢复通过网络外部的“信道”的数据。

— 接收机设备，适合于接收流过所述网络的数据，以便对其施加方法（method them），或者将其显示给用户。

因此，考虑用于将音频和/或视频数据传送到住所中的各个房间的家用数字网络的示例，例如，源设备是通过卫星天线或者通过电缆连接从网络外部接收视频节目的数字解码器，或者通过网络以数字形式传送从盘（在这种情况下，所述盘包含来自网络外部的数据）中读取的数据（音频和/或视频）的光盘读取器。例如，接收机设备是能够观看从网络接收到的视频节目的电视接收机，或者更一般地，能够对已加密数据进行解码的任何类型的设备。

从提供了来自本地网络外部的数据的内容提供商的观点来看，尤其是诸如传送付费TV（电视）节目的服务提供商或者光盘出版商，需要防止所传送的这些数据被复制或者容易地从一个本地网络流动到另一网络（诸如通过将其复制到光盘或其他任何记录介质中）。

为了实现此目的，已知的手段是通过利用已授权接收数据的设备预先知道的密钥、或者根据内容提供商和这些设备之间的特定安全协

议交换的密钥，借助于密码算法对数据进行加密，以便以秘密的形式传送数据。

在1999年4月13日以THOMSON多媒体公司的名义递交的、并且以参考号FR-A-2 792 482公布的法国专利申请涉及一种家用网络，其中，使用网络专用的公用密钥对网络设备之间流动的、典型地从先前提到的源设备流到接收机设备的数据进行加密。只有该网络的接收机设备拥有与所述公用密钥相对应的专用密钥。由于（公用密钥，专用密钥）密钥对专用于所述网络，在该网络的框架内被加密的数据不能够由另一网络的设备进行解密。

在2001年4月25日以THOMSON许可贸易公司的名义提出的法国专利申请No. 01 05568本身涉及一种用于在如上述网络等实质上使用对称密钥的网络中管理密钥的方法。源设备利用非常频繁地更新的第一对称密钥对数据进行加密，然后所述源设备以利用专用于该网络的第二对称密钥进行加密的形式，将该第一密钥发送到网络中的另一设备。所述第二对称密钥包含在接收机设备中。

在上述两种方案中，通过专用于该网络的同一加密密钥（或者同一专用/公用密钥对）以及通过同一加密算法，对数据进行保护。然而，有时候可能需要更新所使用的这些密钥和/或加密算法，特别是如果加密算法使用了过短的密钥，或者如果其不再安全，与密钥的长度无关，从而使用具有更大长度的密钥或者更强大的加密算法。不幸地，在这种情况下，利用新密钥和/或新加密算法不再能够在网络中解密先前所记录的数据。

发明内容

本发明的主题是一种本地数字网络，包括：

- 至少一个源设备，设计用于通过网络广播数据；以及
- 至少一个接收机设备，设计用于接收所述数据，

根据本发明，源设备使用网络有效加密密钥对趋向于要在网络中广播的数据进行加密；以及接收机设备包括：网络有效解密密钥，用于对利用所述有效加密密钥加密过的数据进行解密；以及该网络的至

少一个其他解密密钥，用于对利用先前在网络中所使用的加密密钥加密过的数据进行解密。此外，接收机设备适合于包含自从网络创建以来先前所使用的所有网络解密密钥。

所述本地数据网络还可以包括一个或者多个以下特征：

— 源设备包含网络有效加密密钥，并且该源设备利用网络的所述有效密钥对趋向于要在网络中广播的数据进行加密。

— 源设备包括：第一对称密钥、利用网络有效加密密钥加密过的所述第一对称密钥；所述源设备利用所述第一对称密钥对趋向于要在网络中广播的数据进行加密，以及所述源设备适合于利用所述已加密数据，传送由网络有效加密密钥加密过的第一对称密钥。

