[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 11/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580020427.7

[43] 公开日 2007 年 7 月 25 日

[11] 公开号 CN 101006428A

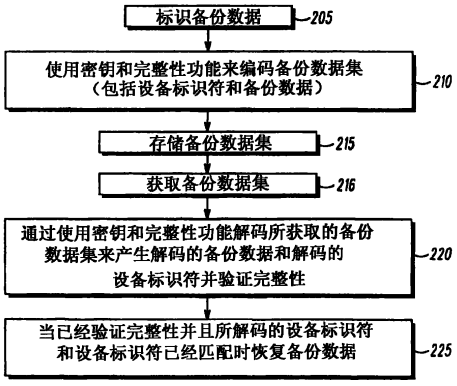
[22] 申请日 2005.6.9
[21] 申请号 200580020427.7
[30] 优先权
[32] 2004. 6.21 [33] US [31] 10/872,723
[86] 国际申请 PCT/US2005/020199 2005.6.9
[87] 国际公布 WO2006/007329 英 2006.1.19
[85] 进入国家阶段日期 2006.12.20
[71] 申请人 摩托罗拉公司
地址 美国伊利诺伊州
[72] 发明人 李宜勤 伊扎特·A·戴彼士
迪安·H·沃格勒
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 张焕生 谢丽娜
权利要求书 3 页 说明书 10 页 附图 7 页

[54] 发明名称

安全数据备份和恢复

[57] 摘要

一种用于对电子设备(100)提供安全数据备份和恢复的技术，该电子设备具有唯一且不可改变的设备标识符(115)。 该技术的方法包括标识(205)待备份的备份数据(405，805，1205)，通过使用密钥(110)和完整性功能编码设备标识符(115)和备份数据(405，805，1205)来编码(210)备份数据集以用于完整性和身份认证，通过使用所述密钥(115)和完整性功能解码所获取的备份数据集(605，1005，1405)来产生(220)解码的备份数据(635，1015，1435)和解码的设备标识符(640，1020，1440)，并且仅当已经验证了完整性并且所述解码的设备标识符与所述设备标识符匹配时才利用所述解码的备份数据恢复(225)所述备份数据。 描述了用于编码和解码的三种方法。



1. 一种用于电子设备的安全数据备份和恢复的方法，所述电子设备具有唯一且不可改变的设备标识符，所述方法包括：

标识备份数据；

使用密钥和完整性功能来编码包括所述备份数据和所述设备标识符的备份数据集以用于完整性和身份认证；

通过使用所述密钥和所述完整性功能来解码所获取的备份数据集，从而产生解码的备份数据和解码的设备标识符并且验证完整性；

通过把所述解码的设备标识符与所述设备标识符相匹配来验证身份；并且

仅当已经验证所述完整性和身份时才利用所述解码的备份数据来恢复所述备份数据。

2. 如权利要求 1 所述的方法，其中所述完整性功能在所述备份数据和所述设备标识符上使用散列功能。

3. 如权利要求 1 所述的方法，其中所述密钥是对称密钥和公钥/私钥对中的一种。

4. 如权利要求 1 所述的方法，其中所述密钥是对称密钥并且其中所述编码包括：

使用所述密钥和含密钥散列功能来产生所述备份数据和所述设备标识符的含密钥散列；并且

根据所述备份数据、所述设备标识符和所述含密钥散列来形成所述备份数据集。

5. 如权利要求 1 所述的方法，其中所述密钥是对称密钥并且其中所述编码包括：

使用散列功能来产生所述备份数据和所述设备标识符的散列；并

且

通过使用加密/解密功能和所述密钥来加密所述备份数据、所述设备标识符和所述散列来形成所述备份数据集以用于保密性。

6. 如权利要求 1 所述的方法，其中所述密钥是公钥和私钥对并且其中所述编码包括：

使用数字签名产生功能和所述私钥来产生所述备份数据和所述设备标识符的数字签名；并且

根据所述备份数据、所述设备标识符和所述数字签名来形成所述备份数据集。

7. 如权利要求 1 所述的方法，其中在可信备份功能的控制之下完成所述备份数据的所述标识，所述可信备份功能把所述备份数据限制成来自定义的数据集。

8. 如权利要求 1 所述的方法，还包括存储合获取所编码的备份数据集。

9. 如权利要求 1 所述的方法，其中在可信备份功能的控制之下进行所述编码、解码和恢复。

10. 一种用于安全数据备份和恢复的设备，包括：

存储器，用于应用程序和用户数据中的至少一个；

可信备份和恢复功能，用于标识所述存储器中的备份数据以用于安全备份，所述备份数据是定义的授权备份数据集中的成员；

密钥功能，用于提供密钥；以及

唯一且不可改变的设备标识符，

其中，所述可信备份和恢复功能执行以下步骤：

使用所述密钥和完整性功能来编码包括所述设备标识符和所述备份数据的备份数据集以用于完整性和身份认证；

通过使用所述密钥和所述完整性功能解码所获取的备份数据集来产生解码的备份数据和解码的设备标识符并且验证完整性；

通过把所述解码的设备标识符与所述设备标识符相匹配来验证身份；并且

仅当已经验证所述完整性和身份时才利用所述解码的备份数据来恢复所述备份数据。

安全数据备份和恢复

技术领域

本发明总体上涉及数据存储方法技术领域并且尤其涉及安全数据备份领域。

背景技术

随着电子设备变得更加复杂，它们更可能根据程序指令来操作，这些程序指令被下载并驻留在诸如随机存取存储器或盘片驱动存储器之类的读/写存储器中。由这类设备的用户所获取或产生的信息也可以保持在这种存储器中。蜂窝式电话是这类电子设备的一个例子。可以下载游戏及其它应用程序。读/写存储器设备难免发生故障，因此用户可能希望能够备份在这种设备中所存储的信息。

在下载的游戏和应用的情况下，通常情况下，提供所述软件的实体许可该软件只能在下载它的设备中使用，并因此可能更愿意确保该软件只是在已经获得许可的设备上被复制并只用于备份的目的。这是数字版权问题。用户可能还想安全地备份该用户已经产生的备份信息，使得它只能被恢复到产生该信息的用户设备。例如，备份服务可以由用户并不绝对可信第三方来提供。因而需要一种安全备份技术，使得只允许在执行备份的设备中进行恢复。用户可能还关心其备份数据的保密性。例如，用户可能想加密信用卡信息或病历（为了保密性）。此外，用户可能只信任驻留有数据并且从中进行备份的设备，并且可能想要确保所述数据只能在用户创建该备份的设备中恢复。

