[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200680002408.6

[43] 公开日 2008 年 1 月 9 日

[11] 公开号 CN 101103587A

[22] 申请日 2006.1.18
[21] 申请号 200680002408.6
[30] 优先权
[32] 2005. 1.18 [33] US [31] 11/037,766
[86] 国际申请 PCT/EP2006/050275 2006.1.18
[87] 国际公布 WO2006/077222 英 2006.7.27
[85] 进入国家阶段日期 2007.7.16
[71] 申请人 国际商业机器公司
地址 美国纽约
[72] 发明人 J·瑟鲁迪 M·卢特科夫斯基

[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 李 峥

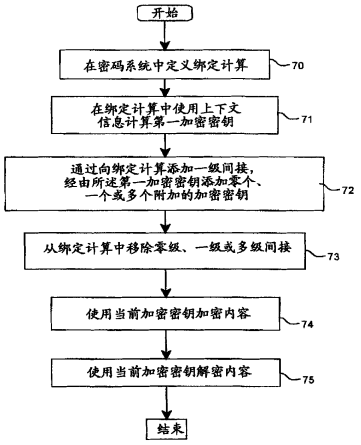
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

安全和便利处理密码绑定状态信息的系统和方法

[57] 摘要

一种可在内容加密应用中使用的通用机制，用于将内容绑定到特定接收器、容器或通信信道，以便将对应用特定的工作从密码细节中分离出来而不管所使用的绑定方案。 此机制包括定义安全绑定状态对象，所述安全绑定状态对象在任何这样的系统中保持并操作包括最敏感信息的所有密钥。 此信息被完全封装在绑定状态信息中，并且不可从对象之外访问，从而使得应用对于外部攻击不会太脆弱。本发明允许应用从一种加密方案迅速改变为另一种，因为它们均使用相同机制，仅在加密计算上不同。 同样，作为在多个应用中重复使用的结果，实现所提出的机制的组件随时间发展得更加稳定。



1. 一种用于使用绑定计算对象加密或解密一个或多个内容文件的密码系统，包括:

用于定义绑定计算对象的装置;

用于在所述绑定计算对象中使用上下文信息计算第一加密密钥的装置，所述第一加密密钥成为当前加密密钥;

用于向所述当前加密密钥添加零级、一级或多级间接的装置;

用于从所述当前加密密钥中移除零级、一级或多级间接的装置;

用于使用所述当前加密密钥加密一段内容的装置；以及

用于使用所述当前加密密钥解密一段内容的装置。

2. 根据权利要求 1 所述的密码系统，其中添加一级间接包括:

用于所述绑定计算对象选择随机的间接密钥的装置;

用于用所述当前加密密钥加密所述间接密钥的装置;

用于用所述间接密钥替换所述当前加密密钥的装置；以及

用于将所述已加密间接密钥传送给用户的装置。

3. 根据权利要求 1 所述的密码系统，其中添加一级间接进一步包括:

用于向所述绑定计算对象指定已加密间接密钥的装置;

用于用所述当前加密密钥解密所述已加密间接密钥的装置；以及

用于用所述间接密钥替换所述当前加密密钥的装置。

4. 根据权利要求 2 或权利要求 3 所述的密码系统，进一步包括:

用于接收附加信息用以在添加或移除若干级间接时使用的装置；以及

用于当重复一级间接计算时使用所述附加信息验证所提供信息的完整性的装置。

5. 根据权利要求 1 所述的密码系统，其中用于解密的装置阻挡用户对已解密间接密钥的访问。

6. 一种用于使用绑定计算对象加密或解密一个或多个内容文件的密码方法，包括以下步骤:

创建绑定计算对象;

在所述绑定计算对象中通过上下文信息生成第一加密密钥，所述第一加密密钥成为当前加密密钥;

向所述当前加密密钥添加零级、一级或多级间接;

从所述当前加密密钥移除零级、一级或多级间接;

使用所述当前加密密钥加密一段内容; 或者

使用所述当前加密密钥解密一段内容。

7. 根据权利要求 6 所述的方法，其中添加一级间接包括以下步骤:

由所述绑定计算对象选择随机的间接密钥;

用所述当前加密密钥加密所述间接密钥;

用所述间接密钥替换当前加密密钥; 以及

将所述已加密间接密钥传送给用户。

8. 根据权利要求 6 所述的方法，其中添加一级间接进一步包括以下步骤:

向所述绑定计算对象指定已加密间接密钥;

用所述当前加密密钥解密所述已加密间接密钥; 以及

用所述间接密钥替换当前加密密钥。

9. 根据权利要求 7 或权利要求 8 所述的方法，进一步包括以下步骤:

由用户提供附加信息用以在添加或移除一级间接时使用; 以及

当重复一级间接计算时使用所述附加信息验证所提供信息的完整性。

10. 根据权利要求 6 所述的方法，其中用于解密的装置阻挡用户对已解密间接密钥的访问。

11. 一种具有记录在计算机可读媒介上的代码的计算机程序，用于与基于符号链接对象的系统进行高速通信，以在密码系统中使用绑定计算对象加密或解密一个或多个内容文件，所述计算机程序包括:

