



[12] 发 明 专 利 说 明 书

专利号 ZL 99810548.1

[45] 授权公告日 2005 年 10 月 5 日

[11] 授权公告号 CN 1221877C

[22] 申请日 1999.8.30 [21] 申请号 99810548.1

[30] 优先权

[32] 1998.8.31 [33] EP [31] 98202891.2

[86] 国际申请 PCT/EP1999/006344 1999.8.30

[87] 国际公布 WO2000/013073 英 2000.3.9

[85] 进入国家阶段日期 2001.2.28

[71] 专利权人 耶德托存取公司

地址 荷兰霍夫多普

[72] 发明人 维赫姆斯·G·P·莫耶

安德鲁·A·瓦杰斯

审查员 曲 颖

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

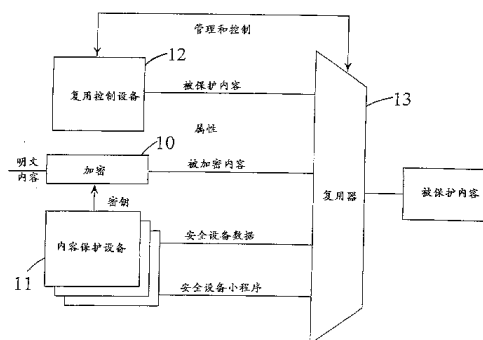
代理人 付建军

权利要求书 3 页 说明书 7 页 附图 3 页

[54] 发明名称 数据加密及解密系统、提供通信接
口的方法和广播方法

[57] 摘要

用于提供将在一个内容播放器中被使用的加密数据的一个系统，这个系统包括用于使用一个加密算法对数据进行加密的一个加密设备，用于提供安全设备数据的一个保护设备，和用于提供关于在内容播放器和一个安全设备之间进行通信的一个协议的信息的设备，用于提供一个被保护内容的一个控制设备，这个被保护内容包括被加密数据，安全设备数据，所述协议信息和关于被保护内容内不同部分的属性数据。被加密数据可以被传输或者被保存在一个合适的存储媒质上。



1. 用于提供将在一个内容播放器(2-5)中被使用的加密数据的系统, 这个系统包括用于使用一个加密算法对数据进行加密的一个加密设备(10), 用于提供安全设备数据和用于提供关于在内容播放器和一个安全设备(8)之间进行通信的一个协议的信息的保护设备(11), 用于提供一个被保护内容的加密系统控制设备(12), 这个被保护内容包括被加密数据、安全设备数据、所述协议信息和关于被保护内容内不同部分的属性数据, 所述安全设备数据包括解密被加密数据所需的信息, 并且其中为了检索解密被加密数据所需的信息, 属性数据包括为在被保护内容中找到在内容播放器和安全设备之间进行通信所用的合适协议所需的信息。

2. 如权利要求1的系统, 其中所述保护设备(11)提供包括关于用于进行通信的一个协议的所述信息的至少一个安全设备小程序。

3. 用于在一个内容播放器(2-5)中对被加密数据进行解密的系统, 这个系统包括用于接收被保护内容的一个输入(14), 这个被保护内容包括被加密数据、安全设备数据、关于在内容播放器和一个安全设备(8)之间进行通信的一个协议的信息和关于被保护内容内不同部分的属性数据, 并且这个系统还包括一个解密设备(15)和一个解密系统控制设备(16), 其中所述安全设备数据包括解密被加密数据所需的信息, 并且其中为了检索解密被加密数据所需的信息, 属性数据包括为在被保护内容中找到在内容播放器和安全设备之间进行通信所用的合适协议所需的信息, 其中解密系统控制设备(16)被编程成使用所述属性数据以找到合适的协议信息来在解密设备(15)和这个内容播放器所使用的安全设备(18)之间建立一个通信接口, 其中这个解密设备适于按照协议信息的控制来与安全设备(8)进行通信, 以获得解密这个加密数据所需要的信息。