附图说明

结合附图以举例方式而非限制性方式来说明本发明，其中相同的附图标记表示同样的要素，并且其中：

参照图 1，依照本发明一些实施例，功能框图示出了电子设备和备份存储器的一部分；

参照图 2，依照本发明一些实施例示出了用于安全数据备份与恢复的方法流程图；

参照图 3、4、5 和 6，依照第一类的本发明实施例示出了用于编码并解码备份数据集的方法流程图和数据流图；和

参照图 7、8、9 和 10，依照第二类的本发明实施例示出了用于编码并解码备份数据集的方法流程图和数据流图；和

参照图 11、12、13 和 14，依照第三类的本发明实施例示出了用于编码并解码备份数据集的方法流程图和数据流图。

本领域技术人员应当理解：为简单和清楚起见，图中的所示元件不必按比例绘制。例如，可以相对于其它元件来放大图中某些元件的尺寸以便帮助理解本发明的实施例。

具体实施方式

在详细描述依照本发明的特定安全数据备份和恢复技术之前，应当提及本发明主要在于有关数据备份与恢复的方法步骤和设备组件的组合。因此，在附图中用常规符号表示了设备组件和方法步骤，只示出了那些与理解本发明有关的具体细节，以避免对那些受本发明启示的本领域普通技术人员来说显而易见的细节模糊了本公开内容。

参照图 1，依照本发明一些实施例，功能框图示出了电子设备 100 和备份存储器 180 的部分。电子设备 100 包括被耦合到可信备份和恢复功能 125 的读/写存储器 120，所述可信备份和恢复功能 125 可以编码读/写存储器 120 中已经被标识为备份数据的部分数据，并且发送所编码的备份数据以存储在备份存储器 180 中，所述备份存储器 180 也可以是读/写存储器。读/写存储器 120 和备份存储器 180 中的每个都是逻辑存储器组，其可以是许多类型物理存储器的一部分或一种或多种，诸如集成电路、硬盘、软盘、存储卡、记忆棒等。

在某些实施例中，电子设备 100 是诸如电话手机之类的无线通信设备，并且备份存储器 180 位于通过无线链路 170 访问的另一电子设备中，响应于所可信备份和恢复功能 125 发送所编码的数据来建立所述无线链路 170。在其它实施例中，电子设备 100 可以是无线电话听筒或许多其它类型的电子设备之一（诸如台式计算机、游戏机、电视机机顶盒等），并且备份存储器 180 被临时地或持久地耦合到所述电子设备 100。例如，备份存储器 180 可以是插入电子设备 100 中的记忆棒或外部硬盘驱动器。在这些情况下，链路 170 可以是有线链路。还应当理解，电子设备 100 可以是在被适当地供电并耦合到输入/输出电路和功能时能够执行这里所描述功能的任何电子设备或集成电路或类似的设备。

可信备份和恢复功能 125 被耦合到数据备份用户接口功能 105，用以向用户提供用来选择要备份的一些数据并且确定备份所选择数据的时间和地点的装置。在本发明的一些应用中，可以允许用户在读/写存储器 120 中所存储的数据中选择哪些数据作为备份数据。例如，这种备份数据可以包括用户已经产生或获取的任何数据，可以包括用户已经购买的软件应用程序。因为本发明的独特设计确保了尽管备份数据可以被任何电子设备接收并存储，然而它只可用在备份它的电子设备 100 上，所以备份这种数据变得实际可行。这对购买用于使用软件应用程序的权利并且希望在读/写存储器 120 中的应用程序或配置数据受到破坏的情况下能够恢复所述应用程序和相关配置数据的用户来说是非常有用的。然而在本发明的其它应用中，可以预定义备份数据，使得用户不能控制数据选择。例如，可信备份和恢复功能 125 可以备份读/写存储器 120 中的整个数据图像，其可以包括与电子设备 100 的操作系统功能相关的数据。

为了实现本发明的这些独特方面，电子设备 100 具有唯一且不可改变的标识符（ID）115 和密钥 110，它们被耦合到可信备份和恢复功

能 125。按照其数据（诸如软件程序）正被备份的实体充分确保可信备份和恢复功能 125 的必要功能实质上不可改变的方式来把所述可信备份和恢复功能 125 结合到电子设备 100 中。“实质上不可改变”指的是执行改变的任务是不可实施的——例如，所述功能可以由存在于只读存储器中的程序代码来执行，其中在与用于执行所述代码的处理器相同的集成电路（IC）内实现所述只读存储器。

唯一且不可改变的 ID 115 的特性由其名称来描述：唯一且不可改变的 ID 115 对电子设备 100 来说应当实质上是唯一的（在所有电子设备的集合内也可以使用备份的数据），并且应当实质上是不可改变的。“实质上是唯一的”只是意味着存在能够接收备份数据集的、具有相同的唯一且不可改变的 ID 115 的另一电子设备的可能性适当地小。这可以借助本领域中的已知技术来实现，诸如大随机数或分配的数或其一些组合。因此唯一且不可改变的 ID 115 的长度和复杂性与可以对备份数据集中的数据进行操作或使用的电子设备的数目相关。ID 的“实质上不可改变”可以是存储在只读、激光器修正的集成电路 ID 中的 ID。作为替换，所述 ID 例如可以存储在一次性可编程存储器或在相同 IC 内实现的电子可编程熔断器（fuse）中，所述 IC 具有用于执行可信备份和恢复功能 125 的各功能的处理器和随机存取存储器。唯一且不可改变的 ID 115 可以不需要保密；在某些实施例中，可能希望所述唯一且不可改变的 ID 115 是可显示的。

密钥 110 是在产生编码的备份数据集期间和在根据所编码的备份数据集恢复备份数据期间在电子设备 100 中所使用的数据集。密钥 110 可以是对称密钥或公钥和私钥对。在基于公钥/私钥的系统中，私钥必须是秘密的，而公钥不必是秘密的。对称密钥必须是秘密的。“秘密”可能意味着密钥不可以让用户知道。除了授权实体之外的所有实体都不可读取对称密钥。优选地是，可信备份和恢复功能 125 是授权实体。密钥 110 的长度和复杂性与电子设备 100 的实施例中所使用的保密类型和希望密码分析所受到的阻力相关。

