(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105474275 A
(43)申请公布日 2016.04.06

(21)申请号 201480046840.X

(22)申请日 2014.08.06

(30)优先权数据
14/011,257 2013.08.27 US

(85)PCT国际申请进入国家阶段日
2016.02.24

(86)PCT国际申请的申请数据
PCT/US2014/049988 2014.08.06

(87)PCT国际申请的公布数据
WO2015/031011 EN 2015.03.05

(71)申请人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 奥利维尔·让·伯努瓦
法布里斯·让·赫尔纳

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛

(51)Int.Cl.
G07C 9/00(2006.01)
H04L 29/06(2006.01)
H04W 12/04(2006.01)
H04W 12/06(2006.01)
H04W 12/08(2006.01)
H04W 84/12(2006.01)
H04W 88/02(2006.01)

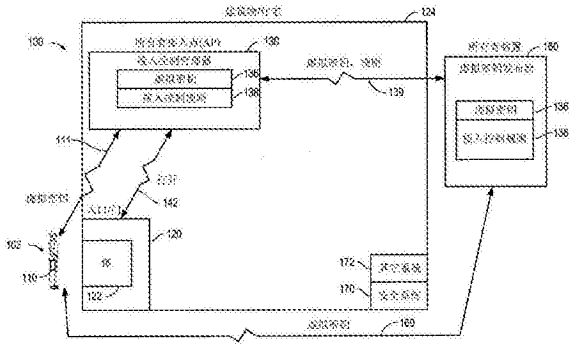
权利要求书5页 说明书9页 附图4页

(54)发明名称

用以控制对入口的解锁的所有者接入点

(57)摘要

本发明揭示一种用以通过所有者接入点(130)来控制针对具有无线装置(110)的访客对入口(120)进行解锁的方法、设备及系统。针对无线装置的虚拟密钥(136)及与所述虚拟密钥相关联的接入控制规则(138)可存储在所述所有者接入点处。所述所有者接入点(130)可确定从无线装置(110)接收的虚拟密钥是否匹配所述所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则。如果所述虚拟密钥匹配,且满足针对所述所存储的虚拟密钥的所述接入控制规则,那么所述所有者接入点可经由链路(142)将打开命令发射到所述入口(120)。



CN 105474275 A

1.一种用以通过所有者接入点来控制针对具有无线装置的访客对入口进行解锁的方法，其包括：

在所述所有者接入点处存储针对所述无线装置的虚拟密钥及与所述虚拟密钥相关联的接入控制规则；

确定从所述无线装置接收的虚拟密钥是否匹配所述所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，

那么将打开命令发射到所述入口。

2.根据权利要求1所述的方法，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

3.根据权利要求2所述的方法，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

4.根据权利要求1所述的方法，其中在所述无线装置中存储匹配的虚拟密钥。

5.根据权利要求1所述的方法，其中针对所述虚拟密钥的所述接入控制规则包含若干次的使用。

6.根据权利要求1所述的方法，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的时间周期的使用。

7.根据权利要求1所述的方法，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的天及时间的使用。

8.根据权利要求1所述的方法，其中当所述无线装置到达所述所有者接入点的范围内时，通过所述无线装置将所述虚拟密钥发射到所述所有者接入点，而不需要访客用户输入。

9.根据权利要求1所述的方法，其中如果所述无线装置与所述所有者接入点之间的链路被加密，那么将所述虚拟密钥从所述无线装置发射到所述所有者接入点。

10.根据权利要求1所述的方法，其进一步包括实施反中继攻击功能。

11.根据权利要求1所述的方法，其中如果所述无线装置与所述所有者接入点之间的链路未被加密，那么所述虚拟密钥用以与所述所有者接入点执行相互认证。

12.根据权利要求1所述的方法，其中所有者装置指派且发射所述虚拟密钥及针对所述虚拟密钥的所述接入控制规则。

13.根据权利要求1所述的方法，其进一步包括在将所述打开命令发射到所述入口之后停用安全系统。

14.一种所有者接入点，其包括：

接口；及

处理器，其用以执行包含以下各项的操作：

存储通过所述接口接收的针对无线装置的虚拟密钥及与所述虚拟密钥相关联的接入控制规则；

确定通过所述接口从无线装置接收的虚拟密钥是否匹配所述所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，

那么将打开命令发射到入口。

15.根据权利要求14所述的所有者接入点，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

16.根据权利要求15所述的所有者接入点，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

17.根据权利要求14所述的所有者接入点，其中匹配的虚拟密钥存储在所述无线装置中。

18.根据权利要求14所述的所有者接入点，其中针对所述虚拟密钥的所述接入控制规则包含若干次的使用。

19.根据权利要求14所述的所有者接入点，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的时间周期的使用。

20.根据权利要求14所述的所有者接入点，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的天及时间的使用。

21.根据权利要求14所述的所有者接入点，其中当所述无线装置到达所述所有者接入点的范围内时，所述虚拟密钥通过所述无线装置发射到所述所有者接入点，而不需要访客用户输入。

22.根据权利要求14所述的所有者接入点，其中如果所述无线装置与所述所有者接入点之间的链路被加密，那么所述虚拟密钥从所述无线装置发射到所述所有者接入点。

23.根据权利要求14所述的所有者接入点，其进一步包括实施反中继攻击功能。

24.根据权利要求14所述的所有者接入点，其中如果所述无线装置与所述所有者接入点之间的链路未被加密，那么所述虚拟密钥用以与所述所有者接入点执行相互认证。

25.根据权利要求14所述的所有者接入点，其中所有者装置指派且发射所述虚拟密钥及针对所述虚拟密钥的所述接入控制规则。

26.根据权利要求14所述的所有者接入点，其进一步包括在将所述打开命令发射到所述入口之后停用安全系统。

27.一种所有者接入点，其包括：

用于存储针对无线装置的虚拟密钥及与所述虚拟密钥相关联的接入控制规则的装置；

用于确定从无线装置接收的虚拟密钥是否匹配所述所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则的装置，及如果是，

用于将打开命令发射到入口的装置。

28.根据权利要求27所述的所有者接入点，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

29.根据权利要求28所述的所有者接入点，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

30.根据权利要求27所述的所有者接入点，其中针对所述虚拟密钥的所述接入控制规则包含若干次的使用。

31.根据权利要求27所述的所有者接入点，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的时间周期的使用。

32.根据权利要求27所述的所有者接入点，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的天及时间的使用。

33.根据权利要求27所述的所有者接入点，其中当所述无线装置到达所述所有者接入点的范围内时，所述虚拟密钥通过所述无线装置发射到所述所有者接入点，而不需要访客

用户输入。

34.根据权利要求27所述的所有者接入点，其中所有者装置指派且发射所述虚拟密钥及针对所述虚拟密钥的所述接入控制规则。

35.根据权利要求27所述的所有者接入点，其中如果所述无线装置与所述所有者接入点之间的链路未被加密，那么所述虚拟密钥用以与所述所有者接入点执行相互认证。

36.一种非暂时性计算机可读媒体，其包含当由所有者接入点执行时致使所述所有者接入点进行以下操作的代码：

存储针对无线装置的虚拟密钥及与所述虚拟密钥相关联的接入控制规则；

确定从无线装置接收的虚拟密钥是否匹配所述所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，

将打开命令发射到入口。

37.根据权利要求36所述的计算机可读媒体，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

38.根据权利要求37所述的计算机可读媒体，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

39.根据权利要求36所述的计算机可读媒体，其中针对所述虚拟密钥的所述接入控制规则包含若干次的使用。

40.根据权利要求36所述的计算机可读媒体，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的时间周期的使用。

