

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

E05B 49/00 (2006.01)

G07C 9/00 (2006.01)

H04M 11/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 00817675.2

[45] 授权公告日 2006 年 2 月 1 日

[11] 授权公告号 CN 1239800C

[22] 申请日 2000.11.30 [21] 申请号 00817675.2

[30] 优先权

[32] 1999.11.30 [33] DK [31] PA199901714

[86] 国际申请 PCT/DK2000/000655 2000.11.30

[87] 国际公布 WO2001/040605 英 2001.6.7

[85] 进入国家阶段日期 2002.6.24

[71] 专利权人 博丁数字有限公司

地址 丹麦格洛斯楚普

[72] 发明人 额恩斯特·L·尼尔森

审查员 汤元磊

[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 付建军

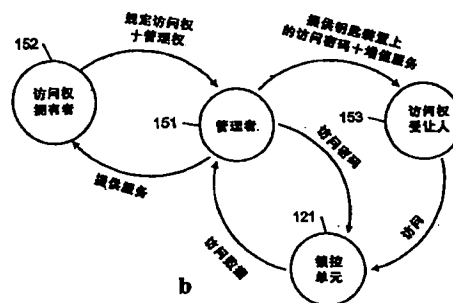
权利要求书 6 页 说明书 27 页 附图 12 页

[54] 发明名称

电子钥匙装置、管理电子钥匙信息的系统和方
法

[57] 摘要

一种高效的方法和一种系统，用于控制对某个区域的访问，该区域由锁控单元控制的锁具保护，这种方法和系统可以提供高度的灵活性和高级别的安全性；该方法包括以下步骤：在锁控单元中存放第一访问密码，第一访问密码表示该区域的预定访问权；在第二存储装置中存放第二访问密码；使用一种电子钥匙装置，通过启动从第二存储装置向锁控单元发送访问密码，请求进入该区域；将发送的第二访问密码与第一访问密码进行对比；以及如果第一访问密码符合第二访问密码，就启动锁具的操作；本发明进一步涉及对区域的预定访问权的一种管理方法。



1. 一种控制对一个由一种锁具(231)保护的一个区域访问的方法,该锁具由一个包括第一存储装置(223、871)的锁控单元(3、121、221、621、721、821)控制,本方法包括下列步骤

在第一存储装置中存放(685、699)第一访问密码,第一访问密码指明对该区域的预定访问权;

在电子钥匙装置(2、201、501、601、701、801)的第二存储装置(507)中存放(683、696)第二访问密码;

采用一个电子钥匙装置,通过从电子钥匙装置向锁控单元传送(688)第二访问密码,请求访问该区域;

将传送的第二访问密码与第一存储装置中存放的第一访问密码对比(689);以及

如果第一访问密码符合第二访问密码,就启动锁具的操作(690);其特征在於

该方法进一步包括下列步骤:在第二存储装置中存放(683、696)多个不同区域的多个第二访问密码,使得用户能够启动向锁控单元传送存储的第二访问密码中选定的一个。

2. 根据权利要求1的方法,其特征在于,该电子钥匙装置是一种移动通讯装置(2、201、501)。

3. 根据权利要求1或2的方法,其特征在于,第二存储装置是一个可移动存储模块(507),适于可拆卸地插入电子钥匙装置。

4. 根据权利要求1的方法,其特征在于,从电子钥匙装置向锁控单元传送第二访问密码的步骤包括通过无线数据通讯传送第二访问密码的步骤。

5. 根据权利要求4的方法,其特征在于,这种无线数据通讯使用红外线数据通讯。

6. 根据权利要求1的方法,其特征在于,该方法进一步包括通过通讯网络,从访问密码管理系统向电子钥匙装置和锁控单元中选定的

一个传送所述第一和第二访问密码中的至少一个。

7. 根据权利要求1的方法，其特征在于，该方法进一步包括一个步骤，在第一存储装置中存放(685、699)对应于多个不同访问权的多个有效第一访问密码。

8. 根据权利要求1的方法，其特征在于，该方法进一步包括一个步骤，在第一存储装置(223、815)中存放(389、679)试图访问区域的有关信息。

9. 根据权利要求1的方法，其特征在于，预定的访问权包括第一属性(406、407、408)，指定该预定访问权的一种性质，并且其中，第一访问密码包括该第一属性的有关信息。

10. 根据权利要求1的方法，其特征在于，预定的访问权具有一个有效期，并且其中，第一访问密码包括该有效期的有关信息(410、411、412)。

11. 根据权利要求1的方法，其特征在于，该方法进一步包括使第一访问密码作废的步骤。

12. 一种控制对一个由一种锁具(231)保护的区域访问的访问控制系统，该访问控制系统包括

一个电子钥匙装置(2、201、501、601、701、801)，包括第一传输装置(204、209、504、509、863)，适于传送第一控制信号，表示请求批准预定的访问权；以及

一个锁控单元(3、121、221、621、721、821)，包括第一接收装置(225、227、873)，适于接收来自电子钥匙装置的所述第一控制信号，第一处理装置(222、872)，适于履行收到的申请的验证，以及控制装置(224、874)，适于根据验证的结果启动锁具的操作；

其特征在于

该电子钥匙装置进一步包括第一存储装置(507、861)，适于存放多个访问密码，以识别多个预定的访问权，使得用户能够启动向锁控单元传送存储的访问密码中选定的一个。

13. 根据权利要求12的系统，其特征在于，该电子钥匙装置进一

步包括第一输入装置(203、204、865、860)，用于接收识别预定访问权的数据内容。

14. 根据权利要求12至13中任何一个的系统，其特征在于，该电子钥匙装置进一步包括第二输入装置(203)，用于接收用户输入的数据内容，该数据内容识别预定的访问权。

15. 根据权利要求12的系统，其特征在于，该电子钥匙装置进一步包括第三输入装置(203)，用于接收用户的输入，该输入表示第一存储装置中存放的多个访问权中第一个的选择，以及显示装置(202、502)，用于显示第一存储装置中存放的多个访问权中至少一个的有关信息。

16. 根据权利要求12的系统，其特征在于，第一控制信号包括申请的访问权的第一访问密码。

17. 根据权利要求12的系统，其特征在于，该电子钥匙装置是一种便携式通讯装置(2、201、501)。

18. 根据权利要求12的系统，其特征在于，第一控制信号是一种无线数据通讯信号。

19. 根据权利要求12的系统，其特征在于，第一传输装置是一种红外线通讯端口(209、509)。

20. 根据权利要求12的系统，其特征在于，该锁控单元进一步包括第四输入装置(225、226、870、876)，用于接收对应于批准预定访问权之访问密码的数据内容。

21. 根据权利要求12的系统，其特征在于，该锁控单元进一步包括第五输入装置(226、876)，用于接收用户输入的数据内容，该数据内容对应于批准预定访问权的访问密码。

22. 根据权利要求16的系统，其特征在于，该锁控单元进一步包括

第二存储装置(223、871)，适于存放对应于不同的预定访问权的多个访问密码的多个数据内容；并且其中

第一处理装置适于收到第一控制信号后，将通过第一控制信号收

到的第一访问密码与第二存储装置中存放的多个访问密码中至少其中之一进行对比。

23. 根据权利要求 12 的系统，其特征在于，该系统进一步包括计算机装置，它包括

第三存储装置（815），适于存放对应于各自的预定访问权及包括各自访问密码的多个数据内容；

第一通讯装置（813），适于向电子钥匙装置和锁控单元中选定的一个传送至少一个访问密码；以及

电子钥匙装置和锁控单元中选定的一个进一步包括第二通讯装置（204、225、860、870），适于接收传送的至少一个访问密码。

24. 根据权利要求 23 的系统，其特征在于，电子钥匙装置和锁控单元中选定的一个进一步包括第三通讯装置（204、225、864、875），向计算机装置传送一个信息信号，表示对应于传送的或收到的请求批准申请访问权的有关信息。

25. 根据权利要求 23 的系统，其特征在于，该第一通讯装置适于向锁控单元传送第二控制信号，使至少一个访问密码作废。

26. 根据权利要求 16 的系统，其特征在于，这个申请的访问权包括第一属性（406、407、408），指定这个申请的访问权的一种性质，并且其中，第一访问密码包括该第一属性的有关信息。

27. 根据权利要求 16 的系统，其特征在于，这个申请的访问权具有一个有效期，并且其中，第一访问密码包括该有效期的有关信息（410、411、412）。

28. 一种电子钥匙装置（2、201、501、601、701、801），用于根据权利要求 12 至 27 中任何一个的系统中，该电子钥匙装置包括第一传输装置（204、209、504、509、863），适于传送第一控制信号，该信号表示请求批准预定的访问权；

其特征在于，该电子钥匙装置进一步包括

第一存储装置（507、861），适于存放识别多个预定访问权的访问密码，使得用户能够启动向锁控单元传送存储的访问密码中选定的

一个。

29. 一个可移动存储模块(507)，用于根据权利要求28的电子钥匙装置中，其特征在于，该可移动存储模块适用于存放识别多个预定访问权的数据内容，使得用户能够启动向锁控单元传送所存储的访问密码中选定的一个。

30. 根据权利要求29的可移动存储模块，其特征在于，该可移动存储模块进一步包括第二处理装置(508)，适于开始传送一个控制信号，表示请求批准多个预定访问权中选定的一个。

31. 一种计算机系统(211、611、711、811)，用于与根据权利要求12至27中任何一个的系统一起使用，其特征在于，该计算机系统包括

第四存储装置(815)，适于存放多个数据内容，对应于表示预定访问权的不同访问密码；

第三处理装置(812)，适于产生表示第一访问权的第二访问密码；

第四通讯装置(813)，适于向电子钥匙装置和锁控单元中选定的一个传送第二访问密码，以便在对应的第一或第二存储装置中存放第二访问密码。

32. 根据权利要求31的计算机系统，其特征在于

第四处理装置适于产生一个第三访问密码，不同于第二访问密码，而对应于第一访问权；

第四通讯装置，适于向锁控单元发送第三访问密码；以及

第四通讯装置，适于向锁控单元发送第三控制信号，启动第二访问密码的废止操作。

33. 根据权利要求32的计算机系统，其特征在于，第四处理装置适于按照用户的请求，对应于第一访问权并且不同于第二访问密码，启动废止第二访问密码和产生一个第三访问密码的操作。

34. 根据权利要求32和33中任何一个的计算机系统，其特征在于，第四处理装置适于按照预定的时间间隔，对应于第一访问权并且不同于第二访问密码，启动废止第二访问密码和产生一个第四访问密

码的操作。

35. 一种方法，使用根据权利要求 12 至 27 中任何一个的访问控制系统，以便管理对一个区域的预定访问权，该访问权由一个访问权所有者（152）拥有，并要批准给一个访问权受让人（153），其特征在于，该方法包括以下步骤

产生（383）一个表示访问权的第一访问密码；

向锁控单元传递（684）这个第一访问密码，该控制单元适于控制访问特定区域；

向电子钥匙装置传递（682、386）一个第二访问密码；

使用第一和第二访问密码中选定的一个时，采集（679、389）有关的信息数据；

根据采集的信息数据，向访问权所有者和访问权受让人中选定的一个提供（389）至少一种附加服务。

电子钥匙装置、管理电子钥匙信息的系统和方法

技术领域

本发明涉及对某个特定区域访问的一种控制方法，由一种锁具限制对该区域的访问。本发明进一步涉及一种访问控制系统，它允许提供货物和服务的人员进入一个特定区域，不然就会阻止货物或服务的送达。本发明进一步涉及一种电子钥匙装置、在这样一种系统中使用的一种锁控单元和一种计算机系统、在这样一种电子钥匙装置中使用的一种存储器模块以及对某个特定区域的预定访问权的一种管理方法。

背景技术

通常必须要穿过许多外门或前门或中门，才能到达服务点，比如住户门口、邮箱、服务站或计量表，或者要清扫的区域等等，特别是在公寓街区或公司中。例如，对于送报纸的情况，送报员往往不得不走上楼梯才能将报纸送到锁着的私人住户门口或者放入信箱。送报员往往很难从一大串钥匙中找到正确的钥匙，而且换锁时也经常不通知投递公司。为了安全的缘故，给后院、住宅区或公司所在地的门上锁也是越来越普遍的现象，如果这些地方可能放置着例如垃圾箱，那么垃圾收集公司具有的问题非常类似于送报纸的公司。可以想象，面对同样问题的还有：

- 邮递员
- 保洁公司
- 急诊医生
- 家务女工和其他护理工人
- 警察
- 消防队员
- 工匠
- 保管人/负责人
- 以及其他。

在提供以上服务的人员中，有些需要每天上门，比如邮递员，有些可能需要按一定的时间间隔上门，比如在一定的工作日或在一天中的一定时间，例如送报员可能需要在早上6点至9点上门。

另外，不同的服务/投递人员可能需要不同的访问权，例如消防员、保安公司或警察可能需要到达所有部位，而邮递员只需要到达邮箱。

国际专利申请书 W0 93/14571 公开了一种保安入口系统，它利用手机作为电子钥匙装置。在采用这种现有技术的系统中，用户操作手机向门锁发送射频信号，使得操作手机按钮的用户如同在操作按键卡上的按钮，以进入保安区域。门锁检验由按钮操作识别的用户是否在门锁存储器中保持的授权用户列表中。