参照图 2，依照本发明一些实施例示出了用于安全数据备份和恢复的方法流程图。在步骤 205，标识待备份的数据。如上所述参考图 1，按照可信备份和恢复功能 125 的限制，利用来自用户的输入来进行这种标识。作为替换，例如可以是那些满足可信备份和恢复功能 125 中所存储的要求的所有数据的自动备份，或者可以借助由电子设备 100 所接收的消息来提示（任何数据选择可能必须被可信备份和恢复功能 125 授权）。在步骤 210，使用密钥 110 和完整性功能来编码备份数据和唯一且不可改变的 ID 115（以下称作设备 ID 115）以用于完整性和身份认证，从而产生备份数据集。此步骤由可信备份和恢复功能 125 的信任备份功能来执行，所述功能包括完整性功能。在这里“完整性”是指可以确保在由电子设备 100 所接收的备份数据集中备份数据和设备 ID 没有被修改。在这里“身份认证”是指只有具有用于产生备份数据集的设备 ID 115 的电子设备 100 可以使用所接收的备份数据集来恢复备份数据。

在步骤 215，备份数据集被电子设备 110 存储在备份存储器 180 中，如上面参考图 1 所述，备份存储器 180 可以是各种类型存储器之一并且可以位于本地或远程。这种存储由可信备份和恢复功能 125 启动并且可以由电子设备 100 之内或之外的其它功能（例如消息格式器、频率发射器和接收器等）来完成。在步骤 216，所获取的备份数据集被提交给可信备份和恢复功能 125，所述可信备份和恢复功能 125 通过在步骤 220 使用其完整性功能和密钥 110 解码所获取的备份数据集来产生所解码的备份数据和解码的设备标识符以及完整性值。在步骤 225，只有当在步骤 220 已经验证备份数据集的完整性并且所解码的设备标识符和设备 ID 115 匹配时，才使用所解码的备份数据来恢复备份数据。

参照图 3 和 4，依照第一类型的本发明实施例示出了用于编码 210 备份数据集的方法流程图和数据流程图。在步骤 305（图 3），使用密钥 110 和含密钥（keyed）散列功能 415 来产生设备 ID 115 和备份数据

405 的含密钥散列 420（图 4）。意思是对包括备份数据 405 和设备 ID 115 的数据集执行含密钥散列功能。可以由诸如 HMAC（基于散列的消息认证代码）之类的公知方法使用诸如 SHA -1（安全散列算法——版本 1）之类的公知散列功能来产生含密钥散列 420。在步骤 310（图 3），所编码的备份数据集 410 由备份数据 405、设备 ID 115 和含密钥散列 420 组成。

参照图 5 和 6，依照第一类型的本发明的实施例示出了用于解码 220 所获取的备份数据集的方法流程图和数据流程图。在步骤 505（图 5），分别把在所获取备份数据集 605 中的备份数据 610（图 6）、设备标识符 615 和含密钥散列 620 标识成解码的备份数据 635、解码的设备标识符 640 和解码的含密钥散列 625。只有当在存储 215 和获取 216 步骤期间编码的备份数据集 410 中没有出现数据错误并且没有对其进行有意的数据改变时，各自解码的数据集 635、640、625 才与用于形成所存储的编码备份数据集 410 的数据集 405、115、420（图 4）相同。在步骤 510（图 5）使用与在步骤 305 所使用的相同含密钥散列功能 415 来编码所解码的备份数据 635 和解码的设备 ID 640，这涉及使用密钥 110，从而产生验证含密钥散列 630。当在步骤 515 验证含密钥散列 630 使用比较功能 655 匹配所解码的含密钥散列 625 时，建立数据完整性；否则完整性失败。当完整性已经失败时，来自所获取备份数据集 605 的备份数据 610 无法用于恢复原始的备份数据 405。在第一类型的这些实施例中，完整性功能包括含密钥散列功能 415 和所解码 625 与验证 630 含密钥散列的匹配 515。密钥 110 是对称密钥。

如上面参考图 2 所述，在步骤 225 使用比较功能 650 把根据所获取备份数据集 605 恢复的解码设备 ID 640 与设备 ID 115 相比较，并且当它们相匹配并且已经建立完整性时，可以使用根据所获取备份数据集 605 解码的备份数据 635 来恢复原始的备份数据 405。参考步骤 510 和 515 可以依照任何次序来完成在步骤 225 的设备 ID 匹配。

参照图 7 和 8，依照第二类型的本发明实施例示出了用于编码 210 备份数据集的方法流程图和数据流程图。在步骤 705（图 7），使用散列功能 815 来产生设备 ID 115 和备份数据 805 的（不含密钥的）散列 820（图 8）。这是指对包括备份数据 805 和设备 ID 115 的数据集执行散列功能。可以由诸如 SHA-1（安全散列算法——版本 1）之类的公知方法来产生散列 820。在步骤 710，通过使用密钥 110 和加密功能 825 来加密备份数据 805、设备 ID 115 和散列 820 来形成编码的备份数据集 830 以用于保密性。

参照图 9 和 10，依照第二类型的本发明的实施例示出了用于解码 220 所获取的备份数据集的方法流程图和数据流程图。在步骤 905（图 9）使用密钥 110 来执行与加密功能 825（图 8）互逆的解密功能 1010（图 10），所述加密功能 825 用于在步骤 710 加密备份数据 805、设备 ID 115 和散列 820。这产生所解码的备份数据 1015、解码的设备 ID 1020 和解码的散列 1025。仅当在存储 215 和获取 216 步骤期间所编码的备份数据集 830 中没有出现数据错误并且没有对其进行有意的数据改变时，这些各自解码的数据集 1015、1020、1025 才与用于形成所存储的编码备份数据集 830 的数据集 805、115、820 相同。在步骤 910，对包括所解码的备份数据 1015 和解码的设备 ID 1020 的数据集使用在步骤 705 所使用的相同散列功能 815，从而产生验证散列 1030。当在步骤 915 验证散列 1030 使用比较功能 1055 匹配所解码的散列 1025 时，建立数据完整性；否则完整性失败。当完整性已经失败时，根据所获取备份数据集 1005 所解码的备份数据 1015 无法用于恢复原始的备份数据 805。在第二类型的这些实施例中，完整性功能包括加密/解密功能 825、1010、散列功能 815 和所解码 1025 与验证 1030 散列的匹配 915。密钥 110 是对称密钥。

如上面参考图 2 所述，在步骤 225 使用比较功能 1050 把从所获取备份数据集 1005 所恢复的解码设备 ID 1020 与设备 ID 115 相比较，并且当它们相匹配并且已经建立完整性时，可以使用根据所获取备份数