用于定义绑定计算对象的装置;

用于在所述绑定计算对象中使用上下文信息计算第一加密密钥的装置，所述第一加密密钥成为当前加密密钥;

用于向所述当前加密密钥添加零级、一级或多级间接的装置；

用于从所述当前加密密钥中移除零级、一级或多级间接的装置；

用于使用所述当前加密密钥加密一段内容的装置；以及

用于使用所述当前加密密钥解密一段内容的装置。

安全和便利处理密码绑定状态信息的系统和方法

交叉引用

2004 年 12 月 14 日提交的转让给共同受让人的 Cerruti 等人的共同待决申请（代理方文档号 No. AUS920040932US1），序列号 No. 11/011,241。特此将该引用引入作为参考。

技术领域

本发明涉及数据加密，并具体涉及内容的加密和解密，其中以安全和便利的方式处理密码绑定状态信息。

背景技术

过去十年以一种由数据处理工业与消费电子工业的融合所驱动的技术革命为标志。随之，其效果驱动了多年来为人所知且可用但相对静止的技术。这些技术中主要的一种是与因特网相关的文档分发。Web 或因特网，其作为松散的学术及政府数据分发设施静静地存续了一代以上，达到了“极其关键的阶段”并开始了显著扩充时期。通过该扩充，企业和消费者可以通过因特网直接访问所有样式的文档和媒体。

随着消费数字技术的出现，诸如音乐和电影的内容不再限于承载它们的物理媒体。消费数据技术中的进展对于想保护其知识产权免遭未授权复制和销售的内容拥有者（诸如唱片公司、工作室、销售网络和艺术家）呈现出新的挑战。广播加密中的最近进展向基于公钥加密技术的更传统的方案提供了一种有效的备选方案。与公钥方法相比较，广播加密所需要的兼容设备中的计算开销的数量级更少。此外，广播加密协议是单向的，不需要任何低级的握手，低级的握手易于削弱拷贝保护方案的安全性。但是，通过消除双向通信，接收方的可能很昂贵的返回信道可被消除，这降低了

设备制造者和用户的开销成本。

IBM 已经开发了一种基于被称为可扩展内容保护（也称为“xCP”）的广播加密的内容保护系统。xCP 支持被称为“群集”的可信域，所述“群集”将多个兼容设备分组在一起。内容可自由地在这些设备之间移动，但它对所述群集之外的设备是无用的。广播加密应用的其他示例包括：对可记录媒体的内容保护（CPRM）的媒体、对预记录媒体的内容保护（CPPM）的媒体、以及高级访问内容系统（AACS）下一代媒体。

广播加密方案把一段内容绑定到特定实体，诸如一段媒体（例如致密盘或 DVD）、服务器或用户。广播加密通过使用媒体密钥块（也被称为密钥管理块 KMB 或会话密钥块）绑定内容，所述媒体密钥块允许兼容设备使用其内部设备密钥来计算密码密钥（媒体或管理密钥），同时防止欺骗（不兼容）设备进行相同动作。绑定方案的一个示例是绑定到标准 PKI 应用中的特定接收器，其中内容用会话密钥加密，其接着用接收器的公钥加密。该内容仅可以用接收器的私钥检索。绑定方案的另一个示例是绑定到 CPRM 和 AACS 媒体中的特定媒体，其中内容用标题密钥（title key）加密，其接着用从媒体标识符和（从上述媒体密钥块计算的）媒体密钥的单向函数中得出的密钥来加密。绑定方案的第三示例是绑定到 xCP 群集协议的特定用户，其中内容用标题密钥加密，其接着用从用户的群集授权表和绑定 ID 以及（从用户的当前媒体密钥块计算的）用户的当前管理密钥的单向函数中得出的密钥来加密。

广播加密不需要设备验证，并且可以用对称加密来实现，这使得它比公钥加密法高效得多。在通过处理密钥管理块（KMB）计算媒体密钥之后，所述方案使用媒体密钥把内容绑定到具有绑定标识符的实体，得出绑定密钥。当标题密钥接着被选定并用绑定密钥加密或解密时，间接（indirection）步骤发生，得出已加密标题密钥或已加密间接密钥。内容自身接着可用标题密钥加密，并且已加密内容可以通过已加密标题密钥来存储。接收已加密内容和已加密标题密钥的兼容设备可使用相同的 KMB 和绑定标识符来解密已加密标题密钥，并接着使用该标题密钥来解密内容。兼容设备首先

必须使用 KMB、绑定标识符及其设备密钥再现绑定密钥，并接着使用绑定密钥从已加密标题密钥中解密标题密钥。一旦兼容设备具有标题密钥，则它可以自行解密内容。欺骗设备将不会具有可被用于处理 RMB 的设备密钥，并因此将不能再现绑定密钥也不能解密内容。同样，如果内容已被不兼容设备拷贝到具有不同标识符的不同实体，则具有有效设备密钥的兼容设备将不能计算正确的绑定密钥，因为绑定标识符与初始的不同。