所以，在采用以上现有技术的系统中，一个问题是它需要手工输入某种类型的用户标识代码，使门锁能够检验识别出的用户是否在授权用户的列表中。然而，手工输入这样一种代码是一种冗长的过程，尤其是为了提供足够的安全性而使代码足够长时。输入代码需要一些时间，尤其是输入代码发生错误时，可能被拒绝进入，而需要再次手工输入。

发明内容

因此本发明的一个目的就是提供一种高效的方法和一种系统，用于控制一个特定区域的入口，该区域由锁控单元控制的锁具保护，这种方法和系统可以提供高度的灵活性和高级别的安全性。

做到这一点需要一种控制一个特定区域入口的方法，该区域由包括第一存储装置的锁控单元控制的锁具保护，该方法包括以下步骤

在第一存储装置中存放第一访问密码，第一访问密码表示该区域的预定访问权；

在一种电子钥匙装置的第二存储装置中存放第二访问密码；

使用该电子钥匙装置，通过从该电子钥匙装置向锁控单元发送第二访问密码，请求进入该特定区域；

将发送的第二访问密码与第一存储装置中存放的第一访问密码进行对比；以及

如果第一访问密码符合第二访问密码，启动锁具操作的特征在于

本方法进一步包括以下步骤：在第二存储装置中存放(683、696)多个不同区域的多个第二访问密码，使得用户能够启动向锁控单元传送存储的第二访问密码中选定的一个。

因此，本发明的一个优点是，对于不同建筑物的多个不同访问密码可以存放在相关的一个或多个电子钥匙装置中，为每个电子钥匙装置定制访问权特性提供了一种灵活的方式。

本发明的另一个优点是，可以为每个锁控单元提供一组特定的有效访问密码，为该锁控单元专用。所以，依据本发明的方法可以执行高级的先进功能，比如对一座指定建筑物有不同的安全级别、自毁访问密码、条件访问密码、有限时期的访问密码等等。

本发明的再一个优点是，按照简短通知或者以规则或随机的时间间隔，可以改变不同电子钥匙装置和锁控单元的访问权特性，以提高访问控制的安全性。

依据本发明，一个特定区域可能是一个有形的位置，比如一座建

筑物、一个区域或某种其它的居住的、工业的、商业的或办公的部位，进入这种特定区域受到一种锁具的控制，比如在门、窗、大门或类似入口上有形的锁。进入这种特定区域可能在入口一个点上受到控制，也可能在多个到达点上受到控制。不仅如此，一个特定区域也可能是一座建筑物、一个区域等等的一部分，依据本发明进入一个特定区域的不同部分可能分别受到控制，比如在外面的大门、前门、允许到达全部或选定楼层的电梯内部、各个住宅单元、办公室、地段、房间的门口、存储装置，比如抽屉、保险柜等等。这种特定区域可能是固定的，比如一座建筑物，也可能是移动的，比如车辆、容器、船只或者类似物体。

另外，这种特定区域也可能是一种装备，比如工业设备的一个控制单元、一台电表、一个计算机系统或类似设施，其中到达这种特定区域受到锁具的控制，比如控制箱上的一把有形锁，或者一把电子锁，比如一台计算机的硬件锁。术语进入一个特定区域也可能包括用户访问一台计算机或计算机程序，其中访问受到一种软件锁具的控制，限制访问一种软件应用程序、存储的数据、通讯设施或类似装置。

依据本发明，访问权可能是与一个特定区域相互作用的权利。访问权的实例包括进入一座建筑物、一个区域、一个机构等等的权利，操作一台机器、一台设备、一部车辆、一台计算机等等的权利，打开或关闭一道门、一扇窗、一个容器、一个箱子等等的权利，以及接收或运送货物数据信息等等的权利，只要这些权利可以被一种锁具所控制。

一种访问权可能具有一定的属性，指明这种访问权的性质。此类性质的实例包括一个或多个有效期、安全级别、有关锁控单元和/或电子钥匙装置的标识、一个密码、访问权有效的次数或指明这种访问权性质的任何其它属性。

当电子钥匙装置是一种移动通讯装置时，可以利用标准装置执行本方法，这些装置可以用于平常的通讯目的。

因此，在一个优选实施例中，本方法进一步包括从电子钥匙装置

向锁控单元发送第二访问密码的步骤。这个实施例的一个优点是，直接通讯快捷而且不需要涉及另外的通讯网络提供者。

当从第二存储装置向锁控单元发送第二访问密码的步骤包括通过无线数据通讯发送访问密码的步骤时，在电子钥匙装置和锁控单元之间可以提供不需要实际接触的一种快捷和方便的接口。

在本发明的一个优选实施例中，无线数据通讯使用红外线数据通讯。这个实施例的一个优点是，这种通讯可以基于可靠的标准组件，它作为部件存在于许多设备中，比如移动电话、个人数字助理或类似装置。

如果第二存储装置是一种可拆卸的存储模块并适于可拆卸地插入电子钥匙装置，一种标准装置可以方便地适应本发明所需的应用，通过插入一个适当的存储模块，可以向电子钥匙装置传递访问密码。

如果本方法进一步包括通过通讯网络传送的步骤，从访问密码管理系统向一个选定的电子钥匙装置和锁控单元传送至少一个访问密码，就可以在中央计算机系统产生和保持访问密码并向电子钥匙装置或锁控单元传送。本发明的一个优点是，实质上一个访问密码可以同时传送到多个电子钥匙装置和锁控单元。因此，每次都确保锁控单元和电子钥匙装置之间的同步。

如果本方法进一步包括以下步骤：从电子钥匙装置向包括第二存储装置的访问密码管理系统发送一个请求，以及从访问密码管理系统向一个选定的电子钥匙装置和锁控单元传送某些第二访问密码，这些访问密码就不必存放在电子钥匙装置中，就能够节省电子钥匙装置中的存储空间。本发明的另一个优点是，访问密码中央管理系统可以监督和跟踪访问密码的使用。

如果本方法进一步包括在第二存储装置中为多个不同的特定区域存储多个访问密码的步骤，一个电子钥匙装置就可以用于多个特定区域而不降低安全级别。

如果本方法进一步包括在第一存储装置中存储对应于多个不同访问权的多个有效访问密码的步骤，就可以通过同一个锁控单元提供不

同类型的访问权。这可能包括在一个特定区域不同的安全级别或不同类型的相互作用或访问。

如果本方法进一步包括在第三存储装置中存储有关试图进入特定区域之信息的步骤，除了提供基本功能以外，还可以提供使用访问密码的高度可见性作为附加服务。

如果访问权包括一个第一属性，指明预定访问权的一种性质，并且其中第一访问密码包括有关该第一属性的信息，就可以产生带有附加功能的访问密码，比如自毁访问密码等等。

在本发明的一个优选实施例中，该预定访问权具有一个有效期，并且第一访问密码包括有关该有效期的信息。

如果本方法进一步包括使第一访问密码作废的步骤，一个访问密码就可以由一个新访问密码取代，例如万一误用或丢失了一个电子钥匙装置时。

如上所述，本发明进一步涉及一种访问控制系统，用于控制由一种锁具保护的一个特定区域的入口，该访问控制系统包括

一种电子钥匙装置，包括第一传送装置——适于传送一个第一控制信号，表明一个请求，申请批准一个预定访问权；以及

一个锁控单元，包括第一接收装置——适于接收来自电子钥匙装置的所述第一控制信号；第一处理装置——适于执行验证收到的请求；以及控制装置——适于按照验证的结果启动锁具的操作；

该系统的特征在于

该电子钥匙装置进一步包括第一存储装置——适于存放识别多个预定访问权的多个访问密码，使得用户能够启动向该锁控单元发送存储的访问密码中选定的一个。

由于以上的系统及其优选实施例对应于以上和下面介绍的本方法及其优选实施例，并且由于它包括对应的优点，所以并非所有这些优点都会再次介绍。

如果电子钥匙装置进一步包括第一输入装置，以便接收识别预定访问权的数据内容，多个特定区域或多个访问权的多个访问密码可以进行输入、编辑、重排或类似操作。

如果电子钥匙装置进一步包括第二输入装置，用于接收用户输入

的数据内容，该数据内容识别预定的访问权，访问密码就可以由用户输入。

如果电子钥匙装置进一步包括第三输入装置——适于接收用户的输入，表明在存放在第一存储装置中的多个访问权中，选择哪个为第一个；以及显示装置，用于显示存放在第一存储装置中的多个访问权至少其中之一的有关信息，就为用户提供了一种用户界面，以便从多个存储的访问权中选择所需的访问权。

如果存放在第一存储装置中的数据内容包括预定访问权的访问密码，锁控单元就可以将收到的访问密码与多个存储的访问密码进行对比。

所以，在本发明的一个优选实施例中，选定的第一和第二控制信号之一包括申请的访问权的第一访问密码。

在本发明的再一个优选实施例中，锁控单元进一步包括第二存储装置——适于存放对应于不同预定访问权的多个访问密码的多个数据内容；并且其中，第一处理装置在收到第一控制信号时，适于对比通过第一控制信号收到的第一访问密码和第二存储装置中存放的多个访问密码中的至少一个。

本发明的一个优点是它提供了一种高级别的安全性。

在本发明的再一个优选实施例中，电子钥匙装置是一种便携通讯装置。

如果第一接收装置适于接收第一控制信号，表明请求批准申请的访问权的第一控制信号就可以从电子钥匙装置向锁控单元传送。

在本发明的再一个优选实施例中，第一控制信号是一种无线数据通讯信号。

在本发明的再一个优选实施例中，第一发送装置是一种红外线通讯端口。

如果锁控单元进一步包括第四输入装置，用于接收对应于批准预定访问权之访问密码的数据内容，对应于多个访问权——比如不同的安全级别、时间限制等等——的访问密码和其它相关数据就可以在锁控单元中存储而且便于修改。

如果锁控单元进一步包括第五输入装置，用于接收用户输入的数据

据内容, 该数据内容对应于批准预定访问权的访问密码, 被授权的用户就可以输入、编辑或删除在锁控单元中存放的访问密码, 可能在提供了一个口令或者说另一种安全验证之后。

如果系统另外或者说又进一步包括计算机装置, 它包括

第三存储装置, 适于存放多个数据内容, 对应于各自的预定访问权并包括各自的访问密码;

第一通讯装置, 适于向选定的电子钥匙装置和锁控单元之一发送至少一个访问密码; 以及

该选定的电子钥匙装置和锁控单元之一进一步包括第二通讯装置, 适于接收发送的至少一个访问密码, 访问密码可能发送自访问密码中央管理系统。这种做法可能是响应为了一种访问权的一个特定请求, 或者是为了在电子钥匙装置中或锁控单元中存放一个或多个访问密码。

在本发明的再一个优选实施例中, 某选定的电子钥匙装置和锁控单元之一进一步包括第三通讯装置, 用于向计算机装置发送一种信息信号, 它表明的有关信息对应于为批准申请的访问权而发送和接收的请求。

本发明的一个优点是, 电子钥匙装置、访问密码、访问权授权者、访问密码使用等等的有关信息可以在中央服务中采集和保持, 以向访问权的拥有者提供最优的透明度和安全性。

在本发明的一个优选实施例中, 第一通讯装置适于向锁控单元发送一个第二控制信号, 使至少一个访问密码作废。

在本发明的一个优选实施例中, 申请的访问权包括一个第一属性, 指明申请的访问权的一种性质, 并且其中, 第一访问密码包括该第一属性的有关信息。

在本发明的一个优选实施例中, 申请的访问权包括一个有效期, 并且第一访问密码包括该有效期的有关信息。

本发明进一步涉及一种锁控单元, 用于以上和后面介绍的系统中, 其特征在于该锁控单元包括

第一接收装置——适于接收一个控制信号, 表明一个请求批准所申请的访问权的请求; 第一处理装置——适于执行验证收到的请求;

以及控制装置——适于按照验证的结果启动锁具的操作。

本发明进一步涉及一种电子钥匙装置，用于以上和后面介绍的系统中，该电子钥匙装置包括第一发送装置——适于发送一个第一控制信号，表明一个请求，为了批准预定的访问权；

其特征在于该电子钥匙装置包括

第一存储装置——适于存放识别多个预定访问权的访问密码，使得用户能够向该锁控单元发送存储的访问密码中选定的一个。

本发明进一步涉及一种可拆卸的存储模块，用于以上和后面介绍的电子钥匙装置中，其特征在于这种可拆卸的存储模块适于存放识别多个预定访问权的数据内容，使得用户能够向该锁控单元发送存储的访问密码中选定的一个。

在本发明的一个优选实施例中，这种可拆卸的存储模块进一步包括第二处理装置——适于发送一个控制信号，表明一个请求，申请批准多个预定访问权中选定的一个。

本发明进一步涉及一种计算机系统，与以上和后面介绍的系统一起使用，其特征在于该计算机系统包括

第四存储装置，适于存放多个数据内容，对应于表示预定访问权的、各自的访问密码；

第三处理装置，适于产生一个表示第一访问权的第二访问密码；

第四通讯装置，适于向选定的一个电子钥匙装置和锁控单元发送第二访问密码，以便在对应的第一或第二存储装置中存放第二访问密码。

在本发明的一个优选实施例中，第四处理装置适于产生一个第三访问密码，不同于第二访问密码，而对应于第一访问权；

第四通讯装置适于向锁控单元发送第三访问密码；以及

第四通讯装置适于向锁控单元发送第三控制信号，启动废止第二访问密码的操作。

在本发明的再一个优选实施例中，第四处理装置适于按照用户的

请求，启动废止第二访问密码和产生一个第三访问密码，它对应于第一访问权并且不同于第二访问密码。

在本发明的另一个优选实施例中，第四处理装置适于按照预定的时间间隔，启动废止第二访问密码和产生一个第四访问密码，它对应于第一访问权并且不同于第二访问密码。

本发明进一步涉及一种方法，用于以上和后面介绍的访问控制系统，以便管理对一个特定区域的预定访问权，该访问权由一个访问权拥有者拥有，并可以批准给一个访问权受让人，该方法包括以下步骤产生一个表示访问权的第一访问密码；