— 源设备和接收机设备使用对称加密方法，并且在网络中所使用的加密密钥和相应的解密密钥是相同的。

本发明还涉及一种在已经包括至少一个接收机设备的前述本地数字网络中安装新接收机设备的方法。根据该方法，网络中的先前存在的接收机设备拥有网络有效解密密钥和在网络中先前使用的至少一个解密密钥，并且能够以安全的方式来发送这些密钥，所述接收机设备向新接收机设备发送所述解密密钥。

本发明的另一方面涉及一种在前述本地数字网络中安装新源设备的方法，在所述本地数字网络中，源设备和接收机设备使用对称加密方法，并且在网络中所使用的加密密钥和相应的解密密钥是相同的。根据该方法，网络中的先前存在的接收机设备拥有网络有效解密密钥和在网络中先前使用的至少一个解密密钥，并且能够以安全的方式来发送这些密钥，所述接收机设备向新源设备发送所述网络有效解密密钥。

本发明还涉及一种由与前述网络链接的源设备传送数据的方法，在所述网络中，所使用的加密密钥和解密密钥是相同的。所述方法在于：利用所述网络有效加密/解密密钥对数据进行加密；以及将所述已加密数据和有效密钥的指纹（fingerprint）一起传送，利用应用于网络的有效密钥的单向函数计算所述指纹。

本发明还涉及一种在与前述网络链接的接收机设备中接收已加密数据的方法，已经根据前述方法对所述数据进行了广播，所述接收机设备还包含其所包括的、利用应用于所述密钥的单向函数计算得到的每个加密/解密密钥的指纹。所述方法在于：从接收到的数据中提取密钥指纹；将所提取的指纹与接收机中所包含的加密/解密密钥的指纹进行比较；以及在所提取的指纹和存储在接收机设备中的指纹之一相同的情况下，利用与所述指纹相对应的密钥对数据进行解密。

本发明还涉及另一种由与如述网络链接的源设备传送数据的方法。所述方法在于：(a) 将单向函数应用于数据的第一部分；(b) 利用网络有效加密密钥对步骤(a)中所进行计算的结果以及要保护的数据的第二部分进行加密；以及(c) 通过网络传送在步骤(b)中已加密的所述数据以及数据的第一部分。

本发明还涉及一种在与前述网络链接的接收机设备中接收按照上述方法进行广播的数据的方法。所述方法在于：(a) 将单向函数应用于未加密数据的第一部分；(b) 利用接收机设备中所包含的网络加密密钥对数据的第二部分进行解密；以及(c) 将在步骤(b)中进行了解密的数据部分的解密结果与在步骤(a)中进行的计算的结果进行比较，从而：

一 在相同的情况下，恢复步骤(b)中所解密的数据的剩余部分；以及

一 在不同的情况下，返回到步骤(b)，以便利用接收机设备中所包含的另一网络解密密钥对数据的第二部分进行解密。

本发明还涉及一种由与前述网络链接的源设备传送数据的第三种方法。所述方法在于：利用网络有效加密密钥对数据进行加密；以及传送所述已加密数据以及与网络的有效密钥相对应的索引。

本发明还涉及一种在与前述网络链接的接收机设备中接收按照上述方法进行广播的数据的方法，所述方法在于：从接收到的数据中提取与用于加密所述数据的网络加密密钥相对应的索引；从该索引推算相应的网络解密密钥；以及利用所述解密密钥对数据进行解密。

附图说明

通过利用附图所进行的多个非限定性的特定典型实施例的描述，本发明的其他特征和优点将变得显而易见，其中：

- 图1示意性地示出了根据本发明的网络；以及
- 图2示出了环流该网络的数据。

具体实施方式

在图1中，我们已经按照示意的方式示出了典型的家用数字网络，其中，通过使用在前述专利申请（以THOMSON多媒体公司的名义的申请FA-A-2 792 482和以THOMSON许可贸易公司的名义的申请FR No. 01 05568）中所描述的原理，针对复制对数据进行保护，可以更详细地对这些申请加以参考。