4. 如权利要求3的系统, 其中所述协议信息被作为一个安全设备小程序而提供, 其中这个解密系统控制设备(16)被编程成作为一个

虚拟机器而工作来执行安全设备小程序，以建立所述通信接口。

5. 如权利要求 3 的系统，其中在被保护内容中至少一个安全设备小程序被认证，其中这个解密系统控制设备（16）包括用于证实对一个安全设备小程序的认证的一个小程序载入器（19），其中仅被证实的安全设备小程序才能够被载入到虚拟机器中，并在由虚拟机器所提供的环境中执行，该虚拟机器是被编程到解密系统控制设备的。

6. 如权利要求 5 的系统，其中在被保护内容中至少一个安全设备小程序被加密，其中这个小程序载入器（19）适于对一个被加密安全设备小程序进行解密。

7. 如权利要求 4，5 或者 6 的系统，其中这个虚拟机器包括一个内容播放器应用程序接口和一个安全性应用程序接口，这个安全设备小程序与内容播放器和安全设备通过所述接口进行通信。

8. 如权利要求 4-6 中任何一个的系统，其中这个解密系统控制设备（16）被安排成确定这个系统中所使用的安全设备（8）的类型，其中这个解密系统控制设备（16）被安排成从被保护内容中检索与安全设备所确定的类型相应的一个安全设备小程序。

9. 如权利要求 4-6 中任何一个的系统，其中这个系统是连接到一个网络（1）的一个内容播放器（2-5）的一部分，其中这个解密系统控制设备（16）被安排成确定这个系统中所使用的安全设备的类型，并且其中这个控制设备被安排成请求从一个服务提供者下载一个相应的安全设备小程序。

10. 用于在一个内容播放器（2-5）中的一个解密设备（15）和一个安全设备（8）之间提供通信接口的方法，包括：接收一个被保护内容，这个被保护内容包括关于在内容播放器和一个安全设备之间进行通信的一个协议的信息和关于被保护内容内不同部分的属性数据，该属性数据包括为在被保护内容中找到合适协议所需的信息，所述协议用来在内容播放器和安全设备之间通信以检索解密被加密数据所需的信息，从被保护内容中检索所述协议信息来在解密设备和这个内容播放器所使用的一个安全设备之间建立一个通信接口。

11. 如权利要求 10 的方法，其中所述协议信息被作为一个安全设备小程序而提供，其中在一个虚拟机器中执行这个安全设备小程序来建立通信接口。

12. 如权利要求 10 或者 11 的方法，进一步包括检测内容播放器所使用的安全设备(8)的类型，并且从被保护的内容中检索相应的协议信息或者一个安全设备小程序。

13. 如权利要求 10 或者 11 的方法，进一步包括检测内容播放器所使用的安全设备的类型，并且从提供被保护内容的一个源请求相应的协议信息或者一个安全设备小程序。

14. 如权利要求 10 的方法，其中所述协议信息或者安全设备小程序是被认证的，并且进一步包括证实该认证，并且仅使用被证实的协议信息或者一个被证实的安全设备小程序来建立所述通信接口。

15. 广播被保护内容的方法，包括下列步骤：

利用加密算法来加密数据，

提供安全设备数据，

提供关于在内容播放器(2-5)和安全设备(8)之间进行通信所需的协议的信息，

提供属性数据，

提供包含被加密数据、安全设备数据、协议信息和该属性数据的被保护内容，以及

广播被保护的内容，其中

所述安全设备数据包括解密被加密数据所需的信息，并且其中属性数据包括为在被保护内容中找到合适协议所需的信息，所述协议用来在内容播放器和安全设备之间进行通信以检索解密被加密数据所需的信息。

数据加密及解密系统、提供通信接口的方法和广播方法

技术领域

本发明一般涉及用于提供将在一个内容播放器中被使用的加密数据的系统，涉及在一个内容播放器中用于解密加密数据的系统，并且涉及用于在一个解密设备和一个内容播放器中的一个安全设备之间提供一个通信接口。更特别地，本发明涉及为一范围很广的多媒体终端产生一个开放的访问接口的系统和一个方法。