据集 1005 解码的备份数据 1015 来恢复原始的备份数据 805。参考步骤 910 和 915 可以依照任何次序来完成在步骤 225 的设备 ID 匹配。

参照图 11 和 12，依照第三类型的本发明实施例示出了用于编码 210 备份数据集的方法流程图和数据流程图。在步骤 1105（图 11），使用数字签名产生和验证功能 1215 和密钥 110 的私钥部分来产生备份数据 1205 和设备 ID 115 的数字签名 1220（图 12），所述密钥 110 包括公钥和私钥。这是指对包括备份数据 1205 和设备 ID 115 的数据集执行数字签名产生和验证功能 1215 的数字签名产生功能。可以由诸如 RSA（Rivest - Shamir - Adleman 算法）之类的公知方法来产生数字签名 1220。在步骤 1110，所编码的备份数据集 1230 由备份数据 1205、设备 ID 115 和数字签名 1220 组成。

参照图 13 和 14，依照第三类型的本发明的实施例示出了用于解码 220 所获取的备份数据集的方法流程图和数据流程图。在步骤 1305（图 13），分别把所获取备份数据集 1405 中的备份数据 1410、设备标识符 1415 和数字签名 1420 标识成解码的备份数据 1435、解码的设备标识符 1440 和解码的数字签名 1425。仅当在存储 215 和获取 216 步骤期间所编码的备份数据集 1230 中没有出现数据错误并且没有对其进行有意的数据改变时，这些各自解码的数据集 1435、1440、1425 才与用于形成所存储的编码备份数据集 1230 的数据集 1205、115、1220（图 12）相同。在步骤 1310 由数字签名产生和验证功能 1215 的数字签名验证功能使用所解码的备份数据 1435、解码的设备 ID 1440 和密钥 110 的公钥部分来验证所解码的数字签名 1425。当所解码的数字签名 1425 的验证结果 1445 正确时，建立数据的完整性；否则完整性失败。当完整性已经失败时，根据所获取备份数据集 1405 所解码的备份数据 1435 无法用于恢复原始的备份数据 1205。在第三类型的这些实施例中，完整性功能包括数字签名产生和验证功能 1215。密钥 110 是公钥和私钥对。

如上面参考图 2 所述，在步骤 225 使用比较功能 1450 把根据所获取备份数据集 1405 恢复的解码设备 ID 1440 与设备 ID 115 相比较，并且当它们相匹配并且已经建立完整性时，可以使用根据所获取备份数据集 1405 所解码的备份数据 1435 来恢复原始的备份数据 1205。参考步骤 1310 可以依照任何次序来完成在步骤 225 的设备 ID 匹配。

应当理解，这里所描述的安全数据备份和恢复可以由一个或多个常规的处理器和唯一的存储程序指令组成，所述程序指令用于控制所述一个或多个处理器实现这里所描述的一些、大部分或所有安全数据备份和恢复功能；这样，这些功能可以被解释为用于执行安全数据备份和恢复的方法步骤。作为替换，一些或所有这些功能可以由无存储程序指令的状态机来实现，其中每个功能或某些功能的一些组合被实现成定制逻辑。当然，可以使用两种方法的组合。因此，这里描述了用于这些或这些中一些功能的方法和装置。在上述说明书中，已经参考具体实施例描述了本发明及其益处和优点。然而，一个本领域内普通技术人员应当理解在不脱离权利要求书所阐明的本发明范围的情况下，可以进行各种修改和变化。据此，应当认为说明书和附图是示例性的而非限制性的，并且所有这种修改应该包括在本发明的范围内。然而，可能导致任何益处、优点或解决方案出现或使其变得更加显著的益处、优点、问题的解决方案和任何元件（一个或多个）不应当被理解为任何或所有权利要求的关键性、必需的或基本特征或要素。

如这里所用，术语“包括”、“包含”或其任何其它变化意在覆盖非排他性的包括，使得包括一列要素的过程、方法、物品或设备并不只包括那些要素，而且还可以包括没有显式列出的其它要素或为这种过程、方法、物品或设备所固有的要素。

如这里所用的“集（集合）”意指非空集（即，对于这里所定义的集合来说，包括至少一个成员）。如这里所用，术语“另一个”被定义为至少是第二个或更多。如这里所使用的，数据“包括”和/或“具

有”被定义为包括。如这里所使用的，参考电光技术的术语“耦合”被定义为连接，不过不一定是直接连接，也不必是机械连接。如这里所使用的，术语“程序”被定义成被设计用来在计算机系统上执行的指令序列。“程序”或“计算机程序”可以包括子例程、函数、过程、对象方法、目的实现方式、可执行应用程序、小应用程序、小服务程序、源代码、目标代码、共享库/动态加载库和/或被设计成用来在计算机系统上执行的其它指令序列。应当进一步理解，相关术语的使用（如果存在的话），诸如第一和第二、顶和底等，仅仅用于把一个实体或动作与另一实体或动作相区分，而不必要求或意指在这种实体或动作之间的任何实际这种关系或次序。

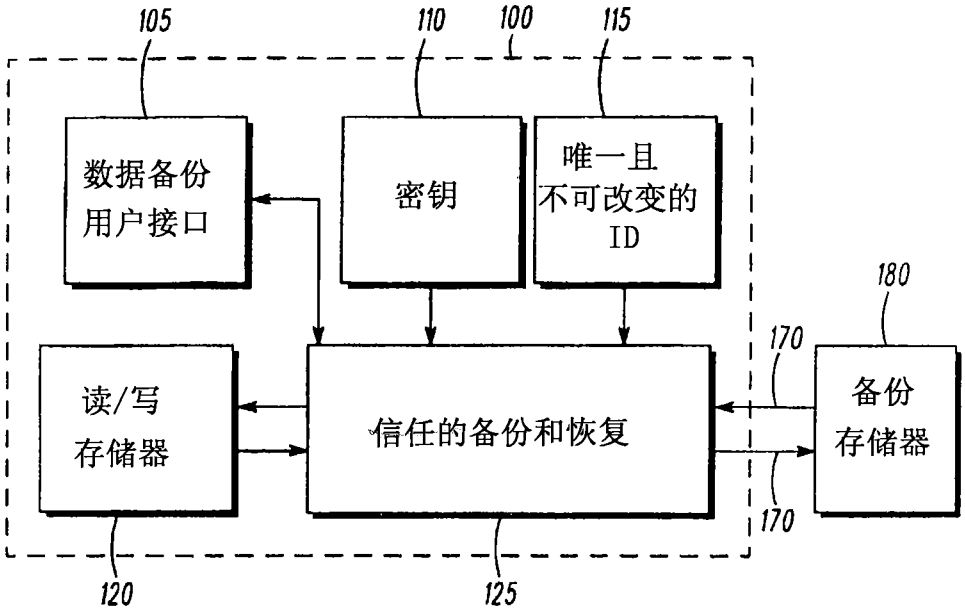

105
110
100
115
数据备份
用户接口
密钥
唯一且
不可改变的
ID
180
170
读/写
存储器
信任的备份和恢复
备份
存储器
170
120
125

