



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 96110338.8

[45] 授权公告日 2003 年 11 月 19 日

[11] 授权公告号 CN 1128522C

[22] 申请日 1996.3.31 [21] 申请号 96110338.8

[30] 优先权

[32] 1995. 3.31 [33] US [31] 415824

[71] 专利权人 皮特尼鲍斯股份有限公司

地址 美国康涅狄格州

[72] 发明人 W · J · 贝克 F · 巴托尔

R · A · 科德里 F · M · 迪波利托

K · D · 亨特 K · V · 劳顿

D · K · 李 L · J · 洛利希

S · J · 保利 L · A · 平特索夫

I · A · 西韦耶

审查员 汪 涛

[74] 专利代理机构 上海专利商标事务所

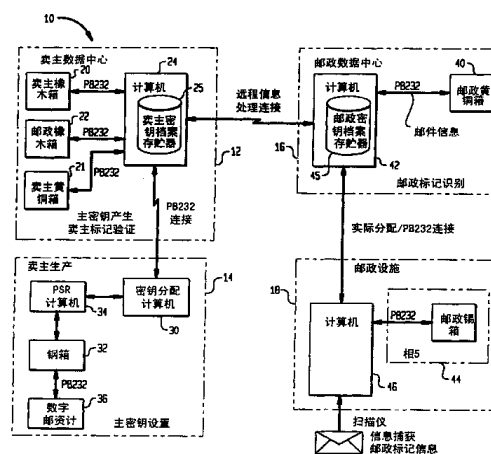
代理人 陈 亮

权利要求书 2 页 说明书 23 页 附图 16 页

[54] 发明名称 在一密钥管理系统中生产通用邮资计的一种方法

[57] 摘要

一种生产交易证实装置如数字邮资计的方法，包括步骤，在一密钥管理系统的一逻辑安全域中产生一主密钥；将该主密钥设置到一数字邮资计中；识别该主密钥的设置；以及将该主密钥注册到该密钥管理系统中的一逻辑安全支域中。产生主密钥的步骤还包括步骤，产生一域；产生至少一支域；将该域设置在该密钥管理系统的安全箱中；在该域中产生一主密钥和测试标记；以及将该主密钥记录在域档案存储器中。设置主密钥的步骤还包括步骤，将该主密钥设置到一数字邮资计中；以及将该主密钥与一唯一的装置识别器相连。



1. 一种构成交易证实装置的方法, 包括步骤:
 - a) 在一密钥管理系统的一逻辑安全域中产生一主密钥;
 - b) 将该主密钥设置到一交易证实装置中;
 - c) 识别该主密钥的设置; 以及
 - d) 将该主密钥注册到该密钥管理系统中的一逻辑安全支域中。
2. 如权利要求 1 所述的方法, 其中所述的产生主密钥的步骤还包括步骤:
 - 产生一域;
 - 产生至少一支域;
 - 将该域设置到该密钥管理系统的安全箱中;
 - 在该域中产生一主密钥和测试标记; 以及
 - 将该主密钥记录到域档案存贮器中。
3. 如权利要求 1 所述的方法, 其中所述的设置主密钥的步骤还包括步骤:
 - 将该主密钥设置到一交易证实装置中; 以及
 - 将该主密钥与一实际的装置识别器相连。
4. 如权利要求 1 所述的方法, 其中所述的识别主密钥的步骤还包括步骤:
 - 在该交易证实装置中产生一标记;
 - 识别该测试标记与交易证实装置产生的标记是相同的;
 - 从该档案存贮器中的一主密钥产生一标记; 以及
 - 识别该交易证实装置产生的标记与该档案存贮器产生的标记是相同的。
5. 如权利要求 1 所述的方法, 其中所述的将主密钥注册到该密钥管理系统中的一逻辑安全支域中的步骤还包括步骤:
 - 给该交易证实装置指定一支域;
 - 在该交易证实装置中设置一逻辑装置识别器;
 - 将该逻辑装置识别器与实际的装置识别器相连;

根据该逻辑装置识别器和该实际装置识别器,在该交易证实装置中产生一注册标记;

使用该档案存贮器中的该主密钥记录产生注册标记;

识别注册标记是相同的;以及

将该主密钥记录在支域中。

6. 如权利要求 1 所述的方法,还包括步骤:

对指定给该交易证实装置的每一域重复步骤 a~d。

7. 如权利要求 1 所述方法,其中该交易证实装置是一数字邮资计。

在一密钥管理系统中生产
通用邮资计的一种方法

本发明一般地涉及用于加密密钥管理的一个系统,特别地,涉及用于分配给邮资计的加密密钥的管理的一系统。

这里提交的本申请与美国申请相关(代理人签条 E-335, E-370),并指定由本发明的代理人代理。

数字打印技术使得邮寄人员可以方便的形式实现数字,即,位映射可寻址(bit map addressable)的打印。人们期望采用这种技术以用于证实邮资的给付。数字打印技术的发展使得打印邮资签条成为可能,该邮资签条对每一邮件而言是唯一的。一个计算机驱动的打印机能够打印,例如在一邮件的表面的期望位置上打印一邮资签条。该签条是唯一的,因为它包括了直接涉及该邮件的信息,例如,邮资值,日期,件数和/或邮寄地邮编。

站在邮局的立场上来看,由于任何合适的计算机和打印机均可用于产生一图像的多个拷贝,因此数字打印和扫描技术使得伪造带有签条的邮资非常容易。

为了确认一邮件,即确保打印在一邮件上的邮资已经过了计算,已知的一种方法是作为邮资已付戳的一部分,包括有一密码,使得从该密码可确定已付邮资的值,从而知道打印在邮件上的值是否正确。例如,见 Edelman 等人的美国专利 4757537 和 4775246, 以及 Eckert 的美国专利 4649266。已知的确认一邮件的另一方法是将地址作为密码的一部分,如 Sansone 等人的美国专利 4725718, 及 Fougere 等人的美国专利 4743747。

Pastor 的美国专利 5170044 描述了一种方法和装置,用于以签条的形式表示二进制信息,该签条包括一二进制的像素矩阵。实际的像素矩阵被扫描以识别邮件的提供者,并还原其他密码简易测试信息。Pastor 的美国专利 5142577 描述了 DES 编码的各种方案,

以对一信息进行加密,并将解码的邮政信息与邮件上的简易测试信息进行比较。

Pastor 等人的美国专利 5390251 描述了一个系统,用于控制来自邮资计的潜在的大量用户的邮件上的签条打印的有效性,该系统包括置于每一邮资计中的装置以用于产生一代码并将该代码打印在各邮件上。该代码是一密码,证实了打印该签条的装置,以及由该邮件上的邮资正当的唯一确定的其他信息。

一数字邮资计通过在信封上用两个“数字标记(digital token)”加注邮政信息而提供邮资给付的数据。一个数字标记向邮政服务部门提供数据,而第二个数字标记向卖主如本发明的代理提供数据。一数字标记是是对加密签条信息的结果的截取,该加密签条信息包括,例如邮资值、件数、邮寄日、以及邮寄地的邮局。

正在开发一种新的数字邮资计,该邮资计采用加密装置以产生邮资给付的数据。该加密采用一加密密钥进行。在各数字邮资计中,采用独立的密钥以产生数字标记。为了安全的缘故,不同邮资计中的密钥也是独立的。有关邮资计和邮件的信息与卖主及邮局主密钥或从其导出的密钥结合并加密。所产生的信息段打印在邮件上作为数字标记。该信息与标记可通过一装置来检验,该装置以同样的方式处理该信息并将得到的数字标记与那些打印在邮件上的进行比较。

需要一密钥管理系统以安全而可靠的方式将加密密钥分配给数字邮资计。该密钥管理系统必须包括检验签条与数字标记以检测出伪造的签条和复制的签条的装置。

人们期望该密钥管理系统具有产生不用指定目的地的邮资计的能力,即产生可以编制的通用邮资计。然而,产生通用邮资计造成的问题是,或者需要在字段中设置密钥,或者需要在域之间进行密钥的变换。两种方式均带来对安全性和密钥的完整性的威胁。人们期望一密钥管理系统包括有避免这些问题的装置。

本发明提供一种产生业务往来显示装置如数字邮资计的方法。一些邮资计是在不知道目的地的情况下产生。这带来的问题是,或者需要在字段中设置密钥,或者需要在域之间进行密钥的变换。两

种方式均对安全性和密钥的完整性构成威胁。在本发明中,通过设置一单独的域,称之为地球域(Earth domain),避免了这些问题的出现。通过设置这里称之为地球域的一单独的域,在本发明中避免了与通用邮资计有关的上述问题。 本发明提供了在制造过程中当目的地不明时安全地管理数字邮资计密钥的能力。

根据本发明,邮资计密钥产生并设置在邮资计产生的邮政域之下的一数字邮资计中。当邮资计的一签条序号注册时,即运行时,邮局的地点即可知道。该地点的识别箱则识别该注册,然后一邮资计密钥被保留,最好通过一签条序号来进行索引。每一地点的识别箱保留该地点的邮资计密钥,以与该地点特定的保密密钥进行加密。

根据本发明,任何接收在制造过程中没有明确针对该地点进行初始化的邮资计的地点,则将接收地球域邮资计。该地点的安全识别箱被启动以作为该地点的数据库加密密钥的地球域识别过程。如果一地点具有明确为该地点的邮政域制造的邮资计和在地球邮政域下制造的邮资计,则该地点的识别箱必须能够在地球域的该地点的支域,以及在该地点的本域中进行操作。

本发明包括下述步骤,在一密钥管理系统的逻辑安全域中产生一主密钥;该将主密钥设置到一数字邮资计中;识别该设置的主密钥;并将该主密钥注册到该密钥管理系统中的一逻辑安全支域中。产生该主密钥的步骤还包括,产生一域的步骤;产生至少一个支域;将该域设置在密钥管理系统的安全箱中;在该域中产生一主密钥和测试标记;并将主密钥记录在域档案存贮器中。主密钥的设置步骤还包括,将主密钥设置到一数字邮资计中的步骤;并使主密钥与一唯一的设备识别器相联系。将主密钥注册到该密钥管理系统中的一逻辑安全支域中的步骤还包括,给数字邮资计指定一支域;在数字邮资计中设置一邮政识别器;使该邮政识别器与该唯一的设备识别器相联系;根据邮政识别器和该唯一的设备识别器在数字邮资计中产生一注册标记;利用记录在档案存贮器中的主密钥,产生注册标记;识别注册标记是同样的;并将主密钥记录在支域中。对于给数字邮资计指定的每一个域,重复上述步骤。

该密钥管理系统包括用于产生、分配和管理加密密钥的装置,该加密密钥由一信息交易系统采用,该交易系统采用加密装置以产生信息完整的数据。该系统包括多个功能不同而操作相互联系的安全箱。每一安全箱的功能分别对应密钥的产生,密钥的设置,密钥的识别或标记的确认。计算机与安全箱的结合运行,提供系统控制并在安全箱中提供方便的通讯。多个单独的逻辑安全域为密钥的产生、密钥的设置、密钥的识别以及通过该域中交易显示装置采用该密钥管理功能而产生的标记的确认提供域的处理。多个域档案存贮器,分别相应于各安全域,安全而可靠地为各域记录密钥的状态记录和主密钥。该密钥管理系统将主密钥设置在交易显示设备中,并确认该标记。该安全箱包括一密钥产生箱以产生、加密并标记一主密钥;一密钥设置箱用于接收、识别和解码该标记的主密钥,并将该主密钥设置到该交易显示设置中;一密钥识别箱用于识别该交易显示设备中设置的主密钥,一标记识别箱用于识别该标记,而至少有一个产生箱用于产生每一域的域密钥并在安全箱中分配该域密钥。

根据本发明的优选实施例,一密钥管理系统产生加密密钥,如卖主密钥、VSPS 密钥和其他地点邮政密钥,并将其分配给多个域的数字邮资计。一个域是通过唯一域确认与加密密钥强制执行的数据与功能的逻辑分离。该密钥管理系统防止域之间密钥的任何调换,提供在一域中密钥在该域中产生,并且由该系统设置在仅一个邮资计中的保证。该密钥管理系统为多个域安全地分配并保持加密密钥。另外,该密钥管理系统这样构造,使得所有域的密钥管理是一样的。

该密钥管理系统支持下述的安全需要:(1)邮资计密钥总是加密的;(2)在系统的生命期内总是具有识别签条信息的能力;(3)邮资计主密钥的状态必须总是精确地保持;(4)域的划分必须保持,以产生和识别签条;以及(5)一个密钥只能设置或试图设置一次。

本发明的上述和其他目的及优点通过下面结合附图的详细描述将会更清楚,其中相同的参考符号表示相同的部件,其中:

图1是根据本发明的一加密密钥管理与确认系统的方框图;

图 2 是一方框图, 显示了图 1 中的密钥管理与确认系统中安全域的关系;

图 3 是图 1 中的密钥管理与确认系统中一卖主数据中心的方框图;

图 4 是图 1 的密钥管理与确认系统中卖主生产设施的方框图;

图 5 是图 1 的密钥管理与确认系统中一邮政数据中心的方框图;

图 6 是图 1 的密钥管理与确认系统中一生产箱的管理域的方框图;

图 7 是一密钥管理过程的流程图;

图 8 是密钥的识别的流程图;

图 9 是生产箱的密钥的内容的方框图;

图 10 是橡木箱的密钥的内容的方框图;

图 11 是钢箱的密钥的内容的方框图;