背景技术

在本发明的说明书中，术语“内容播放器”意味着表示任何类型的消费者设备，例如一个（数字）电视机设备，一个机顶盒，一个 DVD 播放机或者一个（数字）VCR 录像机。为了允许对内容进行访问，例如一个电影，足球比赛，等等，众所周知的是使用一个合适的加密算法来对数据进行加密，以保护其内容。例如，用户被提供了一个机顶盒，和一个安全设备，其中这个安全设备产生对被加密数据进行解密所需要的信息。这个类型的传统系统被提供有一个固定的接口和协议，以在安全设备和内容播放器之间进行通信。一个固定的接口的缺点是，这个内容播放器仅能够被用于一个或者多个特定的安全设备。EPA 0 750 423 公开了一种条件接入模块，通过一个固定接口与一个作为安全设备的智能卡协同工作。

发明内容

本发明的目的是提供上述类型的系统和一个方法来允许在安全设备和一个内容播放器之间提供一个可变的接口。

根据本发明的第一方面，提供了用于提供将在一个内容播放器中被使用的加密数据的系统，这个系统包括用于使用一个加密算法对数据进行加密的一个加密设备，用于提供安全设备数据和用于提供关于在内容播放器和一个安全设备之间进行通信的一个协议的信息的保护

设备，用于提供一个被保护内容的加密系统控制设备，这个被保护内容包括被加密数据、安全设备数据、所述协议信息和关于被保护内容内不同部分的属性数据，所述安全设备数据包括解密被加密数据所需的信息，并且其中为了检索解密被加密数据所需的信息，属性数据包括为在被保护内容中找到在内容播放器和安全设备之间进行通信所用的合适协议所需的信息。

根据本发明的第二方面，提供了用于在一个内容播放器中对被加密数据进行解密的系统，这个系统包括用于接收被保护内容的一个输入，这个被保护内容包括被加密数据、安全设备数据、关于在内容播放器和一个安全设备之间进行通信的一个协议的信息和关于被保护内容内不同部分的属性数据，并且这个系统还包括一个解密设备和一个解密系统控制设备，其中所述安全设备数据包括解密被加密数据所需的信息，并且其中为了检索解密被加密数据所需的信息，属性数据包括为在被保护内容中找到在内容播放器和安全设备之间进行通信所用的合适协议所需的信息，其中解密系统控制设备被编程成使用所述属性数据以找到合适的协议信息来在解密设备和这个内容播放器所使用的安全设备之间建立一个通信接口，其中这个解密设备适于按照协议信息的控制来与安全设备进行通信，以获得解密这个加密数据所需要的信息。

根据本发明的另一个方面，提供了用于在一个内容播放器中的一个解密设备和一个安全设备之间提供通信接口的方法，包括：接收一个被保护内容，这个被保护内容包括关于在内容播放器和一个安全设备之间进行通信的一个协议的信息和关于被保护内容内不同部分的属性数据，该属性数据包括为在被保护内容中找到合适协议所需的信息，所述协议用来在内容播放器和安全设备之间通信以检索解密被加密数据所需的信息，从被保护内容中检索所述协议信息来在解密设备和这个内容播放器所使用的一个安全设备之间建立一个通信接口。

根据本发明的另一个方面，提供了广播被保护内容的方法，包括下列步骤：利用加密算法来加密数据，提供安全设备数据，提供关于

在内容播放器和安全设备之间进行通信所需的协议的信息，提供属性数据，提供包含被加密数据、安全设备数据、协议信息和该属性数据的被保护内容，以及广播被保护的内容，其中所述安全设备数据包括解密被加密数据所需的信息，并且其中属性数据包括为在被保护内容中找到合适协议所需的信息，所述协议用来在内容播放器和安全设备之间进行通信以检索解密被加密数据所需的信息。