图1

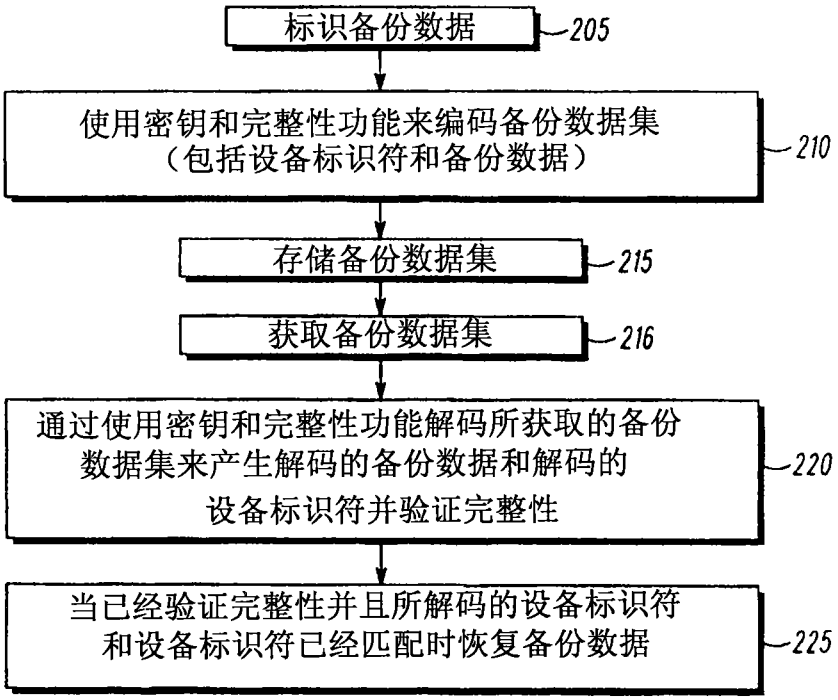

标识备份数据
205
使用密钥和完整性功能来编码备份数据集
（包括设备标识符和备份数据）
210
存储备份数据集
215
获取备份数据集
216
通过使用密钥和完整性功能解码所获取的备份
数据集来产生解码的备份数据和解码的
设备标识符并验证完整性
220
当已经验证完整性并且所解码的设备标识符
和设备标识符已经匹配时恢复备份数据
225

图2

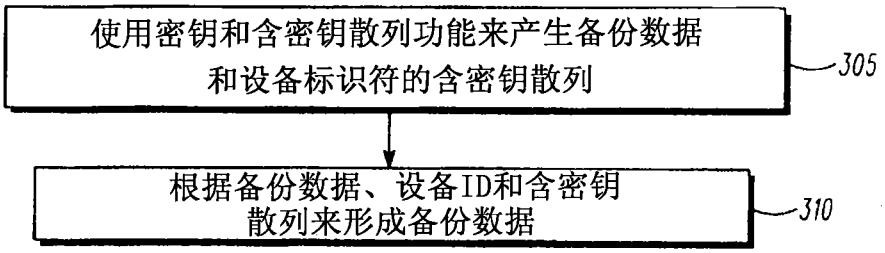

使用密钥和含密钥散列功能来产生备份数据
和设备标识符的含密钥散列
305
根据备份数据、设备ID和含密钥
散列来形成备份数据
310

图3

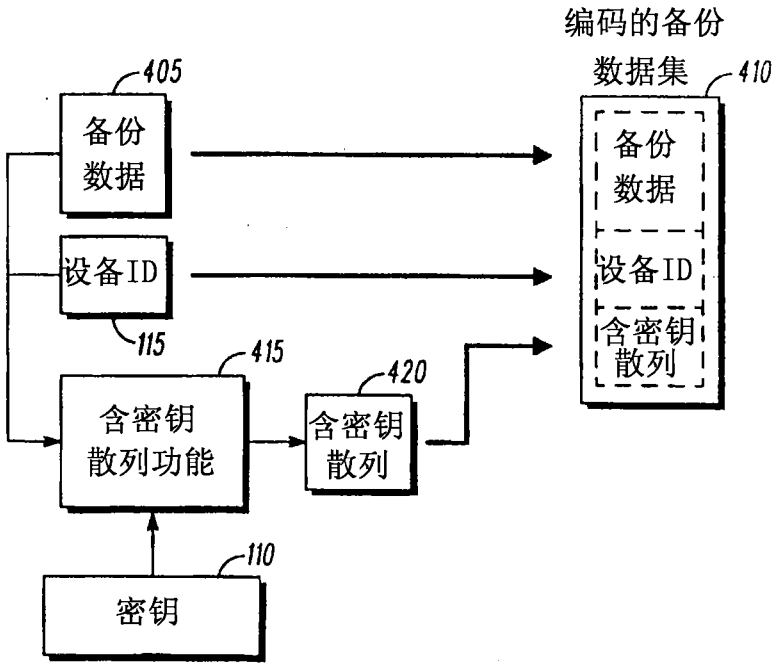

编码的备份
数据集
410
405
备份
数据
设备ID
115
415
420
含密钥
散列功能
含密钥
散列
备份
数据
设备ID
含密钥
散列
110
密钥

图4

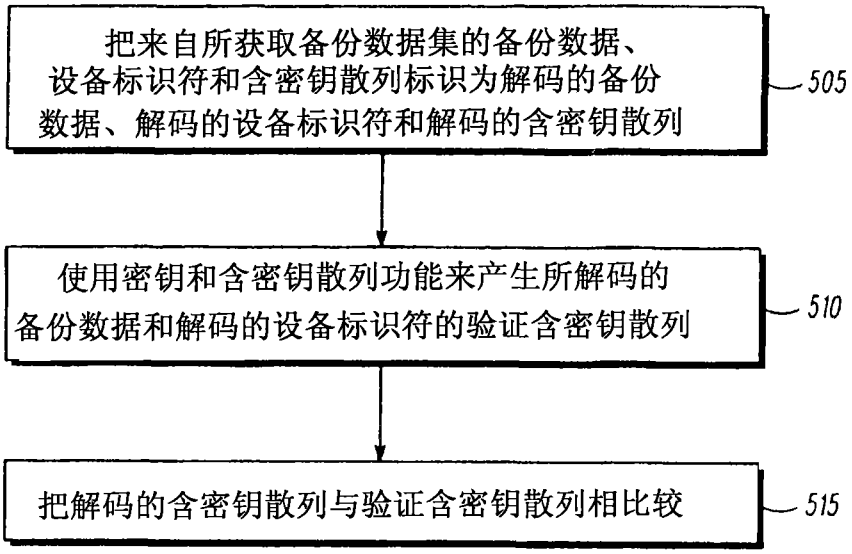

把来自所获取备份数据集的备份数据、设备标识符和含密钥散列标识为解码的备份数据、解码的设备标识符和解码的含密钥散列
505
使用密钥和含密钥散列功能来产生所解码的备份数据和解码的设备标识符的验证含密钥散列
510
把解码的含密钥散列与验证含密钥散列相比较
515