在现有技术的系统下，所有内容将用标题密钥加密，标题密钥自身将用绑定密钥加密。试图访问一段内容的任意设备将必须预先解密该内容。为了这样做，该设备将首先从 KMB 确定媒体密钥，并接着使用该媒体密钥结合绑定标识符和授权表来恢复绑定密钥。该设备接着可使用绑定密钥从已加密标题密钥恢复标题密钥，并接着使用标题密钥解密已加密内容。因为标题密钥用绑定密钥加密，所以对绑定密钥的任意改变会迫使用新的绑定密钥重新加密每个标题密钥。

如果设备中的应用程序被泄密，此解决方法可能导致标题密钥的暴露。由于解密操作暴露了标题密钥，则存在标题密钥可被该程序暴露的风险。当前的解决方法受困于以下技术问题，所述问题为，对于要执行的每一级加密或解密均需要特定的应用程序代码。本发明涉及通过提供可信密码（cryptography）对象来解决此问题，所述对象可以安全地加密或解密密钥或内容而不会暴露秘密密钥。通用的可信密码对象可以递归地使用诸如群集 ID、设备密钥等附加信息来加密密钥，以创建将内容绑定到特定群集或设备的绑定密钥。本发明允许已加密内容被客户端设备解密和播放，而不会将标题密钥暴露在可信密码对象之外。本发明的通用加密机制简化了使用此类加密方案的应用的开发，导致更及时和更节约的应用加密。本发明包括单个绑定计算对象（可信密码对象），其中上下文密钥、间接密钥和实例秘密密钥被保持。由于本发明不允许用户对其中总保持敏感秘密的单个绑定计算对象的访问，所以本发明比现有技术更安全。在高级访问内容系统（AACS）和 4C Entity LLC 的内容保护系统体系结构（CPSA）可记录媒体中，其中可存储若干文件且新的 KMB 可被引入系统中，上述问

题也可能发生。

因此，需要一种在密码系统上加密和解密内容的有效和高效系统，并具体需要安全和便利处理密码绑定状态信息。

发明内容

本发明通过一种用于使用绑定计算对象加密或解密一个或多个内容文件的系统、方法及相关的计算机程序而提供对上述问题的解决方案。更具体地，本发明提供了用于定义绑定计算对象、在所述绑定计算对象中使用上下文信息计算第一加密密钥的装置，所述第一加密密钥成为当前加密密钥。本发明允许向所述当前加密密钥添加或从中移除零级、一级或多级间接。用户可以提供附加信息用以在间接步骤计算中使用。通过使用本发明，使用所述当前加密密钥加密或解密一段内容。稍后，当重复间接步骤计算时用户可以验证所述附加信息的完整性。加密实体可通过阻挡对已解密间接密钥的访问而检测并拒绝对已加密间接密钥进行解密和暴露的尝试。

附图说明

参考以下附图并结合所附的说明书，本领域技术人员将更好地理解本发明，并更加了解本发明的多种目的和优点，在附图中：

图 1 是其中根据本发明的实施例的方法和系统可以被实现的示例性的网络体系结构的绘线图；

图 2 是可用于本发明的实施的系统的一般化视图；

图 3 是描述了本发明的建立用于安全和便利处理密码绑定状态信息的功能的示例性流程图；以及

图 4 是根据图 3 建立的程序的示例性运行的流程图。

具体实施方式

参考图 1，示出了其中根据本发明的实施例的方法和系统可以被实现的示例性的网络体系结构的绘线图。尽管本发明可用各种绑定方案（诸如

绑定到标准 PKI 应用中的特定接收器、绑定到 CPRM 和 AACS 媒体中的特定媒体）操作，但图 1 示出了一种绑定方案，其中绑定到 xCP 群集协议的特定用户内容。图 1 的网络包括兼容 xCP 的网络群集 32，其包括若干兼容 xCP 的网络设备，包括蜂窝电话 18、电视 10、DVD 播放器 16 和个人计算机 14。网络可以是任意类型的有线或无线网络，诸如局域网（LAN）或广域网（WAN）。内容可以是可从源传送到接受者的任意数据，且可以是以下文件的形式，所述文件诸如：音频数据文件、视频数据文件、媒体数据文件、流型媒体文件、应用文件、文本文件或图形。加密系统允许本地网络内的接收设备自由地在它们之间共享和使用已加密内容，同时防止不兼容设备解密已加密内容。接收设备可选地能够将内容记录到记录设备上，用于在本地网络之外使用。

网络群集支持：群集的密钥管理块 38、标识当前授权加入到该群集中的所有设备的授权表 12、该群集的绑定密钥 36 以及群集 ID 46。密钥管理块 38 是一种数据结构，其包含用每个兼容设备密钥对管理密钥的加密。也就是说，所述密钥管理块包含管理密钥的多种加密实例，其中一个实例针对设备的一组设备密钥中的每个设备密钥。该群集的绑定密钥 36 被计算为管理密钥与群集 ID 和该群集的唯一数据权标的密码散列的密码单向函数。该群集的管理密钥从密钥管理块 38 和设备密钥计算出。