图 12 是黄铜箱的密钥的内容的方框图;

图 13 是一地球域数字邮资计过程的流程图;

图 14 是有效主密钥状态转换的流程图;

图 15 是有效主密钥状态转换的方框图;

图 16 是从橡木箱传送到黄铜箱的一信息;

图 17 是从橡木箱传送到钢箱的一信息;

图 18 是检测新密钥的逻辑图;

图 19 是从钢箱传送到黄铜箱的一信息;

图 20 是从一邮资计传送到黄铜箱的一信息;

图 21 是误差处理的方框图;

图 22 是第一生产箱的初始化的流程图;

图 23 是通用箱的初始化的流程图;

图 24 是一密钥请求的处理的流程图;

图 25 是一密钥设置的处理的流程图;

图 26 是一密钥注册的处理的流程图;

图 27 是一失效密钥的处理的流程图;

图 28 是识别处理的流程图;

图 29 是一方框图, 显示了密钥设置信息的流动;

图 30 是图 29 的密钥设置信息的一表;

图 31 是密钥注册信息的一表; 和

图 32 是一方框图, 显示了域与支域间的关系。

在本发明的描述中, 对附图进行了标注, 其中, 可见到一密钥管理与确认系统的各方面, 这里也称之为密钥管理系统。

现在参看图 1, 一密钥管理系统的方框图提供了该密钥管理系统的元件的位置及信息流动的全况。以 10 来表示的该密钥管理系统包括卖主设施 12 与 14, 以及邮政设施 16 与 18。该卖主是管理该密钥管理系统的单位。密钥管理系统 10 包括多个功能专用的安全箱, 计算机和通信线。根据本发明, 密钥管理系统 10 为新一代的数字邮资计产品提供生产和运行支持。这里所称的数字邮资计和数字邮资计产品均指这样的新一代数字邮资计产品。要说明的是, 本发明适于管理加密密钥的产生、分配和对其他应用的加密数据的识别。

根据本发明, 卖主和邮政主密钥由密钥管理系统 10 的元件产生、进行档案存贮并设置到邮资计中。邮政标记密钥由密钥管理系统 10 的元件导出、分配并用于远程识别。卖主和邮政标记由密钥管理系统 10 的元件识别。

密钥管理系统 10 支持数字邮资计产品中加密密钥的设置及长期保持。主密钥的产生由主密钥产生箱 20 和 22 (这里也称之为橡木箱)、一配属的密钥管理系统计算机 24 (这里也称之为 KMC) 以及一档案存贮器盘 25 来支持。主密钥的分配由一密钥分配计算机 30 (这里也称之为 KDC) 来支持。主密钥的设置由一主密钥设置箱 32 (这里也称之为钢箱)、一配属的参数化、搜索及注册 (PSR) 计算机 34 来支持。打印的数字标记的集中识别由标记识别箱 21 和 40 (这里也称之为黄铜箱)、以及配属的相应密钥管理系统计算机 24 和 42 来支持。密钥档案存贮器 25 和 45 安全而可靠地记录了密钥的状态信息和密钥。

现在参看图 2, 密钥管理系统 10 包括独立的逻辑安全域; 一卖主域 50, 以及一个或多个用于邮政当局的域 52。每一域提供密钥的

产生、密钥的分配、密钥的设置及标记的识别服务的全集。每一域可包括多个设施,如卖主与邮政设施。在每一安全箱中可存在多个逻辑安全域。这多个域的划分通过对主密钥数据库中的域信息进行加密而实现。该数据库加密密钥对每一域均不同。在一安全箱中,域的划分通过该箱中受限过程的启动而进行。然而,在一数字邮资计内,安全域仅在一个地方重叠。数字邮资计计算付费标记的二个检验,一个使用卖主主密钥,另一个使用邮政主密钥。对任一数字标记的识别的失败,足以证明是伪造。

现在参看图 3,卖主数据中心 12 对密钥管理系统的元件提供物质和信息的存取控制。卖主数据中心 12 拥有至少一橡木箱 20 作为卖主主密钥产生箱,至少一黄铜箱 21 作为卖主标记识别箱,以及一生产箱 23。为了安全,每一箱具有唯一的 ID。为了增加安全性,产生、识别与生产功能相互从物质上分开,即,橡木箱、黄铜箱与钢箱为独立的箱。要说明的是,如果需要,在一物质箱中可以拥有多于一个的功能箱。

卖主 KMS 计算机 24 管理着安全橡木、黄铜及生产箱,以及其间的信息传送。它支持安全箱通信、卖主密钥档案存贮服务、邮政密钥档案存贮服务,以及与卖主生产设施 14 和邮政数据中心 16 的通信。

现在参看图 4,卖主生产设施 14 对密钥管理系统的元件提供物质与信息存取的控制。一卖主生产设施 14 拥有一卖主密钥分配计算机 30,至少一安全钢箱 32,该钢箱 32 作为主密钥设置箱,以及一相应的 PSR 计算机 34。卖主密钥分配和 PSR 计算机 30 和 34 支持与密钥管理系统计算机 24、其他安全箱及在线数字邮资计 36 的通信。PSR 计算机 30 管理着相应钢箱 32 和数字邮资计 36 的初始化。

现在参看图 5,邮政数据中心 16 对密钥管理系统 10 的元件提供物质和信息存取的控制。邮政数据中心 16 可拥有,作为一邮政主密钥产生箱的一邮政橡木箱 22,以及作为一邮政标记识别箱的一邮政黄铜箱 40。一邮政密钥管理系统计算机 42 可支持安全箱通信,邮政密钥档案存贮服务以及与邮政设施 18 和卖主数据中心 12 的通

信。

现在参看图 6, 需要另一逻辑安全域以支持密钥管理系统元件中的所有其他安全域的设置与保持。这称为密钥管理系统管理域 60, 该域 60 负责密钥管理系统元件中的安全域的产生及设置。

在一地球安全域中地点特定的支域的设置由该地球安全域负责。在安全域中产品代码参数的设置由起作用的安全域负责。这将在下面进行更详细的描述。

下面的段落对密钥管理系统 10 中的所有操作及信息提供概要说明。

密钥管理系统 10 提供多个需要的功能以支持数字邮资计产品的生产及操作。它负责数字邮资计产品中使用的所有加密密钥的产生、分配及长期存贮。它也负责对由采用此加密密钥的数字邮资计产品产生的数字标记进行识别。

密钥管理系统 10 提供两个或更多的安全域。卖主安全域 50 包括密钥的产生、分配、档案存贮以及识别服务。邮政安全域 52 实现类似的服务。这些域在同时含有卖主和邮政主密钥的数字邮资计的一点上重叠, 如图 2 中所示, 即仅在卖主和邮政主密钥可同时获得的邮资计中。

现在参看图 7, 显示了该密钥管理过程的一流程图。当分配之前实际位于卖主生产设施 14 中时, 一数字邮资计 36 接收该卖主主密钥和邮政主密钥。

该密钥管理系统安全箱生产过程与域主密钥产生过程给密钥管理系统 10 和数字邮资计 36 提供加密密钥。数字邮资计 36 的域主密钥由一域橡木过程 70 产生。当域主密钥产生、档案存贮和设置时用于加密域主密钥的域密钥, 由生产箱 23 产生。为了提供安全而不确定的密钥, 采用了两个随机数发生器过程。每一橡木箱和生产箱包括一硬件的随机数发生器。也包括一软件的伪随机数发生器。这两个过程的输出单独进行测试以识别该硬件和软件是否在可接受的限度内运行。两个发生器的输出经一异或运算结合起来。从而, 如果硬件随机数发生器出故障, 则伪随机数发生器提供可接受的密钥材, 直到硬件发生器能调整。

其他的 KMS 安全箱有限地用于产生密钥材。特别地, 在初始化过程中, 由黄铜和钢箱 21 和 32 来产生启动加密密钥。在初始化过程中, 由于有限的需要以及托管机构的出现, 只软件伪随机数发生器被采用。

密钥管理系统 10 必须保证安全性的需要, 一主密钥只能试图或设置在任何数字邮资计 36 中一次。例如, 密钥管理系统 10 必须保证在二个或更多个钢箱 32 用于系统中时, 一域主密钥不设置二次。此需要通过采用域主密钥识别数而得以满足, 该识别数由域特定的单调顺序计数器构成。域橡木过程和域钢过程追踪接收到的最后域主密钥识别数, 以针对一特定的域 ID。当一新的产生密钥或设置密钥信息被接收到时, 该域橡木过程或域钢过程识别该域主密钥识别数大于先前信息中所含的。

当密钥管理系统 10 接收到一请求密钥命令时, 需要一钢 ID。该钢 ID 包括在分配主密钥记录中, 并需由域钢过程 76 来检验。如果该信息中的钢 ID 与钢箱的钢 ID 不匹配, 该信息被拒绝。不破坏该信息的签名, 该信息中的钢 ID 不能修改。域主密钥识别数、钢 ID 以及信息签名的结合满足了一次设置的需要。

现在参看图 8, 密钥分配计算机 30 在 80 处请求一密钥。在 82 处, 密钥管理系统计算机 24 从一域档案存贮器 74 中产生一新的单调增加的密钥 ID。在 84 处, 域橡木过程 70 确定该橡木箱密钥 ID 相对于上次所见的值是否是新的。如果不是新的, 在 86 处启动一橡木箱误差条件。如果该密钥 ID 是新的, 则在 88 处, 橡木箱 20 产生并加密一密钥, 配属到该密钥 ID 上, 并将该信息标记及传送到钢箱 32。在 90 处, 域钢过程 76 确定该钢 ID 是否正确。在 92 处, 域钢过程 76 确定该密钥 ID 相对于上次所见值是否是新的。如果该信息签名测试失败, 钢 ID 不正确或密钥 ID 不是新的, 则一钢箱误差出现。如果没有误差出现, 则在 98 处, 钢箱 32 设置该密钥到一邮资计 36 中。

现在参看图 9~12, 密钥管理系统 10 中的安全箱必须用域组合信息和密钥材来进行初始化。这通过使用生产箱 23 而实现, 该生产箱 23 负责域和域密钥 110 的产生。当一域产生时, 需要一唯一的

域 ID。在生产箱 23 中建立一域以后,其他的安全箱可用该域信息来初始化。

所有的域密钥 110 均由生产箱 23 来产生。域密钥 110 包括由域密钥集 103 加密的保密、确认及操作密钥。域密钥 110 在不同的安全箱中共享。每一安全箱对密钥材有特定的需要。

每一生产箱 23 需要一操作集合 101,该操作集合 101 分为三个 Shamir 隐蔽份额 102。单个的份额写到可移动的介质上并分配给授权的人。每一生产箱 23 需要一域密钥集 103,该集 103 包括一 RSA 密钥对用于保密以及一 RSA 密钥对用于确认。保密与确认密钥分为三个 Shamir 隐蔽份额 104。单个的份额写到可移动的介质上并分配给授权的人。RSA 密钥对在 1978 年 2 月的 Vol.21 No.2 "Communications of the ACM" 第 120 ~ 127 页上,由 R. L. Rivest, A. Shamir 和 L. Adleman 所著的"获得数字签名和公众密钥(Public-Key)加密系统的一种方法"中有描述。Shamir 隐蔽份额在 1979 年 11 月的 Vol. 22. No. 11 "Communication of the ACM" 第 612~613 页上,由 A. Shamir 所著的"How To Share A Secret"中有描述。

在优选的实施例中,每一橡木箱 20 需要一操作集合 105,该集合 105 划分为两个 Shamir 隐蔽份额 106(图 10)。单个份额 106 写到可移动的介质上并分配给授权的人。所有的份额 106 必须在其能操作之前进入橡木箱 20 中。最后进入的份额 106 必须保留在橡木箱中以保持其启动。当最后进入的份额 106 移走时,橡木箱 20 中止。

每一域橡木过程 70 需要一 RSA 密钥对以用于确认。个人确认密钥 (P' oA) 只有域橡木过程 70 和生产箱 23 知道。公众确认密钥 (POA) 由相应的域钢过程 76 和域黄铜过程 72 知道。域橡木过程 70 不需要一个人保密密钥。

在优选实施例中,卖主生产设施中每一钢箱 32 需要一操作集合 119,该集合 119 划分为两个 Shamir 隐蔽份额 120(图 11)。单个份额 120 写到可移动介质上并分配给授权的个人,例如一监控者和操作者。监控者和操作者份额 120 的集在其可操作之前必须进入钢箱 32。最后进入的份额 106,例如操作者份额,必须保留在钢箱 32

中以保持其启动。当操作者份额 120 移出时, 钢箱 32 中止。

每一域钢过程 76 需要一 RSA 密钥对用于确认。个人确认密钥仅由域钢过程 76 知道。公众确认密钥仅由域黄铜过程 72 知道。每一域钢过程 76 需要一 RSA 密钥对用于保密。个人保密(P'_{sc})密钥仅由域钢过程 76 知道。公众保密(P_{sc})密钥仅由域橡木过程 70 知道。

在本发明的优选实施例中, 每一黄铜箱 21 需要一操作集合 121, 该集合 121 划分为两个 Shamir 隐蔽份额 122 (图 12)。单个份额 122 写到可移动的介质上并分配给授权的个人。所有份额 122 在其可操作之前必须进入一黄铜箱 21。最后进入的份额 122 必须保留在黄铜箱 21 中以保持其启动。当最后进入的份额 122 移出时, 黄铜箱 21 中止。