图5

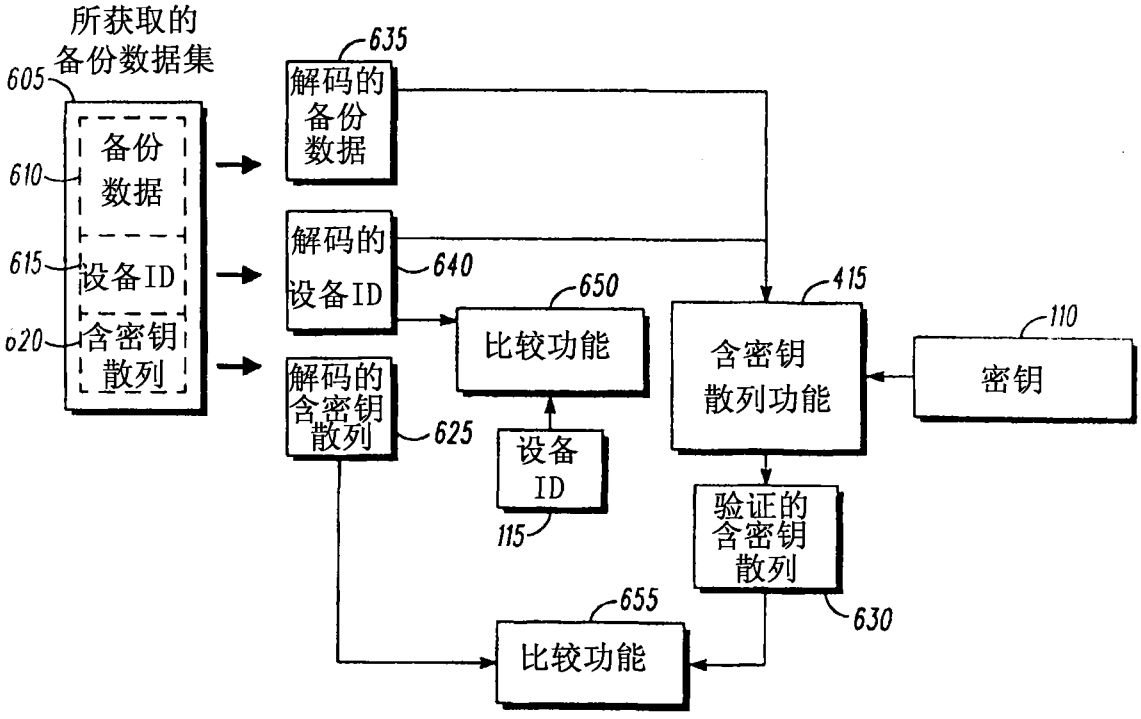

所获取的备份数据集
605
备份数据
610
设备ID
615
含密钥散列
620
635
解码的备份数据
解码的设备ID
640
解码的含密钥散列
625
650
比较功能
设备ID
115
415
含密钥散列功能
110
密钥
验证的含密钥散列
630
655
比较功能

