[19]中华人民共和国专利局

[11] 公开号 CN 1127559A

[12] 发明专利申请公开说明书

[21]申请号 95190326.8

[51]Int.Cl[6]
G06F 9/06

[43]公开日 1996 年 7 月 24 日

[22]申请日 95.4.21
[30]优先权
[32]94.4.22 [33]JP[31]106316/94
[86]国际申请 PCT/JP95/00796 95.4.21
[87]国际公布 WO95/29438 日 95.11.2
[85]进入国家阶段日期 95.12.20
[71]申请人 株式会社前进
地址 日本东京都
[72]发明人 大概和则

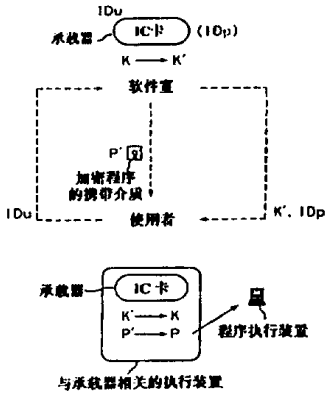
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 张志醒 王 岳

权利要求书 1 页 说明书 10 页 附图页数 3 页

[54]发明名称 数据保护系统

[57]摘要

一种数据保护系统，允许获授权的使用者以简单的操作方式使用目标数据，而不允许未获授权者使用此程序(即使他们能复制该程序)。系统的中心准备了一个专用的算式，它只有此中心秘密持有，通过将中心算式用到数据和使用者所固有的并为公众所知且在使用中无任何变化的数据和使用者的标识符上而准备一保密的算式，从而独立地供数据和使用者所用，该保密算式被提供给使用者和数据供应者，然后当数据供应者须向使用者供应数据时，数据供应者就准备一个在待供应的数据与使用者之间的相同的和专用的加密键码，其中借助了将使用者的标识符输到待供应数据的保密算式中,同时对一部分或全部要根据加密键码直接或间接供应的数据进行加密处理，并将其提供给用户，并由使用者根据所提供的数据标识符，在要提供的数据与用户之间准备相同的加密键码和自己的保密算式，同时对已加密的数据直接或间接地加以解密。



权 利 要 求 书

1.一种数据保护系统，其中有一个中心，该中心准备了一个专用的算式，它只有该中心秘密持有，该中心通过将中心算式用到数据、个别使用者要用的每一数据、和使用者的标识符上而准备一保密的算式，从而独占地供数据和使用者所用，该保密算式被提供给使用者和数据供应者，然后数据供应者依据使用者的标识符和所提供的数据的保密算式，在数据供应者与使用者之间准备一个共用的加密键码，同时对一部分或全部要根据加密键码直接或间接提供的数据进行加密处理，然后将其提供给使用者，并由使用者根据所提供的数据标识符，准备用在数据供应者与使用者之间的共用的加密键码及其自己的保密算式，同时直接地或间接地对已加密的数据进行解密处理。

2.根据权利要求 1 所述的数据保护系统，其特征在于，所述的数据包括软件。

3.根据权利要求 1 所述的数据保护系统，其特征在于，所述的共用键码利用一个随机号码而进一步被加密。

4. 根据权利要求 1 所述的数据保护系统，其特征在于，所述数据是利用一个第二键码而被加密的。

说　明　书

数据保护系统

技术领域

本发明涉及一种保护数据(如应用软件、 OS 软件等)的系统。

背景技术

目前，未获授权者复制数据(如应用程序、 OS 软件、公用程序等)的情况时有发生，但还没有有效的方法来防止这种非法复制程序或软件的未获授权的使用。

发明的描述

本发明的目的在于解决上述已有技术中的问题，提供一种数据保护系统，使已获授权的使用者能以通常方式使用预定的数据(还可包括软件)，而又能简单有效地防止未获授权者使用这些数据。

