



[12] 发明专利申请公开说明书

[21] 申请号 02803770.7

[43] 公开日 2004 年 3 月 31 日

[11] 公开号 CN 1486570A

[22] 申请日 2002.1.15 [21] 申请号 02803770.7

[30] 优先权

[32] 2001.1.16 [33] CH [31] 01/0061

[86] 国际申请 PCT/IB02/00106 2002.1.15

[87] 国际公布 WO02/056592 法 2002.7.18

[85] 进入国家阶段日期 2003.7.16

[71] 申请人 纳格拉卡德股份有限公司

地址 瑞士舍索 - 苏尔 - 洛桑

[72] 发明人 克利斯托弗·尼古拉斯

[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

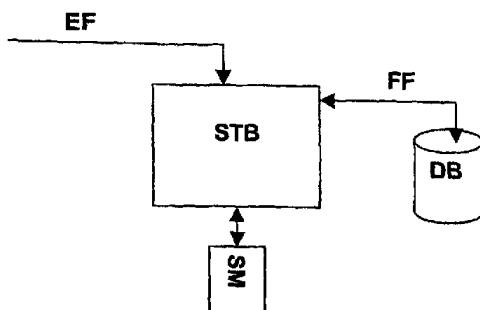
代理人 马 浩

权利要求书 1 页 说明书 5 页 附图 1 页

[54] 发明名称 存储加密数据的方法

[57] 摘要

本发明的目的在于提出一种防止存储在译码器(STB)的存储单元(DB)中的一组数据的密码文件被破解的方法(其中 STB 包括一个安全模块)，从而使许多恶意用户无法通过破解密码文件而从所存储的数据产品非法获利。这个方法在于从一个加密的数据流中提取数据并送到存储单元(DB)，而在把提取出的数据转移到存储单元之前用至少一个特定密码(K1，K2)将这些数据再加密。



1. 一个存储数据的方法，所述数据是从送往一个连着安全模块（SM）和存储单元（DB）的译码器（STB）的加密数据流中提取出来的，这个方法在于，在把加密数据流送到存储单元（DB）之前用至少一个特定密码（K1，K2）将其再加密。
2. 根据权利要求 1 所述的方法，其特征在于使用特定于安全模块（SM）的密码（K1）作为一个单个密码。
3. 根据权利要求 1 所述的方法，其特征在于使用特定于译码器（STB）的密码（K2）作为一个单个密码。
4. 根据权利要求 1 所述的方法，其特征在于用几个密码连续加密数据，或者先用安全模块的密码（K1）然后用译码器的密码（K2）加密，或者采用相反的顺序进行加密。
5. 根据权利要求 1 至 4 所述的方法，其特征在于用包含在存储单元（DB）中的一个加密密码（K3）对将要存储到其中的数据进行加密。
6. 根据权利要求 1 或 2 所述的方法，其特征在于要被加密的数据被传送到安全模块（SM）中进行加密，然后加密过的数据被送到存储单元（DB）。
7. 根据权利要求 1 至 3 中的一条所述的方法，其特征在于在一个位于存储单元（DB）和译码器（STB）之间的低级别的界面中实施数据的加密或解密。

存储加密数据的方法

技术领域

本发明涉及数据加密，尤其涉及加密数据在开放网络上的传输。

背景技术

当我们想要确保只有经过授权的收件人能够使用在开放网络（电缆，卫星，电磁波或者互联网）上传输的数据时，最适当的方法是加密这些数据，并且保证只有经过授权的收件人拥有解密的方法。

抛开使用的算法不谈，我们承认，有强大分析计算能力的第三方是有可能解密这些数据的。

这就是为什么本系统集成了一个常常能够阻止潜在攻击者的密码转换机制。这样，每次对系统的攻击都只局限于一小部分数据，并且在解密之后，只有权进行几秒钟的数据传输。

这种方法被用于付费电视的播送，而被称为“控制字码”的密码只有几秒钟的有效时间。这些数据称为“即时消费数据”，相应的密码被并行传送。

数据存储手段的涌现以及在任意时间观看（或者使用）这些数据的可能性，并没怎么改变数据传输的现状。

为了使客户更加满意，从现在开始，在拥有大量用户的分布式网络上通过加密数据成为可能，这些数据被储存在用户端的存储单元里。一个包含加密密码的文件同这些数据一起被传送，而这个文件根据一个特定算法以及包含在用户端安全模块中密码同样被加密。