每一域黄铜过程 72 需要一 RSA 密钥对应于确认。个人和公众确认密钥(P'_{BA} 和 P_{BA}) 仅由域黄铜过程知道。每一域黄铜过程需要一 RSA 密钥对用于保密。个人保密密钥(P'_{BC}) 仅由域黄铜过程 72 知道。公众保密密钥(P_{BC}) 由域橡木过程 70 知道。每一域黄铜过程 72 需要一 DES 密钥集用于保密, 该密钥集仅由域黄铜过程 72 知道。每一域黄铜过程 72 需要一 DES 密钥集用于确认, 该密钥集仅由域黄铜过程 72 知道。

本领域的技术人员将理解, 操作安全箱需要选择的份额的数量依赖于对密钥管理系统实施的安全性策略。

一生产序列数, 结合一产品代码数, 唯一地限定了卖主生产过程中的数字邮资计 36。生产序列数的分配的优选方法如下。一识别标记源存在该生产线上, 每一识别标记含有唯一的产品代码数和生产序列数对。一个识别标记用到一个数字邮资计 36 上。这些数在密钥设置过程之前进入 PSR 计算机 34 并加载给数字邮资计 36。

邮资计安全地构成, 使得一旦在生产中密钥被设置, 则不留下物质的破坏痕迹在生产环境之外不可能对其进行移动或确定。

在主密钥产生过程中, 域橡木过程 70 采用了一测试信息集。一测试样本用于产生一测试标记集, 以检验生产中的主密钥设置过程。该测试样本由两个预先形成的 64 位二进制值构成。用目标或

主密钥对其进行加密,从得到的密码文本中产生标记的特定位置和数目。

测试样本包括在域橡木和域黄铜过程的操作软件中。在密钥的设置检验过程中,所有数字邮资计采用同样的测试信息。测试样本是在密钥管理系统 10 与目标数字邮资计之间共享的一信息集。对一特定的数字邮资计,测试样本可存在 ROM 中。

地球域数字邮资计在离开生产设施时不具有地点特定的信息。这使得数字邮资计存贮在一地域基础上并在最后一刻确定其特定地点。一地球域数字邮资计的产品代码数是一两字母的产品代码前缀其后紧跟一预定的数。在地点标出之前,一签条序号是一空的信息串。在密钥注册时,产品代码数与签条序号值必须限定,以使域主密钥启动。

现在参看图 13,提供了一地球域数字邮资计的过程流程图。地球域数字邮资计的地球域主密钥由地球域橡木过程 170 产生。地球域主密钥的拷贝存在地球档案存贮器 174 中。地球域主密钥设置在地球域数字邮资计 136 中,并由地球域钢过程 176 检验。地球域主密钥的设置由地球域黄铜过程 172 识别。地球域主密钥记录由地球黄铜过程 172 刷新以设置状态。地球域黄铜过程 172 不参预密钥的注册。

授权的个人通过设定数字邮资计产品代码数和签条序号,指定该地球域数字邮资计 136 给一地点特定的安全域。一旦数字邮资计 136 指定给一地点特定的安全域,则它不能返回地球域中。一数字地标记的密钥注册记录由数字邮资计产生,含有产品代码数、签条序号和生产序号。该数字标记的密钥注册记录返回密钥管理系统计算机 24。

密钥管理系统计算机 24 将从地球域档案存贮器 176 检索地球域主密钥记录。地球域主密钥记录和密钥注册记录送到地点特定的域黄铜过程 272。该记录被识别。如果没有发现问题,域主密钥用地点特定的加密密钥加密。域主密钥记录由地点特定的安全域个人密钥加以标记,以使其完整和得以确认。域主密钥记录将送到地点特定的域档案存贮器 274。

域档案存贮器 74 支持域主密钥的长期存贮及检索。这利用橡木箱 20、域档案存贮器 74 和黄铜箱 21 之间进行的几个交易而完成。

当数字邮资计经过生产、分配和用户现场时, 域主密钥状态更新。每一状态的变化存入域档案存贮器记录, 对域主密钥的生命周期提供完整的密钥活动历史。

现在参看图 14 和 15, 提供了有效主密钥状态传送的流程图。在橡木箱 20 完成密钥的产生过程以后, 域主密钥和信息的加密拷贝进入域档案存贮器 74。在 180 处, 域主密钥的状态将设定到“新”。域档案存贮器 74 将分配数据库存贮并写入信息。

在钢箱 32 和黄铜箱 21 完成密钥的设置过程以后, 域主密钥记录被更新。如果该过程成功, 在 182 处域主密钥的状态可设定到“设置”。如果在密钥的分配或设置过程中出现任何故障, 则在 184 处, 域主密钥的状态将设定到“不好”。这些故障可包括信息丢失、信息错误、域主密钥写入数字邮资计存贮器错误、检验测试标记错误或其他。

当对一特定的邮政域, 指定一签条序号给数字邮资计时, 卖主和邮政域主密钥记录被更新。在 186 处, 主密钥状态设定到启动, 对该数字邮资计的识别服务被允许。当数字邮资计退出服务时, 卖主和邮政域主密钥记录被更新。在 188 处, 主密钥状态设定到“作废”。

密钥管理系统 10 包括实际的安全箱和逻辑的安全域集。这些元件间的信息流必须含有足够的信息, 以使得过程和检验者能识别信息的共享者。

逻辑安全域由称为域 ID 的一地址目标来确定。此地址唯一地限定密钥管理系统 10 中一特定域的一实例。有效域 ID 的例子可以是, 用于卖主安全域的 VE, 美国邮政服务安全域的情形的 VSPS, 以及英国皇家邮政安全域的情形的 VKRM。安全域覆盖了多个安全箱, 并可覆盖多个档案存贮器。在一个安全箱的实际范围中可同时存在多个安全域。在任何给定的时间, 一安全箱中只有一个域启动。在域之间不能有数据传送。

逻辑安全箱目标由称为安全箱型号的一地址目标来确定。此地址唯一地限定参予信息交易的安全箱的功能。橡木箱 20 是主密

钥产生器。钢箱 32 是主密钥设置箱。黄铜箱 21 是标记识别箱。
锡箱 44 是远程标记识别箱。

实际安全箱的识别由称为安全箱 ID 的一地址目标来确定。
此地址唯一地限定密钥管理系统 10 中箱的一实例。它由一安全箱类型和数字标志符构成。

密钥管理系统 10 的每一元件保持多个构造表,以允许操作软件确定密钥管理系统服务信息的有效性和处理需要。命令表用于识别系统的元件想要什么密钥管理系统服务信息和命令。—KMS 系统命令表限定了在系统水平上可接受的所有命令。系统水平上的表的子集由系统元件贮存,该系统元件包括橡木箱 20、黄铜箱 21、钢箱 32、生产箱 23、KMS 计算机 24、密钥分配计算机 30 和 PSR 计算机 34。所接收到的不包括在本地命令表中的信息被拒绝。

构造表用于识别什么样的密钥管理系统域 ID 由系统的元件来识别。—KMS 系统构造表限定在系统水平上可接受的所有域 ID。系统水平上的表的子集由系统的元件贮存,该系统元件包括橡木箱 20、黄铜箱 21、钢箱 32、生产箱 23、KMS 计算机 24、密钥分配计算机 30 和 PSR 计算机 34。所接收到的不包括在本地构造表中的域 ID 的信息被拒绝。

记录表用于识别什么样的密钥管理系统记录被系统的元件识别。—KMS 系统记录表限定在系统水平上被识别的所有信息记录。该系统水平上的表的子集由系统的元件贮存,该系统元件包括橡木箱 20、黄铜箱 21、钢箱 32、生产箱 23、KMS 计算机 24。密钥分配计算机 30 和 PSR 计算机 34。所接收到的含有不包括在本地记录表中的信息记录的信息被拒绝。

域橡木过程 70 将域主密钥传送给域档案存贮器 74。现在参看图 16, 域主密钥(K'_{DM})在其存入域档案存贮器 74 之前用域黄铜过程公众密钥(P'_{BC})加密。从而, 域橡木过程 70 不从域档案存贮器 74 解码域主密钥(K'_{DM})。域橡木过程 70 在域主密钥记录存入域档案存贮器 74 之前用域橡木过程个人密钥(P'_{OA})对其进行标记。从而, 域黄铜过程 72 可确信域主密钥记录由域橡木过程 70 产生。

域橡木过程 70 将域主密钥(K'_{DM})发送给域钢过程 76。现在参

看图 17, 域主密钥(K'_{DM})在其传送到域钢过程 76 之前用域钢过程公众密钥(P'_{SC})加密。从而, 域橡木过程 70 不会从一分配主密钥记录中解码域主密钥(K'_{DM})。域橡木过程 70 在分配主密钥记录传送到域钢过程 76 之前用域橡木过程个人密钥(P'_{OA})对其进行标记。从而, 域钢过程 76 可确信分配主密钥记录由域橡木过程 70 产生。

现在参看图 18, 显示了对密钥的新旧的检测流程。为了支持上述的安全性需要, 一密钥只能设置或试图设置一次, 以保证域主密钥是新的。域档案存贮器给所有的域主密钥指定单调排列的密钥 ID(KID)。对每一域 ID 保留独立的密钥 ID 索引。域橡木过程 70 和域钢过程 76 追踪密钥 ID 值并将其与产生密钥信息和分配主密钥记录中接收到的密钥 ID 值比较。从而, 当一产生密钥信息或分配主密钥记录重播时, 域橡木过程 70 和域钢过程 76 可检测。

现在参看图 19, 域钢过程 76 在主密钥设置记录送到 KMS 计算机 24 之前用域钢过程个人密钥(P'_{SA})对其进行标记。通过这样做, 域黄铜过程 72 可确信主密钥设置记录由域钢过程 76 产生。

在密钥的注册期间, 数字邮资计用卖主主密钥(K'_{VM})和出政主密钥(K'_{PM})来标记密钥注册记录。从而, 邮政和卖主域黄铜过程 72 可确信密钥的注册记录值来源于数字邮资计 36。然后每一域黄铜过程 72 用域黄铜过程隐蔽的 DES 密钥对域档案存贮器记录中的域主密钥进行加密。结果, 域黄铜过程 72 可确信其他的域黄铜过程没有读该密钥材。域黄铜过程 72 在域主密钥记录送入域档案存贮器 74 之前, 用域黄铜处理隐藏的 DES 密钥对其进行标记。从而, 域黄铜过程 72 能确信该域主密钥记录仅由域黄铜过程 72 修改。对黄铜过程信息的一邮资计的一个例子如图 20 中所示。

密钥管理系统 10 在域主密钥的有效生命期间, 保持时间过程的检查跟踪。这些过程表明密钥管理系统 10 何时采取行动。对于成功的域主密钥应用, 列出的时间过程必须增加。时间过程超越在先过程的系统信息将被拒绝。所接收到的其时间超越密钥管理系统密钥注册时间的识别请求将被拒绝。

在本发明的优选实施例中, KMS 计算机 24 记录 KMS 请求时间, 该时间是当从密钥分配计算机 30 接收到一请求命令时。PSR 计算机

34 记录 PSR 设置时间, 该时间是当一设置密钥命令发送给一钢箱 32 时。KMS 计算机 24 记录 KMS 设置时间, 该时间是当从密钥分配计算机 30 接收到一设置密钥识别命令时。数字邮资计 36 记录邮资计注册日期, 该日期是当从通信口或用户接口接收到一注册签条命令时。KMS 计算机 24 记录 KMS 密钥注册时间, 该时间是当从数字邮资计接收到一注册签条识别命令时。

在另一实施例中, 当从 KMS 计算机 24 接收到产生密钥命令时, 橡木箱 20 记录本地时间。当接收到设置密钥命令时, 钢箱 32 记录本地时间。当从密钥管理系统计算机 24 接收到一密钥识别请求时, 黄铜箱 21 记录本地时间。

密钥管理系统 10 对密钥管理系统服务信息提供误差检测和报告进程集。当信息在准备、通过通信线传送、接收或由接收单元处理时, 可能出现误差。当在系统中检测到误差时, 命令源将被告知, 在系统误差记录表中将做一个记录。

现在参看图 21, 提供了误差处理的一概要的方框图。系统中的误差以三个不同的级别来检测。误差处理的第一级别在 PB232 协议中执行。此协议通过使用 STX 和 ETX 控制标志, 给信息提供框架。通过使用预定的类代码(Class Code), 提供信息的识别。通过使用误差检测代码, 提供信息的完整性。如果接收到的信息符合这些进程, 则接收者将发送一正的确认控制符号。如果不, 则接收者将发送一非确认控制符号。发送元件将试图重新传送信息或采取其他校正行动。PB232 误差处理进程是一常规的类型。

误差处理的第二级别通过密钥管理系统 10 命令处理过程来执行。它们将接收到的命令与限定在一命令表中的期望的命令集进行比较。命令域被识别。期望的参数的数目被检测。单个参数的句法被检测。如果在命令中发现任何误差, 则一命令误差信息将返回给命令源。

误差处理的第三级别通过密钥管理系统 10 命令处理过程来执行。它们将命令中的参数与定义在一构造表中的期望的参数进行比较。单个参数对照构造表进行检验。不同参数的组合对照构造表进行检验。硬件源与数据库记录的有效性被检验。信息元件的标

记和加密信息元件的有效性被检验。如果在命令中或命令的处理中发现任何误差,则一命令响应信息将随一响应代码返回。如果在响应中发现任何误差,则一命令响应误差信息将随一响应代码返回。