图 1 的网络包括内容服务器 31，其能够用由内容提供者、内容拥有者或合法的特许机构提供给它的标题密钥对内容加密。在给出足够的有关群集的信息时，内容服务器 31 也能够计算出该群集的绑定密钥，并且使用绑定密钥 36 对标题密钥加密并将其与已加密内容一起打包。更具体地，内容服务器 31 可通过从网络群集 32 中的网络设备接收群集 32 的密钥管理块 38、群集 32 的唯一数据权标以及加密的群集 ID，而从群集的外部控制该群集的内容的广播加密。所述内容服务器能够使用群集 32 的密钥管理块 38、群集 32 的唯一数据权标及已加密的群集 ID 计算出该群集的绑定密钥。

图 1 的网络进一步包括数字权限服务器 39，其能够存储定义了广播加密内容的权限的权限对象。此外，在给出足够的有关群集的信息时，数字

权限服务器 39 还能够计算出该群集的绑定密钥，并且使用该绑定密钥对标题密钥加密并将其插入权限对象。更具体地，如果存在第三方 DRM 解决方法，则本发明与所述第三方 DRM 解决方法兼容，以通过用绑定密钥 36 对标题密钥加密、将已加密的标题密钥插入所述权限对象，而控制从网络群集 32 的外部对网络群集 32 的内容的广播加密。在此时，在使得内容可从参与设备获得之前，可以对第三方 DRM 解决方法进行外部检查。如果 DRM 解决方法存在，则基于来自请求设备的已加密内容的唯一标识授予或拒绝访问。数字权限服务器能够使用群集 32 的密钥管理块 38、群集 32 的唯一数据权标及已加密的群集 ID 计算出该群集的绑定密钥。

图 2 中示出了可用于本发明的实施的密码系统的一般化的简图。密码系统可以是可执行诸如加密或解密以及将密钥附加到内容的一个或多个任务的硬件和/或软件的任意组合。典型的密码系统可以是具有计算机程序的通用计算机，所述计算机程序当被加载并执行时实现此处所述的方法。可替换地，密码系统可以是包含用于实现密码系统的一个或多个功能任务的专用硬件的专用计算机系统。专用计算机系统可以是接收设备的一部分，诸如关联于 DVD 播放器的加密/解密模块。密码系统可包括一个或多个中央处理单元（CPU 19）、输入/输出（I/O）接口 22、包括绑定计算对象 28（其中含有上下文密钥 40、间接密钥 42 和加密密钥 44）的用户应用 26、外部设备 24 以及数据库 49。

密码系统还可与源 57 或接受者 47 通信。源 57 可以是能够发送传输的任何实体或者要加密或解密的任何内容的源，诸如内容所有者、内容服务提供者或者本地网络中的接收器。从源 57 接收的信息可包括任何类型的信息，诸如已加密内容、内容、内容使用条件、KMB、已加密标题密钥或绑定标识符。类似地，接受者 47 可以是能够接收传输的任何实体，或者其是任何已加密内容或其他信息的目的地，诸如本地网络中的接收器。

CPU 19 可包括单个处理单元或可以跨位于一个或多个位置的（诸如在客户端及服务器或多处理器系统上的）一个或多个处理单元分布。I/O 接口 22 可包括用于与外部源交换信息的任何系统。外部设备 24 可包括任

何已知类型的外部设备，诸如扬声器、视频显示器、键盘或其他用户输入设备、或者打印机。数据库 49 可提供用于促进所公开实施例的执行的信息的存储。数据库 49 可包括一个或多个存储设备，诸如磁盘驱动器或光盘驱动器。

用户应用 26 可包括对应用特定的信息的组件，诸如媒体 ID 或授权表。绑定计算对象 28 可包括：经由用户的特定信息建立的上下文密钥 40、一个或多个间接密钥 42 以及用于加密内容的最终加密密钥 44。绑定计算对象 28 可在若干不同应用中重复使用，并且其是标准定义机制。此标准定义机制可被用于创建可信实体，其处理对于应用的绑定事务状态。诸如标题密钥、媒体密钥或会话密钥的秘密信息可被保持在这些可信实体（绑定计算对象）之内，从而降低了在应用组件中传输敏感信息的安全风险。可采用特定度量来检测和防止在可信实体之外对标题密钥的解密。

绑定计算对象或可信密码对象 28 可被实现为在可信操作系统环境中执行的可信软件组件。例如，计算机系统可供应有可信 Java 虚拟机（Java 是 Sun Microsystems 公司的商标），所述可信 Java 虚拟机的执行选项对于系统所有者已知并受其控制。在可替换方案中，绑定计算对象 28 可在只读存储器设备或对应用特定的硬件设备中实现，以确保不会执行泄密操作。优点在于，诸如标题密钥的已解密的秘密信息总是被维护在绑定对象 28 中，对其的外部访问被阻挡从而无法被泄密。

图 3 是示出了根据本发明用于安全和便利处理密码绑定状态信息的过程发展的流程图。在用于传送已加密广播内容到已授权设备的密码系统中定义绑定计算对象（步骤 70）。在绑定计算中使用上下文信息计算第一加密密钥（步骤 71）。通过向绑定计算对象添加一级间接，经由所述第一加密密钥添加零个、一个或多个附加的加密密钥（步骤 72）。通过请求绑定计算对象选择随机的间接密钥、用当前密钥加密所述随机的间接密钥、并接着用间接密钥替换当前的已加密密钥，一级间接可被添加到绑定计算。得到的已加密间接密钥被传送到用户。可替换地，通过由用户指定对于绑定计算对象的已加密间接密钥、请求绑定计算对象用当前加密密钥解密所