图6

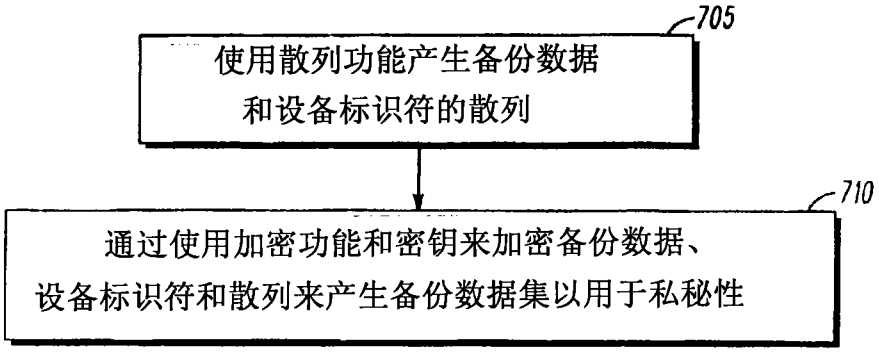

705
使用散列功能产生备份数据
和设备标识符的散列
710
通过使用加密功能和密钥来加密备份数据、
设备标识符和散列来产生备份数据集以用于私秘性

图7

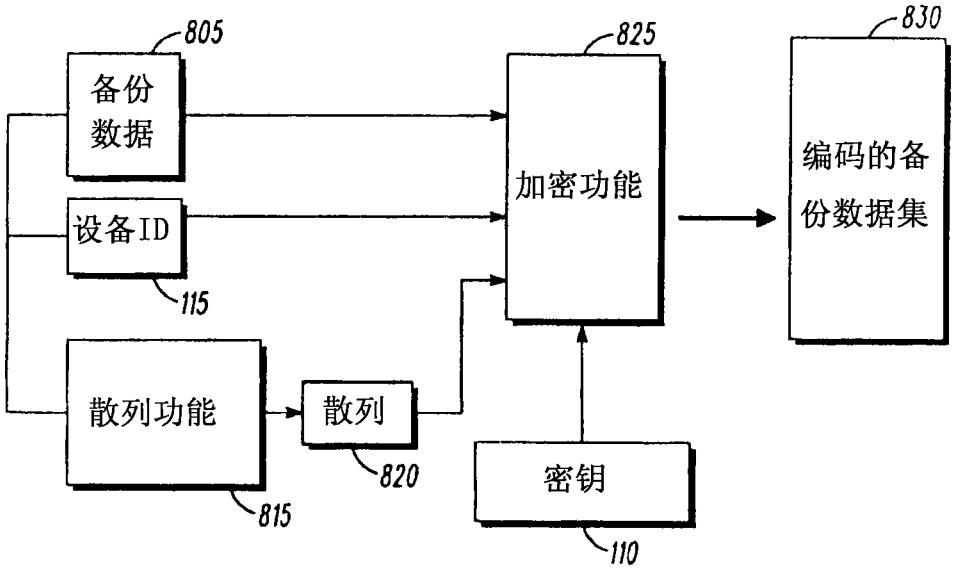

805
备份
数据
设备ID
115
散列功能
815
散列
820
825
加密功能
密钥
110
830
编码的备
份数据集

图8

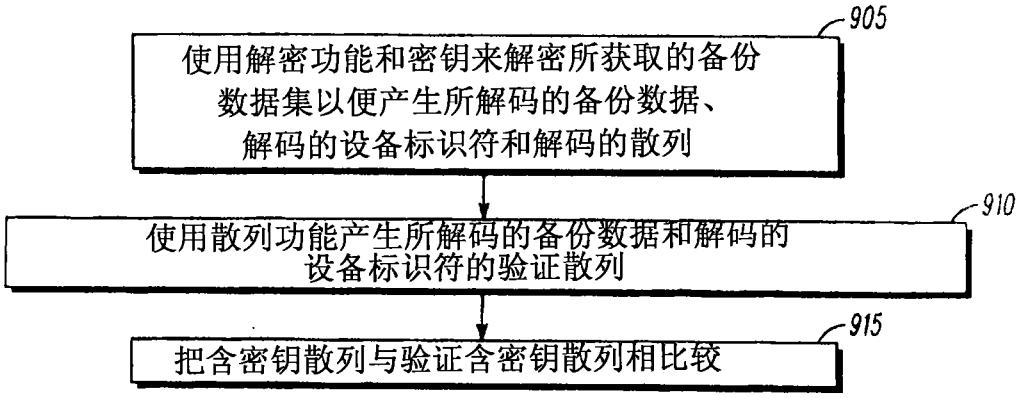

905
使用解密功能和密钥来解密所获取的备份
数据集以便产生所解码的备份数据、
解码的设备标识符和解码的散列
910
使用散列功能产生所解码的备份数据和解码的
设备标识符的验证散列
915
把含密钥散列与验证含密钥散列相比较

图9

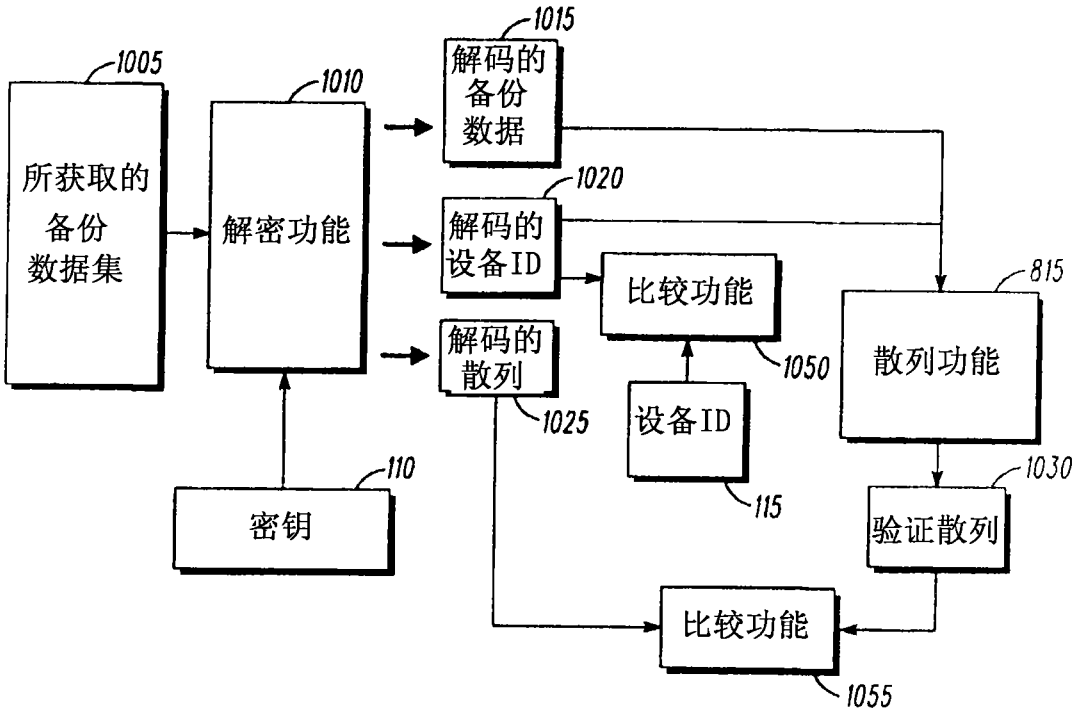

1005
所获取的
备份
数据集
1010
解密功能
1015
解码的
备份
数据
1020
解码的
设备ID
解码的
散列
1025
比较功能
1050
设备ID
115
815
散列功能
1030
验证散列
110
密钥
比较功能
1055