向锁控单元传递这个第一访问密码，该锁控单元适于控制访问特定区域；

向电子钥匙装置传递一个第二访问密码；

使用第一和第二访问密码中选定的一个时，采集有关的信息数据；

根据采集的信息数据，向访问权拥有者和访问权受让人中选定的一个提供至少一种附加服务。

附图说明

下面将连同优选实施例和参考以下附图更全面地讲解本发明：

图 1a 和图 1b 显示了依据本发明的两个访问密码管理实施例的数据流示意图；

图 2a 至图 2c 显示了依据本发明的一个特定区域访问控制系统的三张框图；

图 3 显示了依据本发明的一个实施例，访问密码管理过程的一张流程图；

图 4 显示了依据本发明的一个实施例，一个访问密码的一个实例；

图 5a 和图 5b 显示了依据本发明的一种电子钥匙装置的两个实施例；

图 6a 至图 6c 显示了依据本发明的访问控制过程的三个实施例的流程图；

图 7a 至图 7e 显示了依据本发明的访问控制过程的不同实施例的

数据流示意图;

图 8a 和图 8b 显示了依据本发明的访问密码管理系统中两个软件组件实施例的框图;

具体实施方式

图 1a 显示了本发明一个实施例的原理,它使用送报纸作为一个实例。不过,本发明并非局限于送报纸。如果在第一个实例中,想象本发明由单个公司实施,可将图 1a 讲解如下:

一个送报公司 5 具有许多订户,要求将其报纸送到其各自的住处。这些订户及其电子访问密码的信息保存在送报公司 5 的一个数据库中。这些信息可以从这个数据库传递到许多电子钥匙装置,比如移动电话 2。以包括访问密码的打印列表形式,一个送报员 1 可以接收其途中订户的有关信息。然后送报员 1 可以把访问密码输入其移动电话 2,最好是通过移动电话 2 上的键盘。这些访问密码最好是存放在移动电话 2 的 SIM 卡中,而且它们可以采用特殊的顺序输入,以符合货物和服务的投递,比如沿着预定的途径送报纸。如果向移动电话 2 提供了正确的电子访问密码信息,这种信息可以从移动电话 2 向住处的门锁 3 以电子方式发送,那么利用这个移动电话 2,送报员 1 就可以进入建筑物中锁着的楼梯。门锁 3 适于接收来自移动电话 2 的信号,并使得门开锁。可以采用手工方式把有效的访问密码输入门锁中,例如从送报公司 5 收到有效访问密码及其对应门锁的打印列表后,由服务人员 4 进行。服务人员 4 可以通过袖珍键盘、双列直插式开关或类似装置,把访问密码输入门锁中。依据本发明的这个实施例,作为本系统一个另外的优点,送报公司 5 能够了解送报员 1 是否打开了楼梯的门锁,例如在发生了报纸未送达的投诉时。

不过,本发明的电子钥匙装置和电子访问密码信息的、相关联的管理形成的基础,也可以用于几个不同公司。

再次以报纸作为实例,参考图 1b 介绍多个公司的不同角色和相应的数据流。涉及的第一个公司可能是印刷和投递报纸的公司,所以它需要访问订户的住处。作为一个访问权受让人 153,第一个公司从访问密码的管理者 151 处接收访问密码,该管理者是第二个公司、组织或个人,管理着电子钥匙系统并且可以作为投递许多不同货物和服务

的服务供应商。管理者 151 也向锁控单元 121 传递访问密码，后者控制着订户住处的锁具。管理者 151 也可以向访问权受让人 153 供应电子钥匙装置，还可能有其它必需的有形和无形工具，例如，利用这些工具，访问权拥有者 152 也许能够同时管理锁控单元 121 和电子钥匙装置与访问密码。这可能是在管理者 151 的控制下发生的。另外或者说进一步可能涉及第三个公司，它拥有电子钥匙装置，或者它可能是网络操作员，向用作电子钥匙装置的移动电话发送访问密码信息。第四个公司可能拥有建筑物或者与建筑物的拥有者有商业协议，所以第四个公司可能是访问权的拥有者 152，它与管理者 151 达成有关安装锁控单元 121 的协议，而且它对不同的访问权持有者 153 规定各自的访问权。电子控制单元 121 可能是由管理者 151、访问权拥有者 152、访问权受让人 153 或者第五个公司拥有和安装。管理者 151 也可以根据从锁控单元 121 采集的访问数据，向访问权受让人 153 或访问权拥有者 152 提供增值服务，比如使用次数统计。这些服务可能是自助的功能、有形的服务、时间和材料服务或者普通的信息服务。

所以本发明表明了使用现代技术能够形成新服务公司的基础，使货物和服务的传递效率更高，并能够确保消费者依据本发明的电子钥匙所要求的、必需的安全系统。

依据本发明的电子钥匙可能应当由许多其它信息进行补充，这些信息可能与电子钥匙的使用有关。例如，有关订户的变化发生后，一个投递员能够很快地获得更新后的知识。急诊医生在大的公寓街区中能够获得帮助，以便通过锁着的门。保洁人员能够获得更新后的信息，了解有关当前行动的变化。

管理者 151 与访问权拥有者 152 之间的关系，最好能在一份合同中写明，它最好说明访问权拥有者 152 向管理者 151 保证一定权限的条款，比如批准其它人——例如在管理者的组织之内或管理者可能与之有一个合同的第三方人员——访问一个特定区域或者履行与该特定区域有关功能的权限。

参考图 2a，依据本发明的访问控制系统的第一个实施例，包括一

个移动电子钥匙装置 201 和一个锁控单元 221, 后者控制着一个锁具 231, 比如一个门锁。电子钥匙装置 201 包括一个显示屏 202——用于显示至少一个访问密码的相关信息, 一个袖珍键盘 203——用于输入命令和选择一个访问密码, 以及一个通讯端口——最好是遵从已知标准比如 IrDa (红外线数据协会) 标准的 IR (红外线) 端口。电子钥匙装置 201 可能是一个移动电话、一个 PDA (个人数字助理)、一台掌上电脑、一片智能卡、一台 PSION 终端、一台条形码阅读器、或者能够发射红外线或无线电信号或其它类型信号的另一台终端, 控制一他特定区域访问比如控制一个门锁的锁控单元 221 能够接收这些信号。电子钥匙装置也可以安装在车辆中。连同图 5a 和图 5b 会进一步介绍依据本发明的电子钥匙装置 201 的实施例。

一般说来, 所有类型的电子钥匙装置都应当能够更新访问密码的信息和能够识别一个锁控单元 221 或一个锁和一扇门之结合的其它信息, 例如必须通过袖珍键盘 203 输入的数字组合的信息。电子钥匙装置 201 最好能够发射一种包括访问密码的电子信号, 或者以无线方式, 或者通过某种其它类型的连接, 该信号能够激活锁控单元 221。最好是使用红外线信号或者无线电传输。

锁控单元 221 包括接收器 227, 接收电子钥匙装置 201 的通讯端口 209 发送的、带有访问密码的信号。接收器 227 应当与通讯端口 209 兼容, 而且接收器 227 最好是一种 IrDa 端口。接收器 227 连接到一个处理单元 222, 它连接到一个存储器 223, 比如 RAM 或 EPROM。存储器 223 能够存放对于锁控单元 221 有效的访问密码, 而且处理单元 222 适于对比收到的访问密码和存放的访问密码。处理单元 222 进一步控制访问密码的存放和检索, 以及其它可能的操作比如产生日志文件并把它们存放在存储器中、自检功能或类似操作。处理单元 222 进一步连接到一个锁控接口 224, 它适于控制锁具 231。如果收到的访问密码有效, 处理单元 222 可以向锁控接口 224 发送一个控制信号, 使锁控接口 224 启动锁具 231 的操作, 从而准许特定区域的访问。锁控单元 221 进一步包括一个用户接口 226, 包括显示屏 226a 和袖珍键盘

226b, 获得授权的用户可以通过它输入、编辑和删除有效的访问密码, 以及用其它方式控制锁控单元 221, 例如有关的维护、测试、手工操作或类似工作。输入的访问密码存放在存储器 223 中。锁控单元 221 另外或者说进一步可能包括一个输入端口, 比如一个标准串行接口, 连接一个分离的设备, 输入访问密码并控制锁控单元 221。

锁控单元 221 连接到锁具 231, 比如一个门锁系统、一个阀控系统或者类似设施。这种连接可能是电气的或机械的连接或者一种无线通讯连接。另外, 锁控单元 221 可能不是连接到一个分离的锁具 231, 而是本身就包含相应的电气的、电子的和/或机械的部件, 比如能够打开一个阀门的一个电动引擎, 或者能够打开一扇门的电气装置。

锁具 231 包括一个单元, 它能够激活例如安装在一扇门上的一把锁(未显示), 例如通过一种电气的/电子的继电器。锁具 231 可以连接到建筑物中已有的门口电话系统, 或者它可以适于独立运作, 通过它自己的机械零件和它自己的电源供应。锁具 231 最好能够从锁控接口 224 接收一个信号, 并且可选地也能够向接口 224 发送信号。从而提供一个验证过程, 其中甚至进一步增强了涉及依据本发明的访问控制系统的安全性。

不仅如此, 例如, 若是投递员在其环路上有许多磁卡阅读器保护的楼梯或公司, 电子钥匙装置可能是一片带有芯片的智能卡, 由钥匙管理人把信息已经输入在芯片中, 所以利用这片智能卡就能打开环路上的各扇门。

图 2b 说明了依据本发明的锁控系统的第二个实施例, 包括电子钥匙装置 201, 例如一个移动电话, 带有显示屏 202 和袖珍键盘 203, 用于控制装置 201 和选择该装置中存放的访问密码之一。电子钥匙装置 201 配备了通讯端口 209, 用于向锁控单元 221 发送控制信号。通讯可以使用电磁辐射, 比如 IR 或无线电通讯, 或者任何其它适当的通讯技术比如声音。通讯可以遵从从一个专有的协议或者最好是一个标准协议, 比如 TCP/IP、IrDa、电话数据协议移动电话数据协议、http、蓝牙、声音等等。信息的传递或者是采用专有的数据格式, 或者最好是采用

标准格式，比如 wml、html、二进制代码、机器代码、AT 命令、语音命令或类似格式。

在电子钥匙装置 201 和锁控单元 221 之间的无线通讯，可以由包括单元之间实际接触的通讯形式取代，例如，电子钥匙装置是一片智能卡或存放着信息的磁卡或其它装置，可以实际接触锁控单元，例如通过插头或者说接插件。

电子钥匙装置 201 进一步配备了通讯接口 204，例如移动电话的发射/接收天线。电子钥匙装置 201 可以通过通讯接口 204 连接到访问密码管理系统 211。这种通讯可能是基于无线电的通讯，最好是通过标准的通讯网络 241，例如标准的移动电话网络。通过电子钥匙装置 201 和访问密码管理系统 211 之间的通讯连接，可以从访问密码管理系统 211 向电子钥匙装置 201 传送访问密码。这种数据传输可以使用所谓的短信服务 (SMS) 或者其它高速数据通道，例如 GSM 数据、WAP 或 CDMA 传输系统中各种各样的数据通道。另外或者说进一步，也可以使用其它适当的通讯通道，它们使用专有的或标准的协议，比如 TCP/IP、http、语音消息等等。

访问密码管理系统 211 最好是一种计算机系统，最好包括一台或多台标准的计算机，比如个人计算机、工作站、应用程序服务器、数据库和网络服务器，通过局域网互相连接并访问通讯网络 241，例如通过一个服务供应商。访问密码管理系统 211 产生和管理访问密码，正如连同图 3、图 9a 和图 9b 所介绍的。访问密码管理系统 211 向电子钥匙装置 201 和/或锁控单元 221 发送访问密码。发送访问密码是根据用户的请求或者是自动的。另外，访问密码可以定期发送，以便取代锁控单元和相应的电子钥匙装置中的访问密码，从而改善系统的安全性。访问密码管理系统 211 也可以自动地或者根据请求向锁控单元 221 和/或电子钥匙装置 201 发送相应的控制信号，废止访问密码。

锁控单元 221 包括通讯单元 225，以介绍从访问密码管理系统 211 发送的数据。另外或者说进一步，锁控单元 221 可能包括用户接口 226 或另一个输入端口，正如连同图 2a 中展示的、访问控制系统的第一个

实施例所介绍的。锁控单元 221 进一步包括处理单元 222、存储器 223——存放访问密码和可执行的计算机程序代码、接收器 227——从电子钥匙装置 201 接收控制信号、锁控接口 224——正如连同图 2a 中展示的、访问控制系统的第一个实施例已经介绍过的。