述已加密间接密钥、并用间接密钥替换当前的加密密钥，一级间接也可被添加到绑定计算对象。移除零级、一级或多级间接（步骤 73）。

如果间接步骤被移除，则之前的当前加密密钥必须被建立为当前加密密钥。当前加密密钥被用于加密内容（步骤 74）。当前加密密钥被用于解密内容（步骤 75）。所述当前加密密钥可以是在绑定计算对象中使用上下文信息建立的第一加密密钥。本发明包括用于用户提供附加信息用以在间接步骤计算中使用的装置，当附加加密密钥被建立时所述间接步骤计算出现。当重复间接步骤计算时所述附加信息的完整性可以被验证。提供了用于解密的装置，其中用户对已解密间接密钥的访问被阻挡。

现在将结合图 4 的流程图描述图 3 中建立的过程的简化运行。首先，确定是否使用密码系统加密或解密内容文件（步骤 80）。如果否，则过程结束。如果是，则定义绑定计算对象（步骤 81）。接着使用上下文信息计算第一加密密钥（步骤 82）。确定是否建立附加级的间接，即，是否使用所述第一加密密钥添加附加加密密钥（步骤 83）。如果是，则一级间接或间接步骤被添加到绑定计算对象（步骤 84）。通过请求绑定计算对象选择随机的间接密钥（步骤 85），接着使用当前加密密钥加密间接密钥（步骤 86），并用所述间接密钥替换当前加密密钥（步骤 87），间接步骤可被添加到绑定计算。已加密间接密钥被传送给用户（步骤 88）。通过向绑定计算对象指定已加密间接密钥（步骤 89）、请求绑定计算对象用当前加密密钥解密已加密间接密钥（步骤 90）、并用所述间接密钥替换当前加密密钥（步骤 91），间接步骤也可被添加到绑定计算对象。过程继续，回到步骤 83，其中用户有机会建立附加的加密密钥。如果未建立附加的加密密钥，则确定是否移除间接步骤（步骤 92）。如果是，则之前的当前加密密钥被建立为当前加密密钥（步骤 93）。过程继续，回到步骤 83，其中用户有机会建立附加的加密密钥。如果未移除间接步骤，则确定是否加密或解密内容（步骤 94）。如果是，则用当前加密密钥加密或解密内容（步骤 95），并且过程继续，回到步骤 83，其中用户有机会建立附加的加密密钥。如果内容未被加密，则确定是否结束过程（步骤 96）。如果否，则过程继续，

回到步骤 **83**，其中用户有机会建立附加的加密密钥。如果是，则过程结束。

在本说明书中根据用于安全和便利处理密码绑定状态信息的方法描述了本发明。本领域的技术人员应当了解，控制本发明的过程能够以各种形式的计算机可读媒体的形式分发。本发明也可在计算机程序产品中实现，诸如软盘或其他记录媒介，以通过任何合适的数据处理系统使用。计算机程序产品的实施例可使用用于机器可读信息的任何记录媒介（包括磁性媒体、光学媒体或者其他适当的媒体）来实现。本领域的技术人员将立即认识到，任何具有适当的编程装置的计算机系统都将能够执行如程序产品中实现的本发明的方法的步骤。尽管已经示出并描述了某些优选实施例，但将会理解，在此可进行多种改变和修改，而不会背离权利要求的意图的范围。