下面的段落对密钥管理系统 10 的安全箱初始化过程提供一概述,如图 22 和 23 中所示。如上所述,在本发明的优选实施例中有四种类型的密钥管理系统安全箱。生产箱 23 负责密钥管理系统和安全箱的初始化。橡木箱 20 负责域主密钥的产生。钢箱 32 负责域主密钥的设置。黄铜箱 21 负责域主密钥注册和标记识别。在另一实施例中,锡箱是一远程标记识别箱。

现在参看图 22,第一生产箱 23 必须初始化。生产箱操作软件被装入并测试。安全箱 ID 初始化到 M00000000。当生产箱 23 启动时,安全箱 ID 被询问。如果它设定到 M00000000,生产箱 23 等待来自 KMS 计算机 24 的设定第一安全箱 ID 信息。然后 KMS 计算机 24 命令第一生产箱 23 将安全箱 ID 设定到 M00000001。然后第一生产箱 23 接收并检验该信息。如果没有发现误差,第一生产箱 23 产生一操作集合 101 和操作共享密钥 102 的集。操作共享密钥 102 写到可移动介质上。

接着,第一生产箱 23 产生两个 RSA 密钥对,一个用于域密钥集的保密,另一个用于域密钥集的确认。这些密钥划分为域共享(Domain Share)并写到可移动介质上。密钥用于在域密钥集送到 KMS 计算机 24 和写到档案存贮器或可移动介质上之前对其进行加密和标记。第一生产箱 23 产生安全箱确认密钥集。为每一类型的箱,即生产、橡木、钢和黄铜,产生一 RSA 密钥对。每一类型的箱的公众密钥写到可移动介质上。然后该密钥必须通过软件工程写入安全箱操作软件中。在所有操作共享和确认密钥成功写入之后,安全箱 ID 将设定到 M00000001。

KMS 计算机 24 请求生产箱 23 产生一域。生产箱 23 在内存中建立域 ID,并产生需要的域密钥 110,该域密钥 110 用域密钥集 103 保密密钥来加密,并用域密钥集 103 确认密钥来标记。该加密和标记过的域密钥写到档案存贮器和/或可移动介质上。

额外的生产箱 23 由一源生产箱来初始化,该源生产箱是已经初始化的任一生产箱。生产箱操作软件装入每一额外的生产箱 23 并在其中测试。安全箱 ID 设定到 M00000000。当生产箱 23 第一次启动时,它对安全箱 ID 进行询问。如果是 M00000000,生产箱 23 从源生产箱等待一设定安全箱 ID 信息。KMS 计算机 24 命令生产箱初始化每一额外的生产箱 23。源生产箱分配下一生产安全箱 ID,用生产箱个人启动确认密钥对信息加以标记,并将其送入生产箱 23。生产箱 23 存贮安全箱 ID 并产生一生产箱启动保密密钥。安全箱 ID 和公众启动保密密钥送回源生产箱,并用生产箱个人启动确认密钥加以标记。KMS 计算机 24 命令源生产箱给生产箱产生一域产生过程。需要的域密钥元件用启动保密密钥发送到生产箱 23。这个过程对所有需要的域进行重复。

任何时候当域增加到一生产箱 23 时,其他初始化的生产箱必须更新以反映这另外的域。在优选实施例中,所有初始化的生产箱用相同的密钥数据来成形。

对于橡木箱的初始化,橡木箱操作软件被装入并测试。安全箱 ID 设定到 000000000。当橡木箱 20 第一次启动时,对安全箱 ID 进行询问。如果是 000000000,橡木箱 20 从生产箱 23 等待一设定安全箱 ID 信息。KMS 计算机 24 命令生产箱 23 初始化橡木箱 20。生产箱 23 分配下一橡木安全箱 ID,并用个人橡木箱启动确认密钥对信息加以标记,并将其送入橡木箱 20,橡木箱 20 存贮安全箱 ID 并产生一橡木箱启动保密密钥。将安全箱 ID 和公众启动保密密钥送回生产箱,并用橡木箱公众启动确认密钥加以标记。KMS 计算机 24 命令生产箱 23 给橡木箱 20 产生一域橡木过程。需要的域密钥元件用启动保密密钥传送到橡木箱 20。此过程使得橡木箱 20 对一域执行域橡木过程 70。此过程对一特定的橡木箱需要的所有域重复。

对于钢箱的初始化,钢箱操作软件被装入并测试。安全箱 ID 设定到 S00000000。当钢箱 32 第一次启动时,对安全箱 ID 进行询问。如果是 S00000000,钢箱 32 从生产箱 23 等待一设定安全箱 ID 信息。KMS 计算机 24 命令生产箱 23 初始化钢箱 32。生产箱 23 分

配下一钢安全箱 ID,并用钢箱个人启动确认密钥对信息加以标记,并将其送到钢箱 32。钢箱 32 存贮安全箱 ID,并产生一钢箱启动保密密钥。将安全箱 ID 和公众启动保密密钥送回生产箱 23,并用钢箱公众启动确认密钥加以标记。KMS 计算机 24 命令生产箱 23 给钢箱 32 产生一域钢过程 76。需要的域密钥元件用启动保密密钥发送给钢箱 32。此过程使得钢箱 32 对一域执行域钢过程 76。此过程对一特定钢箱需要的所有域重复。

对于黄铜箱的初始化,黄铜箱操作软件被装入并测试。安全箱 ID 设定到 B00000000。当黄铜箱 21 第一次启动时,对安全箱 ID 进行询问。如果是 B00000000,黄铜箱 21 从生产箱 23 等待一设定安全箱 ID 信息。KMS 计算机 24 命令生产箱 23 初始化黄铜箱 21。生产箱 23 分配下一黄铜安全箱 ID,用黄铜箱个人启动确认密钥对信息加以标记,并将其送入黄铜箱 21。黄铜箱 21 存贮安全箱 ID 并产生一黄铜箱启动保密密钥。将安全箱 ID 和公众启动保密密钥送回生产箱 23,并用黄箱公众启动确认密钥加以标记。KMS 计算机 24 命令生产箱 23 给黄铜箱 21 产生一域黄铜过程。需要的域密钥元件用启动保密密钥发送给黄铜箱 21。此过程使得黄铜箱 21 对一域执行黄铜过程。此过程对一特定黄铜箱需要的所有域重复。

现在参看图 24~27,显示了密钥管理系统 10 的域主密钥设置过程的概况。在卖主与任何邮政域之间不存在区别。每个均以类似的独立方式操作。为了将域主密钥的全集成功地设置到数据邮资计 36,对卖主域运行操作集,而对选择的邮政域运行另一操作集。

现在参看图 24、29 和 30,在生产过程的产生期间,域主密钥请求来自密钥分配计算机 30。在 300 处,该请求在信息 MIO 中带着钢箱 32 的识别号从密钥分配计算机 30 送到 KMS 计算机 24。在 302 处,KMS 计算机 24 从域档案存贮器 74 中请求一密钥 ID,然后为该域产生一唯一的密钥 ID。在 304 处,域档案存贮器 74 在信息 MIO' 中将一密钥 ID 响应发送给 KMS 计算机 24。KMS 计算机 24 对一检查追踪记录本地时间,并在 306 处,在一产生密钥信息 MI1 中将信息发送给橡木箱 20。橡木箱 20 检查该请求,以确定域的有效性,对于该域钢箱 ID 的有效性,以及对于此域密钥 ID 是否高于上次处理的。

如果检查的任何一次出错,则橡木箱 20 返回一错误信息给 KMS 计算机 24。如果检查无误差,则橡木箱 24 产生一域主密钥以及测试标记集。在 308 处,橡木箱 20 在信息 MI2 中发送一域主密钥记录给 KMS 计算机 24。在 310 处,KMS 计算机 24 在信息 MI3 中,将域主密钥记录提供给域档案存贮器 74。域档案存贮器 74 将域主密钥记录存入数据库中,并在 312 处将一响应送给 KMS 计算机 24。在 314 处,KMS 计算机 24 发送该响应给橡木箱 20,橡木箱 20 在 316 处发送一产生响应信息给 KMS 计算机 24。在 318 处,KMS 计算机 24 在一请求响应信息 MI4 中将设置密钥记录发送给密钥分配计算机 30。

现在参看图 25,当在生产线上出现一数字邮资计 36 时,在 330 处,PSR 计算机 34 从密钥分配计算机 30 请求一设置域密钥记录。在 330 处,密钥分配计算机 30 在信息 MI4' 中发送一设置域密钥记录给 PSR 计算机,该信息在 334 处进一步发送给钢箱 32。钢箱 32 询问数字邮资计 36 的信息,然后在 336 处,将信息 MI5 中的域主密钥发送给数字邮资计 36。数字邮资计设置和检测该密钥,并将状态返回钢箱 32,钢箱 32 向数字邮资计询问邮资计测试标记集。在 338 处,邮资计测试标记在信息 MI6 中返回钢箱 32,钢箱 32 对比从橡木箱 20 接收到的测试标记对该邮资计测试标记进行检验。从而,钢箱 32 检验由橡木箱 24 产生的域主密钥是否与设置在数字邮资计 36 中的密钥相同。在 340 处,钢箱 32 经 PSR 计算机和密钥分配计算机 30 在信息 MI7 中发送设置状态和信息给密钥管理计算机 24。密钥管理计算机 24 从域档案存贮器中检索一域主密钥记录,取用一本地时间标记,并在 342 处,在信息 MI8 中发送信息给黄铜箱 21。黄铜箱 21 从域档案存贮器 74 的域主密钥记录中产生测试标记。这些标记与邮资计测试标记比较。这过程检验域档案存贮器中的域主密钥是否与数字邮资计中设置的密钥相同。如果检查完毕,则域主密钥记录更新,并于 344 处在信息 MI9 中发送给密钥管理计算机 24。密钥管理计算机 24 在信息 MI9 中将域主密钥记录发送给域档案存贮器 74,如果成功,则在 346 处返回一响应给黄铜箱 21。黄铜箱 21 检查响应,并在信息 MI10 中返回一成功或失败识别给 KMS 计算机 24(于 348 处)以及给密钥分配计算机 30。

密钥的注册由注册地点、签条号与产品代码号和密钥的组合构成。该密钥然后采用一保密密钥存入设置域的地点支域中,该保密密钥对于该地点支域是特定的。基本的特征是,对于该地点支域为特定的黄铜过程依赖于设置域以安全而完整地设置密钥。密钥不会从一设置域转到另一设置域。

现在参看图 26 和 31,当数字邮资计准备用于一特定的安全域时,信息 MR1 中的签条序号和/或产品代码号进入数字邮资计中。在 360 处,PSR 计算机 34 从数字邮资计 36 中请求注册标记。数字邮资计产生两个数字标记并在 362 处将其返回 PSR 计算机。PSR 计算机将标记与其他邮资计信息结合,并在 364 处将得到的记录经密钥分配计算机 30 发送给密钥管理计算机 24。在 366 处,密钥管理系统计算机 24 从域档案存贮器检索一域主密钥记录,取用一本地时间标记,并在信息 MR2 中发送信息给黄铜箱 21。黄铜箱 21 从域档案存贮器 74 的域主密钥记录产生注册标记。这些标记与邮资计注册标记比较。此过程检验签条序号、产品代码号和生产序号是否由数字邮资计正确地报告。如果检查完毕,则域主密钥记录更新,并在 368 处发送给 KMS 计算机 24。密钥管理系统计算机 24 在信息 MR3 中发送域主密钥记录给域档案存贮器 74,如果成功,则在 370 处返回一响应给黄铜箱 21。黄铜箱 21 检查响应,并在 372 处在信息 MR4 中返回一成功或失败识别给密钥管理系统计算机 24。

每一域具有至少一支域,该支域负责将密钥注册到签条号,并在该支域中进行签条识别。特定的地球域具有多个地点支域。一地点可以在地球域的一支域中具有邮资计,以及在其本身的邮政域的唯一支域中具有邮资计。在图 32 所示的例子中,地点 3 具有唯一的邮政域和地球域的一邮政支域。然而,地点 A 仅有其密钥设置在该地点的唯一邮政域中的邮资计。

现在参看图 27,如果一数字邮资计退出服务,则该信息被记录并发送给 KMS 计算机 24。密钥管理计算机 24 从域档案存贮器检索一域主密钥记录,取用本地时间标记,并在 380 处发送信息给黄铜箱 21。域主密钥记录更新,并在 382 处发送给密钥管理计算机 24。

密钥管理计算机发送域主密钥记录给域档案存贮器,如果成功,则

在 384 处返回一响应给黄铜箱 21。黄铜箱 21 检查响应,并在 386 处,返回一成功或失败识别给密钥管理计算机 24。

每一邮资计采用域主密钥为每一域产生一暂存密钥,这里也称之为标记密钥,该暂存密钥用于从邮件数据产生一标记。密钥管理系统将邮政暂时密钥分配给具有一分配器标记识别箱 44(图 1)的授权的邮政识别点,在这里箱 44 也称为锡箱。邮政暂存密钥被锡箱 44 用于签条的本地识别。在这样的结构下,密钥管理系统提供更高水平的安全性,因为邮件能得到签条的本地识别,不用将主密钥数据库分配到多个点。

下面的段落提供对密钥管理系统 10 的识别过程的概述。在卖主和任一邮政域之间不存在区别。每一过程以类似的方式独立地操作。为了成功地识别两个标记,对卖主域运行一操作集,而对选择的邮政域运行另一操作集。