41.根据权利要求36所述的计算机可读媒体，其中针对所述虚拟密钥的所述接入控制规则包含预先设置的天及时间的使用。

42.根据权利要求36所述的计算机可读媒体，其中当所述无线装置到达所述所有者接入点的范围内时，所述虚拟密钥通过所述无线装置发射到所述所有者接入点，而不需要访客用户输入。

43.根据权利要求36所述的计算机可读媒体，其中所有者装置指派且发射所述虚拟密钥及针对所述虚拟密钥的所述接入控制规则。

44.根据权利要求36所述的计算机可读媒体，其中如果所述无线装置与所述所有者接入点之间的链路未被加密，那么所述虚拟密钥用以与所述所有者接入点执行相互认证。

45.一种用于向具有无线装置的访客发布虚拟密钥的方法，其包括：

针对访客的无线装置发布虚拟密钥；

向所述虚拟密钥指派接入控制规则；

将所述虚拟密钥发射到所述访客的无线装置；及

将所述虚拟密钥和所述接入控制规则发射到所有者接入点。

46.根据权利要求45所述的方法，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

47.根据权利要求46所述的方法，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

48.根据权利要求45所述的方法，其中针对所述虚拟密钥的所述接入控制规则包含以下各项中的至少一者：若干次的使用、预先设置的时间周期的使用或者预先设置的天和时

间的使用。

49.根据权利要求45所述的方法，其中当所述无线装置到达所述所有者接入点的范围内时，通过所述无线装置将所述虚拟密钥发射到所述所有者接入点，而不需要访客用户输入，且所述所有者接入点确定从所述无线装置接收的所述虚拟密钥是否匹配所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，那么将打开命令发射到所述入口。

50.一种所有者装置，其包括：

接口；及

处理器，其用以执行包含以下各项的操作：

针对访客的无线装置发布虚拟密钥；

向所述虚拟密钥指派接入控制规则；

命令通过所述接口将所述虚拟密钥发射到所述访客的无线装置；及

命令将所述虚拟密钥和所述接入控制规则发射到所有者接入点。

51.根据权利要求50所述的所有者装置，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

52.根据权利要求51所述的所有者装置，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

53.根据权利要求50所述的所有者装置，其中针对所述虚拟密钥的所述接入控制规则包含以下各项中的至少一者：若干次的使用、预先设置的时间周期的使用或者预先设置的天和时间的使用。

54.根据权利要求50所述的所有者装置，其中当所述无线装置到达所述所有者接入点的范围内时，所述虚拟密钥通过所述无线装置发射到所述所有者接入点，而不需要访客用户输入，且所述所有者接入点确定从所述无线装置接收的所述虚拟密钥是否匹配所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，那么将打开命令发射到所述入口。

55.一种所有者装置，其包括：

用于针对访客的无线装置发布虚拟密钥的装置；

用于向所述虚拟密钥指派接入控制规则的装置；

用于将所述虚拟密钥发射到所述访客的无线装置的装置；及

用于将所述虚拟密钥和所述接入控制规则发射到所有者接入点的装置。

56.根据权利要求55所述的所有者装置，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

57.根据权利要求56所述的所有者装置，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

58.根据权利要求55所述的所有者装置，其中针对所述虚拟密钥的所述接入控制规则包含以下各项中的至少一者：若干次的使用、预先设置的时间周期的使用或者预先设置的天和时间的使用。

59.根据权利要求55所述的所有者装置，其中当所述无线装置到达所述所有者接入点的范围内时，所述虚拟密钥通过所述无线装置发射到所述所有者接入点，而不需要访客用

户输入，且所述所有者接入点确定从所述无线装置接收的所述虚拟密钥是否匹配所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，那么将打开命令发射到所述入口。

60.一种非暂时性计算机可读媒体，其包含当由所有者装置执行时致使所述所有者装置执行以下操作的代码：

针对访客的无线装置发布虚拟密钥；

向所述虚拟密钥指派接入控制规则；

将所述虚拟密钥发射到所述访客的无线装置；及

将所述虚拟密钥和所述接入控制规则发射到所有者接入点。

61.根据权利要求60所述的计算机可读媒体，其中所述虚拟密钥包含无线局域网络WLAN证书及认证证书中的至少一者。

62.根据权利要求61所述的计算机可读媒体，其中所述WLAN证书包含识别符，且所述认证证书包含密码。

63.根据权利要求60所述的计算机可读媒体，其中针对所述虚拟密钥的所述接入控制规则包含以下各项中的至少一者：若干次的使用、预先设置的时间周期的使用或者预先设置的天和时间的使用。

64.根据权利要求60所述的计算机可读媒体，其中当所述无线装置到达所述所有者接入点的范围内时，所述虚拟密钥通过所述无线装置发射到所述所有者接入点，而不需要访客用户输入，且所述所有者接入点确定从所述无线装置接收的所述虚拟密钥是否匹配所存储的虚拟密钥及是否满足针对所述所存储的虚拟密钥的所述接入控制规则，且如果是，那么将打开命令发射到所述入口。

用以控制对入口的解锁的所有者接入点

技术领域

[0001] 本发明涉及用以当访客具有在所有者接入点的范围内的无线装置和适当数字密钥和权限时，修改所有者系统的状态(例如，对入口的解锁)的方法、设备和系统。

背景技术

[0002] 允许访客打开锁闭的门或入口方式的现有程序需要使用机械密钥、PIN码到键盘的入口或使用近场通信(NFC)密钥。目前这些程序中的每一者均包含各种不利问题。

[0003] 例如，待由访客使用的机械密钥可在任何时候使用，可能会丢失或复制，且需要实际地给到访客(例如，雇佣人员、管家、医务助理等)。

[0004] 关于使用PIN码(例如，与使用数字键盘的门锁一起使用)，密钥码可能很容易被忘记，且可与未授权的人一起共享，这两者都有问题。另外，为了改变代码，门需要实际被接入。此外，保持跟踪用于许多门的代码是有困难的。

[0005] 关于使用NFC密钥(例如，用使用NFC技术的门锁)，NFC密钥通常以物理NFC令牌的形式起作用，且具有许多与机械密钥相关联的相同问题(例如，可能丢失、被复制等)。此外，以数字令牌形式起作用的NFC密钥通常需要使用NFC启用的智能电话，且需要用户去拿智能手机，且触摸门以便打开它。