也就是，本发明涉及到一种数据保护系统，其中有一个中心，例如数据自动出售机，该中心准备了一个专用的算式，即一个中心算式，它只有该中心秘密持有。于是该中心制定一个保密算式，通过对个别使用者要用的每一种数据将中心算式加到数据(还可包括软件)上，同时利用使用者的标识符，独占地供数据和供用户使用。该保密算式同时提供给使用者和数据或软件的供应者，并且由数据或软件供应者依据使用者的标识符和所提供的数据或软件的保密算式，在数据或软件供应者与使用者之间准备一个共用的加密键码，同时对一部分或全部要根据加密键码直接或间接供应的数据或软件进行加密处理，然后将其提供给用户。接着，使用者根据所提供的数据或软件标

识符，在数据或软件供应者与使用者之间准备该共用的加密键码，以及其自己的保密算式，并直接地或间接地对已加密的软件进行解密处理。

附图的简要说明

图 1 至图 3 是实施本发明的方法的示意图。

完成本发明的最佳方式

在下述实施例中，软件作为本发明的保护对象。然而如上所述，任何数据(包括软件)都能由本发明加以保护。

按照上述本发明，提出了一种软件保护系统，其中一个中心准备有一个专用的算式即中心算式，它只有该中心秘密持有。该中心准备一个保密算式，通过将中心算式分别加到软件和使用者所固有的软件标识符和使用标识符上而独占地供软件和供用户使用，这些标识符是公众所已知的，并在使用过程中没有任何实质的变化。该保密算式既为用户所用也为软件供应者所用，于是，当软件供应者须向用户供应软件时，软件供应者即准备一个由待供应的软件和使用者所共用的加密键码，其中借助了将使用者的标识符输入到待供应的软件的保密算式中，同时对一部分或全部要根据加密键码直接或间接提供的软件进行加密处理，并将其提供给用户。使用者通过将所提供的软件标识符输入到其自己的保密算式中而在待供应的软件与使用者之间准备该共用的加密键码，并直接或间接地对已加密的软件进行解密处理。于是，获授权的使用者就被允许以简单的操作程序使用该软件，而未获授权的其他使用者即使可复制也无法使用该软件。

也就是，按照本发明，设有一个中心(例如管理机构)，该中心持有一个保密的中心算式。

所述中心从中心算式中准备一个保密算式，并准备用户标识符和软件标识符(名称、地址、管理号、给定码、符号、编号等)，同时将其分配给使用者和该软件。应指出，这些标识符可以是公众已知的或未知的，或者是用户或软件所固有的，例如在使用过程中没有任何改变。中心欲将为软件而准备的保密算式加于其上的软件例如可以是软件本身，也可以是软件供应者，或者两者都是。

这里，该软件可以是一个应用程序、一个 OS 、一个公用程序，或者任何其他程序或数据，同时，将中心准备的保密算式加到每一个打算供应给用户的软件上，而不管该软件本身的内容怎样。

软件供应者可以是提供软件予用户的供应者，例如软件室、有关制造商、软件自动出售机或软件供应设备、或者其他任何供应软件给用户(付费或免费)的机构。

软件供应者通常可并到一个中心里，而该中心通常又可与用户合并。当软件供应者处于使用软件的地位时，他也可以成为使用者。

这里，使用者和所要使用的软件在操作将要进行之前或刚欲开始之前将从中心接受一个保密算式。

“使用者”是指这样一个人，他使用所述程序以及直接或间接为使用者所拥有的并执行所述软件的装置、与该装置相联系的设备、软体本身等等。

图 1 示意性地示出了本发明的工作过程。

用一个单独的加密键码(即程序和保密算式所固有的第一个加密键码(K))事先对软件供应者分配给使用者的程序(P)的至少一部分进行加密(P')。建立该程序时，使用者要求软件供应者提供他的标识符(IDu)。