标记识别请求来自邮政设施 18 上的一数据捕获系统 19。该请求含有打印在实际邮件上的信息的一 ASCII 文本表示。现在参看图 28,在 400 处,请求被送到位于卖主或邮政数据中心里的一密钥管理系统计算机 24。密钥管理系统计算机 24 检查邮件数据校验位,如果需要予以校正。密钥管理计算机 24 从域档案存贮器检索一域主密钥记录,并在 402 处发送信息给黄铜箱 21。黄铜箱 21 检查该请求,并识别域主密钥是否启动。黄铜箱 21 利用来自域档案存贮器的域主密钥和邮件信息,重新计算所选择的域的标记。计算得到的标记与邮件标记比较,看其是否匹配。一好/坏比较结果在 404 处送给 KMS 计算机 24。第二个例子如图 28 中所示,以强调需要另一识别以识别其他的域标记。

本发明的上述描述是优选的实施例,其中,邮局授权一卖主产生邮政主密钥并将其设置到数字邮资计中。该密钥随后被送到邮政数据中心 16 以用于邮政标记的确认。密钥管理系统具有功能、安全箱和数据库的不同分配的能力。例如,在另一实施例中,一邮局授权卖主或另一单位维持和操作邮政数据中心 16,包括邮政密钥的产生、保持、标记识别以及将密钥传送给卖主的功能。在此实施例中,邮政黄铜箱 40 和邮政密钥档案存贮器 42 实际位于卖主或其

他单位的位置上。在另一实施例中, 邮局管理其数据中心, 而邮政橡木箱 22 实际位于邮政数据中心 16 内。

在另一实施例(未显示)中, 密钥管理系统功能, 即域橡木过程、域钢过程或域黄铜过程的任何组合可以集中到任一安全箱中。

从而, 可以理解, 密钥管理系统具有特有的灵活性, 允许不同的域即邮局实现同样的逻辑密钥管理系统的不同的实际执行过程。该密钥管理系统在保持高水平的系统完整性和安全性的同时提供这样的灵活性。进一步可以理解, 本发明允许多个卖主支持多个邮局。

利用涉及数字邮资计的表示的优选实施例, 已对本发明进行了描述。本领域的技术人员可以理解, 本发明也适用于作为通用的交易证实的一密钥管理系统, 如货币交易、产品交易和信息交易。

在这里使用时, “数字邮资计”这个词表示与固定的打印装置连在一起的常规类型的数字邮资计, 以及与非固定的打印装置连在一起的或具有与此常规数字邮资计不同的其他构造的别的类型的数字邮资计。

虽然本发明仅用一个实施例来进行了公开和描述, 显然, 如上所述, 可以做出变化和修改。因此, 在下面的权利要求中, 期望覆盖落入本发明的实质和范围中的每一变化和修改。

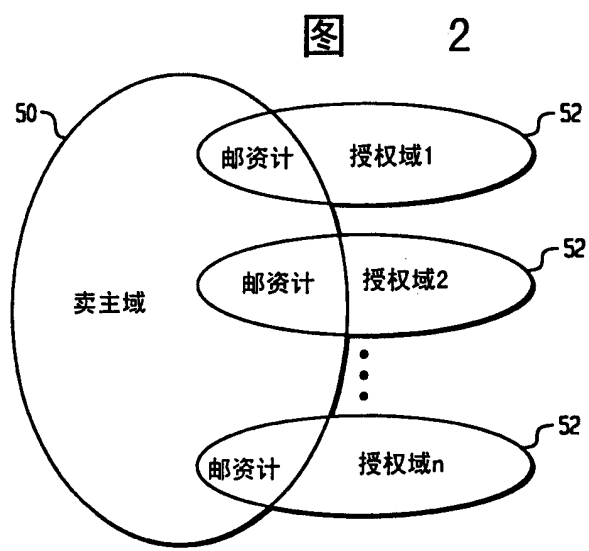
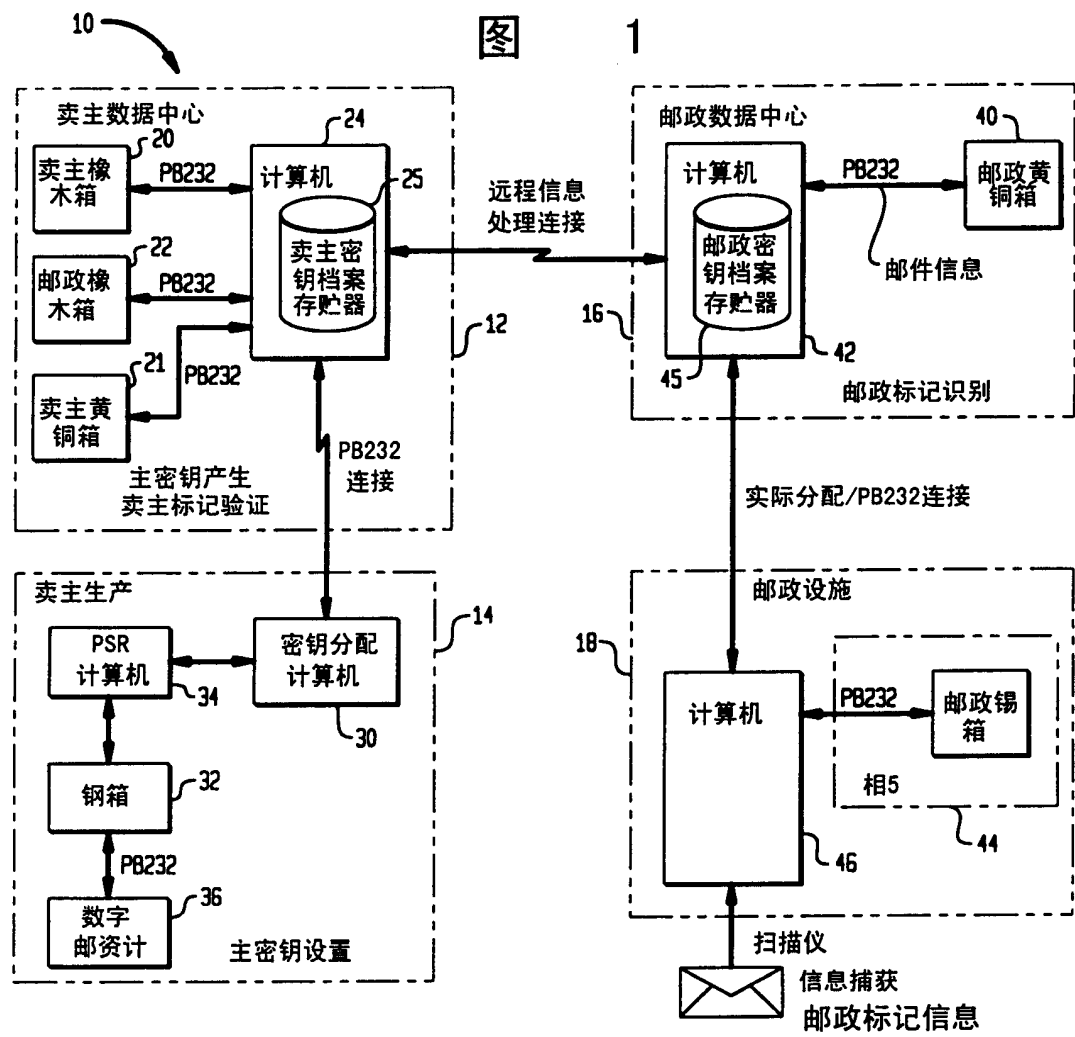


图 3

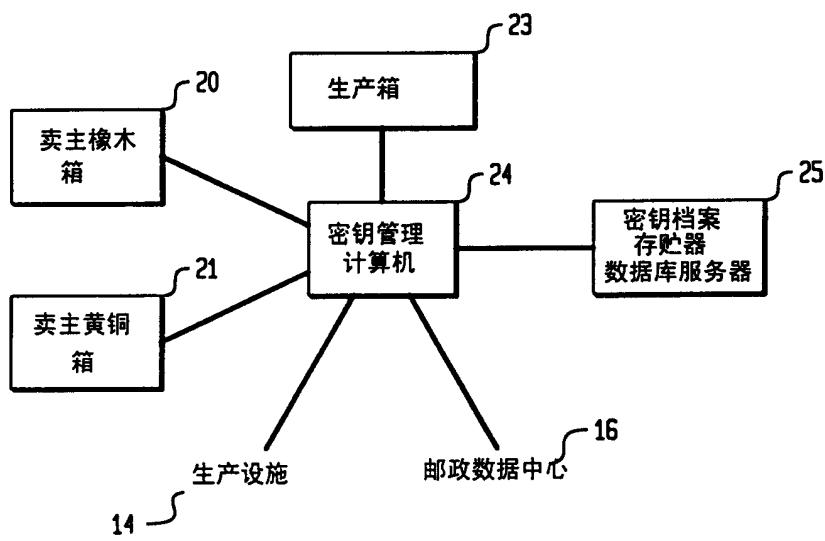
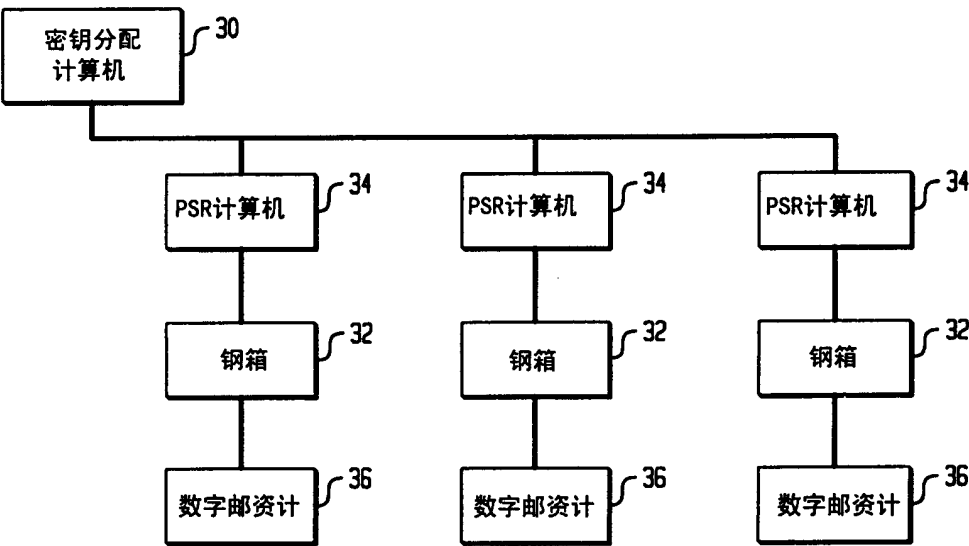


图 4



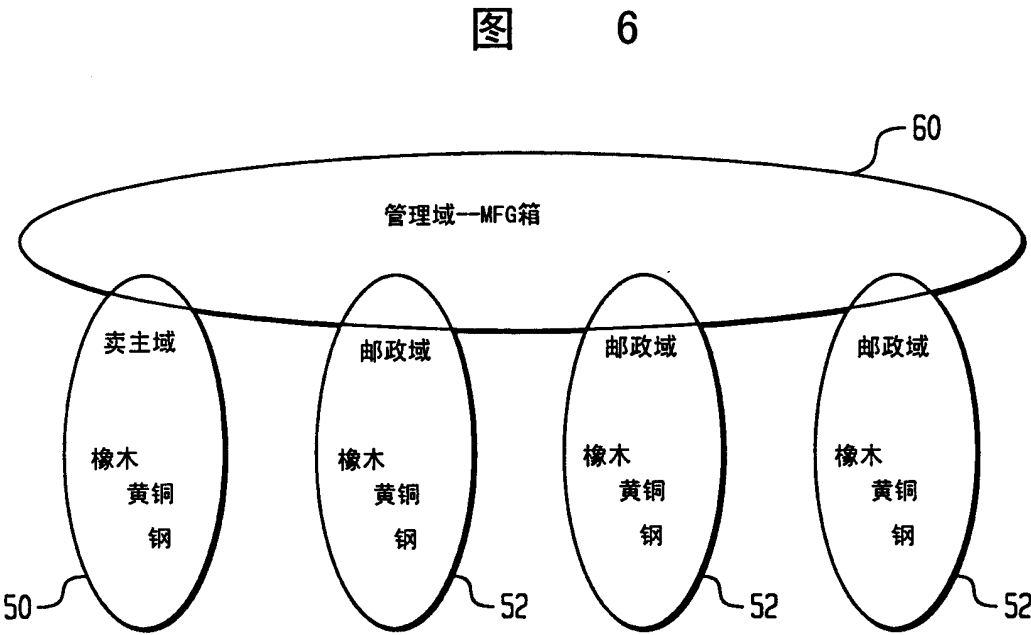
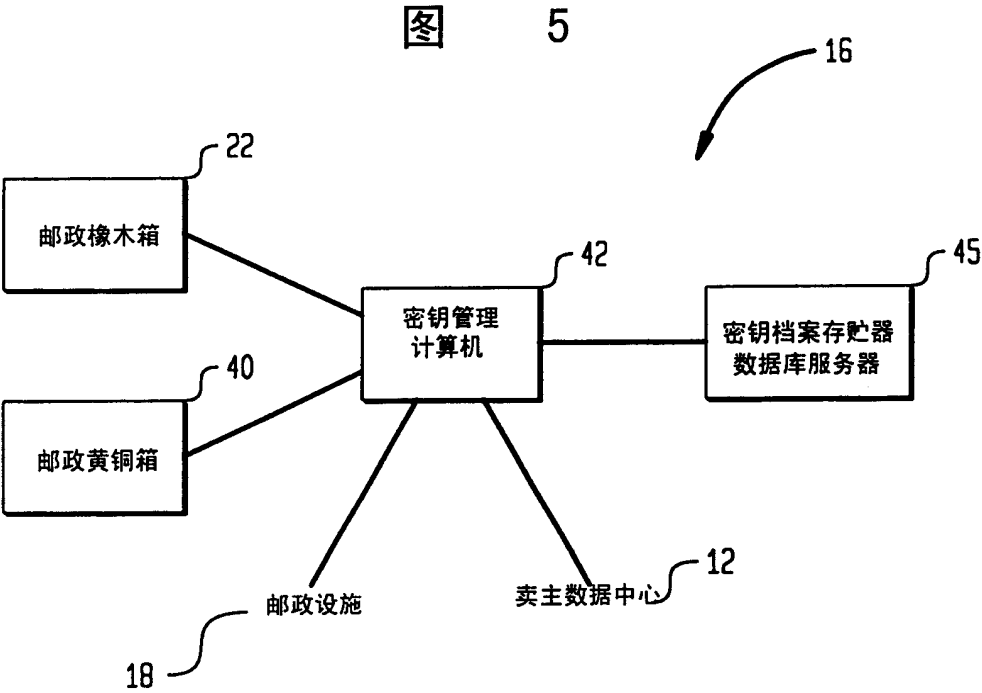