所述网络包括源设备1、接收机设备2和记录设备3，这些设备通过如按照IEEE 1394标准的总线等数字总线B链接在一起。

源设备1包括安装有智能卡读取器的数字解码器10，所述智能卡读取器配备有智能卡11。该解码器接收数字数据，尤其是由服务提供商分布的音频/视频节目。

接收机设备2包括安装有智能卡读取器的数字电视接收器（DTV）20，所述智能卡读取器配备有智能卡21，而记录设备3特别是数字录像机（DVCR）。

通常根据付费TV的原理，对经由源设备1输入网络的数字数据进行数据加扰。利用以加密密钥K加密的形式在数流中发送的、并包含在控制消息（ECM，表示权利控制消息）中的控制控制字（CW），对数据进行加扰。使加密密钥K对已经付费来接收数据的用户有效，特别地，通过将其存储在智能卡中。在图1的示例中，假定智能卡11包含这样的密钥K。

接收这些已加扰数字数据的源设备1随后对数据进行成形，从而使其通过数字网络进行广播。为此，由包含在智能卡11中的转换器模块12将包括利用密钥K进行了加密的控制字的ECM消息转换为包含已解密控制字的LECM消息（表示本地权利控制消息），利用专用于本地家用

网络的密钥来保护所述的LECM消息。

因此，环流该网络数据由图2所示的分组60组成。所述分组60包括：已加扰数据62和LECM消息61。LECM消息自身包括两个部分：

- 包括明文数据的部分610，即未加密数据。该部分可以特别是具有LECM消息大小的分组报头、复制保护系统的版本号等；以及
- 包含受保护数据的部分611，特别是控制字CW。

在以下描述中，出于简化的原因，将考虑利用网络的秘密密钥（或对称密钥） K_n 对在LECM消息中的部分611中所保护的数据进行加密。然而，本发明还用作在使用一种用于管理密钥的更复杂系统的情况下的一种变体，如在前述以THOMSON许可贸易公司的名义的申请FR No. 01 05568中所描述的那样。在随后描述的实施例中，将更简要地描述该变体。

由以智能卡21的终端模块22中的LECM消息为方法的接收机设备2来接收如分组60等数据分组。终端模块22包含网络的秘密密钥 K_n ，因此，能够解密LECM消息中受保护的部分。利用这些已解密消息的内容，接收机设备恢复已经用于对“有用”数据62进行加扰的控制字CW，因而能够对这些数据进行解扰，以便将其显示给用户。

将会注意到，记录设备3接收要以包含已加扰数据的分组60的形式进行记录所述数据。

当然，家用数字网络可以包含多个源设备、多个接收机设备和多个记录设备。在这种情况下，源设备的所有转换器必须包含网络的秘密密钥 K_n ，以便产生LECM消息，并且接收机设备的所有终端必须包含密钥 K_n ，以便对LECM消息中受保护的部分进行解密。

而且，家用数字网络可能会发展。因此，用户可以添加设备或从网络中去除设备。可能需要改变网络的密钥 K_n ，或者使用新的加密算法，特别是在危及到系统的安全性时。

根据本发明的原理，接收机设备的每一个终端模块保存自从家用数字网络创建以来已经使用过的所有密钥 $K_n[i]$ 。在这些密钥中，单一密钥是“有效的”，在下文中将其表示为 $K_n[0]$ 。另一方面，源设备的转换器模块只包含该激活网络密钥 $K_n[0]$

因此，在网络中较早记录的数据仍然可以由拥有自从网络创建以来用于对LECM消息加密的所有密钥的接收机设备来读取。就其所关心的，源设备只需要激活密钥 $Kn[0]$ ，以便产生针对输入网络的新数据的LECM消息。

在这一点上，将要注意的是，输入网络的数字数据不必依照上述形式（利用加密形式包含在ECM消息中的控制字进行了加扰的数据），而与源设备接收来自网络外部的数据的形式无关，源设备以如图2所示的分组的形式通过网络来发送这些数据。如果需要的话，源设备自身产生控制字，并在LECM消息的受保护部分中发送这些数据之前，利用这些控制字对数据进行加扰。