软件供应者利用所加的标识符(IDu)和程序所固有的保密算式准备一个第一加密键码，利用第一加密键码和加密算式对上述第二加密

键码K进行加密(K')，并将加密后的第二加密键码(K')分配给使用者。

使用者利用所分配的已加密的第二加密键码(K')建立加密的程序(P')，并建立直接或间接附于该加密程序(P')上的建立的软件。

所建立的软件设有一个包括已加密的第二加密键码(K')的装入程序，该软件并与加密程序(P')连接。当执行装入程序时，装入程序利用使用者的保密算式和程序标识符而始终设有一个共用键码(第一加密键码)，对已加密的第二加密键码(K')进行解密，与解密算式一起以准备第二加密键码，然后利用第二加密键码和解密的算式对加密的程序(P')进行解密(P)。

以上所述的是利用两个加密键码对程序进行加密或解密的间接方法。但是，本发明并不只限于用多个加密键码的上述间接方法，本发明亦可是利用单独一个加密键码(由其自己的保密算式和用户的标识符或程序标识符所获得的共用键码)对程序进行加密或解密的直接方法。

这些方法和涉及准备共用键码的步骤方面的内容，如准备中心算式的方法、准备保密算式的方法、准备共用加密键码、机构、限定标识符等等的方法，均在尚未审查的日本专利公开文件(Kokai)36634/1988和107667/1988号中作了描述。

各标识符不仅能利用上述公开文件中所述的系统加到保密算式中，也可以用以下文件所述的系统加到保密算式中： Matsumoto, Takashima, Imai的“简化的一步算式的组成”， Shingakugiho公司，IT89-23， 1989年7月。

所述的两种或多种加密或解密算式可以是相同的算式，例如由DES(数据加密标准)系统、 FEAL(快速数据加密算式)系统等所表示的算式。但是，任何其他的系统亦可采用，只要考虑到加密的速度和程度即可。

实施例 1

图 2 是用以说明本发明第一实施例的附图。其中心部分与前述的相同，故不再赘述。

(1)使用者有一个承载器(例如 IC 卡、软磁盘、或任何其他存储介质)，用以储存从中心得到的保密算式和个人鉴别算式，还有一个与承载器配合工作的承载器执行单元以及一个标识符。与此类似，软件供应者也有一个承载器，用以在其中储存一个算式，还有一个承载器执行单元。软件供应者无须具有由承载器和承载器执行单元组成的组件形式的算式。

(2)后续程序可自由地执行。

(3)可应用于全部软件室(软件供应者)和应用于全部程序中。

环境条件和定义

软件室(软件供应者)：管理待出售的某一程序(P)的保密算式的机构(程序标识符以 IDp 表示)。

程序售出时，须售出一个加密的程序(P')，加密程序是利用一随机给定的号码(K)(第二加密键码)(属于 P 所固有的)和一加密的算式，通过对程序(P)的至少一部分进行加密而获得的。所述程序(P')是一个不能被执行的文件。

使用者是购买所述加密程序(P')的人，他使用自己的标识符(IDu)。于是，在收到已获授权的使用者的申请时，利用所述标识符(IDu)和保密算式产生第一加密键码，然后，利用第一加密键码和加密算式对一随机号码(K)(即第二加密键码)进行加密，以产生一个加密的随机号码(K')，再将该加密的随机号码(K')(K'包括与第一加密键码准备系统有关的数据)分配给使用者。

使用者：要求软件室提供他的标识符(IDu)并于此时建立其购置的程序的人。有时，并不须要提出供应请求。将软件室送来的已加密

的随机号码(K')输到建立者的软件中。利用建立者的软件所准备的装入程序来使用所述程序。

建立的软件: 利用使用者所输入的标识符(IDp)和加密的随机号码(K')准备一个装入程序，并将其链接到加密的程序(P')上。将建立者的软件附加到加密的程序(P')上或分开获得建立者的软件(得以免费)，并可公用所有程序。