图 7

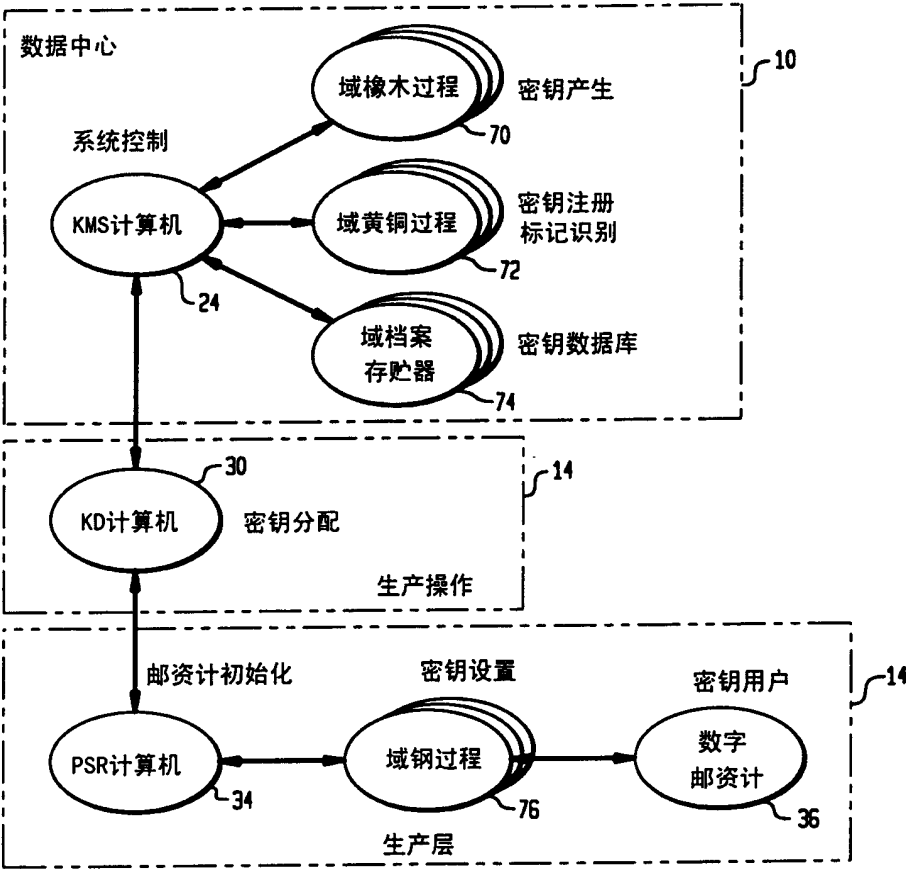


图 9

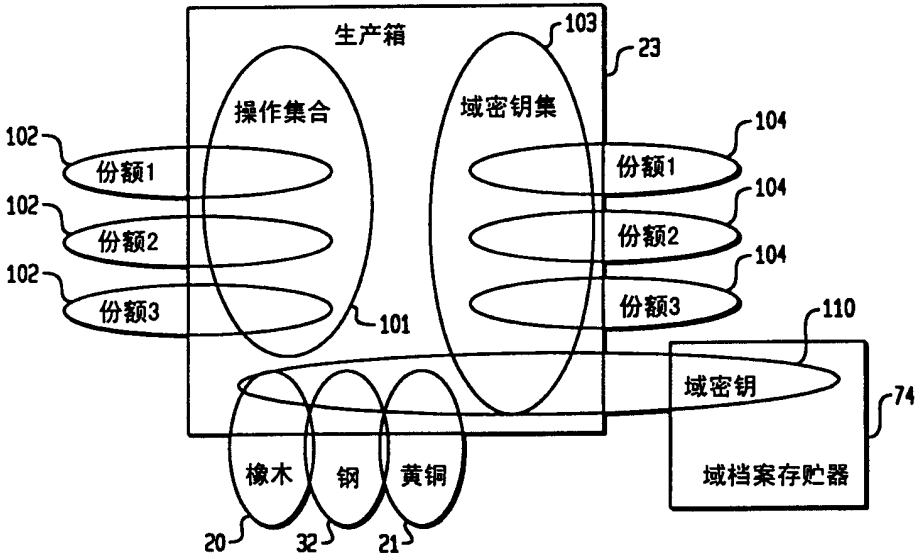


图 8

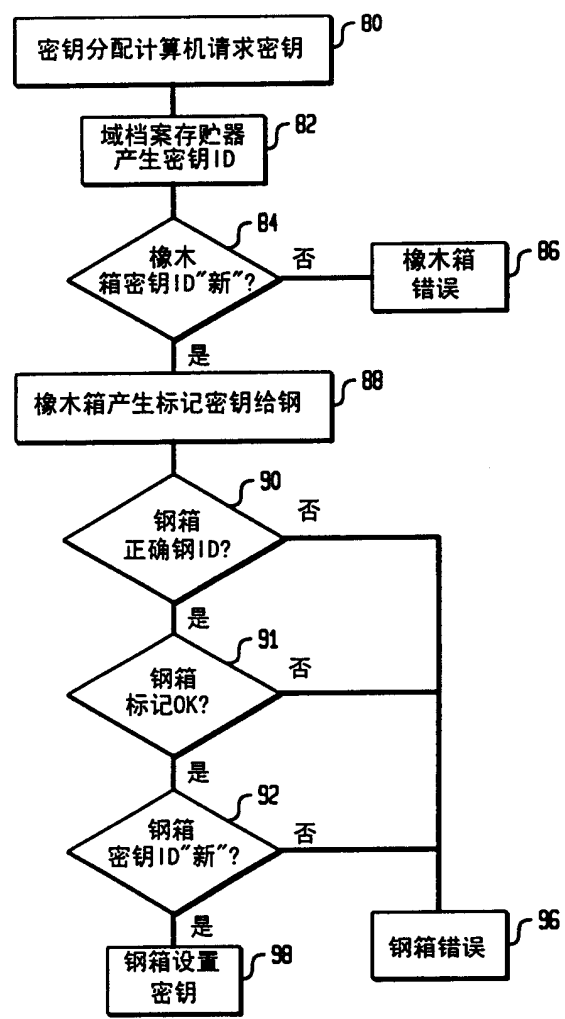
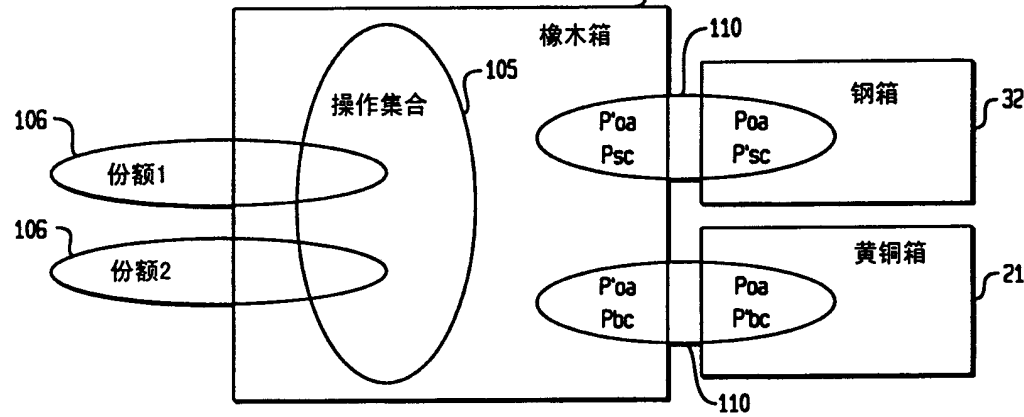
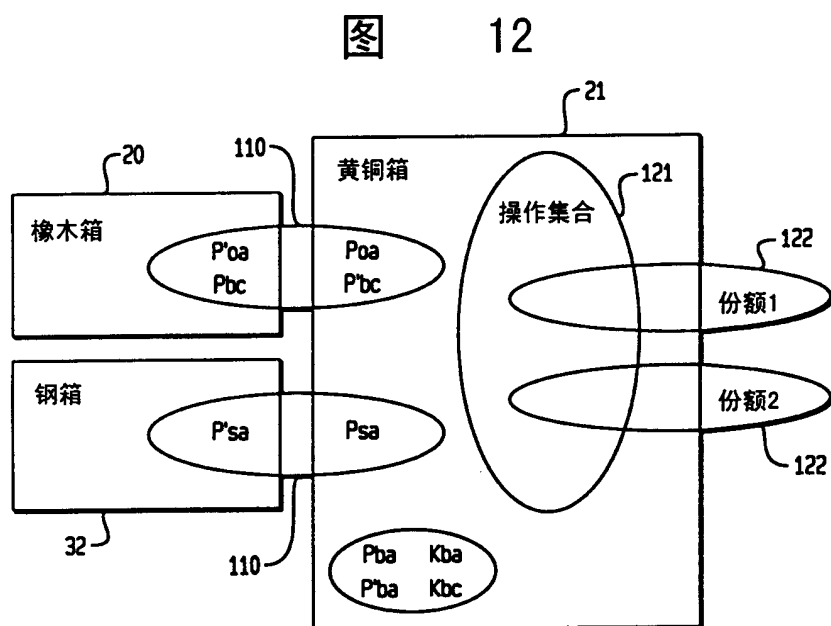
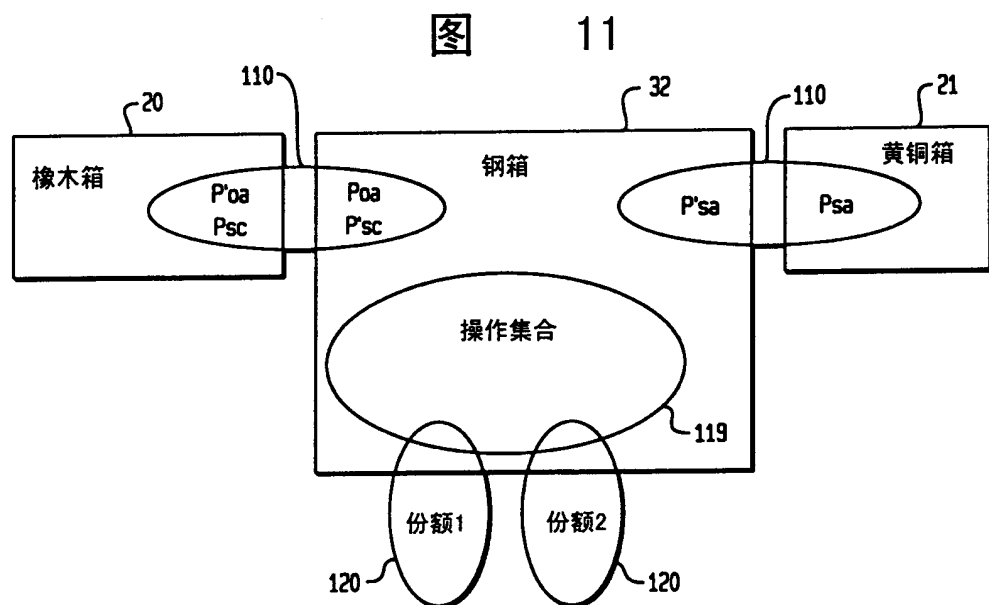
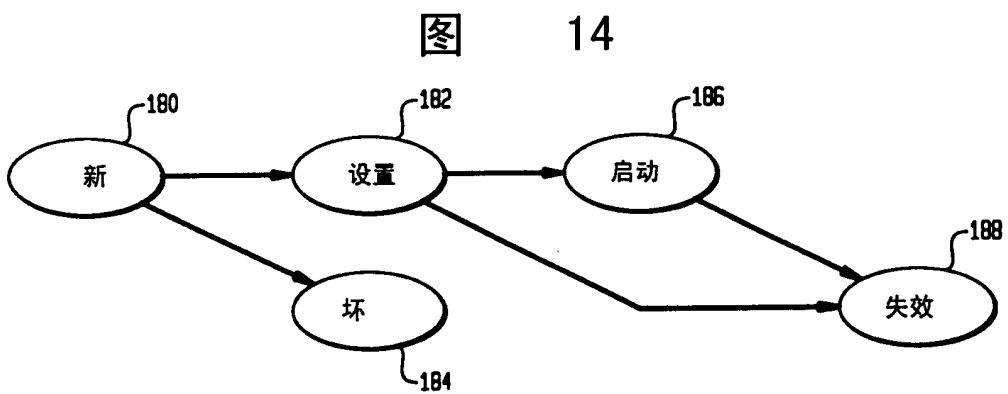
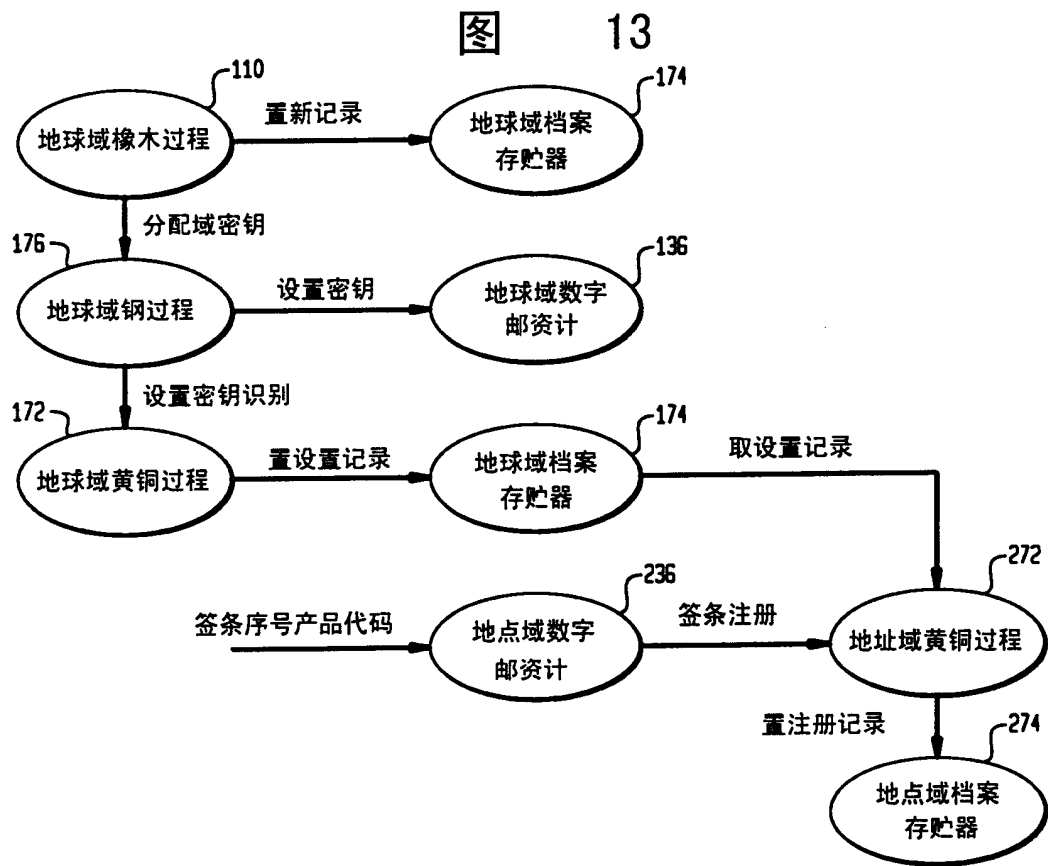