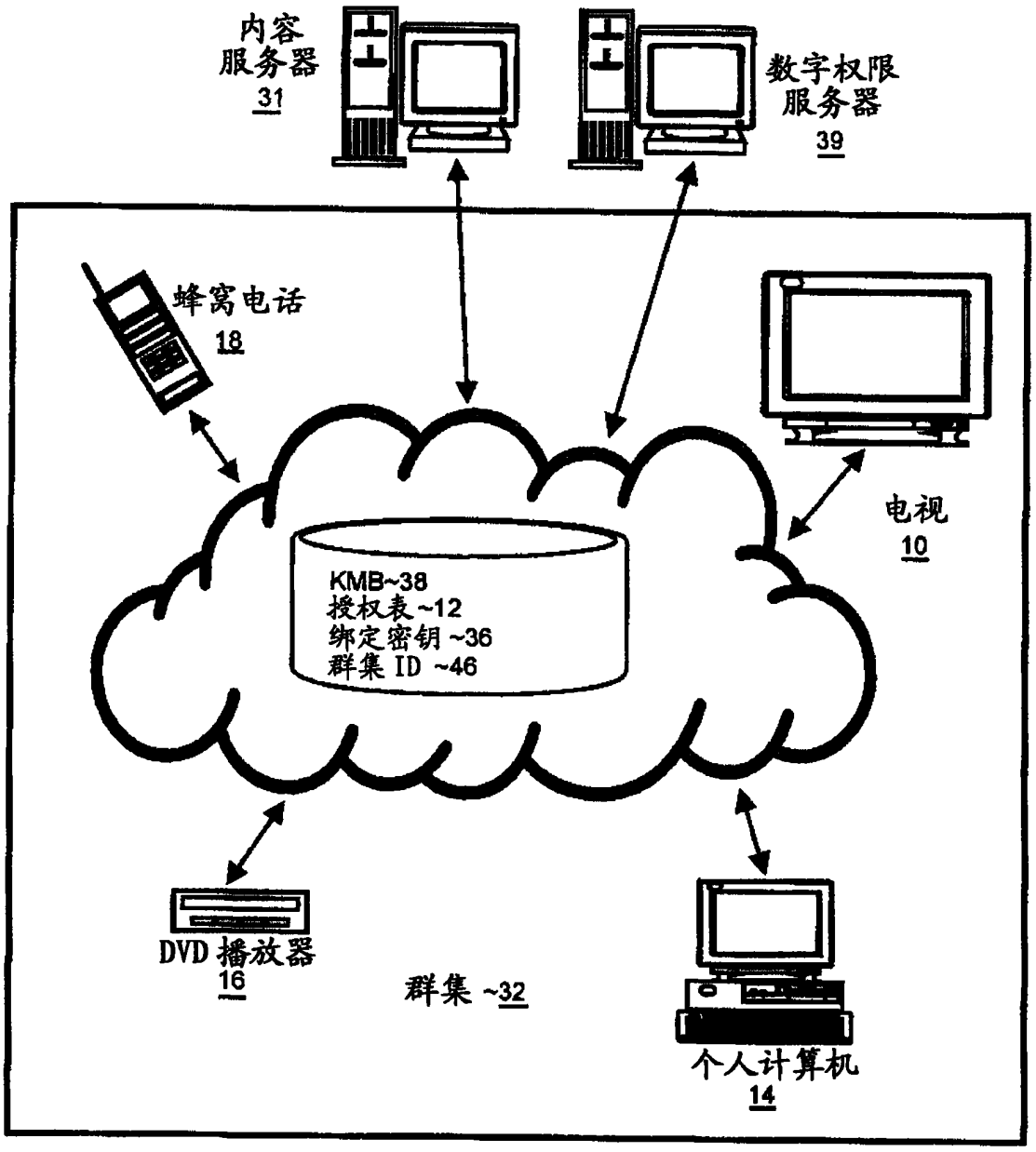

内容
服务器
31
数字权限
服务器
39
蜂窝电话
18
电视
10
KMB~38
授权表~12
绑定密钥~36
群集 ID ~46
DVD 播放器
16
群集 ~32
个人计算机
14