装入程序: 利用使用者所所具有的承载器和承载器执行单元并作为参数给出文件中所具有的程序的标识符(IDp)和加密的随机号码(K')，对加密的程序(P')进行解密，从而获得所述程序(P)。但是，该程序(P)只存在存储器中，而没有采用文件的形式。只对加密程序(P')中所要求的部分作了加密处理，并且程序(P)也不是以完整形式存在。在装入程序中不存在解密规则。

承载器执行单元: 该单元是一个与目标程序执行单元(如个人电脑、办公室电脑、 WS 或任何其他执行单元)整体形成、分开形成、或配合一起形成的、并与其相连接(借助红外线、电、光、超声波、电磁波等方式)的单元，且装有一个用于读写承载器(例如 IC 卡、软磁盘、或任何其他记录介质)的机构，还包含一个解密程序(解密算式)(适配器密码机械: ACE)，以及根据承载器输出的随机号码(K)对加密的程序(P')进行解密。随机号码(K)仅存在于承载器执行单元中，而不能输给外部单元。

考虑到本系统的进一步用途，还须要将 ACE 进一步设计成能提升其等级或能对其加以改进(DES → FEAL 等)。承载器和承载器执行单元仅是一些例子而已，它们还可合并到目标程序执行单元中和与之配合工作，或者可形成一整体结构，或者可彼此分开形成，或者可附加地或居中地连接到一个接口上，再与一台打印机或 RS232C 的连接部分连接，或彼此连接，或者编程为可在目标程序执行单元中进行操

作。

此外，承载器执行单元可以是一个装置，该装置中包括一个承载器的函数，而不用与该单元分开形成的承载器(例如 IC 卡)。

处理过程

(1)在软件室一方进行的处理－分配程序之前－

· 软件室将目标程序(P)分为多个可装入的模块，进而将该程序编制成在一旦存入存储器后各模块就全不能再装入的程序。

· 软件室对所分出的每一模块的给定部分进行加密。加密部分的地址数据存在于加密的程序(P')中。地址数据本身也可加密。

· 对于每一程序，用于加密的随机号码(第二加密键码)(K)是唯一的。对于每一模块也可进一步做成唯一的。

· 可用任何加密装置，只要其可由解密程序(解密算式)ACE 配合承载器执行单元进行操作即可。当软件供应者有其自己的 ACE 并将其分配给使用者时，加密装置不必对所有软件供应者为公用的。

(2)在用户一方进行的处理－当购置程序以后－(假定承载器、承载器执行单元和建立者的软件均已提供)

· 软件供应者对使用者进行登记，提供个人标识符。

(3)在软件室一方进行的处理－当用户登记后－

· 利用使用者所用的标识符(IDu)和专用于所分配程序的保密算式(Xp)，对随机号码(K)进行加密(K')。

在这方面，当用保密算式(Xp)时，如图 2 所示，输入一个过渡字码(PIN-P)，并根据个人鉴定算式(CHA-P)进行判断，以确定持有该过渡字的人是否是真正已登记的个人。由所述中心提供个人鉴定算式(CHA-P)和过渡字码(PIN-P)以及保密算式(Xp)，并可任意使用，和再次由中心任意得到。在用户一方同样也可持有个人鉴定算式(CHA-U)和过渡字码(PIN-U)。

软件供应者将加密的随机号码(K')送给使用者。加密随机号码(K')可以任何方式送达，例如利用电话、传真、个人电脑通信或软盘传送(当用 DES 对程序 P 加密时，要送达用户的数据量例如为 16 字节(当转换成字符串时相当于 32 个字符))。程序标识符(IDp)连同加密的随机号码(K')一起通知给使用者，或者亦可在分配加密程序(P')的同时打印到程序包上。

(4)在用户一方进行的处理－当程序建立后－

· 使用者启动建立者的软件，并输入送到的加密随机号码(K')和程序标识符(IDp)中。

· 利用输入的加密随机号码(K')和程序标识符(IDp)，由建立的软件准备装入程序，同时链接到加密的程序(P')上(带有装入程序的 P')。装入程序是一个有用的程序，它能由 OS(MS-DOS)进行处理，可作为 OS 与加密程序(P')之间的中间媒介而工作。这时，加密程序(P')仍保持在加密状态。