图 10







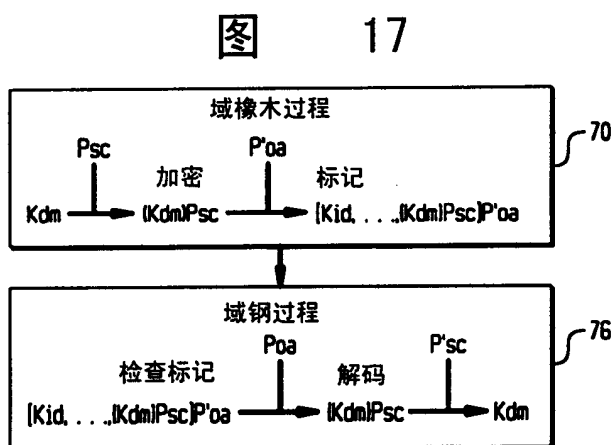
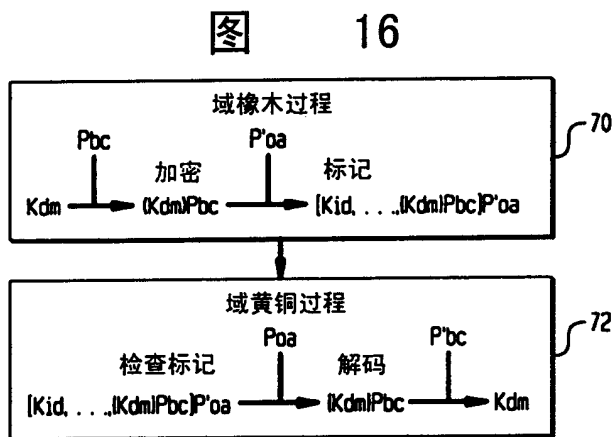
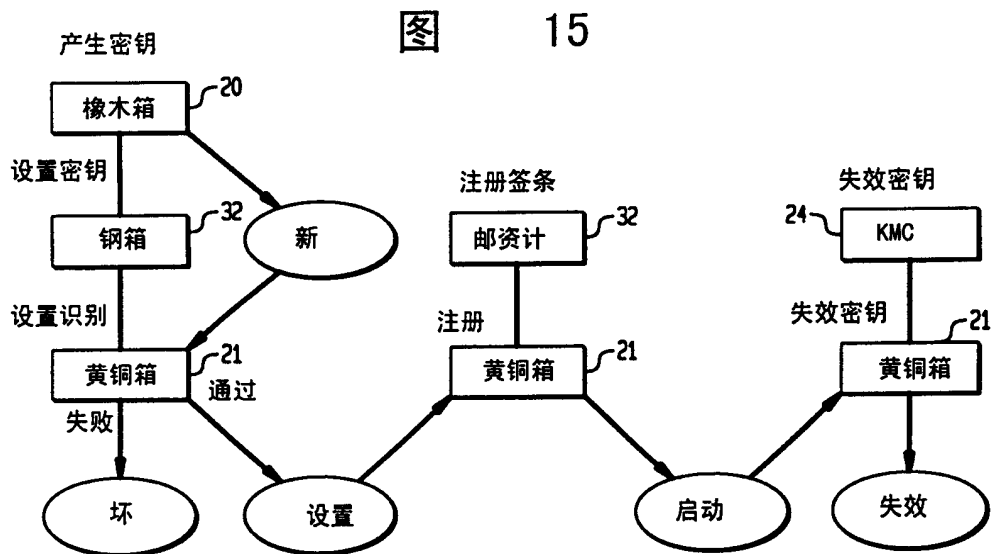