现在参考图 2c, 在依据本发明的访问控制系统的第三个实施例中, 电子钥匙装置 201 可以只包括一个通讯接口 204, 例如移动电话的发射/接收天线, 用于连接该装置到通讯网络 241, 比如移动电话网络。在这个实施例中, 电子钥匙装置 201 或者直接与锁控单元 221 通讯, 例如通过通讯网络 241 发送 SMS 消息的方式, 或者通过访问密码管理系统 211 与锁控单元 221 通讯, 例如通过 SMS 消息、WAP、语音或其它通讯通道。

在一个优选实施例中, 电子钥匙装置 201 也可能是一台计算机, 比如固定式或便携式 PC, 能够访问因特网。在这个实施例中, 用户可以通过软件应用程序, 比如浏览器, 向访问密码管理系统 211 发送一个选定的访问密码, 以便验证和/或进一步向锁控单元 221 传输。在这个实施例中, 用户可以获得远程访问, 从其计算机到一个特定区域, 比如一台机器或设备。不仅如此, 访问密码管理中心 211 可能改变对可遥控机器的访问密码, 例如以随机选定时间间隔, 并且向用户的计算机和控制着该机器访问的锁控单元 221 发送访问密码。

图 3 说明了依据本发明的管理访问权过程的一个流程图。图 3 也说明了各个处理步骤是否由管理者 351、访问权拥有者 352 或访问权受让人 353 执行或受其控制。在初始步骤 381 中, 访问权拥有者 352 规定要批准的访问权, 也许包括可能的访问权受让人的一个列表。在步骤 382 中, 访问权拥有者 352 授权管理者 351 产生和分配访问钥匙。这种授权可以包括不同的权限级别, 并且最好在一份合同中说明, 正如连同图 1 所介绍的。利用一个访问密码管理系统, 管理者 351 在步骤 383 中把访问权的规定转换为一组电子访问密码, 以识别各个权限或各组权限, 正如连同图 4 所介绍的。访问密码的规定和生成, 可能还有电子钥匙装置的设计和生成, 可以由管理者 351 根据访问权拥有

者 352 的请求或者这两者和可能的第三方的协作而执行。在步骤 384 中, 访问密码和其它相关的设计存放在最好是访问密码管理系统的数据库中, 正如连同图 8b 所介绍的。

在访问密码的生成 383 和存储 384 之后, 在步骤 385 中从访问密码管理系统向各个特定区域的锁控单元传递访问密码。访问密码的传递可以是由管理者 351 进行, 也可以是访问权拥有者 352、访问权受让人 353 或者第三方进行。同样, 向电子钥匙装置的访问密码传递 386 可以是由管理者 351 进行, 也可以是访问权拥有者 352、访问权受让人 353 或者第三方进行。接收 387 访问密码之后, 访问权受让人 353 就可以访问该特定区域(步骤 388)。

除了访问密码以外, 访问权受让人 353 还有电子钥匙装置, 它的操作能够与依据本发明的访问控制系统结合。这可能意味着特定的硬件、软件和通讯需求, 它们可能是能够与访问权拥有者 352 指定的锁控单元通讯的先决条件。这些需求最好是分别在访问权拥有者 352 和管理者之间以及管理者 351 和访问权受让人 353 之间的合同中规定。合同可以指明使用装置的类型, 或者包括某些条款, 规定电子钥匙装置的一种可能的设计和制造方法以及它们可能的外部设备(硬件还有软件)。

最好在步骤 389 中, 在访问密码管理系统的日志中记录使用访问密码和电子钥匙装置的有关数据。另外或者说进一步, 日志数据也可以存放在锁控单元和/或电子钥匙装置中。日志数据可以采用预定的时间间隔、按照请求或者在线地传送到访问密码管理系统。

管理者 351 可以提供附加的服务, 由访问权拥有者 352 接收 390。另外或者说进一步, 管理者 351 可以向访问权受让人 353 或一个第三方提供服务。最好这些附加服务包括提供和/或分析对应于访问权的信息, 这些信息与以下诸项有关:

- 锁控单元的特定区域。

- 访问权和密码, 指定对应的访问权受让人 352, 规定的项目包括特定区域、锁控单元、允许访问的次数、允许访问的类型等等。

- 电子钥匙装置的规定，它有或者说有了一个给定的访问密码或者说访问权分配给它。

- 有关锁控单元的状态信息，其中状态可以包括 “ 锁闭 ”、“ 开启 ”、“ 需要维修 ”、“ 手工操作 ”等等。

- 有关特定区域的状态信息。

- 哪个电子钥匙装置已经连同哪个锁控单元或特定区域使用的有关信息，何时、如何、何处、多少次、为何等等。

因此，系统信息和接口信息可以用于产生信息服务和追踪系统，以增加整个系统的价值。连接到外部服务比如 GIS、GPS、因特网服务，或者类似形式，可以进一步增加可提供服务的种类。例如把锁控单元连接到 GPS，就可以允许追踪容器，使哪个容器在何时、何处被打开过受到监督。

以上服务也可以用于需要监督批准的访问权的使用之处。这种情况可能是货物只允许按特定的时间运送到特定的位置，以及管理者 351 可以提供相关投递人员获准何时、何处和如何访问的有关信息。

批准有限次数访问的可能性也是一个选件，它可以支持例如电子商务投递。在这种情况下管理者 351 能够允许访问权的拥有者批准特定区域的一次性或预定次数的访问。这种功能或者可以由管理者 351 按照请求提供，或者访问权拥有者 352 可以具有执行这种功能的工具或功能，例如通过锁控单元的用户界面，或者通过与访问密码管理系统的远程通讯，例如通过电话、因特网应用程序或类似方式。不仅如此，一次性访问权可能与一个口令相耦合以便获得额外的安全性。

图 4 说明了依据本发明的访问密码数据格式的一个实施例。如上所述，访问密码是由访问密码管理系统产生的。访问密码最好包括一系列的数据内容，它们可以传递到锁控单元和电子钥匙装置。应当理解，优选的数据格式可能取决于访问权的类型、电子钥匙装置或锁控单元的存储能力。访问密码可能包括一个二进制代码、一个 ASCII 代码、一系列音素或者说语音命令、按键音、声音或类似信息。图 4 中展示的访问密码数据格式包括一系列字节，以头部 401 开始，它包括

例如一个 4 字节的访问密码 ID。访问密码进一步包括下列标识符：一个锁控单元 ID 402，它识别访问密码对之有效的锁控单元或一组锁控单元，一个钥匙装置 ID，识别被授权使用这个访问密码的电子钥匙装置或一组钥匙装置，以及管理者 ID 404。应当理解，这些附加的 ID 是可选的，它们可以省略设置为默认值。图 4 中展示的访问密码进一步包括附加的可选区域，包括访问权的类型 405 和附加的访问密码属性 406 的有关信息。访问权 407 的类型可能是例如一个 1 字节的区域，指明访问权的类型，比如安全级别、是否为有时间限制的访问权，或者为次数有限制的访问权等等。访问条件区域 408 指明访问权是否以例如一个口令为条件。某些类型的访问权需要附加的参数，例如有效期 410、每个工作日的时间段 411、允许的入口数目 412。

最后，访问密码包括附加的报告属性 413，控制着例如锁控单元日志数据的细节、向管理者报告每次访问事件的请求或者类似信息。

在访问密码中包括这些功能的可能性允许生成自毁访问密码和具有独特性质的密码（例如只能在早上 4:00 到 6:00 使用）。

应当理解，向电子钥匙装置和/或锁控单元传送的访问密码中，可能包括这些选项。为了减少电子钥匙装置中的存储器需求，该装置可能包括一片带有有限存储能力的 SIM 卡，在电子钥匙装置中仅仅存放访问密码的某些部分例如仅包括访问密码 ID 401 就够了，而其余区域与访问密码 ID 401 一起存放在锁控单元中。在这种情况下，锁控单元可以根据访问密码 ID 401 识别访问密码，并检索存放在锁控单元中的其余参数，以便处理收到的请求。

图 5a 显示了依据本发明的电子钥匙装置的第一个实施例。电子钥匙装置 501 可能是一部标准的 GSM 电话，如图 5a 所示。该电子钥匙装置包括可拆卸的 SIM 卡（用户标识模块）506、发射/接收天线 504、发射/接收电路 505 和用于向用户显示访问密码信息的显示屏 502。

SIM 卡 506 包括一个处理器或者说控制电路 508 和存储器 507。该存储器可能分为存放着 SIM 操作系统和其它程序代码的 ROM 507a，和存放着数据内容和为控制单元使用 RAM 和/或 EPROM 507b。

如果天线 504 接收来自访问密码管理系统或服务供应商的、包括访问密码的数据内容，它们经由电路 505 到 SIM 卡 506，其中控制单元 508 将数据存放在存储器 507b 中。

如果用户通过电子钥匙装置的袖珍键盘（未显示）请求一个访问密码，控制单元 508 从存储器 507b 中检索该访问密码，并在显示屏 502 上显示该访问密码和/或有关的信息。

依据本发明，用户可以通过袖珍键盘发布一个命令，以便开始使用一个选定的访问密码。按照用户的请求，控制单元 508 开始通过电路 505 和天线 504 向锁控单元或者是访问密码管理系统发送选定的访问密码。控制着访问密码存放、检索、选择和发送的应用程序软件存放在存储器 507a 中。

图 5b 显示了依据本发明的电子钥匙装置的第二个实施例。图 5b 中的电子钥匙装置 501 包括可拆卸的 SIM 卡 506、发射/接收天线 504、发射/接收电路 505 和用于向用户显示访问密码信息的显示屏 502。

在这个实施例中，访问密码的接收、存放和选择的操作类似于图 5a 中所示的第一个实施例。不过，图 5b 中的电子钥匙装置进一步包括红外线通讯端口 509，最好遵从 IrDa（红外线数据协会）标准。红外线端口连接到电路 505。

依据本发明，控制单元 508 适于通过电路 505 和红外线端口 509 向锁控单元的相应端口传送选定的访问密码。例如，这项功能的实现可能是通过调整存放在存储器 507a 中的操作系统，使应用程序软件能够控制通讯端口 509。控制着访问密码存放、检索、选择和发送的应用程序软件存放在存储器 507a 中。

红外线通讯的一个优点是，它使访问密码能够快速传送到锁控单元，所以用户向操作锁具的锁控单元发布命令后，响应时间很短。不仅如此，红外线传输具有不使用通讯网络从而不增加成本的优点。

应当理解，除此以外，也可以使用其它通讯装置，比如蓝牙通讯端口、超声波信号或类似方式。

图 6a 显示了依据本发明的、电子钥匙装置 601 和锁控单元 621 之

间的通讯过程的第一个实施例的流程图。

依据这个实施例，若干访问密码由手工输入电子钥匙装置 601 和锁控单元 621 中，并存放在它们各自的存储器中，分别如步骤 694-696 和步骤 697-699 所示。例如，用户手工输入访问密码的步骤 695、698 可以使用分别位于电子钥匙装置和锁控单元上的开关，比如双列直插式开关，或者袖珍键盘。电子钥匙装置也可以连接到访问密码管理系统，例如通过电缆连接、连接站、红外线或蓝牙端口或者类似方式。手工输入可以由管理者、访问权拥有者、访问权受让人或者第三方执行。

图 6a 中的步骤 687-692 说明了一个访问控制对话，其中一个访问权受让人请求通过电子钥匙装置 601 和锁控单元 621 访问一个特定区域。按照用户的请求，在步骤 688 中一个选定的访问密码从电子钥匙装置 601 传送锁控单元 621，例如通过正如连同图 5b 所介绍的红外线通讯。在步骤 689 中，锁控单元将收到的访问密码与锁控单元的存储器中存放的访问密码核对。如果收到的访问密码符合存放的有效访问密码之一，就在步骤 690 中操作锁具，从而准许对这个特定区域的访问。这种操作可能包括锁具的开锁和/或锁闭，因为限制对一个特定区域的访问也可能需要一种批准的访问权。如果访问密码核对 689 失败，锁具就不操作。在两种情况下，都可以产生以上对话的有关日志数据，并存放在锁控单元和/或电子钥匙装置的存储器中，分别如步骤 691 和 692 所示。

图 6b 说明了依据本发明的、电子钥匙装置 601 和锁控单元 621 之间通讯的第二个实施例。

不是如连同图 6a 所介绍的那样手工输入访问密码，可以通过一种通讯通道，比如连同图 5b 所介绍的数据或电话通讯，从访问密码管理系统 611 向电子钥匙装置和/或锁控单元 621 传送访问密码。传送和存放访问密码的步骤见图 6b 中步骤 681-685 的说明。

从访问密码管理系统 611 到电子钥匙装置 601 的传输 682 可能进一步包括传送应用程序软件组件和可能有的通讯软件组件，以便使电

子钥匙装置 601 能够执行存放、检索、选择和传送访问密码的操作。如果电子钥匙装置 601 是一种标准的装置比如 PDA 或移动电话, 应用程序软件的传输有利的。应用程序软件可能进一步包括压缩和/或加密特性。

应用程序和通讯软件组件的传送可能利用例如因特网、连接站、移动通信(OTA)、无线电通讯、本地无线电网络比如蓝牙或者其它数据通讯装置。

一旦访问密码和可能需要的软件组件发送到并存放在电子钥匙装置 601 和锁控单元 621, 就可以执行访问控制对话的步骤 687-690, 正如连同图 6a 所介绍的。不是如连同图 6a 的步骤 691-692 所介绍的, 将日志数据存放在本地的锁控单元 621 和电子钥匙装置 601 中, 在这个实施例的步骤 693 中, 识别以上对话的一条消息可能发送到访问密码管理系统, 其中在步骤 679 它被存放在最好是一个数据库中。