(5)在用户一方进行的处理－当程序被执行以后－

· 启动带装入程序的加密程序(P')，以对具有承载器的个人进行鉴别。

·装入程序从程序标识符(IDp)和保密算式(Xu)准备第一加密键码(Kup)，将加密的随机号码(K')赋给承载器执行单元，并根据第一加密键码(Kup)和解密程序(D)对加密的随机号码(K')进行解密。但是，已解密的随机号码(K)仍留在承载器执行单元中，不输往外部单元。

· 装入程序赋予承载器执行单元所述加密程序(P')的一加密部分，该单元利用解密程序(DE)和随机号码(K)对其解密，从而获得程序(P)，于是可执行程序(P)。

· 装入程序在全部时间内监视程序(P)的执行情况，并于加密程序(P')的加密部分每次被读出后使承载件执行单元对加密程序(P')进

行解密。

在这方面，加密的程序(P')自身不能被解密，在各种情况下只能提供予被授权的使用者。这可以是某种状况，例如此状况下已经有或将要有一保密算式的多个程序(但是当未给予其过渡字时，其函数不能被执行)被记录在一个大容量的记录介质(如 CD-ROM)上，已拥有或将拥有该保密算式的使用者可利用这些程序，并于付了使用费后获得他希望的过渡字和程序标识符。

对此，甚至对于软件供应者，也有如下的好处。

·软件供应者可只以复制操作来准备加密的程序，故可大批量生产加密程序。

· 所需的硬件可供多个软件供应者使用。

另一实施例示于图 3 中，其中将第三个加密键码、加密算式和解密算式加添到图 2 所述的实施例中。

应用保密算式和使用者或程序的标识符(IDp)(涉及使用者，目标程序为该程序的标识符)，以数学方法获取第一加密键码(Kup)。

第二加密键码(r)这一随机号码，并可任意设定。第三加密键码(K2)可用第二加密键码同样的设定方法任意设定。

利用第二加密键码(r)和加密算式(E2)，软件供应者可将部分或全部的第三加密键码(K2)转换成加密的第三加密键码(K2')。

另外，利用第一加密键码(Kup)和加密算式(E1)，软件供应者可将部分或全部第二加密键码(r)转换成加密的第二加密键码(E(r))。

软件供应者将加密程序(P')、加密的第二加密键码(E(r))和加密的第三加密键码(K2')提供给使用者。

使用者准备第二加密键码(r)，该键码是利用第一加密键码(Kup)和解密算式(D1)从加密的第二加密键码(E(r))中解密的；并利用第二加密键码(r)和解密算式(D2)对加密的第三加密键码(K2')进行解密，从而

准备第三加密键码(K2)。

利用第三加密键码(K2)和解密算式(D3)，通过对加密程序(P')进行解密而准备程序(P)。

以上对图 3 的工作已按图作了说明，其他方面的情况可参看对图 2 的说明。

按照以上详细叙述过的本发明，通过对所述中心提出请求的授权，赋予软件和使用者以专用的保密算式和一标识符。用户因拥有加密的软件，一旦要简单地去解密并使用软件时，就可将软件标识符输到他自己的保密算式中。