图 18

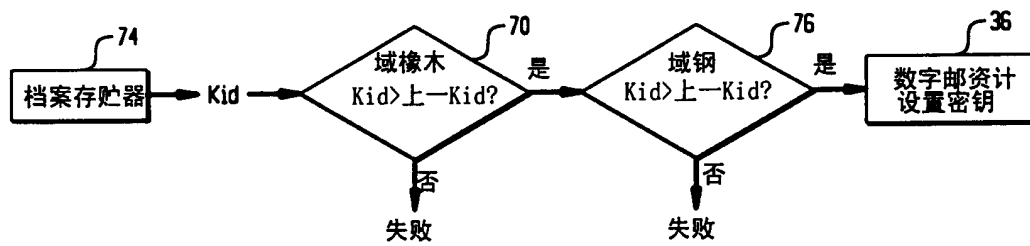


图 19

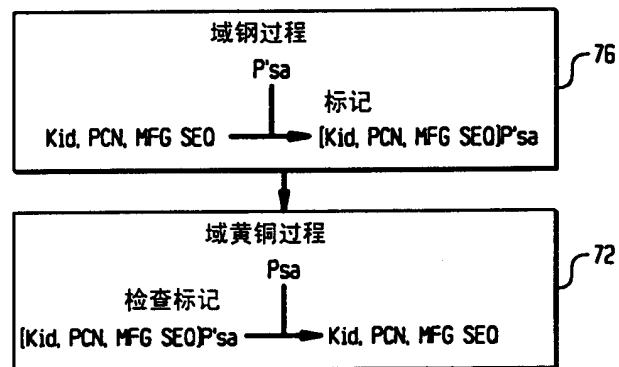


图 20

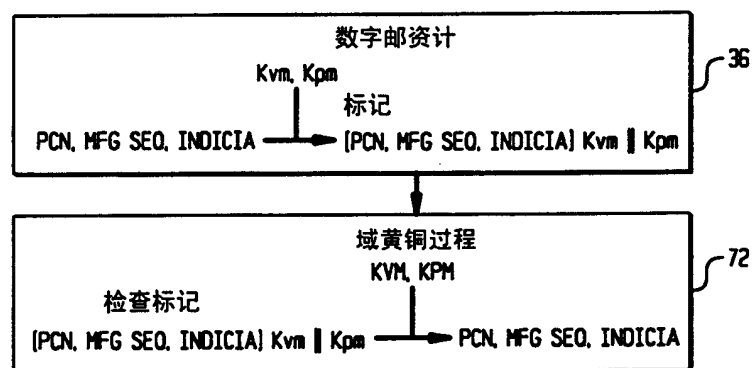


图 21

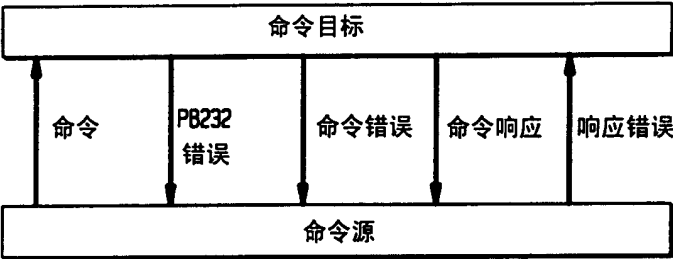


图 22

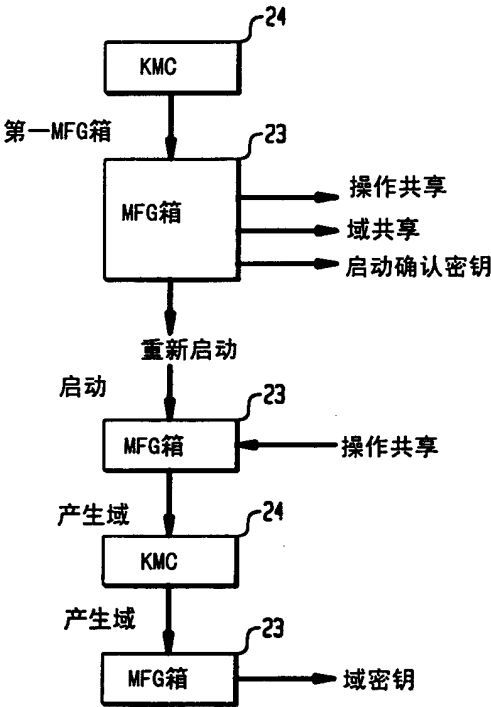


图 23

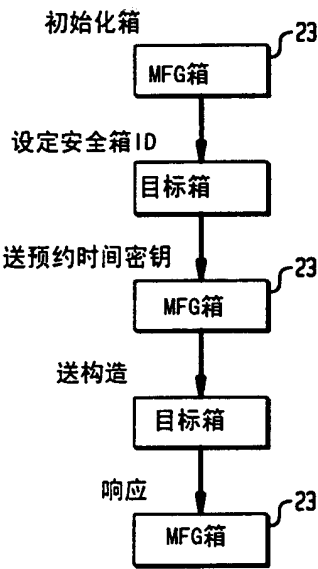


图 24

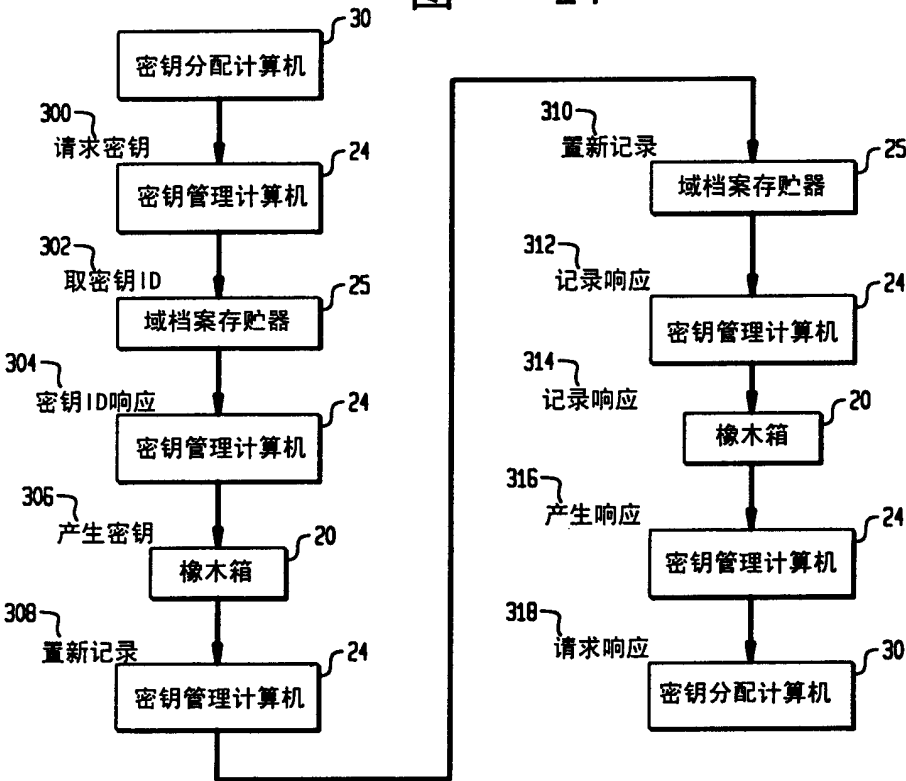


图 25

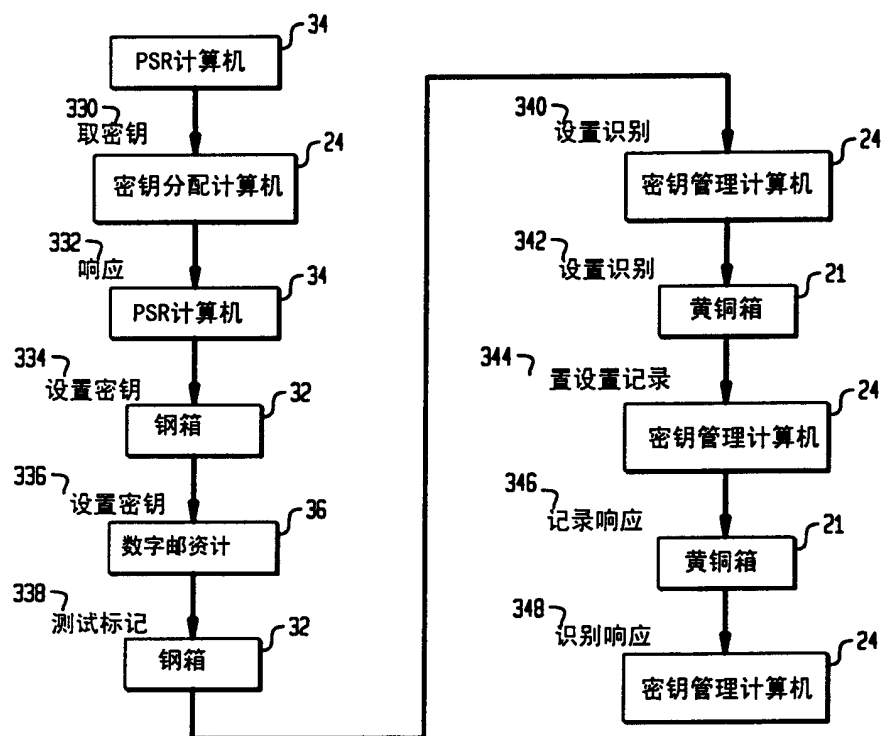
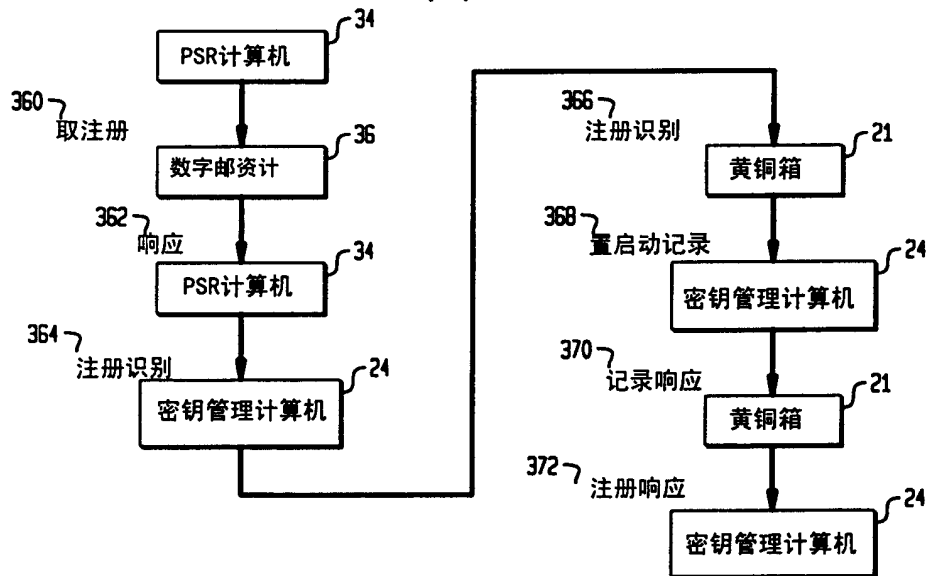


图 26



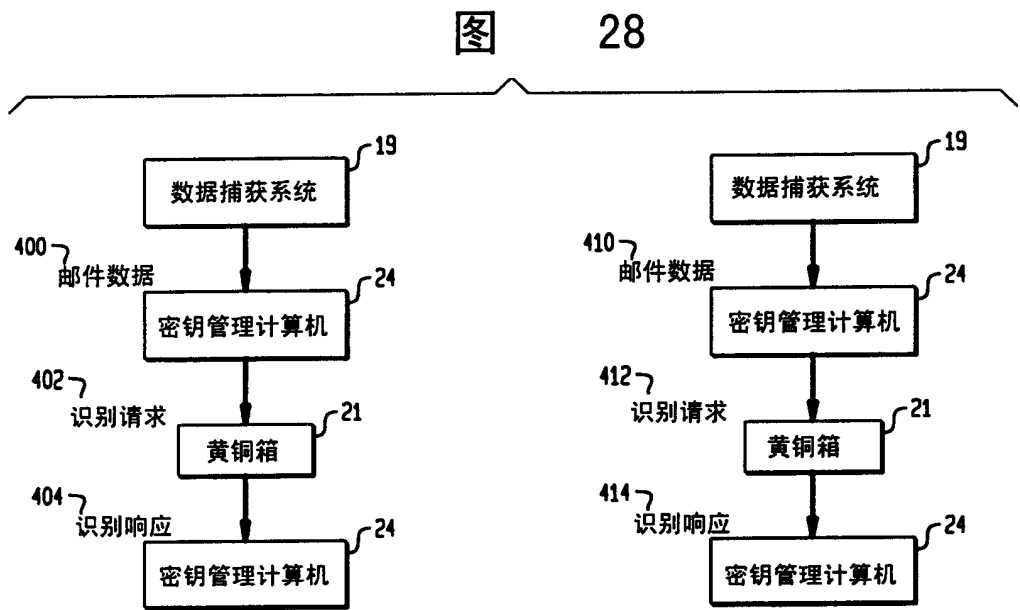
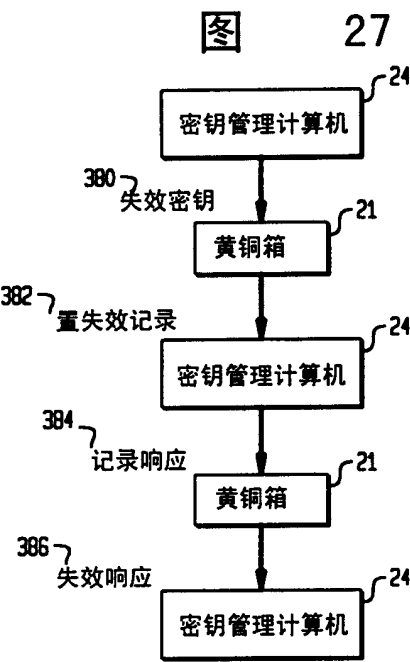


图 29

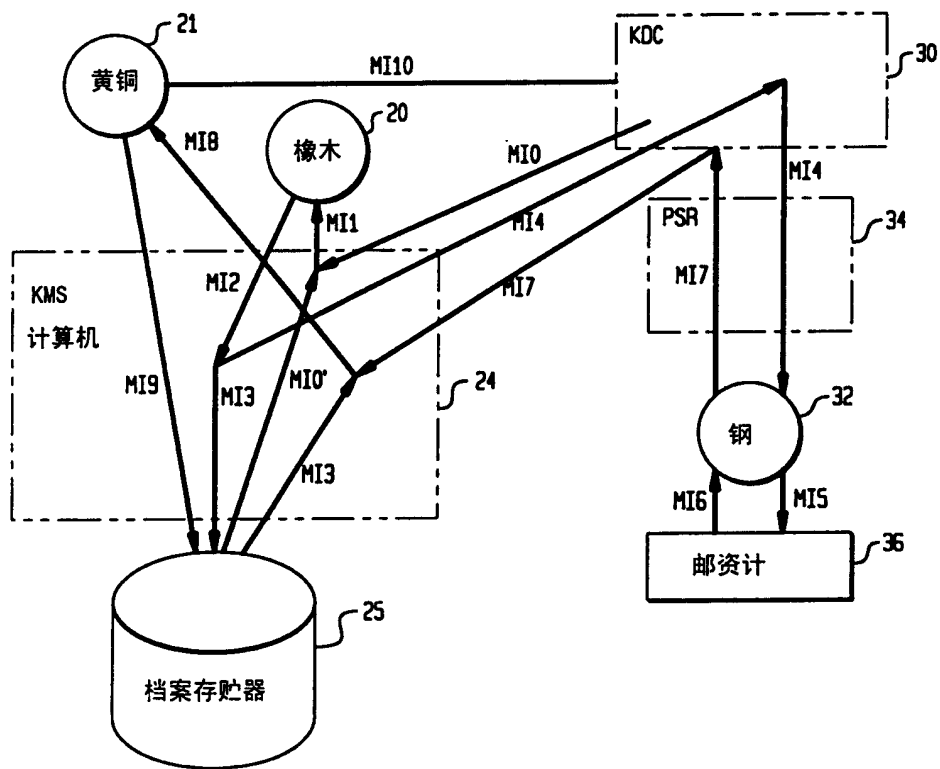


图 32

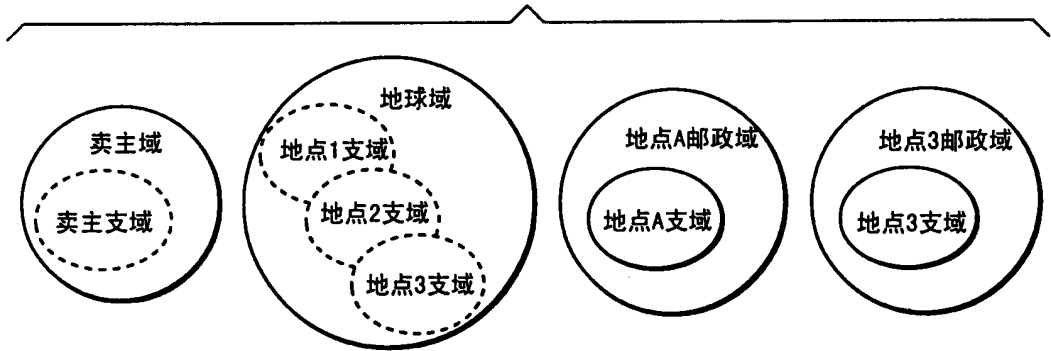


图 30

密钥设置信息		
信息	目的	内容
MI0	请求密钥	KDC→KMC: 域, S _{ID}
MI0'	新密钥产生	→KMC: 密钥 _{ID}
MI1	请求密钥	KMC→O: 域, S _{ID} , 密钥 _{ID}
MI2	新密钥产生	MI3, MI4具有相同密钥, 密钥 _{ID}
MI3	存档黄铜的新密钥	O→B: {新, O _{ID} , 域, S _{ID} , 密钥 _{ID} KIP _S p' _O }
MI4	要设置的新密钥	O→S: {新, O _{ID} , 域, S _{ID} , 密钥 _{ID} KIP _S , {测试数据K} p' _O }
MI5	设置密钥	S→邮资计: K
MI6	设置的密钥的表示	邮资计→S: MSN, {测试数据} K
MI7	密钥设置	S→B: {装入, O _{ID} , 域, S _{ID} , 密钥 _{ID} MSN, {测试数据} K} p' _S }
MI8	确认密钥设置请求	KMS→B: MI3, MI7 肯有相同的密钥 _{ID}
MI9	存档密钥的设置	B→档案存贮器{装入, O _{ID} , 域 S _{ID} , 密钥 _{ID} MSN, KIP _B } p' _B }
MI10	确认密钥 设置到MFG	B→KDC: {装入, 密钥 _{ID} MSN} p' _B .

设置信息

注解:

(密钥)P: 用公众密钥P加密该密钥

(M) p' : 利用个人密钥P' 标记信息M

P / p' : 一公众/个人密钥对用于保密

P / p' : 一公众/个人密钥对用于确认

S: 一保密密钥用于保密

s: 一保密密钥用于确认

S_{ID} : 钢箱的识别号

O: 橡木

B: 黄铜

K: 邮资计密钥

密钥ID: 唯一指定给密钥K的一号

测试数据: 用于识别密钥已正确设置到邮资计中的一预定的数据集

图 31

密钥登记信息

信息	目的	内容
MR1	密钥注册报告	邮资计→B 地点 : [MSN, 签条号, 地点, 日期]密钥
MR2	注册请求	KMS→B 地点 : MR1, MI9, 具有同样的MSN
MR3	档案存储器密钥注册	B 地点 → 档案存储器: [注册, 域, MSN, 签条号, 地点, (密钥) s_B] s'_B
MR4	确认注册	B 地点 → KMS 地点 [注册, 域, MSN, 签条号, 地点] s'_B