图 6c 显示了依据本发明的、电子钥匙装置 601 和锁控单元 621 之间的通讯的第三个实施例的流程图。这个实施例最好是连同访问控制系统使用, 该系统依据图 2b 中说明的实施例。这个实施例中, 从访问密码管理系统 611 把访问密码在线传送到锁控单元 621。这个实施例的一个优点是, 它不受 SIM 卡上能够存放的数据多少的限制, 也无须由特定的网络操作员来处理 SIM 卡。

图 6c 中说明了依据这个实施例的一个访问控制对话的一个实例。按照用户的请求, 电子钥匙装置 601 在步骤 671 中联系访问密码管理系统 611。电子钥匙装置 601 可能是例如移动终端, 比如移动电话或 PDA, 最好支持 WAP。WAP 应用程序使依据本发明的电子钥匙装置受到管理, 而不涉及网络操作员。另外, 在线通讯可以使用另一个通讯通道, 比如 SMS。在步骤 672 中, 访问密码管理系统 611 识别电子钥匙装置 601, 例如通过其 SIM 卡或另一个标识。在步骤 673 中, 访问密码管理系统 611 向电子钥匙装置 601 发送可用特定区域的有关信息。在步骤 674 中, 传送的信息可以显示在电子钥匙装置 601 处, 用户可以选择显示的特定区域和锁控单元之一。在随后的步骤 675 中,

一个对应的请求发送到访问密码管理系统 611。在步骤 676 中，访问密码管理系统 611 联系对应的锁控单元 621，并发送电子钥匙装置 601 的访问密码和标识。在步骤 677 中，锁控单元联系识别的电子钥匙装置 601，最好是通过一个短程和快速的通讯通道，比如 IrDa 或蓝牙，它在步骤 688 中将其标识信息传递到锁控单元 621。在随后的步骤 689-690 中，锁控单元 621 核对电子钥匙装置的标识并操作锁具。然后，锁控单元可以向访问密码管理系统 611 发送日志数据，正如以上已经介绍过的。

图 7a 至图 7e 说明了依据本发明的不同访问密码控制方案中访问密码管理系统 711、电子钥匙装置 701 和锁控单元 721 之间的数据流。

图 7a 对应于连同图 6a 所介绍的实施例，其中访问密码从访问密码管理系统 711 脱机传递到钥匙装置 701 和锁控单元 721，如图 7a 中的虚线箭头所示。在电子钥匙装置 701 和锁控单元 721 中，可以分别存放多个有效的访问密码。在实际的访问控制对话期间，电子钥匙装置 701 向锁控单元 721 传送一个选定的访问密码，其中执行了一次核对。这个实施例的一个优点是，它不需要电子钥匙装置 701 和访问密码管理系统 711 之间或锁控单元 721 和访问密码管理系统 711 之间的在线通讯。

图 7b 说明了一个实施例，其中访问密码只是脱机传递到和存储在锁控单元 721 中。在访问控制对话期间，电子钥匙装置 701 向访问密码管理系统 711 发送一个请求，后者核对电子钥匙装置 701 的标识，例如通过 SIM 卡，并且向电子钥匙装置 701 发送一个对应的访问密码。然后电子钥匙装置 701 向锁控单元 721 发送该访问密码，后者将它与其存储的访问密码进行对比。这个实施例的一个优点是，它不需要在电子钥匙装置 701 中存储用于不同特定区域的、大量的访问密码。

在图 7c 中，访问密码从访问密码管理系统 711 脱机传递到电子钥匙装置 701，并存放在其中的存储器中。在访问控制对话期间，电子钥匙装置 701 向锁控单元 721 发送一个选定的访问密码，后者然后联系访问密码管理系统 711，并把收到的访问密码向访问密码管理系统

711 发送。访问密码管理系统 711 执行核对并向锁控单元 721 发回一个回答，后者然后可以操作锁具。这个实施例的一个优点是，访问密码仅仅需要存放在访问密码管理系统 711 和电子钥匙装置 701 中。

在图 7d 中，访问密码从访问密码管理系统 711 脱机传递到锁控单元 721。在访问控制对话期间，电子钥匙装置 701 向访问密码管理系统 711 发送一个请求，申请一个选定的访问权，管理系统核对电子钥匙装置 701 的标识并向锁控单元 721 发送一个对应的访问密码。锁控单元 721 与存储的访问密码进行核对。

在图 7e 中，访问密码从访问密码管理系统 711 同时脱机传递到锁控单元 721 和电子钥匙装置 701。在访问控制对话期间，电子钥匙装置 701 向访问密码管理系统 711 传送一个选定的访问密码，后者可能在第一个核对过程之后，将该访问密码传送到锁控单元 721，它再与存储的访问密码进行对比。另外，在锁控单元 721 中的最终核对可以省略，在这种情况下访问密码仅仅需要存放在访问密码管理系统 711 中。

应当理解，依据本发明，可能有其它的数据流或以上数据流的组合。

图 8a 和图 8b 显示了依据本发明的两个实施例的软件架构实例。

参考图 8a，电子钥匙装置 801 的应用程序软件存放在存储器中，并在电子钥匙装置 801 的处理单元上执行，正如连同图 5a 和图 5b 中展示的实施例所介绍的，其中显示了存储器 507a 和处理单元 508。应用程序软件最好包括访问密码输入模块 865，它接收用户通过袖珍键盘输入的访问密码，并将访问密码存放在访问密码寄存器 861 中，它最好实际上位于存储器 507 的 RAM 部分 507b 中。访问密码检索模块 862 从访问密码寄存器检索选定的访问密码，并将它们显示在显示屏 502 上，或者将它们传送到访问密码传输模块 863 中，它控制着选定的访问密码向锁控单元 821 的传输。应用程序软件可能进一步包括日志模块 864，最好是带有通向访问密码输入模块 865 和访问密码传输模块 863 两者的接口。日志模块 864 可以在存储器中存放有关的日志

数据，比如哪个访问密码何时存放、改变或删除，或者哪个访问密码何时传送到哪个锁控单元的有关信息。

在锁控单元 821 的处理单元上执行的软件组件存放在锁控单元 821 的存储器中，正如连同图 2a 至图 2c 所示的锁控单元实施例所说明的，其中显示了存储器 223 和处理单元 222。锁控单元 821 的软件组件包括访问密码输入模块 876，用于接收用户通过用户接口 226 或其它输入装置输入的访问密码数据。访问密码输入模块 875 将访问密码数据存放在存储器 223 中的访问密码寄存器 871 中。

锁控单元 821 进一步包括访问密码接收模块 873，它接收电子钥匙装置 801 发送的访问密码。访问密码接收模块 873 作为访问密码核对模块 872 的接口，后者负责核对收到的访问密码。访问密码核对模块 872 进一步访问访问密码寄存器 871，以便检索存储的访问密码，并将它们与收到的访问密码进行对比。

访问密码核对模块 872 进一步作为锁控模块 874 的接口，以便向锁控模块 874 传送核对结果的有关信息。锁控模块 874 产生控制信号，该信号发送到锁具（未显示）处并启动锁具的操作。

锁控单元 821 的软件也可以包括日志模块 875，负责记录有关的数据和事件，并将日志事件存放在存储器 223 中。

现在参考图 8b，依据本发明的访问控制系统软件组件的第二个实施例还包括访问密码管理系统 811 的软件，正如连同图 2b 和图 2c 所介绍的。访问密码管理系统 811 的软件包括访问密码生成模块 812，负责依据批准的访问权产生访问密码。图 4 中显示了访问密码可能的数据格式的一个实例。访问密码生成模块 812 将产生的访问密码传送到访问密码管理模块 814，它负责管理访问密码，也就是将它们与相关数据一起存放在数据库 815 中，这些数据是关于有关的电子钥匙装置、锁控对应、特定区域、访问权拥有者、访问权受让人等等。访问密码管理模块 814 最好提供适当的用户接口，以便输入和观察相关的数据。不仅如此，访问密码管理模块 814 还可以应付附加的管理任务，比如访问密码的自动过期、启动访问密码向电子钥匙装置和/或锁控单

元传输。访问密码管理模块 814 作为访问密码传输模块 813 的接口，后者按照请求将访问密码向电子钥匙装置和/或锁控单元传输，例如通过实现通讯所用的分层通讯协议的一层或多层。

电子钥匙装置 801 的软件包括对应的访问密码下载模块 860，适于接收访问密码管理系统 811 传送的访问密码数据。同样，锁控单元 821 的软件也包括对应的访问密码下载模块 870。

访问密码管理系统 811 的软件进一步包括日志模块 817，它适于分别作为电子钥匙装置和锁控单元的日志模块 864、875 的接口。这个软件接口最好使用与访问密码传输相同的通讯接口，这个实施例的一个优点是，可以从电子钥匙装置 801 和/或锁控单元 821 向访问密码管理相同 811 在线传送日志数据。日志数据最好存放在访问密码管理相同 811 的数据库 815 中，电子钥匙装置 801 的其余组件 861-863 和锁控单元的组件 871-874，已经在上面连同图 8a 介绍过了。

访问密码管理系统 811 的软件可能进一步包括一个或多个附加的服务模块 816，它可以提供附加的服务，比如有关服务密码使用的统计，正如连同图 3 所介绍的。

访问密码管理系统 811 的功能最好能确保访问权持有者完全可见存储的、有关访问权的信息。为了获得最高级别的安全性，所有电子通讯都可以加密，或者由特定的协议，或者利用标准的加密方法，例如 RAS、数字签名、公钥证书等等。

为了管理电子钥匙，公司最好能够编制特殊的软件，以便对不同的供应商定制钥匙信息的管理，例如对本说明书开始所述的类型。定制的解决方案中也可以加入对所涉及的货物和服务供应商必需的、数据安全的等级。因此，可以设想在一座建筑物或一个公司中有几个安全级别，其中某些供应商仅仅需要通过第一级别，而其它供应商必需通过更高的安全级别。

访问密码管理系统 811 最好能够进一步包括一个或多个通向其它系统的接口 818，以便将访问密码管理系统 811 与其它服务结合和集成。这种集成可以允许访问权拥有者和/或访问权受让人从他们各自的

管理应用程序连接到访问密码管理系统 811，例如从一种 SAP 解决方案或者从另一种标准的或专有的基于计算机的管理系统内部进行连接。

集成服务也可以延伸到其它外部服务，比如 GPS 导航系统和 GIS 系统，其中锁控单元的特定区域和电子钥匙装置可以通过它们各自到访问密码管理系统 811 的通讯接口来定位。这又意味着依据本发明的访问控制系统 811 可以用于追踪移动物体的访问事件，比如容器、箱体、车辆等等。