[0006] 所有目前这些程序均需要所有者进行高度密钥管理，且牵涉到访客进行的难办的解锁步骤。

发明内容

[0007] 本发明的方面可涉及一种用以通过所有者接入点来控制对针对具有无线装置的访客的入口进行解锁的方法、设备及系统。针对无线装置的虚拟密钥及与虚拟密钥相关联的接入控制规则可存储在所有者接入点处。所有者接入点可确定从无限装置接收的虚拟密钥是否匹配所存储的虚拟密钥及是否满足针对所存储的虚拟密钥的接入控制规则。如果所述虚拟密钥匹配，且满足针对所存储的虚拟密钥的接入控制规则，所有者接入点可将打开命令发射到入口。

附图说明

[0008] 图1是其中可实践本发明的实施例的系统的实例的图。

[0009] 图2是说明本发明的实施例的组件的图。

[0010] 图3是说明由所有者AP实施的过程的实例的流程图。

[0011] 图4是说明由所有者装置实施的过程的实例的流程图。

[0012] 图5是说明接入控制规则的实例类型的表格。

具体实施方式

[0013] 词语“示范性”或“实例”在本文中用来指“充当实例、例子或说明”。本文中描述为

“示范性”或“实例”的任何方面或实施例不是必须解释为比其它方面或实施例优选或者有利。

[0014] 本发明的实施例提供用以通过所有者接入点(AP)来控制对针对具有无线装置的访客的入口进行解锁的方法。在一个实施例中，所有者AP存储针对特定无线装置定义的虚拟密钥及针对所述虚拟密钥的接入控制规则。虚拟密钥及针对所述虚拟密钥的接入控制规则从所有者装置发布且从所有者装置发射到所有者AP。在一个实施例中，所有者装置可包含虚拟密钥发布器，其发布针对访客无线装置的虚拟密钥，且使针对访客无线装置的虚拟密钥的接入控制规则相关联，以使得带有具有适当虚拟密钥且满足预定义的接入控制规则的无线装置的访客可通过使入口由所有者AP打开而被授权接入。可在检测和认证访客的无线装置而无任何用户交互作用时对入口(例如，建筑物的门)进行解锁。例如，不必在小键盘上键入PIN码或者利用NFC密钥且使用NFC启用的智能手机接触门等。

[0015] 参看图1，说明其中可实践本发明的实施例的环境100的实例。例如，通过利用所有者接入点(AP)130来实现用以控制对针对具有无线装置110的访客102的建筑物124(例如，住宅)的入口120(例如，门)进行解锁的系统和方法。

[0016] 在一个实施例中，所有者AP 130存储针对特定访客无线装置的虚拟密钥136及与虚拟密钥相关联的接入控制规则138。特定来说，所有者AP 130可具有存储针对多种不同的访客无线装置的多个虚拟密钥136及相关联的接入控制规则138的接入控制管理器应用程序。如将要描述的，所有者装置160具有发布由所有者AP 130存储的虚拟密钥及针对所述虚拟密钥的相关联的接入控制规则的虚拟密钥发布器应用程序。特定来说，所有者装置160的虚拟密钥发布器应用程序可定义针对访客无线装置的虚拟密钥及与所述虚拟密钥相关联的接入控制规则，以使得带有具有适当虚拟密钥且满足预定义的接入控制规则的无线装置110的访客102可通过经由链路142从所有者AP 130发送的打开命令使入口120解锁(例如，对锁122进行解锁)而被授权接入。

[0017] 例如，当具有访客无线装置110的访客102靠近建筑物124的入口120时，虚拟密钥可经由无线链路111发射到所有者AP 130，且在接入控制管理器应用程序控制之下的所有者AP 130可确定从访客无线装置110接收的虚拟密钥是否匹配针对无线装置存储的虚拟密钥136，及是否匹配针对虚拟密钥存储的接入控制规则138，且如果是，那么所有者AP 130经由链路142发射打开命令(其对锁122进行解锁)，且允许通过访客102打开入口120。同样，在一个实施例中，虚拟密钥的所有权证明可通过访客无线装置110发射到所有者AP 130，且所有者AP 130可确定从访客无线装置110接收的虚拟密钥的所有权证明是否经验证，且如果是，那么所有者AP 130经由链路142发射打开命令(其对锁122进行解锁)，并允许由访客102打开入口120。

[0018] 结合图1额外参看图2，下文将描述实例实施例。应了解，访客无线装置110可为任何类型的无线装置。访客无线装置110可包含处理器112、存储器114、接口116、传感器117、显示器装置118及接口119。处理器112可经配置以执行下文将描述的操作。特定来说，处理器112可实施虚拟密钥容器应用程序113，虚拟密钥容器应用程序113控制存储在存储器114中的虚拟密钥115的使用和存储。存储器114可存储这些应用、程序、例行程序等，以实施这些操作和功能以及虚拟密钥115。

[0019] 访客无线装置110还可包含一般装置特征，例如显示器装置118、用户接口119(例

如，键盘，小键盘、触摸屏幕输入等)以及网络接口116。访客无线装置110可包含多种不同类型的I/F 116，以用于经由无线网络(例如，WLAN、蜂窝网络等)进行无线通信。例如，访客无线装置110可包含可与蜂窝网络进行通信的蜂窝式收发器(例如，包含发射器和接收器)。访客无线装置110可包含无线局域网络(WLAN)I/F 116(例如，包含无线收发器的合适无线调制解调器，无线收发器包含无线接收器和发射器)以经由WLAN接收和发射数据。在一个特定实施例中，I/F 116可经由WLAN与所有者AP 130和所有者装置160进行通信，如下文将描述。

[0020] 访客无线装置110还可包含传感器117，传感器117包含接近传感器、运动传感器、加速器传感器、位置传感器、定位传感器、压力传感器、麦克风、相机、声音传感器、光传感器等。

[0021] 应了解，访客无线装置110可为具有无线能力的任何类型的计算装置，例如：智能手机、蜂窝手机、平板计算机、个人数字助理、个人计算机、桌上型计算机、膝上型计算机、移动计算机、移动装置、无线手机、机器对机器(M2M)装置，或任何类型的包含无线能力的计算装置。

[0022] 另外，如图2中特定显示，所有者AP 130可包含处理器132以实施接入控制管理器应用程序133，以实施下文将描述的操作，以及存储器134以存储虚拟密钥136及从所有者装置160接收的接入控制规则138。所有者AP 130还可包含无线I/F 131以无线地与访客无线装置110及所有者装置160进行通信。所有者AP 130可为Wi-Fi类型的WLAN装置或任何种类的WLAN装置、接入点等。

[0023] 类似地，所有者装置160可包含处理器162以实施虚拟密钥发布器应用程序163，如下文将描述的，以及存储器164以存储虚拟密钥166及接入控制规则168。另外，所有者装置160可包含无线I/F 161以便与所有者AP 130及访客无线装置110进行通信。应了解，所有者装置160可为任何类型的具有无线能力的计算装置(例如，智能手机、平板计算机、膝上型计算机、个人计算机等)。应了解，术语所有者装置或所有者计算装置并不是关于执行这些功能的装置类型的限制。例如，所有者装置的虚拟密钥发布器可在网络服务器上运行，所述网络服务器由所有者经由所有者装置上的应用或浏览器接入。以相同方式，无线装置110和所有者AP 130可为任何种类的具有无线能力的计算装置。然而，应了解，在某些实施例中，虚拟密钥和接入控制规则的发射不必须是无线的，而是可经由有线或经由方向连接实施。