图 1

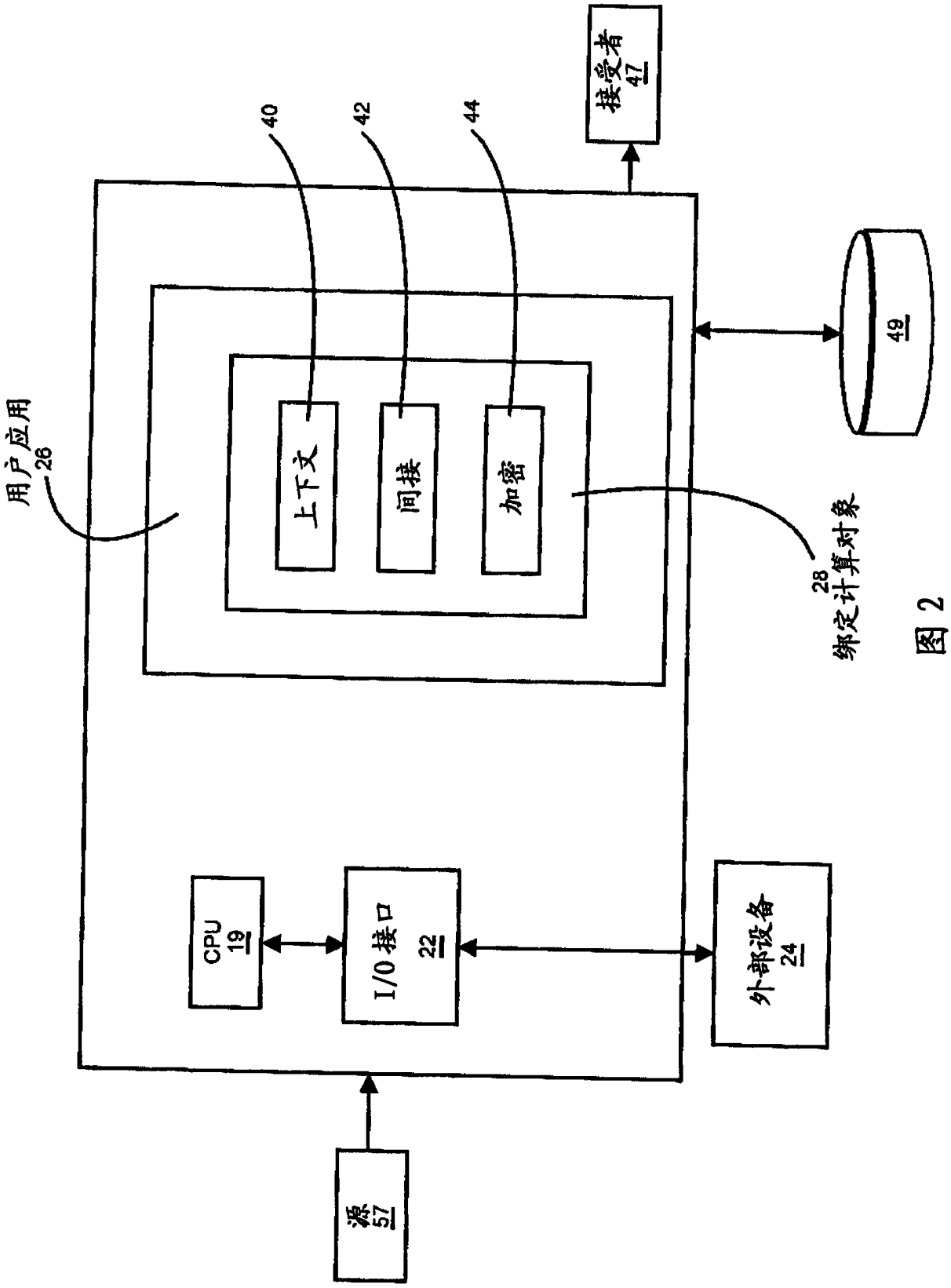

接受者
47
40
42
44
49
用户应用
26
上下文
间接
加密
28
绑定计算对象
CPU
19
I/O 接口
22
外部设备
24
源
57

图 2

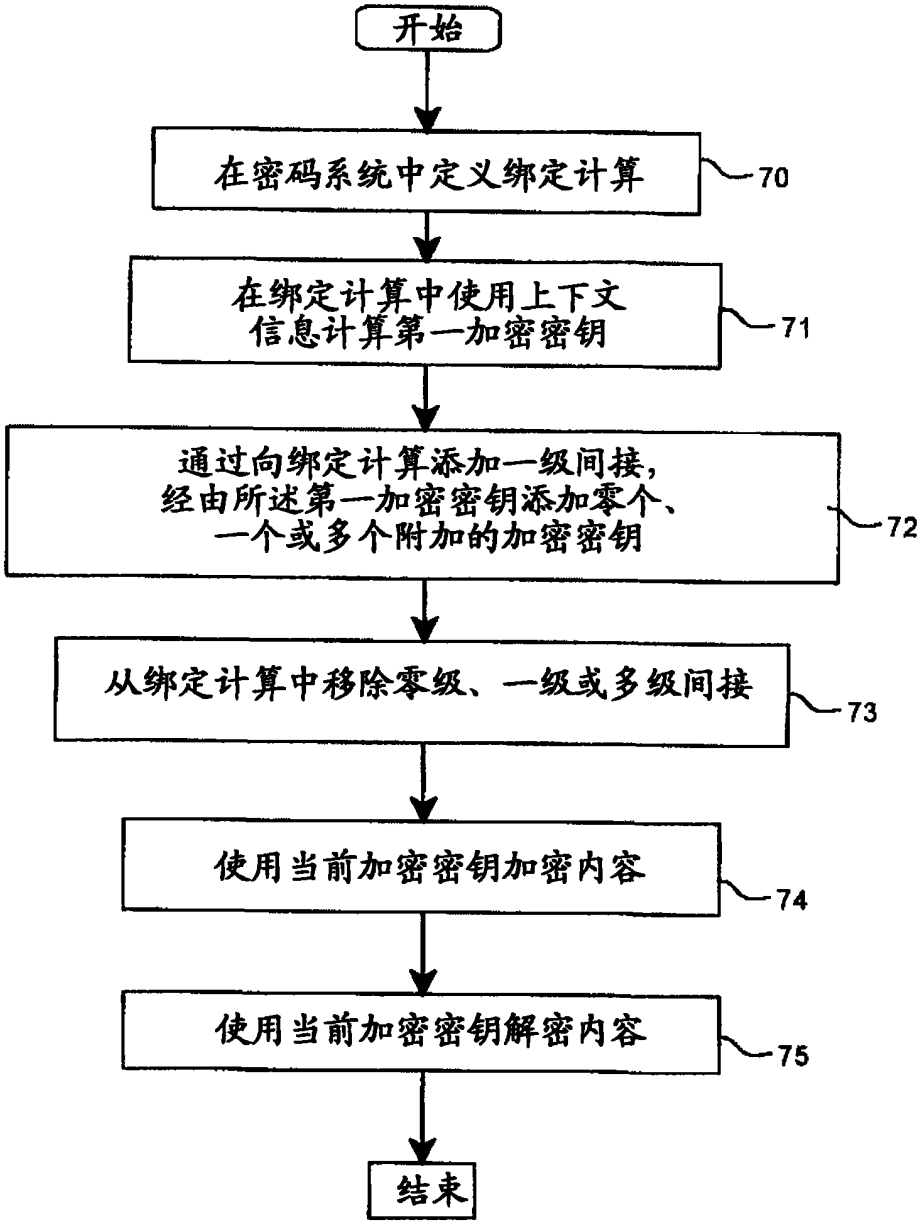

开始
在密码系统中定义绑定计算
70
在绑定计算中使用上下文信息计算第一加密密钥
71
通过向绑定计算添加一级间接，经由所述第一加密密钥添加零个、一个或多个附加的加密密钥
72
从绑定计算中移除零级、一级或多级间接
73
使用当前加密密钥加密内容
74
使用当前加密密钥解密内容
75
结束