其操作是如此简单方便。此外，由于有了保密算式，用户即被允许使用该软件，只要利用标识符，即使改变了软件也无影响，于是用户的负担就减小了。

另一方面，对于未经授权的使用者，尽管他们可以得到这些软件，他们也很难对已加密的软件进行解密。

说　明　书　附　图

图　1

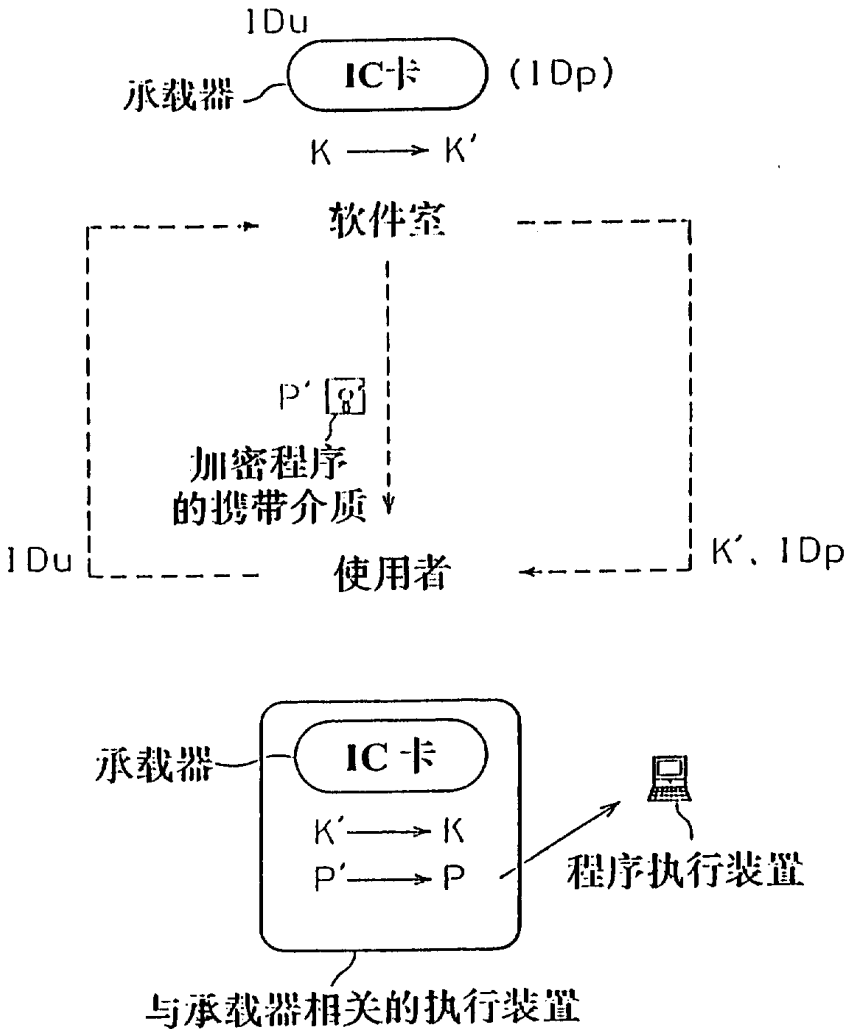

IDu
承载器
IC卡
(IDp)
K ⟶ K′
软件室
P′
加密程序
的携带介质
IDu
使用者
K′、IDp
承载器
IC卡
K′⟶K
P′⟶P
程序执行装置
与承载器相关的执行装置