[0024] 参看特定实施方案，在一个实施例中，所有者AP 130在接入控制管理器应用程序133的控制之下，可存储针对特定访客无线装置的虚拟密钥136和与虚拟密钥136相关联的接入控制规则138。虚拟密钥136和相关联的接入控制规则138可由虚拟密钥发布器160定义和发布，且经由链路139无线发射到所有者AP 130。类似地，所发布的虚拟密钥136可经由链路169无线地发射到访客的无线装置169。这可经由WLAN链路(或经由直接有线链路——非无线地)本地完成，或经由蜂窝链路非本地完成。

[0025] 当具有访客无线装置110的访客102在虚拟密钥容器应用程序113控制之下密切接近所有者AP 130时，访客无线装置110变得与所有者AP相关联，且经由无线链路111将虚拟密钥(或对所述虚拟密钥的了解的证明)安全地发射到所有者AP 130。所有者AP 130在接入控制管理器应用程序133的控制之下确定从访客无线装置110接收的虚拟密钥是否匹配针对无线装置存储的虚拟密钥136，及是否满足与所存储的虚拟密钥相关联的接入控制规则138(例如，正确的天和时间)，且如果是，所有者AP 130经由链路142将打开命令发射到入口

120，以使得锁122被解锁，且访客可进入建筑物124。

[0026] 所有者装置160的虚拟密钥发布器应用程序163可针对特定访客无线装置发布虚拟密钥136，且定义待与虚拟密钥136相关联的接入控制规则138，使得带有具有合适虚拟密钥且满足相关联的接入控制规则(例如，正确的天和时间)的无线装置的访客可通过所有者AP 130使入口120打开而被授权接入。例如，利用所有者装置160、操作虚拟密钥发布器应用程序163的所有者可针对特定访客无线装置定义和发布虚拟密钥136，且可经由无线链路169将虚拟密钥136发射到特定访客无线装置110，其中虚拟密钥136可存储在存储器114中。此外，用于所述访客无线装置的针对虚拟密钥136定义的接入控制规则138联合虚拟密钥136可经由无线链路139发射到所有者AP 130，其中接入控制规则138和虚拟密钥136可存储在存储器134中。

[0027] 以此方式，当具有访客无线装置110的访客102足够接近所有者AP 130，使得访客无线装置110经由链路111将虚拟密钥115发射到所有者AP 130时，所有者AP 130确定从访客无线装置110接收的虚拟密钥136是否匹配针对所述无线装置110存储的虚拟密钥136，及是否满足针对所述虚拟密钥存储的相关联的接入控制规则138(例如，正确的天和时间)。如果满足这些要求，那么所有者AP 130可经由链路142发射打开命令，使得通过对锁122进行解锁而针对访客打开入口120。然而，应了解，虚拟密钥115不是必须从访客无线装置110发射到所有者AP 130。虚拟密钥的发射可取决于链路111是否被加密。例如，在一个实施例中，如果链路未被加密，那么可在相互认证过程中使用虚拟密钥115，例如基于密码的认证方案或基于秘密密钥的认证方案(例如，挑战响应)以及基于公共密钥的认证。虚拟密钥的目的是对访客进行认证。

[0028] 在一个实施例中，虚拟密钥136可包含无线局域网络(WLAN)证书及认证证书中的至少一者。例如，WLAN证书可包含识别符(例如，AP识别符)，且认证证书可包含密码。如更特定的实例，WLAN证书可为Wi-Fi证书(例如，访客服务集识别符(SSID)、MAC地址、口令短语等)。另外，与虚拟密钥136相关联的各种接入控制规则138可由所有者装置的所有者经由所有者装置160的虚拟密钥发布器应用程序163定义。这些接入控制规则的实例包含：若干次的使用(例如，一次、十次、一百次等)；预先设置的时间周期的使用(例如，一天、一周、一年等)；或预先设置的天(周三和周四)以及预先设置的时间(例如，下午2-4点)。

[0029] 在一个实施例中，当无线装置到达所有者AP 130的范围内时，虚拟密钥可由访客无线装置110自动无线发射到所有者AP 130，而不需要访客用户输入。例如，当通过访客无线装置110检测到虚拟密钥136中的一者中所列举的SSID时，虚拟密钥容器应用程序113可通过经由链路111发射虚拟密钥来触发认证过程。此外，在所有者AP 130在接入控制管理器应用程序133控制之下授权访客无线装置110并经由链路142发射打开命令以打开入口120之后，所有者AP 130还可启用其它功能，例如停用安全系统170以及启用其它系统172(例如，光，加热等)。应了解，基于存在于访客102的口袋或钱包中的现有无线装置110(例如，智能电话或平板计算机)的使用，可在检测和认证访客102后无需任何用户交互(例如，无需在小键盘上键入PIN码、刷卡等)对入口/门120进行解锁。

[0030] 简要参看图3，下文将描述根据本发明一个实施例的在接入控制管理器应用程序133的控制之下由所有者AP 130实施的过程300。在方框302处，在所有者AP 130处存储针对特定访客无线装置的虚拟密钥136及与所述虚拟密钥相关联的接入控制规则138。如之前所

描述，在虚拟密钥发布器应用程序163的控制下，所有者装置160可针对特定访客无线装置110定义虚拟密钥136及由所有者所定义的相关联的接入控制规则138，且可发射这些虚拟密钥136及接入控制规则138以供所有者AP 130利用。另外，在方框304处，所有者AP 130确定从访客无线装置110接收的虚拟密钥是否匹配针对访客无线装置所存储的虚拟密钥136，及是否满足针对虚拟密钥存储的接入控制规则138。如果是，那么在方框306处，所有者AP 130经由链路142发射打开命令以对锁122进行解锁，使得入口120可由访客102打开。

[0031] 在一个特定实例中，参看图1到2，所有者装置160在处理器162的控制之下可运行可定义和发布针对特定访客的无线装置110的虚拟密钥136的虚拟密钥发布器应用程序163，其中虚拟密钥可包含任何类型的WLAN证书，例如Wi-Fi证书(例如，访客服务设置识别符(SSID)、MAC地址、口令短语等)，及认证证书(例如，密码)。虚拟密钥可经由链路169无线发射到访客的无线装置110(例如，雇佣人员的智能手机、管家的智能手机、修理工人的智能手机等。)。另外，所有者装置160可经由链路139将虚拟密钥136以及预定义的接入控制规则138发射到所有者AP 130。在一个实施例中，接入控制规则138可附加于虚拟密钥136，且可包含关于何时或多久可使用虚拟密钥的此类规则，例如：虚拟密钥可使用一次；虚拟密钥可在每周三下午2点到下午4点使用等。