根据本发明的另一个方面，提供了用于对被加密数据进行传输或者类似操作的一个方法，其中这个被加密数据是通过根据本发明而提供被加密数据的系统而获得的。

使用这个方式，本发明提供了一个可变接口的平台，其中可以在一个安全设备和内容播放器之间建立任何类型的通信接口。本发明允许内容保护技术被调节成与目前消费者设备所使用的已有技术进行互通并且维持互通性能。使用这个方式，就获得了对内容保护系统和安全设备接口的后向兼容性。

附图说明

通过参考附图可以更进一步对本发明进行解释，附图中，以一个示意图的方式显示了采用本发明方法的一个本发明系统的一个实施方式。

图 1 显示了用于互联一些消费者内容播放器的一个家庭内分布式网络。

图 2 显示了根据本发明，用于提供将在一个内容播放器中被使用的加密数据的系统的一个实施方式的结构图。

图 3 显示了根据本发明，用于在一个内容播放器中对被加密数据进行解密的系统的一个实施方式的结构图。

具体实施方式

通过示例，图 1 显示了用于互联多个消费者内容播放器，例如一个电视机设备 2，一个 DVD 播放器 3，一个 DVCR 4 和一个 PC 5，的一个家庭内分布式网络。另外，一个摄像机 6，一个机顶盒 (STB) 7 和一个安全设备 8，例如一个智能卡可以被连接到网络 1。最后，这个

网络被连接到一个广域网，例如互联网，如标号 9 所显示的。在一个家庭内分布式网络 1 的这个示例中，STB 7 和安全设备 8 通过一个通信接口进行通信，以对从被保护内容中所获得的任何被加密数据进行解密，如后面将描述的。在这个示例中，STB 7 和安全设备 8 对内容播放器 2-5 是公共的，尽管有可能为每一个内容播放器配备与其自己的安全设备进行通信的、其自己的解码器/解密设备。应注意，使用一个合适的协议和寻址技术，被保护内容可以通过网络 1 被移动到一个目的内容播放器，但这已不是本发明的一部分。

图 2 显示了用于提供将在一个内容播放器中被使用的加密数据的一个系统，这个系统包括一个加密设备 10，一个保护设备 11 和包括一个复用器 13 的一个控制设备 12。使用一个合适的加密算法，在加密设备 10 中可以对明文内容，例如一个电影，一场足球比赛，等等进行加密。在这个加密算法中，使用了保护设备 11 所提供的密钥，并且这些密钥自己被这个保护设备 11 以一个或者多个格式进行加密。被加密的密钥被作为安全设备数据而提供。保护设备 11 进一步提供了关于在内容播放器和安全设备 8 进行通信的一个协议的信息。在所显示的实施方式中，关于这个协议和加密格式的信息被作为一个或者多个安全设备小程序而提供。

加密设备所提供的被加密内容，安全设备小程序和安全设备数据被复用到被保护内容中，并且也包括控制设备 12 所提供的属性数据。属性数据是发现被保护内容结构中相关部分所需要的。复用器 13 的输出可以例如被广播，或者被保存在一个合适的存储媒质中，以在以后被使用。

图 2 所显示的系统可以被调节成处理一个或者多个不同的安全设备格式，并且对每一个这样的安全格式，保护设备 11 提供了一个安全设备小程序。安全设备小程序的主要功能是在内容播放器中实现与连接到内容播放器的安全设备进行通信的协议和格式。使用这个方式，可以在安全设备和内容播放器之间提供一个接口，而不需要预先知道所使用的特定安全设备所需要的特定协议知识。

优选地，每一个安全设备小程序被进行认证，例如使用显示它是从一个合法的源被发送来的一个签名。可以使用合适的公钥加密 hash 函数。

图 3 显示了用于在如所显示的一个内容播放器中对被加密数据进行解密的一个系统，这个系统包括用于接收被保护内容的一个输入 14，一个解密设备 15 和包括一个解复用器 17 的一个控制设备 16。一个安全设备 8 被连接到控制设备 16。另外，所显示的一个解码器 18 被用于使用一个本质上众所周知的方式对被加密数据进行解密。解码器 18 不是本发明的一部分。属性数据在控制设备 16 中被使用来对被保护内容进行解复用，以检索一个安全设备小程序或者多个安全设备小程序，安全设备数据和一个被解密的内容，并且将内容的相应部分提供到内容播放器的相应部件。