这个安全模块通常是一块智能卡的形式，在这块智能卡的内存里有其用来解密数据的密码。

在下面的说明中，用来定义产品的有条件访问的数据将被称为

“产品数据”。对“产品数据”，我们可以理解为一部电影，一条体育广播，一个游戏或者一个软件。

我们将会考虑这样一个事实：大量的用户端在他们的存储单元里存有同样的“产品数据”和一个密码文件。

如果用户决定购买这个产品，用户端的安全模块就会收到必要的指令来解密密码文件，从而在有效时间内为解密“产品数据”提供密码。

这样，在“产品数据”被大量密码加密的情况下，一个恶意的第三方就会攻击这个由特定密码加密的密码文件。

此外，和产品数据相比，密码文件是很小的。一部加密的电影大约是 1 千兆字节大小；而在解密解压缩后同样的电影能够占用 10 千兆字节。

这样，当这个第三方成功破解了密码文件，其中的信息就会很容易的在互联网上传播，从而使其他人能够通过使用一个修改过的译码器解密“产品数据”。

大家应该知道，译码器所收到的数据流的格式是播送公司所独有的，这就意味着在数据的接收阶段很难将不同的信息包离析出来以得到加密形式的“产品数据”。这也是为什么通常总是存储单元或者硬盘受到攻击的原因，而后者由于经济原因成为一种标准设备（比如说 IDE）。然后这个硬盘被转接到个人电脑以从其他通道接受密码文件。

出于在硬盘上存储产品以备以后观看的相似目的，在文件 FR 2 732 537 中描述了第一个操作步骤。这个文件试图解决的问题是和数据一同传输的密码的有限有效性的持续时间。这也是为什么所提出的解决方案是解密包含密码（CW）的文件后用一个本地密码将它们再加密，以便在任何时间都能使用数据。应该注意的是，在进入译码器后数据本身的存储状态不变。

考虑到本地再加密的密码存储在一张智能卡中，文件 EP 0 912 052 中描述的实施方案相应的有所变动。

这两个文件并没有解决当数据储存在易于访问的存储平台时其容易受到攻击的问题。

发明内容

本发明的目的在于防止许多恶意用户破解数据或密码文件，从而使其无法从“产品数据”非法获利。

这个目的通过一个存储数据的方法来实现，这些数据是从送到一个连着安全模块和存储单元（DB）的译码器的加密数据流中提取出来的。这个方法在于，在把加密数据流送到存储单元（DB）之前用至少一个特定密码（K1, K2）将其再加密。

这样，每一个存储单元里的数据对于所考虑的译码器来说都是特定的，而密码文件的解密则只允许解密“产品数据”。

进入译码器的数据流首先被解译以便离析出构成“产品数据”的部分。这些数据由包含在译码器中的第一个密码加密。

从译码器被认为并非是不可破解的这一事实可以看出，用包含在安全模块里的一个密码代替、或者附加于译码器中的第一个密码是有可能的。

附图说明

本发明在附图的帮助下能够更好的被理解，作为一个普适的实例，如图：

图1示出了译码器的不同组成部分。

图2示出了根据本发明所进行的操作步骤。

具体实施方式

图1示出了进入数据流（EF）译码器（STB）以进行处理。要被存储的数据根据预定存储的特定格式被离析出来，在被转移入存储单元之前被送到一个加密模块。这个模块使用由安全模块SM提供的密码K1，这个安全模块的形式一般是连接到译码器的一块智能卡。

这块卡被认为是不可破解的，在卡和译码器 STB 之间的不同的交换由这两个元件的一个特定密码加密。从那时起就不可能阅读被交换的信息以输出修改过的译码器的信息交换。数据在加密后经由通道 FF 传输到存储单元 DB。

由安全模块 SM 提供的密码 K1 能够与一个特定于译码器的密码 K2 相结合。从这个事实可以看出，安全模块 SM 与存储在存储单元 DB 中的数据内容的偏差，将不允许解密这些数据。

这些密码是特定的，也就是说，每个译码器或者安全模块都使用不同的密码。这个密码或者在初始化阶段根据选定的生成模式随机生成，或者由系统的操作中心送达。

图 2 以图表的形式描绘了进入流 EF 经过一个第一过滤器 Sdata 后的同样的处理进程。这个过滤器把预定存储的数据离析出来；用于其他目的的数据则经由出路 EX 被指定进行其他的处理。

第一阶段加密 NK (K1) 通过使用来自安全模块 SM 的第一密码 K1 来实现。这些数据然后被送到第二加密模块 NK (K2)，这个模块的密码 K2 来自译码器 STB。