[0032] 在一个实施例中，访客的无线装置110在处理器112的控制之下可实施虚拟密钥容器应用程序113，当通过访客的无线装置检测到所有者AP 130的识别符(例如，SSID)(其列举在由访客的无线装置所存储的虚拟密钥136中的一者中)时，所述应用113经由链路111通过发射虚拟密钥136与所有者AP 130一起触发认证过程。另外，实施接入控制管理器应用程序133的所有者AP 130可基于所接收的虚拟密钥通过确保其匹配所存储的虚拟密钥136及满足针对所存储的虚拟密钥的接入控制规则138且因此进行强制来执行对访客的无线装置110的认证。其后，接入控制管理器应用程序131可发射经由无线链路142发射的打开命令以对锁122进行解锁，使得可打开入口/门120。

[0033] 简要参看图4，下文将描述根据本发明一个实施例的说明可通过所有者装置160的虚拟密钥发布器应用程序163实施的过程400的流程图。在方框402处，所有者装置160创建和发布针对特定访客的无线装置110的虚拟密钥。在方框404处，所有者装置160将接入控制规则指派到虚拟密钥。在方框406处，所有者装置160将虚拟密钥136发射到访客无线装置110和所有者AP 130。另外，在方框408处，所有者装置160将与虚拟密钥相关联的接入控制规则138(如，由所有者定义的)发射到所有者AP 130。应了解，有益地，所有者装置160可为任何类型的一般计算装置(例如，智能手机、平板计算机、膝上型计算机等)，以易于供所有者使用。

[0034] 关于接入控制规则的特定实例，简要参看图5，下文将描述说明根据一个实施例的接入控制规则的类型的表格500。如在表格500中所显示，对于特定的虚拟密钥502，若干不同类型的接入控制规则可由用户来定义，例如：若干次的使用504(例如，一次、十次、一百次等)；预先设置的时间周期的使用506(例如，一天、一周、一个月、一年等)；或预先设置的天及时间的使用508(例如，仅周三和周四的下午2-4点)。应了解，这些仅接入控制规则的实例，且很多不同类型的接入控制规则可通过所有者装置160的所有者定义，且可经由虚拟密钥发布器应用程序163实施。

[0035] 再次参看图1和2，提供特定实例说明，住宅124的家庭所有者可利用其所有者装置

160来根据针对访客102(例如,管家)的由所有者定义的接入控制规则通过访客的门120向其住宅124提供预定义的接入权。如先前所描述,这可通过利用所有者装置160的虚拟密钥发布器应用程序163来完成,所述所有者装置160将所有者指派给访客102的所发布的虚拟密钥136以及具有针对访客的预定义特征的接入控制规则138发射到所有者AP 130。另外,还将所指派的虚拟密钥136发射到访客的无线装置110。

[0036] 基于此,当管家的无线装置110到达所有者AP 130的范围内时,执行AP协议,如果成功,那么致使所有者AP 130检查虚拟密钥136和接入控制规则138,且如果虚拟密钥匹配且满足接入控制规则138,那么所有者AP 130经由链路142将打开命令发射到锁122以使得其被解锁。然后,门120可通过管家102打开,使得管家可执行其工作功能。应了解,这仅是可通过本发明的方面利用的许多不同类型实例中的一者。另外,所有者也可关于门120保持打开和/或解锁的情况定义规则。例如,门可在预先设置的时间周期(例如,访客到达且门打开后的10分钟)内保持打开和/或解锁或直到满足某些条件(例如,访客离开家庭网络)。应了解,可通过所有者实施很多不同的功能类型。

[0037] 如更特定的实例,应了解,本发明的方面可基于使用现有的无线装置110(例如,智能手机)及现有Wi-Fi基础设施(例如,Wi-Fi路由器130)来实施,使得可在检测及认证访客102而无任何用户交互作用(如,在小键盘上键入PIN码)时对门120进行解锁。例如,无线装置110(例如,智能手机或平板计算机)可存在于访客102的口袋或钱包中,且门可在认证后自动打开。系统所有者通过利用所有者计算装置160可基于其所有者计算装置160(例如,智能手机、膝上型计算机、平板计算机等)上的虚拟密钥发布器应用程序163向任何第三方提供虚拟密钥136。类似地,第三方(例如,访客)的访客的无线装置110(例如,智能手机)经由包含合适的虚拟密钥136的虚拟密钥容器应用程序113变成虚拟密钥容器。特定地,虚拟密钥136可包含如下各项:Wi-Fi证书(例如,SSID、MAC地址、口令短语等)及额外的认证证书(例如,密码等)。如先前所描述,虚拟密钥认证证书(例如,虚拟密钥)可通过访客无线装置110提交到所有者AP网关130以一旦访客无线装置110连接到访客Wi-Fi网络则进行验证。

[0038] 另外,如先前所描述,虚拟密钥136可与接入控制规则138相关联以限制其使用(例如,某些日期/时间间隙,使用次数等)。以此方式,所有者AP 130可基于认证成功/失败自动对门120和/或其它系统进行解锁。门120和其它系统可通过各种方式(例如,有线、Wi-Fi、蜂窝等)连接到所有者AP 130。

[0039] 应了解,本发明的方面可与很多不同的实施方案有关,且先前所描述的那些仅是实例。例如,结构124可以是具有入口的建筑物、住宅、公寓、政府建筑物或设施、大学建筑物或设施、公司建筑物或设施、或任何种类的房间、建筑物、结构等。此外,入口120可以是具有锁122的典型的门、专业的门,车库门,或任何种类打开/关闭的入口(内部打开、外部打开、滑动打开等)。另外,应了解,锁122可为任何种类的锁定机制,其允许可接收打开或关闭命令142的入口方式的打开及关闭。此外,尽管许多链路(例如,链路111、139、142、169等)已被描述为无线链路,但在许多实施方案中这些可为有线链路。因此,应了解,本发明的方面可与很多不同的移动无线装置110、接入点130及所有者计算装置160有关,所述装置可实施本发明的与使用虚拟密钥及接入控制规则有关的实施例,以允许访客通过所有者以非常特别的、预定义的接入控制规则进行虚拟密钥的指派和利用。

[0040] 另外,本发明的实施例可实施反中继攻击功能以防止潜在的中继攻击。例如,中继

攻击可由接近具有带有虚拟密钥的访客无线装置的访客且激活具有与所有者AP相同的身份(SSID)的欺骗AP的黑客及其搭档组成。基于此，访客无线装置可将其虚拟密钥发射到欺骗AP。然后，虚拟密钥可由黑客1(靠近访客)中继到黑客2(靠近所有者住宅/AP)。其后，利用黑客2装置的黑客2可通过向所有者AP提供虚拟密钥来模仿访客。这种类型的中继攻击(如，2个人在中间)可通过实施反中继攻击功能解决。在一个实施例中，访客无线装置110可利用其GPS特征来发射无线装置的密码保护的GPS位置以及虚拟密钥，使得所有者AP 130可对密码保护的GPS位置信息进行解码以认证访客无线装置110。所有者AP 130通常处于固定位置处，且可检查访客无线装置的110的位置是处于预定义的位置的某一半径内。在另一实施例中，所有者AP 130可向访客无线装置110认证其自己。这可通过基于Wi-Fi的安全(例如，Wi-Fi受保护的接入(WPA))来实施。