如上面所看到的那样，所有接收机设备（在其终端模块中）拥有所有的密钥 $Kn[i]$ 。当新接收机设备与网络连接时，该接收机设备从作为先辈的网络中的特定接收机设备那里接收所有这些密钥，还表示出哪一个密钥是有效的。

实际上，每一个接收机设备可以处于以下状态之一：未成熟的、先辈的、或者无子代的（Virgin, Progenitor, Sterile）。

未成熟接收机设备被定义为不包括网络密钥 $Kn[i]$ 的情况。这典型地是还未与网络链接的设备。这是接收机设备的默认状态。

无子代设备被定义为拥有网络密钥 $Kn[i]$ 、但是其不能向另一设备发送这些密钥的情况。

先辈设备被定义为拥有网络密钥 $Kn[i]$ 、并且其可以向网络中的另一设备发送这些密钥的情况。在网络中只存在一个先辈。

由如位于接收机设备的终端模块22中的寄存器等状态指示器来存储接收机设备的状态。

此外，在前述专利申请（以THOMSON多媒体公司的名义的申请FR-A-2 792 482和以THOMSON许可贸易公司的名义的申请FR No. 01 05568）中可以找到与创建新网络的方式、以及当新设备与网络连接时在设备之间交换密钥的方式有关的另外的细节。

当新源设备与网络连接时，先辈接收机设备只向其发送有效网络密钥 $Kn[0]$ 。然后将密钥 $Kn[0]$ 存储在新源设备的转换器中。在利用更

为复杂系统来管理密钥的实施例变体中，源设备不接收其自身的有效网络密钥，而是接收基于该密钥的信息项。更准确地说，如在前述申请FR No. 01 05568中所述，新的源设备产生对称加密密钥 K_c ，该密钥 K_c 随后用来加密LECM消息中要保护的数据。该新源设备将此对称密钥 K_c 以安全的方式发送到网络的先辈接收机设备，该先辈接收机设备向其发回利用有效网络密钥 $K_n[0]$ 加密的密钥 K_c 。然后，新源设备将加密 $E_{K_n[0]}(K_c)$ 的结果存储在其转换器模块中。当随后该新接收机设备在网络中传送数据时，该新源设备将在LECM消息的未编码部分610中包括利用有效网络密钥 $K_n[0]$ 对对称密钥 K_c 的加密 $E_{K_n[0]}(K_c)$ 。

当接收机设备接收要显示给用户的数据时，以分组60的形式发送的这些数据中的每一个都包含已加扰数据和LECM消息，接收机设备必须首先确定用于对LECM消息中的数据进行了加密的密钥 $K_n[i]$ 。

这可以通过对存储在接收机设备的终端模块中的所有密钥进行穷举尝试（下述实施例B）、或者通过使用索引（下述实施例C）、又或者优选地，通过使用包含在LECM消息中的密钥指纹（下述实施例A）来进行。

A] 使用指纹

在本实施例中，假定每一个接收机设备包含存储在其终端模块中的表，例如下面的表1，其中：

— “密钥”列包含已经存在于网络中或者在网络中有效的 N 个网络秘密密钥中的每一个；有效网络密钥是密钥 $K_n[0]$ 。包含密钥的字段具有固定尺寸，大到足以考虑到密钥尺寸的未来可选值，但是所存储的密钥可以具有比字段尺寸更小的尺寸；

— “ H （密钥）”列包括应用于每一个密钥 $K_n[i]$ 的单向函数 H 的结果；优选地，使用散列函数SHA-1；

— “@process_function”列包含指向嵌入在包含终端模块的智能卡中的软件中所包括的处理函数的指针。

密钥	H (密钥)	@processing_function
Kn[0]	H(Kn[0])	@processing_function[0]
.....
Kn[i]	H(Kn[i])	@processing_function[i]
.....
Kn[N]	H(Kn[N])	@processing_function[N]