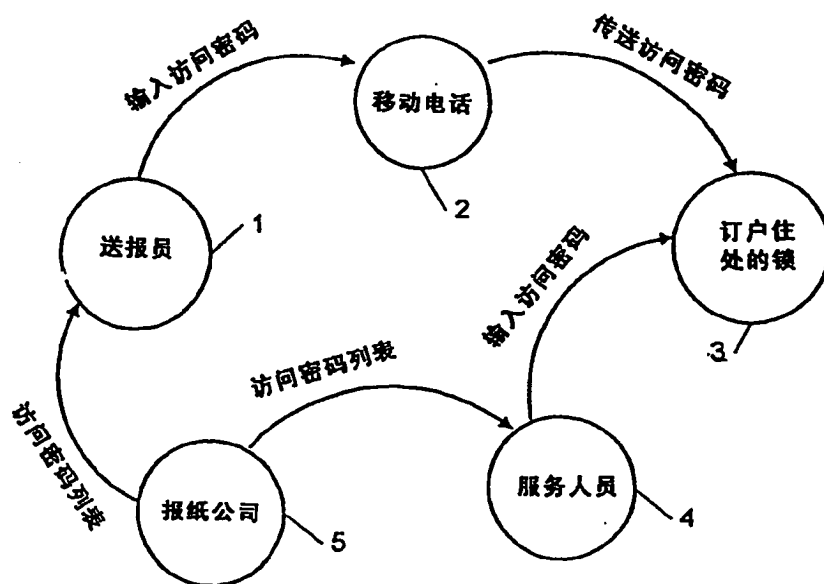


图 1a

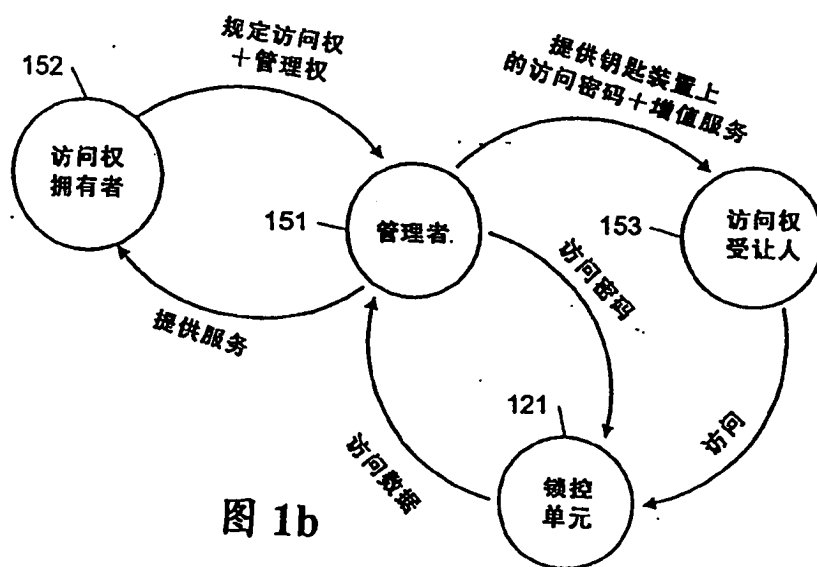
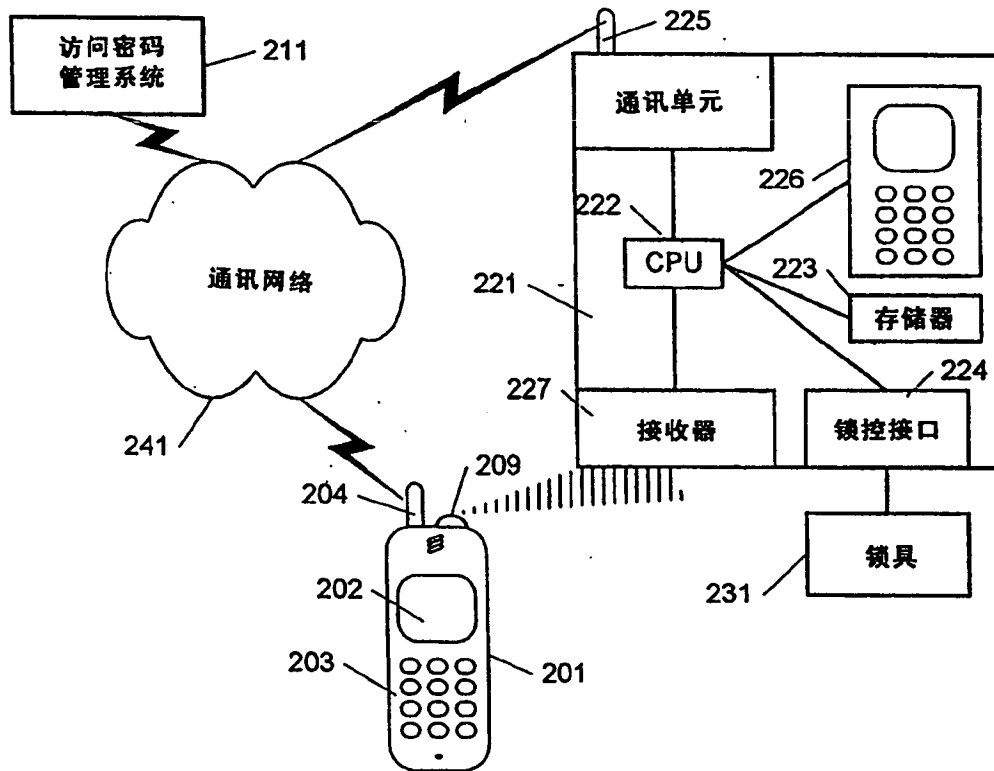
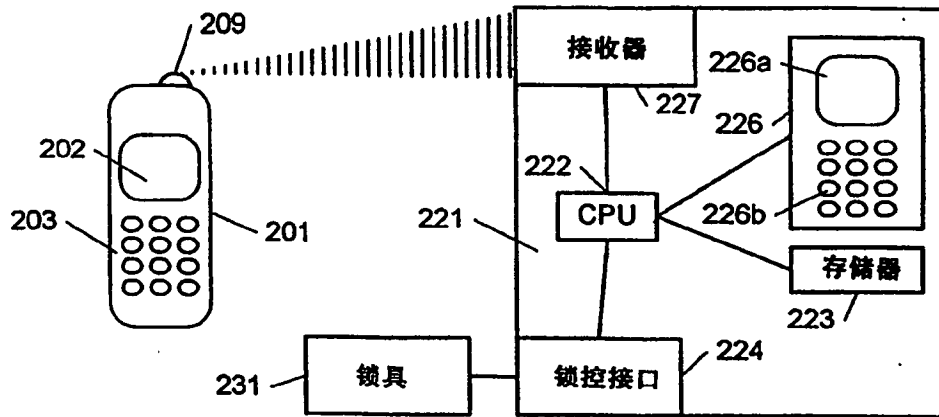


图 1b



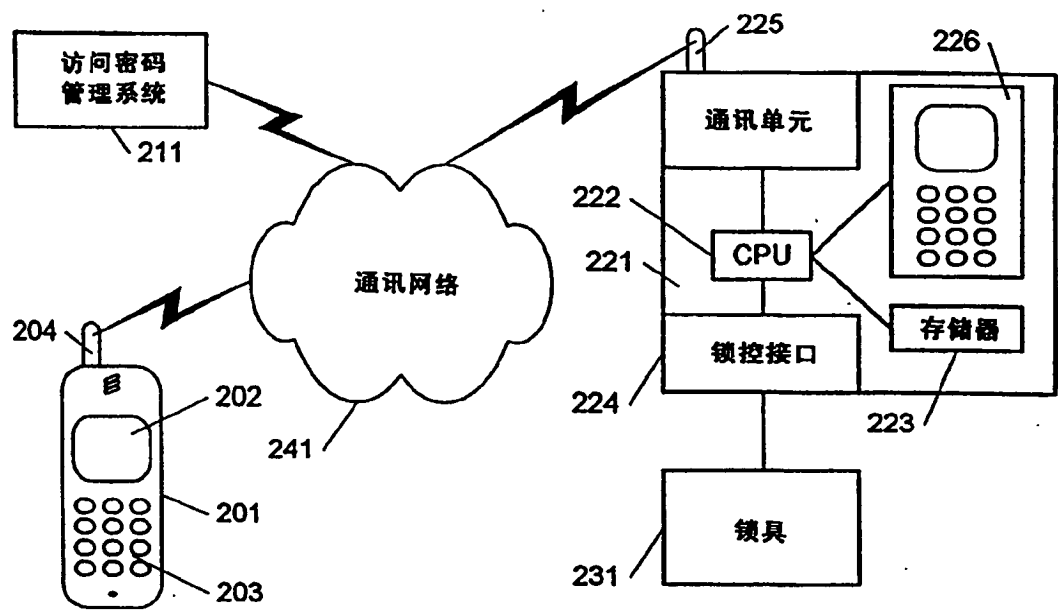


图 2c

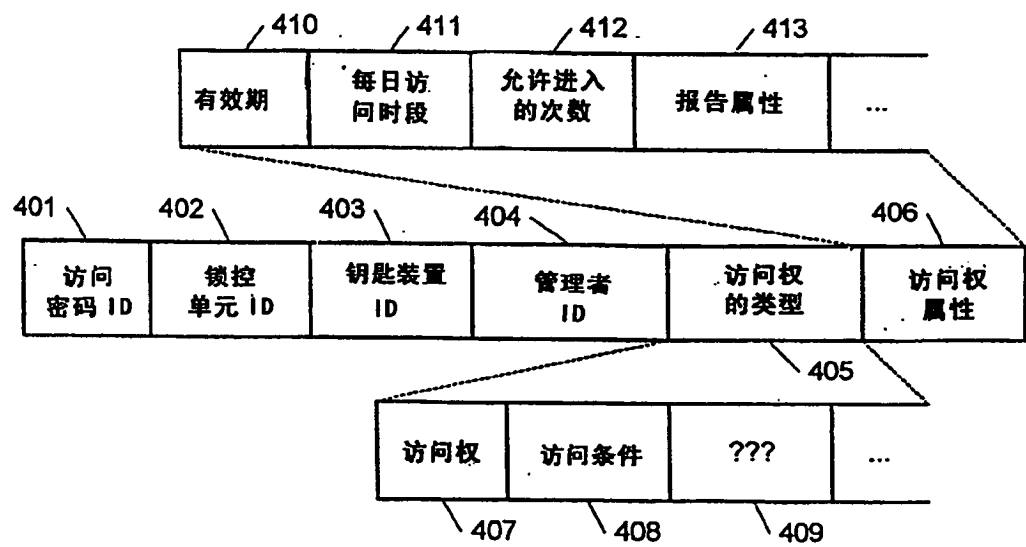


图 4

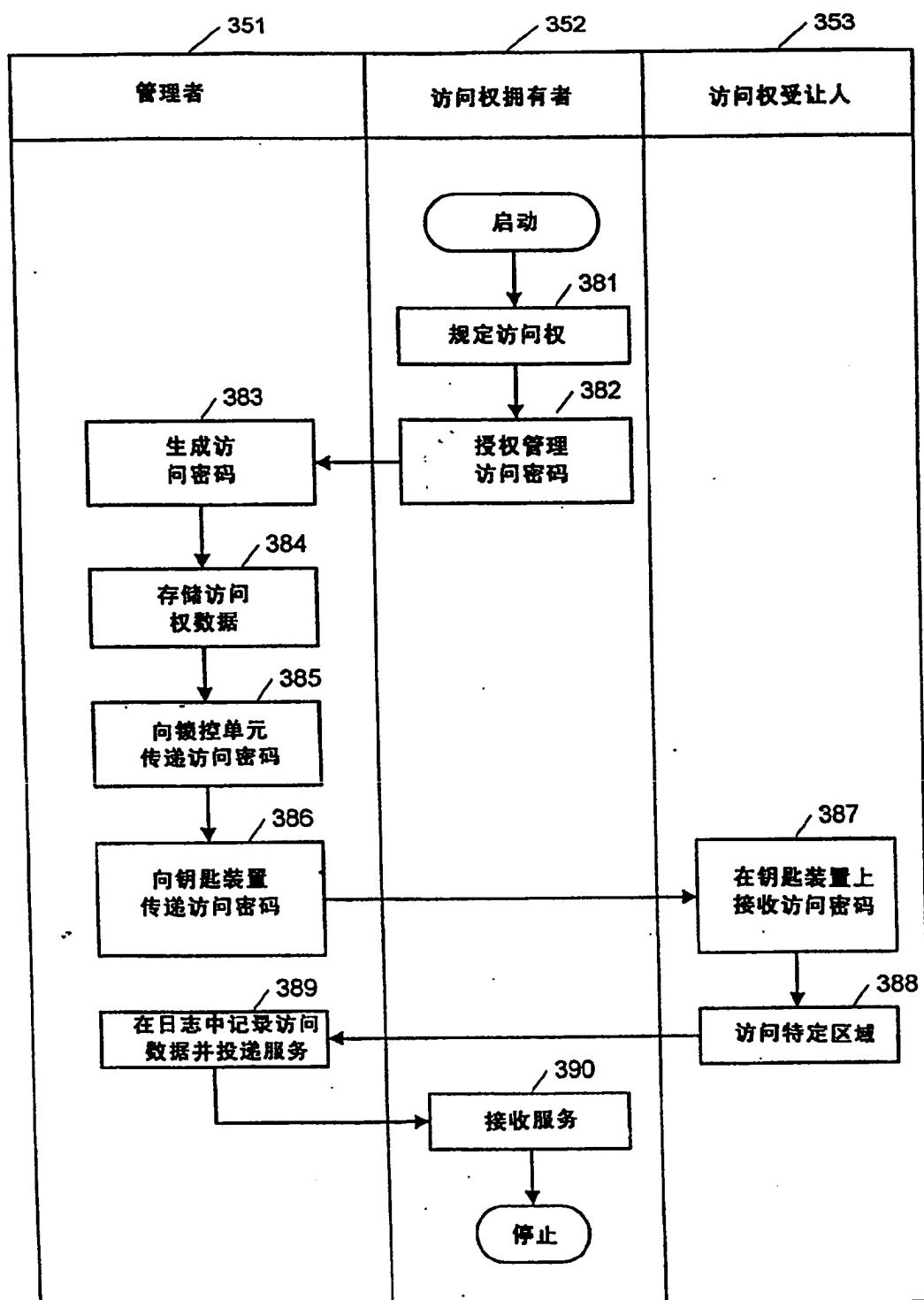
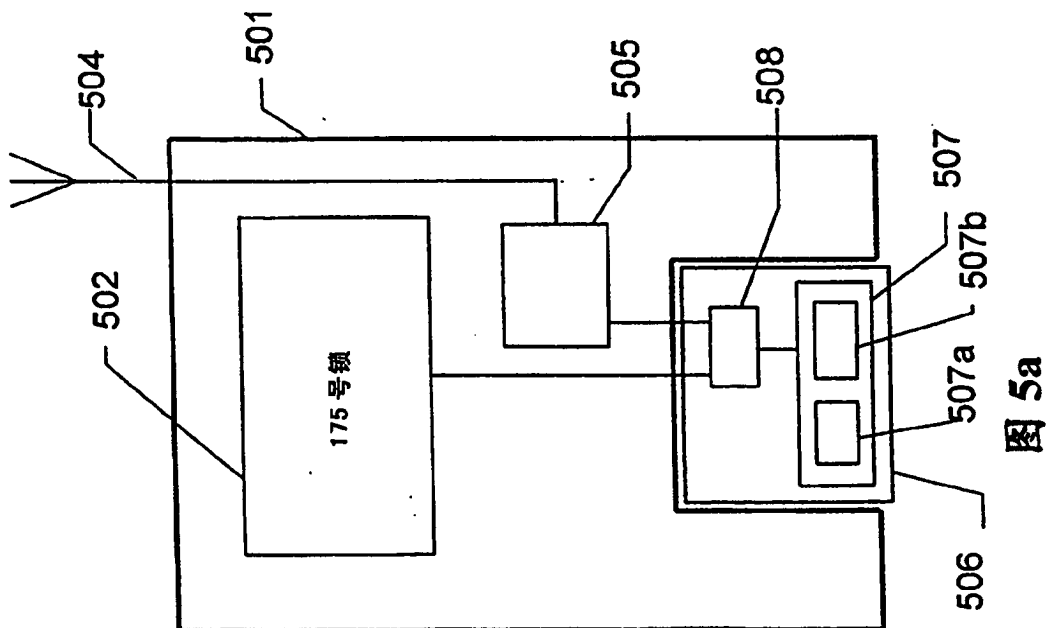
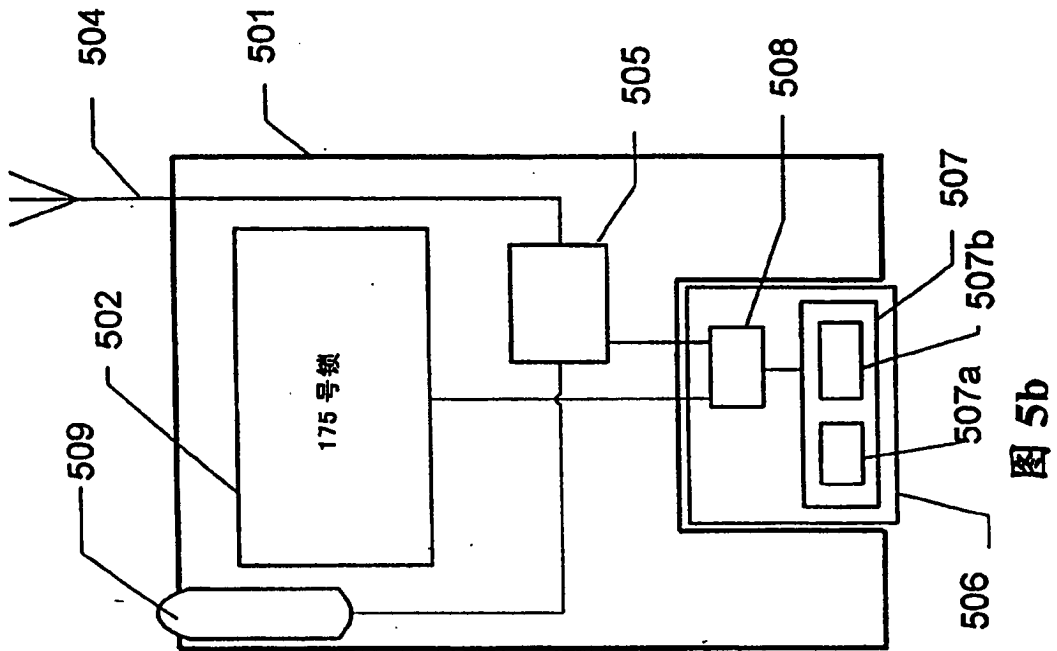