[0041] 应了解，先前所描述的本发明的方面可连同通过如先前所描述的装置(例如，无线装置110、所有者AP 130、所有者装置160)的处理器执行指令(例如，应用)来实施。特定地，包含但不限于处理器的装置的电路可在应用、程序、例行程序或指令的执行的控制之下操作，以执行根据本发明的实施例的方法或过程(例如，图3和4的过程300和400)。例如，此程序可在固件或软件(例如，存储在存储器和/或其它位置中)中实施，且可通过装置的处理器和/或其它电路来实施。另外，应了解，术语处理器、微处理器、电路、控制器等是指任何类型的能够执行逻辑、命令、指令、软件、固件、功能等的逻辑或电路。

[0042] 应了解，当装置是移动或无线装置时，那么其可通过基于或其它支持任何合适的无线通信技术的无线网络经由一或多个无线通信链路来通信。例如，在某些方面中，无线装置及其它装置可与包含无线网络的网络相关联。在某些方面中，网络可包含体域网或个域网(例如，超宽带网络)。在某些方面中，网络可包含局域网(例如，WLAN)或广域网。无线装置可支持或另外使用一或多个的多种无线通信技术、协议或标准，例如，举例来说3G、LTE、高级LTE、4G、CDMA、TDMA、OFDM、OFDMA、WiMAX及WiFi。类似地，无线装置可支持或另外使用一或多个的多种对应的调制或多路复用方案。因此，无线装置可包含合适的组件(例如，空中接口)以经由一或多个通信链路无线使用以上或其它无线通信技术来建立和通信。例如，装置可包含具有相关联的发射器及接收器组件(例如，发射器和接收器)的无线收发器，所述组件可包含促进在无线媒体上通信的各种组件(例如，信号产生器及信号处理器)。众所周知，移动无线装置可因此与其它移动装置、手机、其它有线和无线的计算机、互联网网站等进行无线通信。

[0043] 本文中所描述的技术可用于各种无线通信系统，例如：码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、正交频分多址(OFDMA)、单载波FDMA(SC-FDMA)及其它系统。术语“系统”和“网络”经常互换使用。CDMA系统可实施无线电技术，例如，通用陆地无线电接入(UTRA)、CDMA2000等。UTRA包含宽带CDMA(W-CDMA)及CDMA的其它变体。CDMA2000涵盖临时的标准(IS)-2000、IS-95及IS-856标准。TDMA系统可实施无线电技术，例如，全球移动通信系统(GSM)。OFDMA系统可实施无线电技术，例如，演进的通用陆地无线电接入(演进UTRA或E-UTRA)、超移动宽带(UMB)、电气和电子工程师协会(IEEE)802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、快闪OFDM.RTM等。通用陆地无线电接入(UTRA)及E-UTRA是通用移动通信系统(UMTS)的部分。3GPP长期演进(LTE)是使用E-UTRA的UMTS的将来版本，其在下行链路上采用OFDMA，且在上行链路上采用SC-FDMA。UTRA、E-UTRA、UMTS、LTE和GSM在来自于名叫

“第三代合作伙伴计划”(3GPP)的组织的文档中描述。CDMA2000和UMB在来自于名叫“第三代合作伙伴计划2”(3GPP2)的组织的文档中描述。此外，较新的标准包含4G和高级LTE。

[0044] 本文的教示可并入(例如，在……内实施或由……执行)多种设备(例如，装置)中。例如，本文教示的一或多个方面可并入智能手机(例如，蜂窝电话)、个人数据助理(“PDA”)、平板计算机、移动计算机、膝上型计算机、娱乐装置(例如，音乐或视频装置)、头戴受话器(例如，头戴耳机，耳机等)、医疗装置(例如，生物计量传感器、心率监视器、计步器、EKG装置等)、用户I/O装置、计算机、有线计算机、固定计算机、桌上型计算机、服务器、销售点装置、机顶盒或任何其它合适的装置。这些装置可有不同的功率及数据要求。

[0045] 在某些方面中，无线装置可包括用于通信系统的接入装置(例如，Wi-Fi接入点)。例如，此接入装置可经由有线或无线通信链路提供与另一网络(例如，广域网，例如互联网或蜂窝网络)的连接。因此，接入装置可启用另一装置(例如，WiFi站)以接入其它网络或某一其它功能。

[0046] 所属领域的技术人员将了解，可使用任何多种不同技艺和技术来表示信息和信号。例如，可贯穿以上描述引用的数据、指令、命令、信息、信号、位、符号和芯片可由电压、电流、电磁波、磁场或磁粒子、光学场或光学粒子或其任何组合来表示。

[0047] 所属领域的技术人员将进一步了解，结合本文中所揭示的实施方案所描述的各种说明性逻辑块、模块、电路和算法步骤可实施为电子硬件、计算机软件或者两者的组合。为清楚地说明硬件和软件的此可互换性，上文已在其功能性方面大体描述了各种说明性组件、块、模块、电路和步骤。此功能性是实施为硬件还是软件取决于施加于整个系统上的特定应用和设计约束。技术人员可针对每一特定应用以各种方式实施所描述的功能性，但此类实施方案决策不应被阐释为导致脱离本发明的范围。

[0048] 结合本文中所揭示的实施例所描述的各种说明性逻辑块、模块和电路可用以下各项来实施或执行：通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件、或经设计以执行本文中所描述功能的其任何组合。通用处理器可为微处理器，但在替代方案中，处理器可为任何常规的处理器、控制器、微控制器或状态机。处理器也可实施为计算装置的组合，例如，DSP和微处理器的组合、多个微处理器的组合、一或多个微处理器结合DSP核心的组合，或任何其它此类配置。

[0049] 结合本文中所揭示的实施例所描述的方法或算法的步骤可直接在硬件、由处理器执行的软件模块或两者的组合中实施。软件模块可驻留在RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动磁盘、CD-ROM、或所属领域中已知的任何其它形式的存储媒体中。示范性存储媒体耦合到处理器，使得处理器可从存储媒体读取信息，并将信息写入到存储媒体。在替代方案中，存储媒体可与处理器为一体。处理器和存储媒体可驻留在ASIC中。ASIC可驻留在用户终端中。在替代方案中，处理器和存储媒体可作为离散组件驻留在用户终端中。

[0050] 在一或多个示范性实施例中，可在硬件、软件、固件或其任何组合中实施所描述的功能。如果在软件中实施为计算机程序产品，那么所述功能可作为一或多个指令或代码存储在计算机可读媒体上，或经由计算机可读媒体发射。计算机可读媒体包含计算机存储媒体和包含促进计算机程序从一个地方传递到另一个地方的任何媒体的通信媒体。存储媒体