为了对被加密内容进行解密，这个内容播放器需要从这个安全设备 8 中检索密钥。为了这个目的，控制设备 16 决定连接到内容播放器的安全设备 8 的类型，并且搜寻属性数据来选择合适的、相应的安全性设备小程序。控制设备 16 包括用于证实安全设备小程序的签名的一个小程序载入器 19。如果证实了这个安全设备小程序，这个安全设备小程序就在被编程到控制设备中的一个虚拟机器中被下载，并且在这样一个环境下被执行来在安全设备 8 和内容播放器和解密设备 15 之间进行建立一个通信接口。一旦已经建立了通信接口，这个安全设备小程序就进行工作来从被保护内容中拾取安全设备数据，这个被保护内容被安全设备 8 转换成解密设备 15 解密被加密数据所需要的密钥。

如所注意的，小程序载入器 19 证实这个安全设备小程序是否是一个可信的安全设备下小程序。使用这个方式，这个小程序载入器仅允许从一个可信源发送来的那些小程序访问这个虚拟机器。实现对安全设备小程序的证实的一个标准方法是使用一个公钥加密 hash 函数的认证。可选地，可以使用一个传统的密钥加密算法来对小程序进行加密。属性数据包括规定加密算法类型和签名认证过程中将使用的密钥索引的字段。

在这个虚拟机器中，安全设备小程序使用了一个内容播放器应用程序接口来与旁边的内容播放器进行通信，并且使用一个安全性应用程序接口来与安全设备 8 和解密设备 15 进行通信。

控制设备 12 被安排成在属性数据中指出这个内容播放器中所支持的安全设备 8 的类型。当这个安全设备 8 已经被确定时，例如，通过以一个本质上众所周知的方式来发现唯一的标识符，通过一个匹配标识符来从这个属性数据中选择与这个安全设备相应的安全设备小程序。根据这个信息，小程序载入器从被保护内容中检索这个安全设备小程序。这个过程一般在一个应用中被使用，其中被保护内容是在一个连续流中被接收的，例如在一个广播环境下。当被保护内容被保存在一个磁带或者磁盘上时，也可以使用相同的过程。在一个广播环境下或者广域网环境下，小程序载入器 19 也可以请求一个服务提供者或者类似的来转发与被检测安全设备类型相应的一个安全设备小程序。

可以看出，所描述的系统的安全性至少和任何已有的安全系统一样好。因为被保护内容一直被加密，直到它到达了目的内容播放器，所以很难获得内容的一个明文内容版本。另外，所描述的系统的灵活性允许对目前已有的攻击技术采取保护和反攻击措施，在已有的保护系统中没有反攻击的措施。

应注意，术语“内容播放器”应被理解为上面所提到的任何设备，或者甚至是具有与安全设备进行通信的一个接口的一个分离解码器设备。另外，应注意，尽管上面的描述中建议在描述的系统使用分离的设备，但是很清楚，加密和解密系统均可以用按照合适软件所控制的所描述方式而工作的、一个微处理器和合适的外围电路来实现。

所描述的系统支持范围很宽的应用。如已经提到的，一第一应用区域是一个广播环境。在这个情形下，内容播放器可以是被连接到一个电视机或者一个 DVCR 的一个机顶盒。可以使用 JAVA 语言来实现这个虚拟机器。一般，一个 ISO 7816 智能卡可以被用作安全设备。根据一个优选的实施方式，非用户也可以使用一个标准的用户卡来购买一个特定的“事件”，例如一场足球比赛，其中这个小程序载入器请求

服务提供者来下载一个合适的安全设备小程序。其它应用是预记录的媒质，例如 CD，DVD，DVCR 磁带和其它磁带。在所描述的本发明系统中，被保存的被保护内容包括一些被支持的安全设备小程序，以使控制设备的这个小程序载入器可以检索与特定内容播放器所使用的安全设备相应的安全设备小程序。使用这个方式，再一次允许后向兼容，而同时也允许以一个灵活的方式在将来进行升级。