图 2

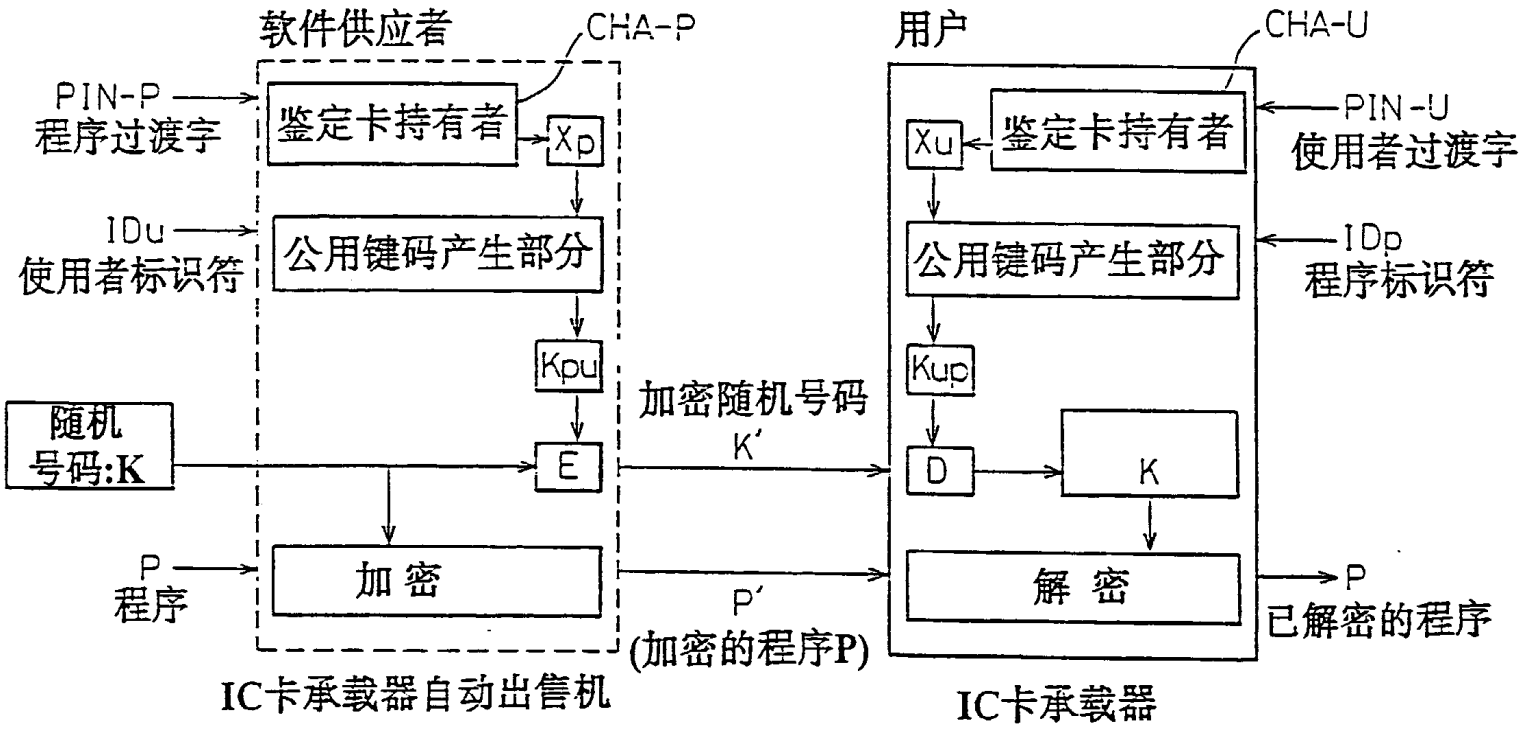
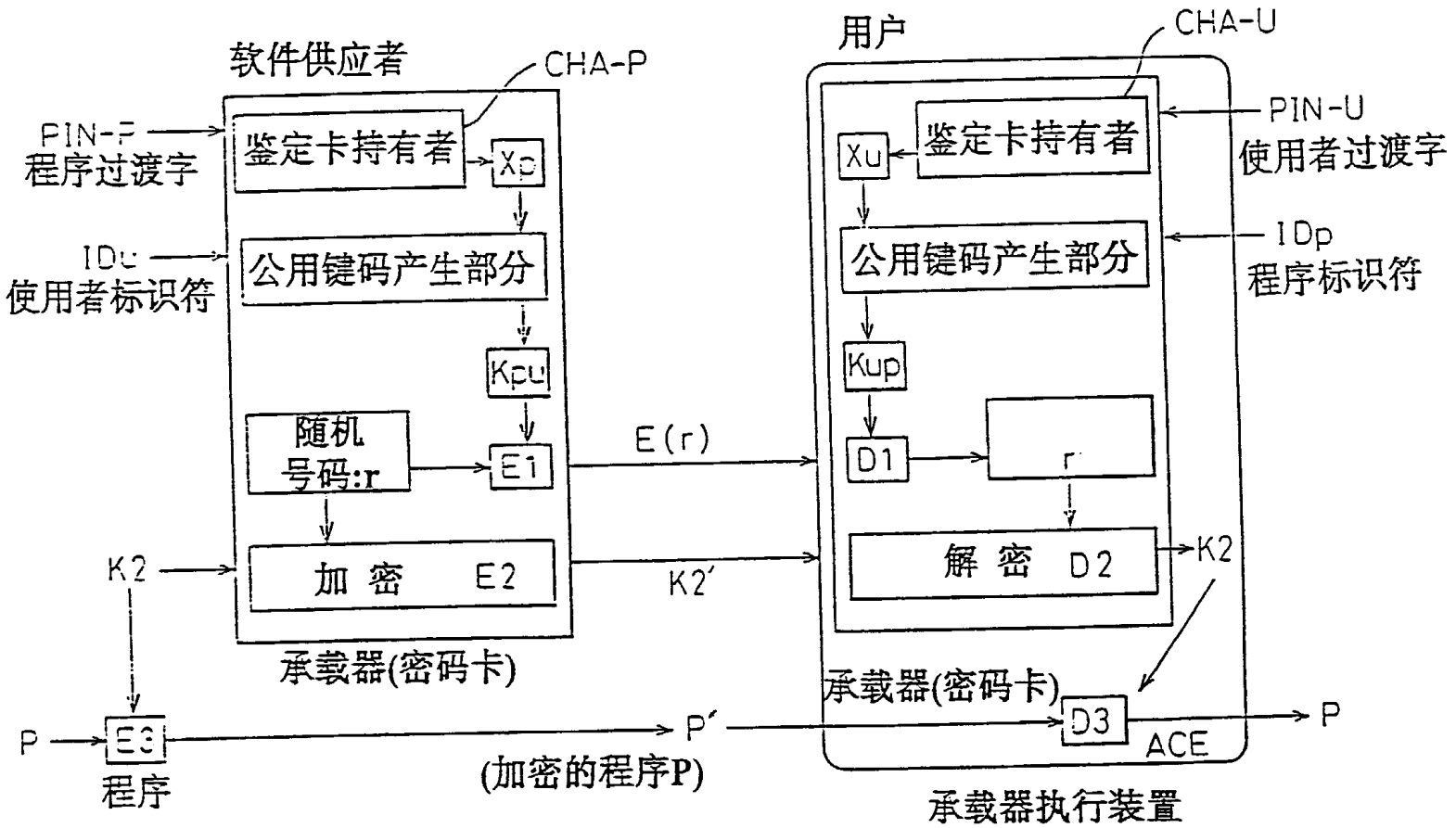

软件供应者
CHA-P
PIN-P
程序过渡字
鉴定卡持有者
Xp
IDu
使用者标识符
公用键码产生部分
Kpu
随机
号码:K
E
加密随机号码
K'
P
程序
加 密
P'
(加密的程序P)
IC卡承载器自动出售机
用户
CHA-U
PIN-U
使用者过渡字
Xu
鉴定卡持有者
IDp
程序标识符
公用键码产生部分
Kup
D
K
解 密
P
已解密的程序
IC卡承载器

图 3


软件供应者
CHA-P
PIN-P
程序过渡字
鉴定卡持有者
Xp
IDu
使用者标识符
公用键码产生部分
Kpu
随机
号码:r
E1
E(r)
K2
加 密 E2
K2'
承载器(密码卡)
P
E3
程序
P'
(加密的程序P)
用户
CHA-U
PIN-U
使用者过渡字
鉴定卡持有者
Xu
公用键码产生部分
IDp
程序标识符
Kup
D1
r
解 密 D2
K2
承载器(密码卡)
D3
ACE
P
承载器执行装置