这些由译码器 STB 和安全模块 SM 提供的密码可以按照任何顺序使用。

根据一个实施方案，加密模块被直接放置在译码器和存储模块之间的界面。这样，加密的施行就处在一个低的逻辑级上，并且在某种程度上独立于译码器的中央管理软件。

根据另一个实施方案，安全模块 SM 有足够强大的加密装置接收将被加密的数据流并以加密的形式返回数据。在这种情况下，仅仅是安全模块 SM 包含并使用加密密码。

数据的加密能够以来自安全模块 SM 的第一个密码 K1 为基础第一次被执行，然后以来自译码器 STB 的第二个密码 K2 为基础第二次被执行。此外，根据存储模块的容量，该存储模块还可能提供一个密码 K3 来对数据进行加密。

这样就有必要集合这三个元件以便使解密数据成为可能。

这个原则适用于所有能够存储自身密码的元件，而这个密码能够被一个新的数据解密层所应用。

在大多数情况下，根据上述方法使用存储的数据需要获得一个权利。这个得自操作中心的权利能够在下载“产品数据”前后获得。这个权利包括一份产品的说明以及一个用来解密控制字码的密码。

根据我们的发明，至少一个阶段的解密需要从安全模块（SM）获得一个密码，而这时也需要有数据的使用权。在对所存储数据的存储方法进行解密的期间，如果数据使用权的验证通过，密码 K1 将只被提供给解密模块。这样，如果用户有使用权的话，存储单元 DB 中的数据将只恢复原来发送时的加密形式。

根据这个实施方案，存储单元 DB 中的数据将附有一个纯文本的说明，以说明使用这些数据的必要权利。而安全模块 SM 在使用密码 K1 解密前，将用包含在其安全存储器中的信息验证这些权利。

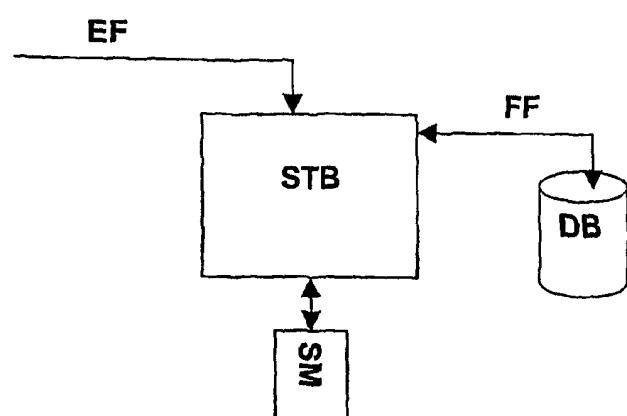


图1

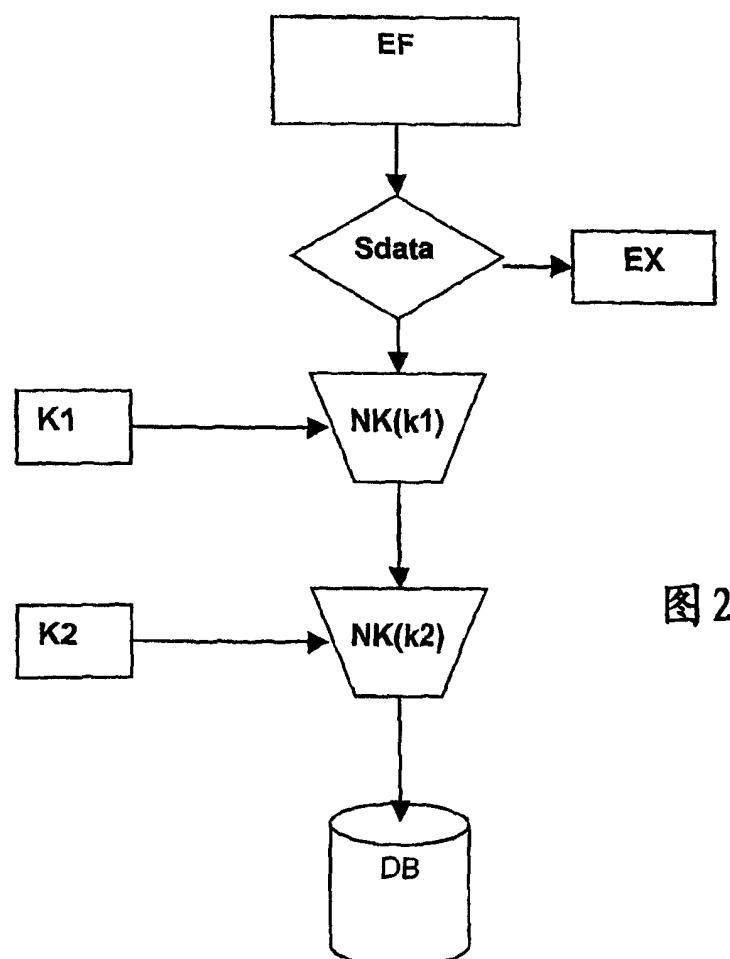


图2