本发明不局限于上面所描述的实施方式，上面所描述的实施方式可以在下面的权利要求书的范围内以多个方法而变化。

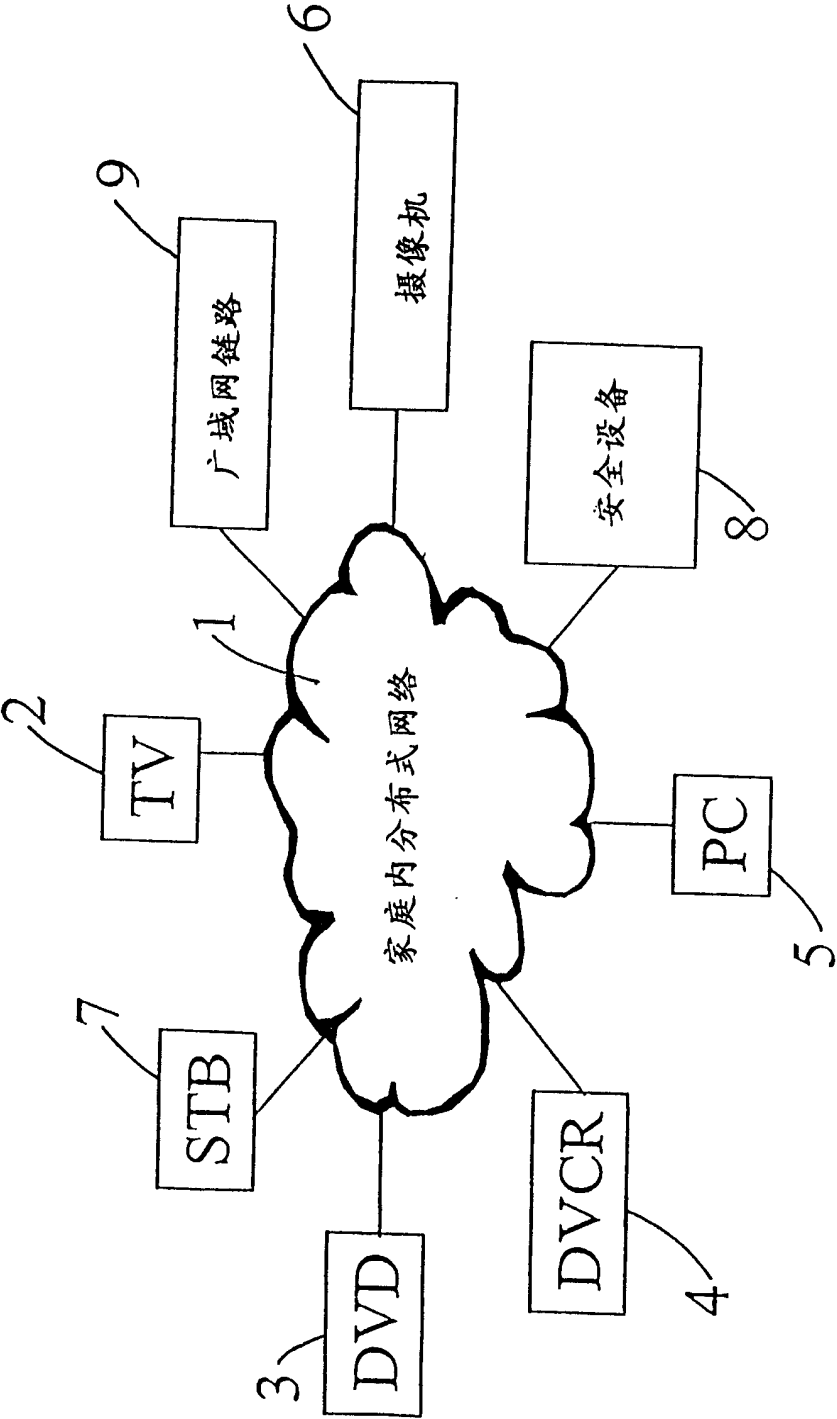


图1

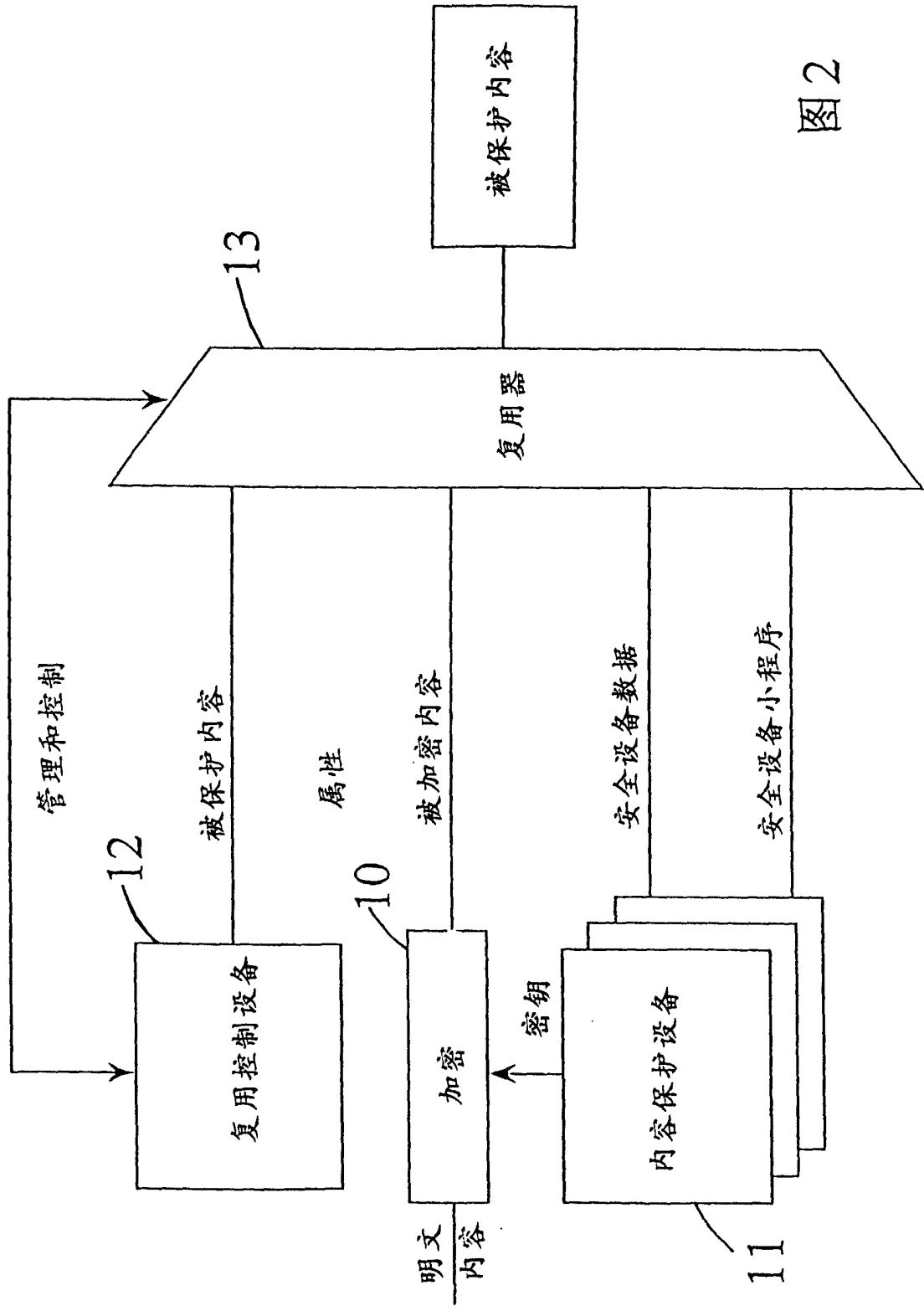