可为可由计算机存取的任何可用媒体。举例来说且无限制地，此计算机可读媒体可包含RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁存储装置，或任何其它可用于携带或存储所要的呈可由计算机存取的指令或数据结构形式的程序代码的媒体。同样，任何连接适当地称为计算机可读媒体。例如，如果从网站、服务器或其它使用同轴电缆、光纤电缆、双绞线、数字订户线路(DSL)或例如红外线、无线电和微波的无线技术的远程源发射软件，那么同轴电缆、光纤电缆、双绞线、DSL或例如红外线、无线电和微波的无线技术包含在媒体的定义中。如本文中所使用的磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字通用光盘(DVD)、软磁盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘则用激光以光学方式再现数据。上文的组合同样应包含在计算机可读媒体的范围内。

[0051] 提供所揭示的实施例的先前描述以使所属领域内的任何技术人员能够制作或使用本发明。这些实施例的各种修改对于所属领域的技术人员来说将显而易见，且本文中定义的一般原理可应用于其它实施例而不脱离本发明的精神或范围。因此，本发明无意受限于本文中所显示的实施例，而是将被赋予与本文中所揭示的原理和新颖特征相一致的最广范围。

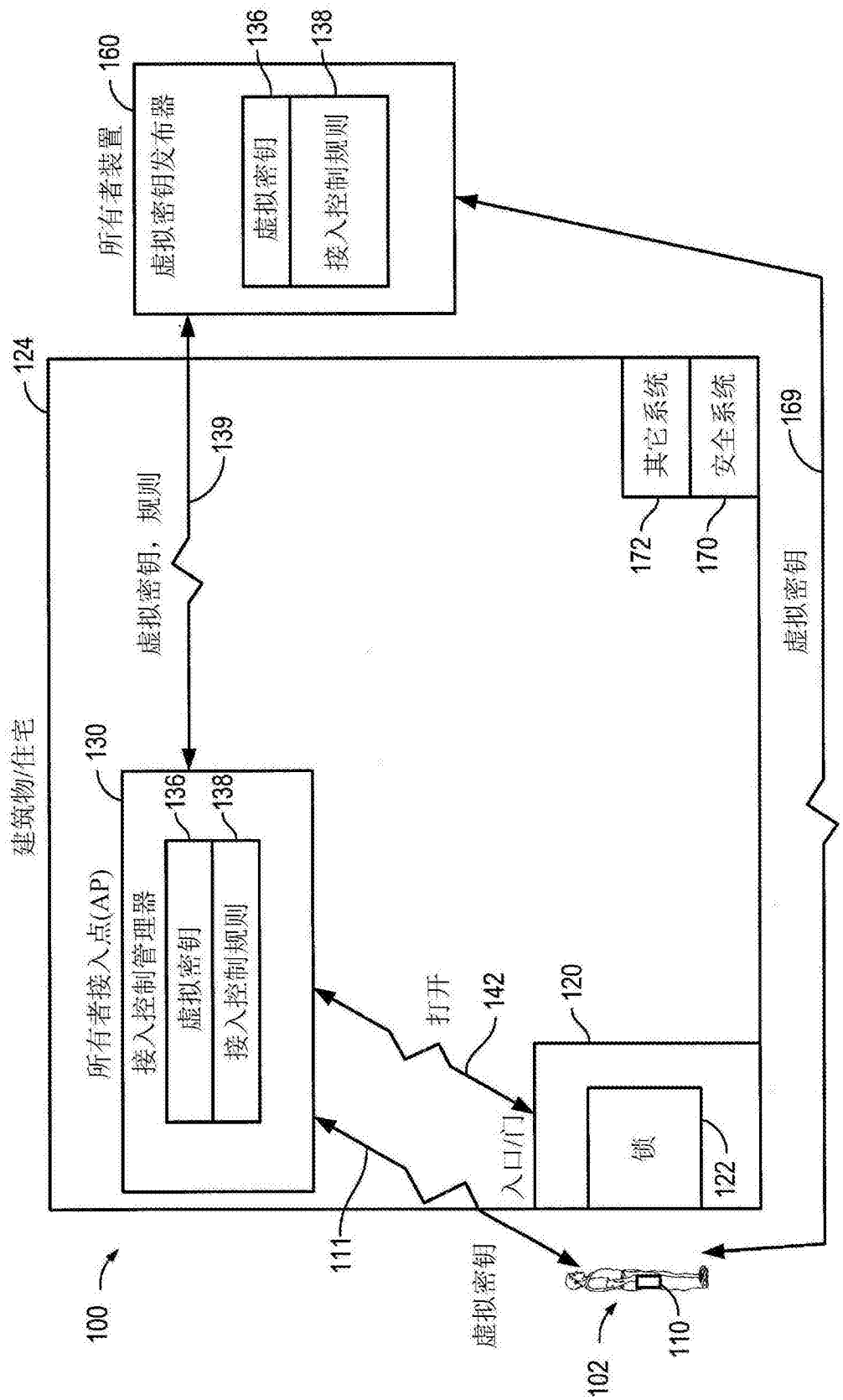

所有者装置
160
虚拟密钥发布器
136
虚拟密钥
138
接入控制规则
124
建筑物/住宅
虚拟密钥，规则
139
其它系统
172
安全系统
170
169
虚拟密钥
所有者接入点(AP)
130
接入控制管理器
136
虚拟密钥
138
接入控制规则
打开
142
120
入口/门
锁
122
111
虚拟密钥
100
102
110