图 3

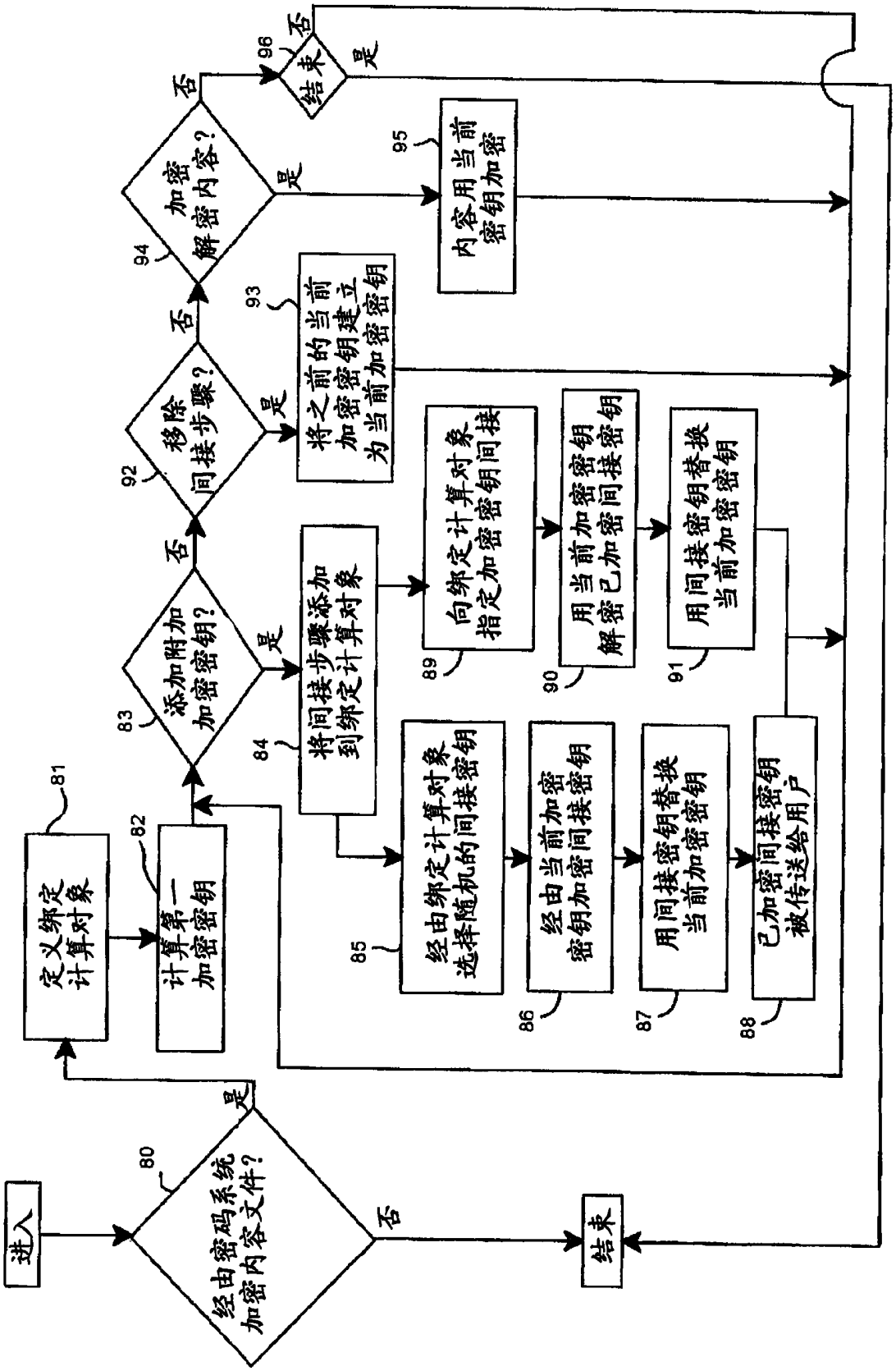

进入
经由密码系统加密内容文件?
80
是
否
结束
定义绑定计算对象
81
计算第一加密密钥
82
添加附加加密密钥?
83
是
否
将间接步骤添加到绑定计算对象
84
经由绑定计算对象选择随机的间接密钥
85
经由当前加密密钥加密间接密钥
86
用间接密钥替换当前加密密钥
87
已加密间接密钥被传送给用户
88
向绑定计算对象指定加密密钥间接
89
用当前加密密钥解密已加密间接密钥
90
用间接密钥替换当前加密密钥
91
移除间接步骤?
92
是
否
将之前的当前加密密钥建立为当前加密密钥
93
加密内容解密内容?
94
是
否
内容用当前密钥加密
95
结束
96
是
否

图 4