图2

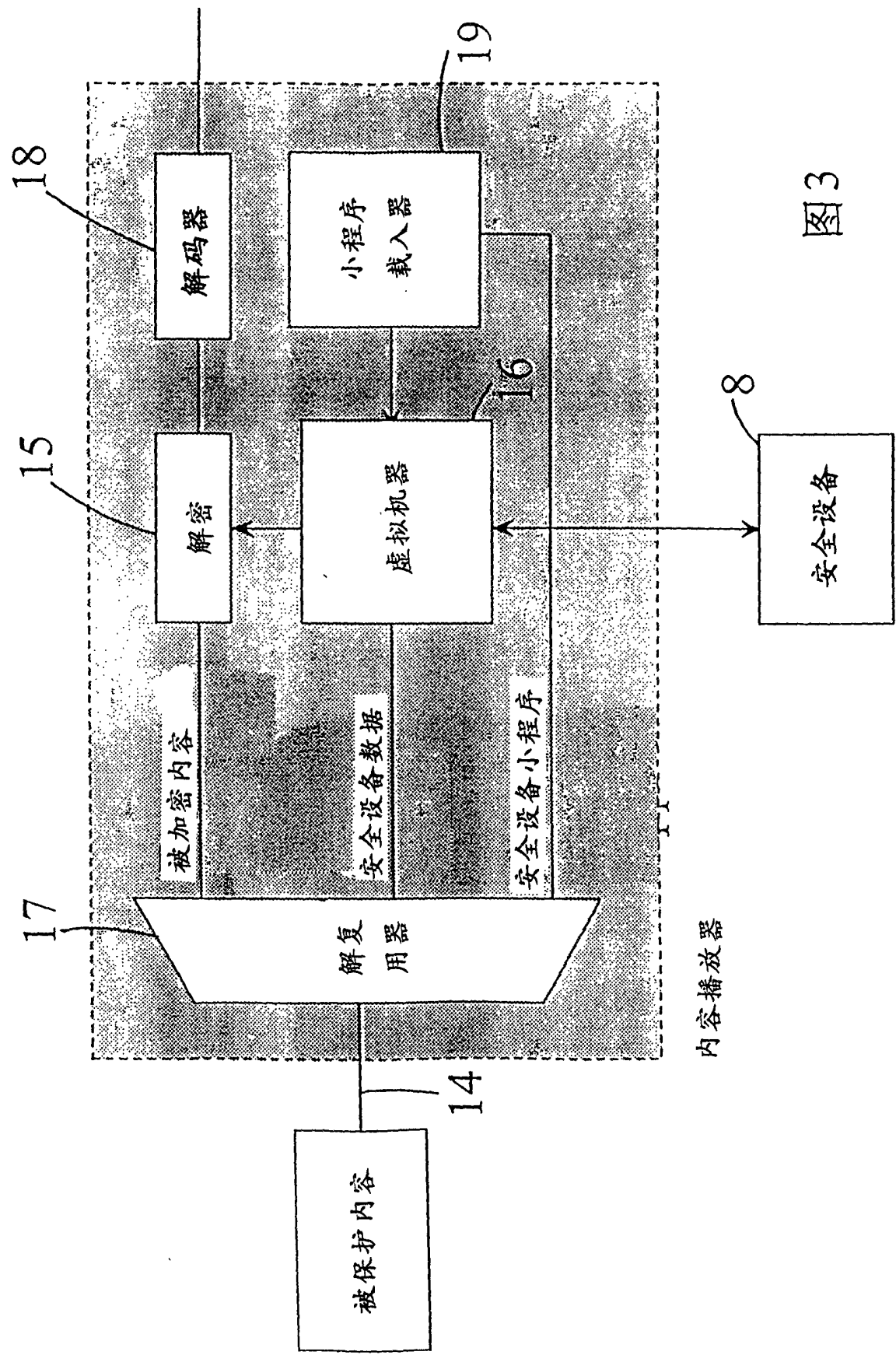


图3