图 3



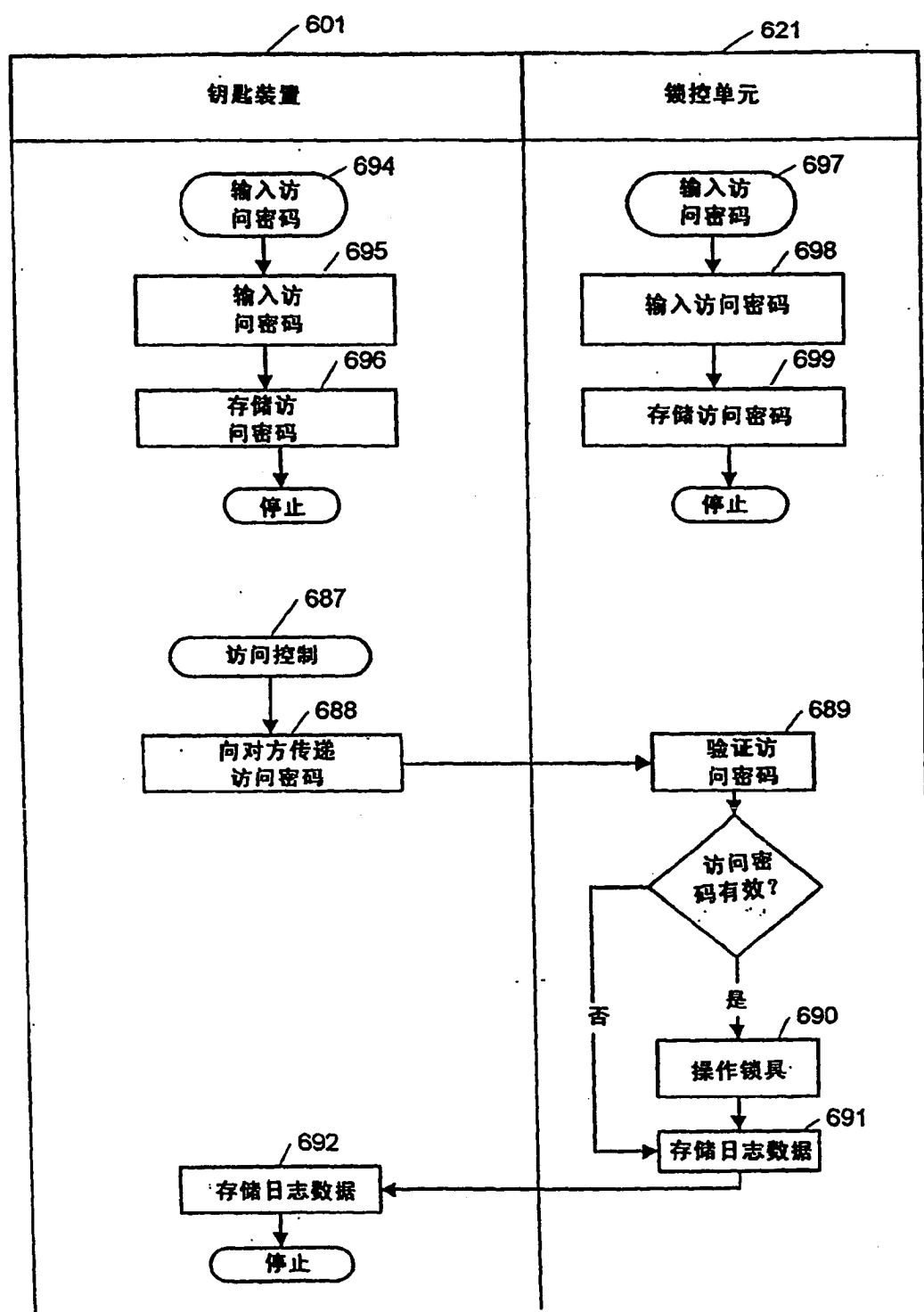


图 6a

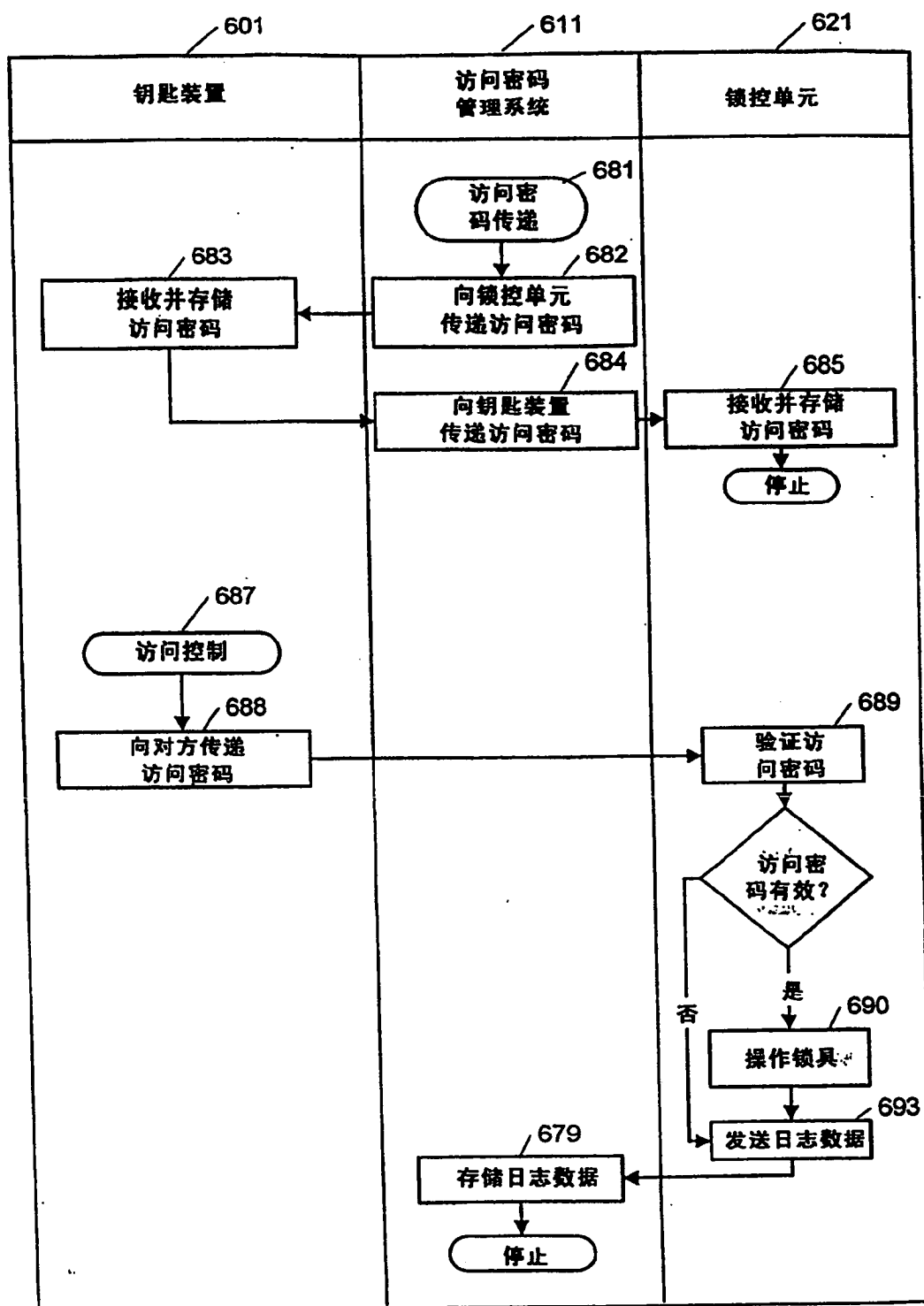


图 6b

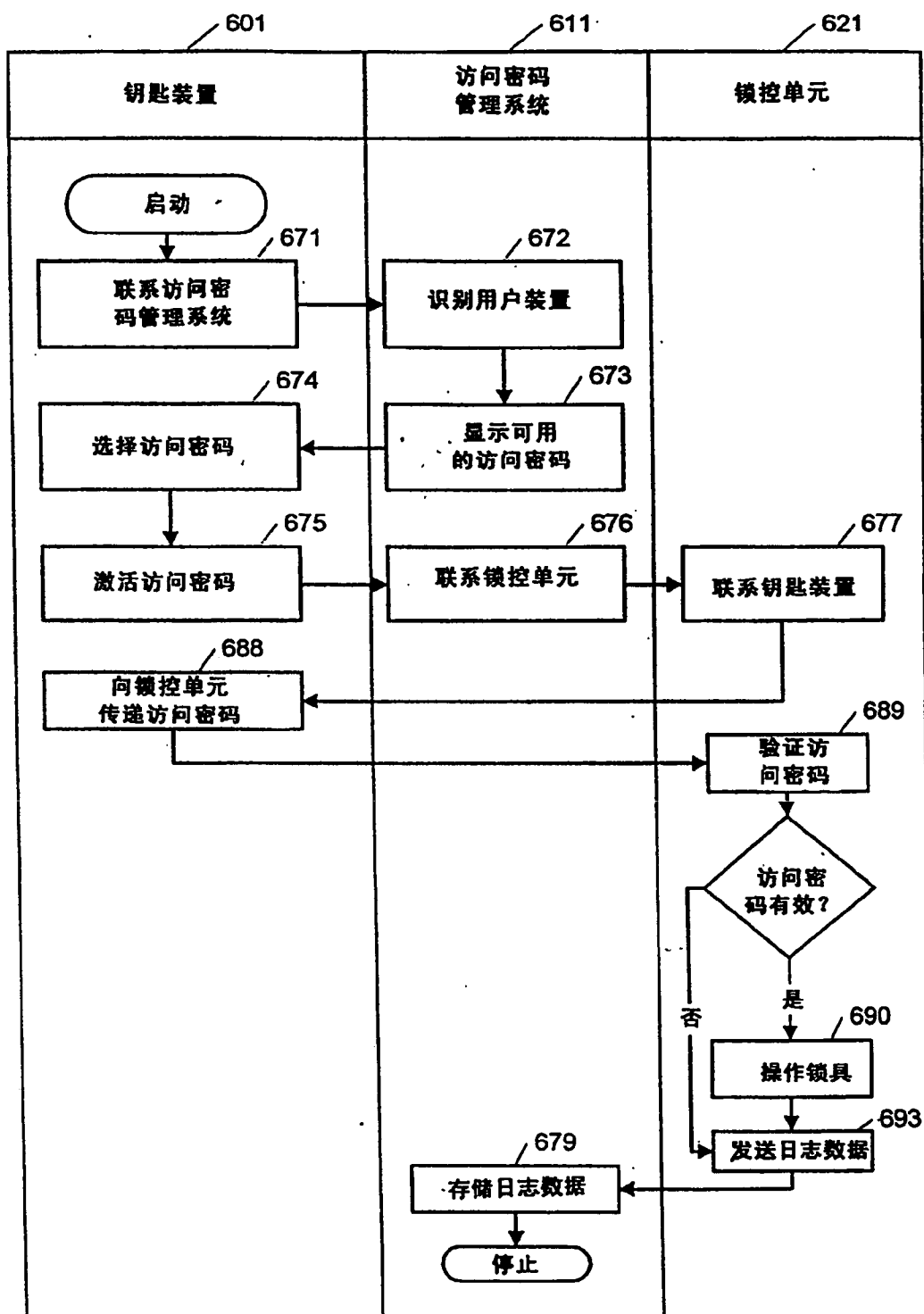
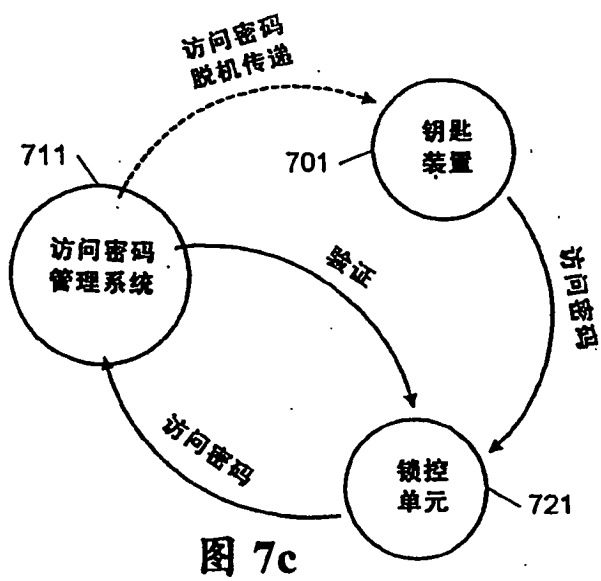
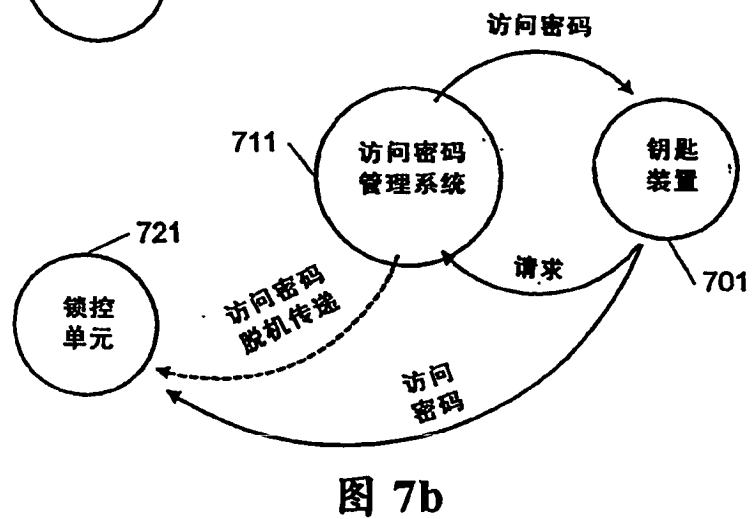