表1

根据本实施例，当新源设备与网络链接时，先辈接收机设备向其发送有效网络密钥Kn[0]。将密钥Kn[0]存储在源设备的转换器模块中，并且转换器模块利用前述单向函数H来计算该密钥的指纹H(Kn[0])。

因此，网络的源设备的所有转换器模块拥有密钥Kn[0]及其指纹H(Kn[0])。

当源设备的转换器模块必须产生新的LECM消息以便通过网络来发送新数据时，该源设备使用有效密钥Kn[0]来加密LECM消息的受保护部分的数据（尤其是对控制字CW进行加密），并且将有效密钥的指纹H(Kn[0])插入到包含未编码数据的LECM消息的部分中。

在使用更为复杂的系统来管理密钥的实施例变体中，源设备不接收有效网络密钥Kn[0]自身，而是接收基于该密钥的信息项（ $E_{Kn[0]}(Kc)$ ）。根据该实施例A，所述源设备还接收有效密钥的指纹H(Kn[0])，然后该源设备将其存储在转换器模块中。当源设备产生新的LECM消息时，转换器模块利用对称加密密钥Kc来加密要保护的的数据，并将有效密钥的指纹H(Kn[0])以及利用该有效密钥Kn[0]进行了加密的密钥Kc插入到LECM消息的未编码部分。

当网络随着时间发展并且新的密钥被用作网络密钥时，在网络中记录的数据包含利用连续用作网络密钥的各个密钥进行了加密的LECM消息。

当用户想要在接收机设备上重放先前记录的数据时，接收机设备的终端模块接收LECM消息，该终端模块必须利用存储在表1中的适当密钥来进行解密。为了这样做，终端模块首先从LECM消息的未编码部分

中提取用来对LECM消息中的受保护部分的数据进行加密的密钥的指纹 $H(Kn[j])$ 。然后，该终端模块将该指纹 $H(Kn[j])$ 与存储在表1中的所有指纹进行比较，如果数值相对应，则该终端模块调用位于地址@processing_function[j]处的函数，该函数利用密钥 $Kn[j]$ 对LECM消息的受保护部分进行解密。

如果相反地，指纹与表1中的指纹不对应，则表示所接收到的数据还没有被记录在家用网络中。因此，不能够对LECM消息进行解密，并且不能够对相应的数据进行解扰。

将要注意的是，所使用的各个处理函数不仅使用不同的加密算法，而且对数据进行其他的处理。

例如，当在实施例变体中利用上述对称密钥 Kc 来加密LECM消息的受保护部分时，处理函数首先执行对从LECM消息的未编码部分中所提取的信息项 $E_{Kn[0]}(Kc)$ 的解密，以便在利用该密钥 Kc 对受保护数据进行解密之前，恢复密钥 Kc 。

B] 密钥的系统尝试

根据本实施例，接收机设备的每一个终端模块包含自从其创建以来在网络中已经使用过的密钥 $Kn[0]$ 、 \dots 、 $Kn[i]$ 、 $\dots\dots$ 、 $Kn[N]$ 的列表。

源设备的每一个转换器模块包含有效网络密钥 $Kn[0]$ 。当其必须产生LECM消息时，转换器利用密钥 $Kn[0]$ 对要保护的数据进行加密。该转换器还对LECM消息的未编码数据的全部或部分，计算单向函数的结果，特别是“CRC”（表示“校验冗余码”），并且该转换器利用密钥 $Kn[0]$ 来加密该CRC，将该加密结果插入到LECM消息的受保护部分中。

当接收机设备的终端模块接收到要解密的LECM消息时，该终端模块利用存储在终端模块中的每一个密钥 $Kn[i]$ 对LECM消息中的受保护部分中所包含的数据系统地解密。该终端模块还根据包含在LECM消息的未编码部分中的数据，计算CRC，然后将CRC的每一个解密结果与从未编码数据计算得到的结果进行比较。当结果相同时，表示用于解密的密钥是用来对LECM消息进行加密的密钥。