图10

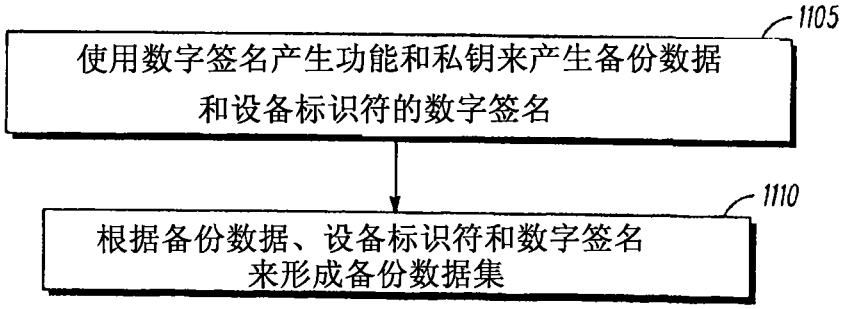

1105
使用数字签名产生功能和私钥来产生备份数据
和设备标识符的数字签名
1110
根据备份数据、设备标识符和数字签名
来形成备份数据集

图11

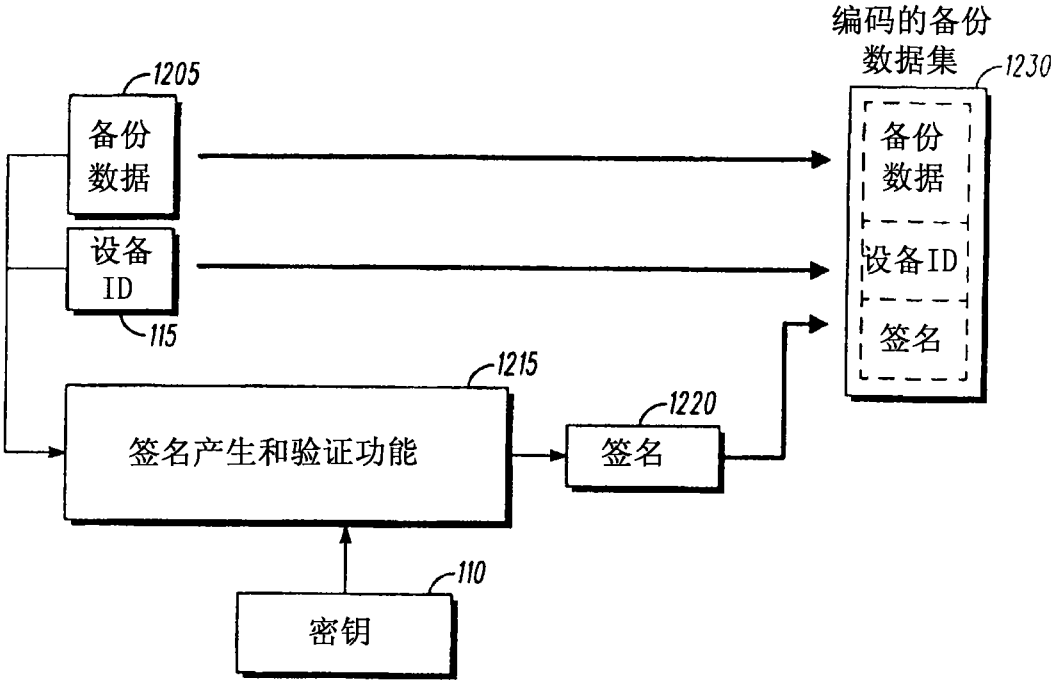

编码的备份
数据集
1230
1205
备份
数据
设备
ID
115
备份
数据
设备ID
签名
1215
1220
签名产生和验证功能
签名
110
密钥

图12

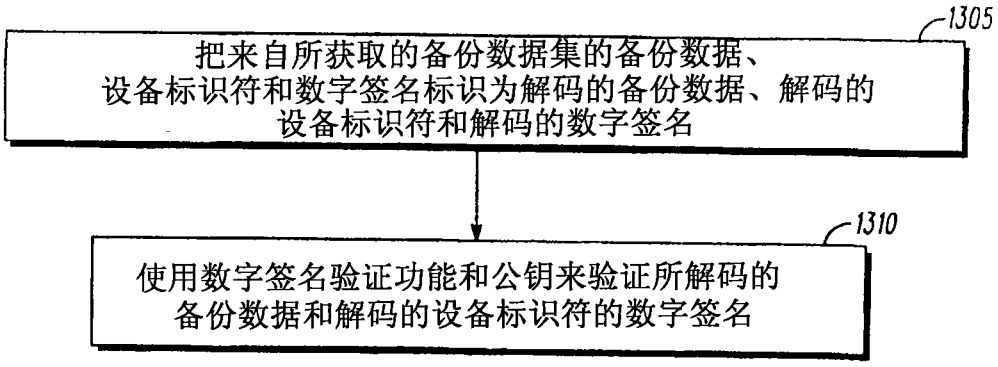

1305
把来自所获取的备份数据集的备份数据、
设备标识符和数字签名标识为解码的备份数据、解码的
设备标识符和解码的数字签名
1310
使用数字签名验证功能和公钥来验证所解码的
备份数据和解码的设备标识符的数字签名

图13

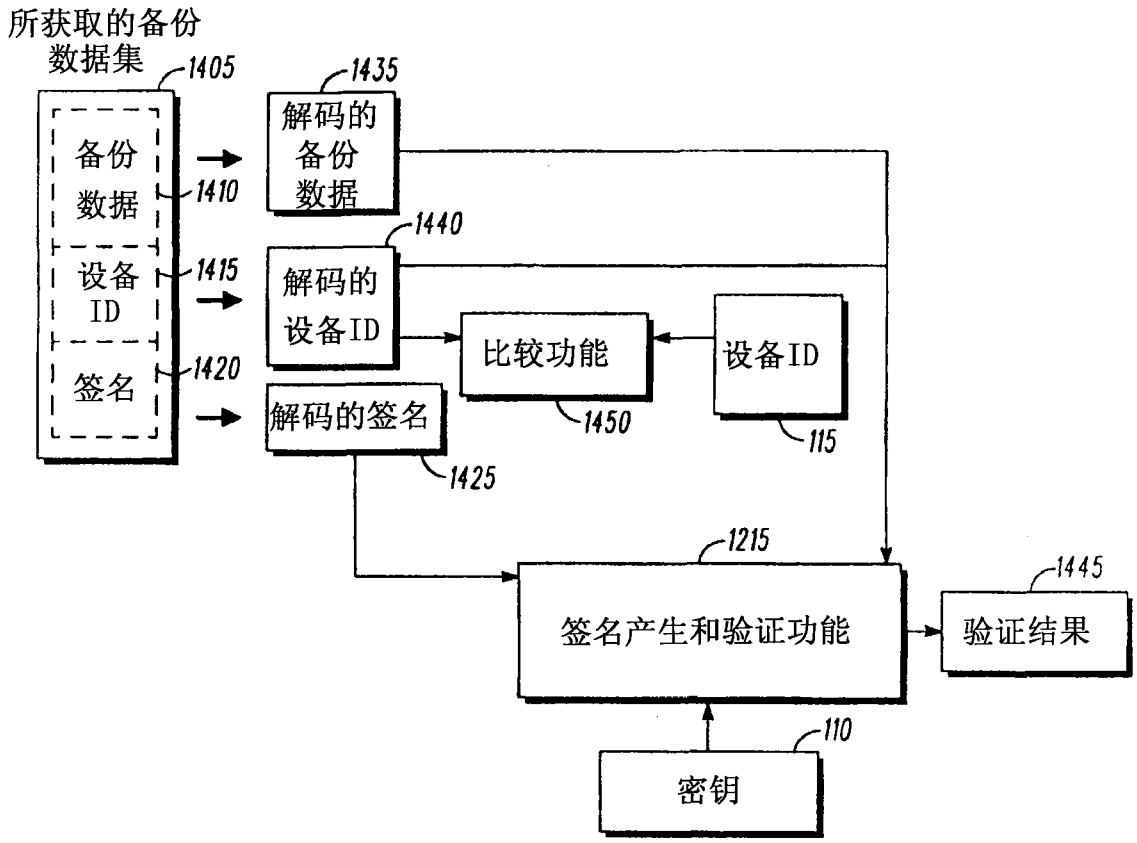

所获取的备份
数据集
1405
备份
数据
1410
设备
ID
1415
签名
1420
1435
解码的
备份
数据
1440
解码的
设备ID
比较功能
1450
设备ID
115
解码的签名
1425
1215
签名产生和验证功能
1445
验证结果
110
密钥

图14