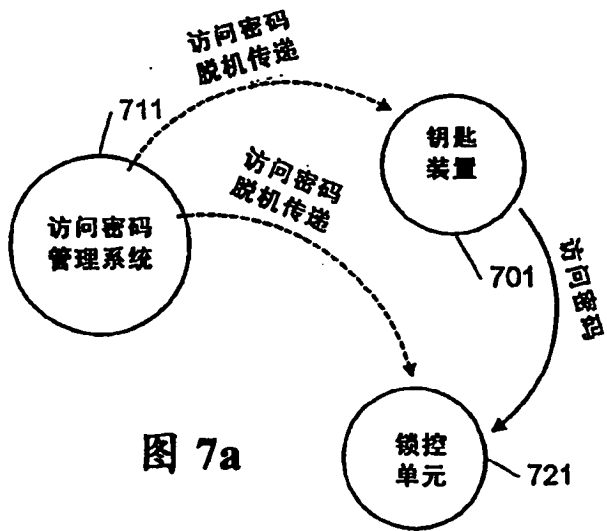


图 6c



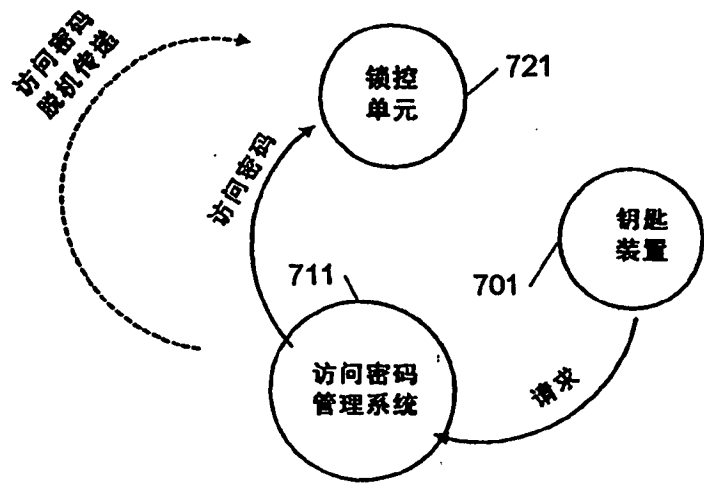


图 7d

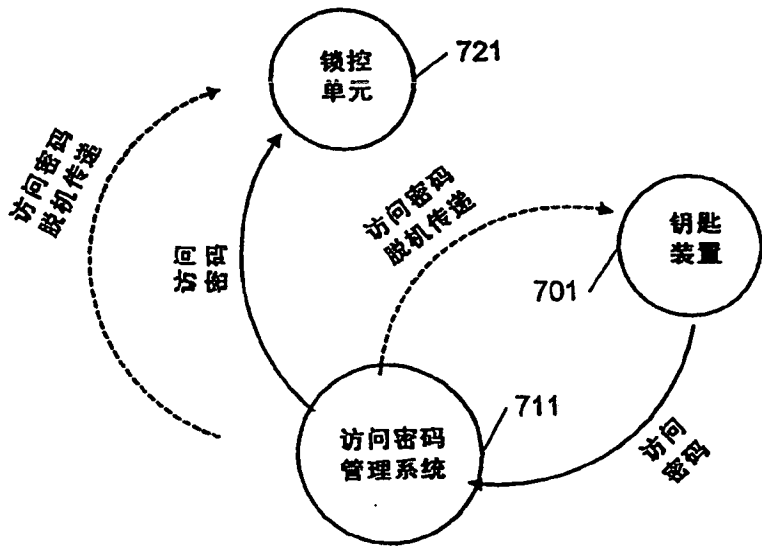


图 7e

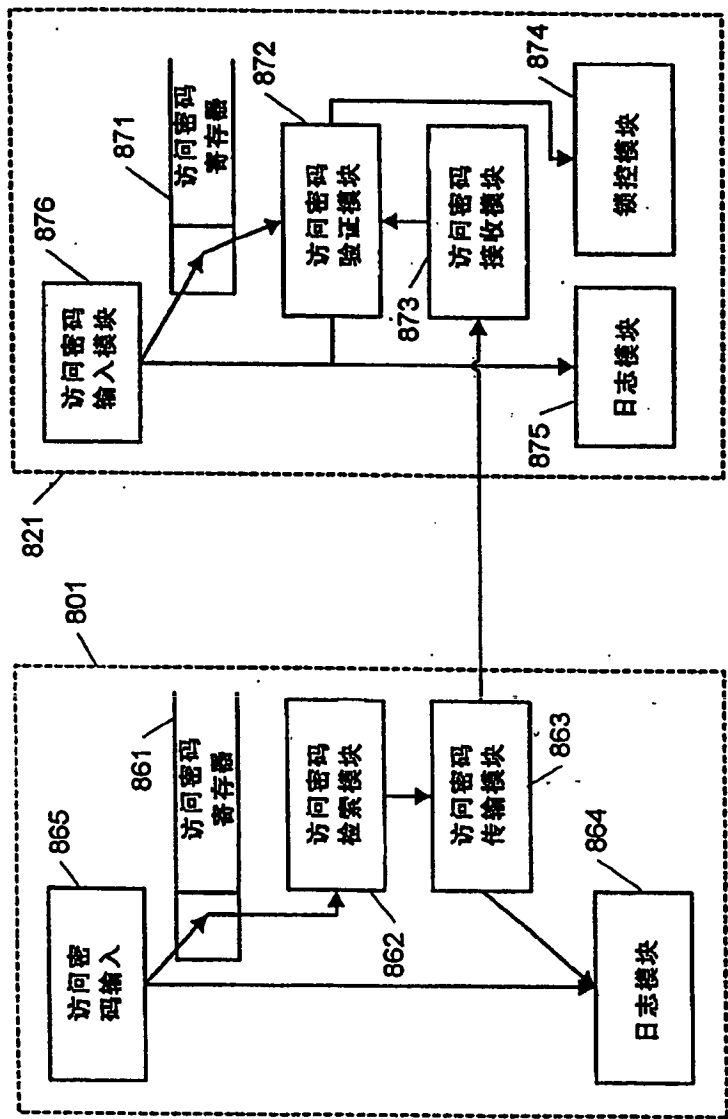


图 8a

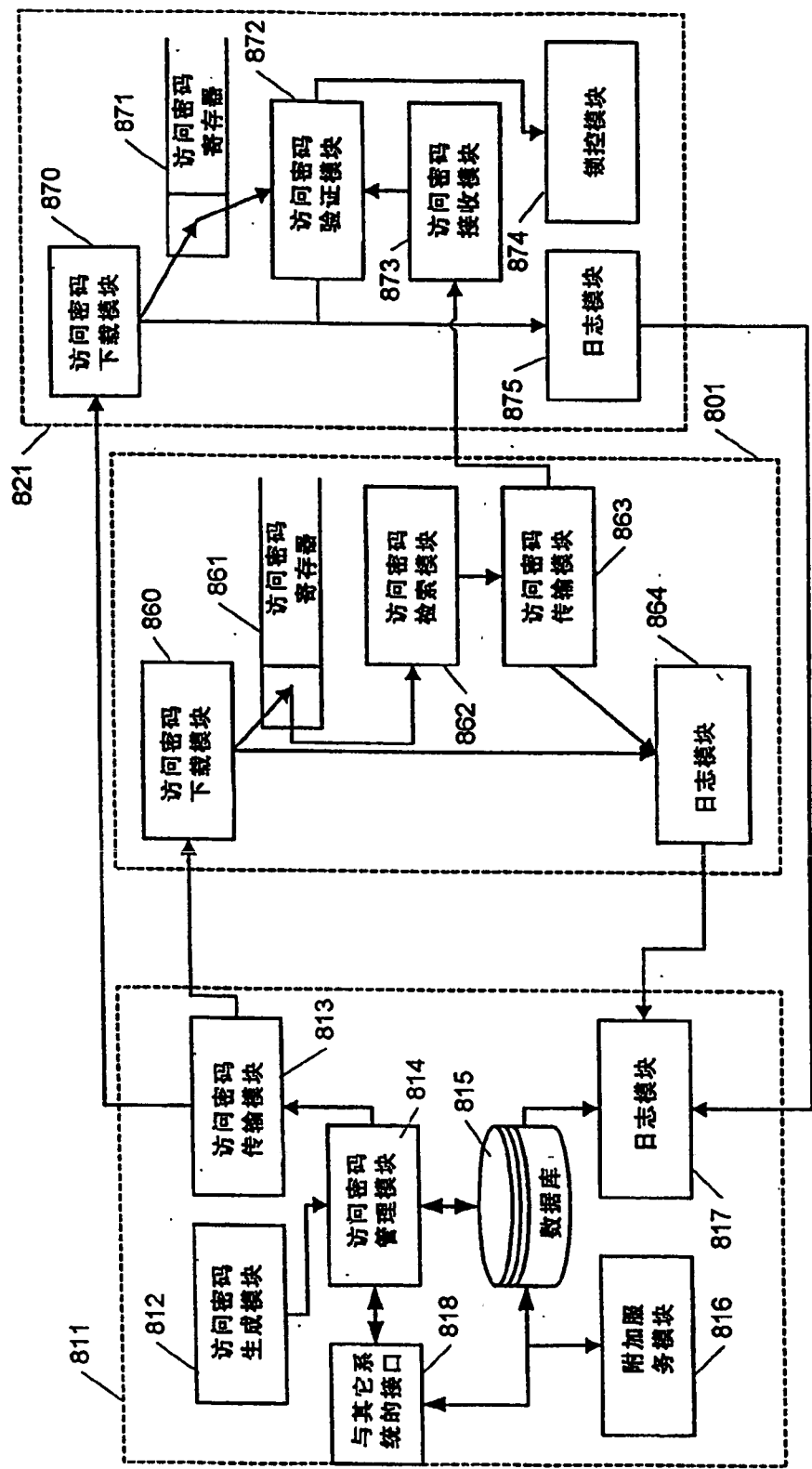


图 8b