因此，终端模块能够恢复LECM消息中的受保护数据（包括控制

字), 并对数据进行解扰, 然后将其显示给用户。

当使用具有更复杂系统来管理密钥的上述实施例变体时, 源设备的转换器模块利用对称密钥 K_c 对LECM消息中要保护的数据(包括CRC的结果)进行加密, 然后将利用有效网络密钥 $K_n(0)$ 加密了的密钥 K_c 插入到LECM消息中的未编码部分。

接收到这样的LECM消息的接收机设备的终端模块执行除了附加步骤之外与上述相同的操作, 即, 终端模块首先利用第一密钥 $K_n[i]$ 对从LECM消息中的未编码部分中提取的项 $E_{K_n[i]}(K_c)$ 进行解密, 以便恢复假定的密钥 K_c 。然后, 该终端模块设法利用该密钥 K_c 对LECM消息的受保护部分进行解密。如果密钥 $K_n[i]$ 对应于已用来对密钥 K_c 进行加密的密钥, 则从数据的受保护部分获得的CRC将与对数据的未编码部分计算得到的CRC相对应。否则, 该终端模块通过尝试另一密钥 $K_n[i+1]$ 来继续。

C] 使用索引

根据本实施例, 接收机设备的每一个终端模块拥有被称为“Key_space”的大规模随机数。优选地, 在对系统进行初始化时, 例如当创建了包含终端模块的智能卡时, 创建该随机数。

从该随机数Key_space中提取网络中所使用的所有连续密钥 $K_n[i]$:

- 每一个密钥表示该随机数Key_space的子集;
- 或者每一个密钥是根据随机数Key_space或者该数的一部分进行计算的结果。

而且, 在本实施例中, 假定每一个接收机设备包含存储在其终端模块中的表, 例如下面的表2, 所述的表2包含: 索引; 以及针对每一个索引, 指向嵌入在包含终端模块的智能卡中的软件中所包括的处理函数的指针。

索引	@processing_function
[0]	@processing_function[0]
.....
[i]	@processing_function[i]
.....
[N]	@processing_function[N]

表2

表2中的每一个索引对应于不同密钥 $K_n[i]$ 的使用，并且位于地址@processing_function[i]处的处理函数能够根据该随机数Key_space来提取该密钥。

位于源设备中的转换器模块包含有效网络密钥 $K_n[0]$ 和相应的索引[0]。当转换器模块产生LECM消息时，这些转换器使用 $K_n[0]$ 来加密受保护部分的数据，并且将索引[0]插入到LECM消息的未编码部分。

因此，当终端模块接收LECM消息时，该终端模块从未编码部分中读取包含在其中的索引[i]，并调用位于地址@processing_function[i]处的函数，以计算已用来加密LECM消息的一部分的密钥 $K_n[i]$ 。然后，该终端模块可以利用该密钥 $K_n[i]$ 对LECM消息的受保护部分进行解密。

在利用更复杂密钥管理的实施例变体中，转换器模块利用对称密钥 K_c 对LECM消息中要保护的数据进行加密，并将以下内容插入到LECM消息的未编码部分中：有效密钥的索引[0]和利用有效网络密钥 $K_n[0]$ 加密了的密钥 K_c 。接收到这种消息的终端模块如上述那样利用从消息的未编码部分中提取的索引[0]来恢复密钥 $K_n[0]$ 。然后，该终端模块通过对项 $E_{K_n[0]}(K_c)$ 进行解密来获得密钥 K_c ，然后利用 K_c 对受保护数据进行解密。

通过本发明，能够实现家用数字网络的可选方案，同时还确保针对违法复制的保护，并使诚实的用户能够读出过去所记录的数据。

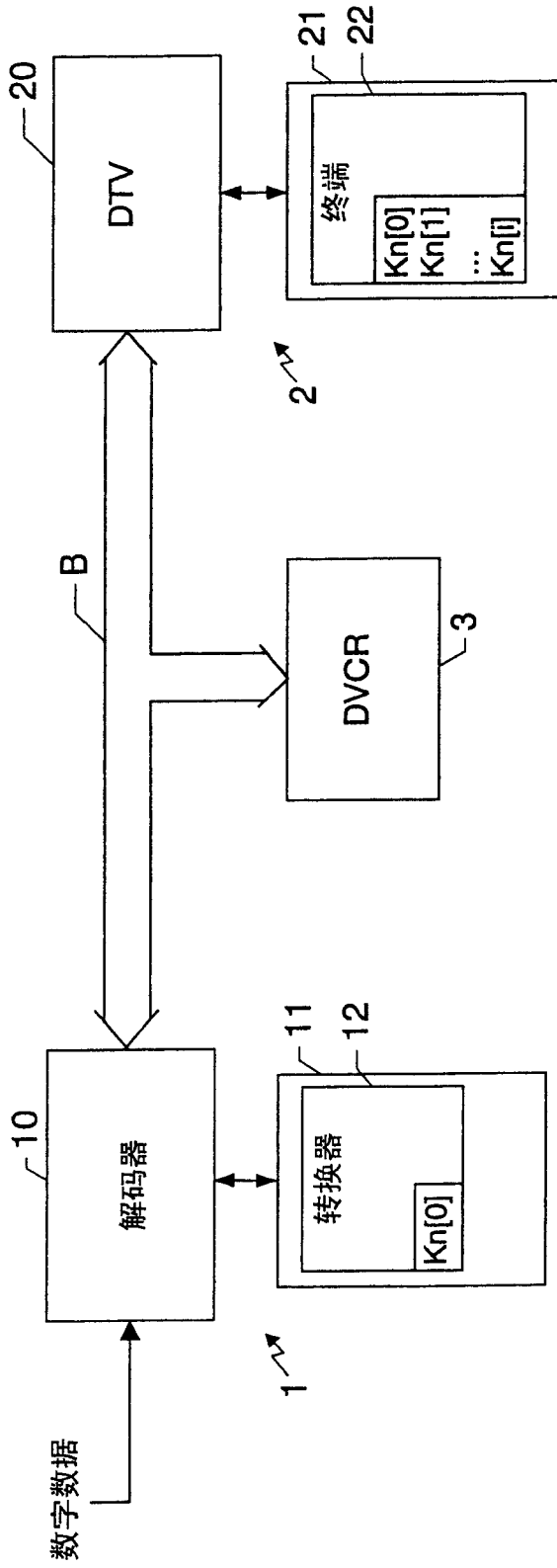


图 1

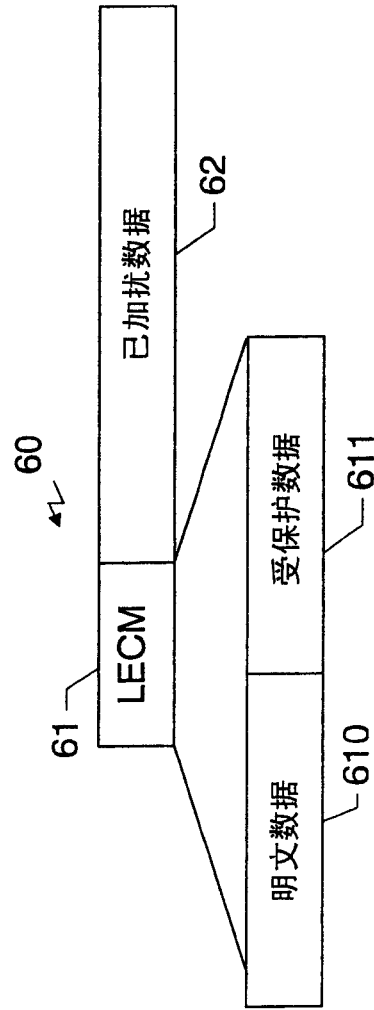


图 2