图1

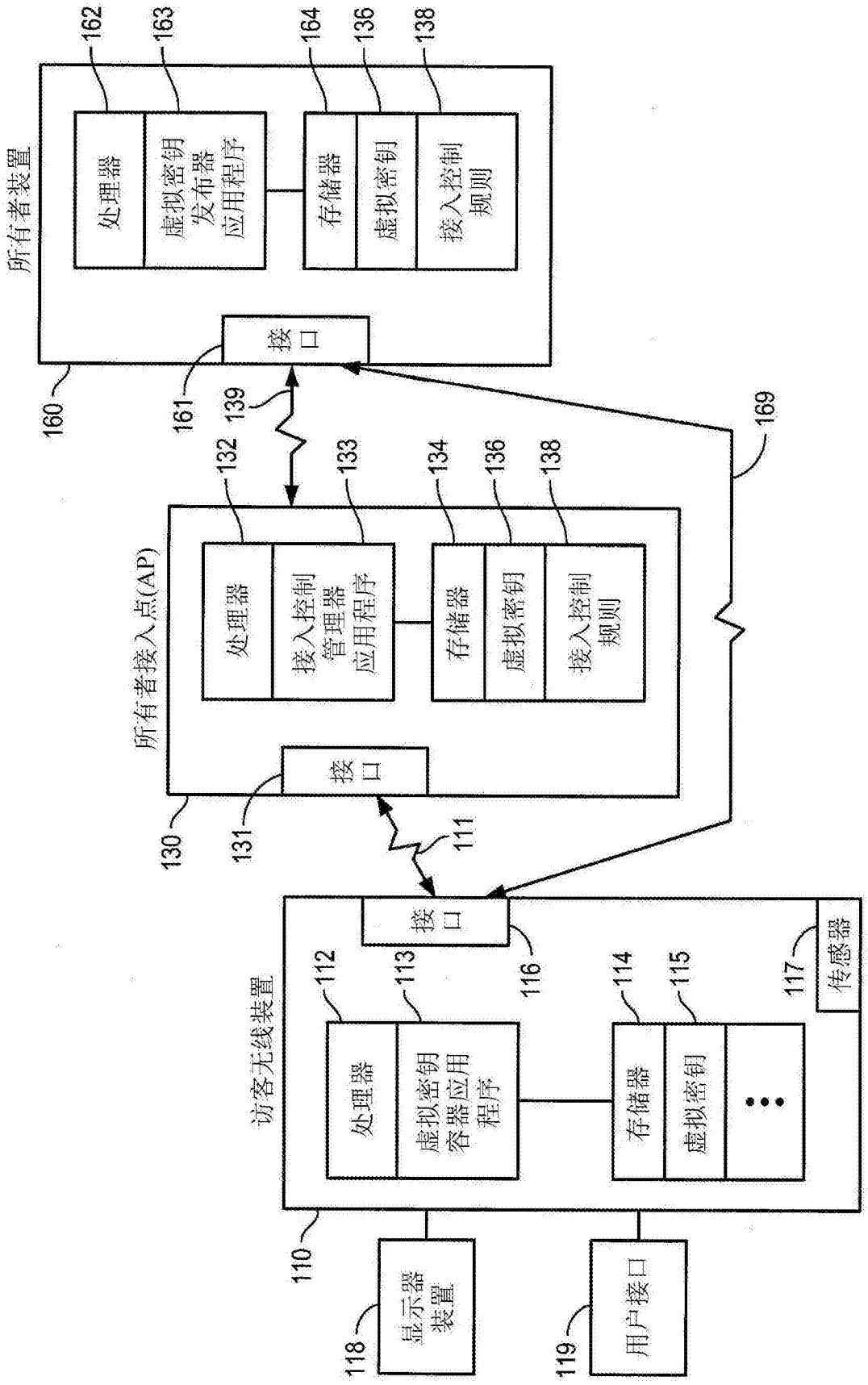

所有者装置
162
163
164
136
138
处理器
虚拟密钥发布器应用程序
存储器
虚拟密钥
接入控制规则
接口
160
161
139
169
所有者接入点(AP)
132
133
134
136
138
处理器
接入控制管理器应用程序
存储器
虚拟密钥
接入控制规则
接口
130
131
111
访客无线装置
接口
112
113
116
114
115
117
传感器
处理器
虚拟密钥容器应用程序
存储器
虚拟密钥
110
显示器装置
118
用户接口
119

图2

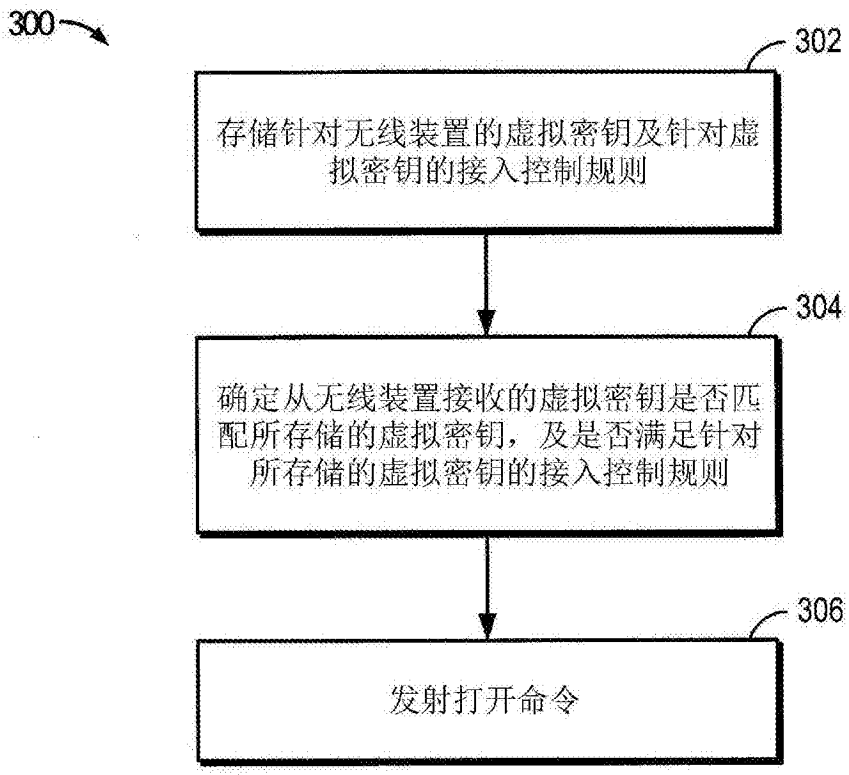

300
302
存储针对无线装置的虚拟密钥及针对虚拟密钥的接入控制规则
304
确定从无线装置接收的虚拟密钥是否匹配所存储的虚拟密钥，及是否满足针对所存储的虚拟密钥的接入控制规则
306
发射打开命令

图3

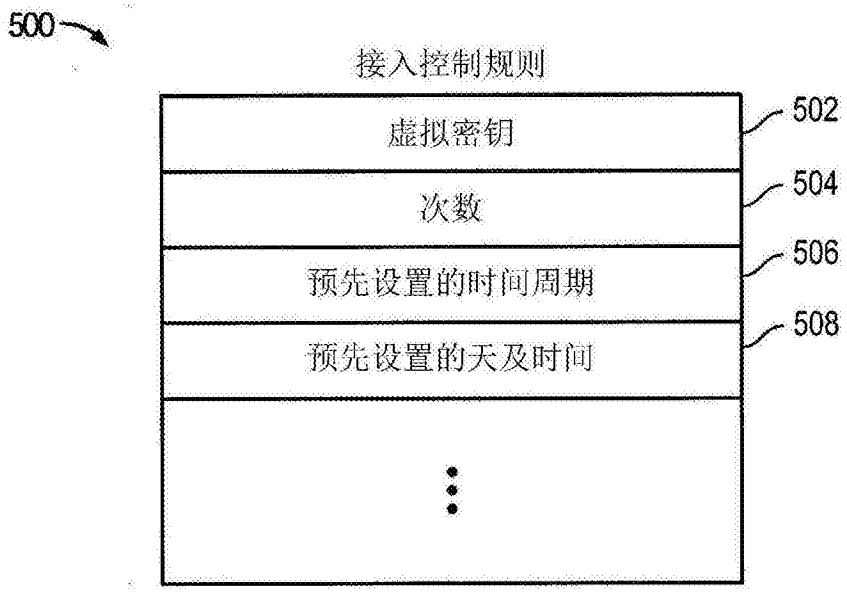

500
接入控制规则
虚拟密钥
502
次数
504
预先设置的时间周期
506
预先设置的天及时间
508

图5

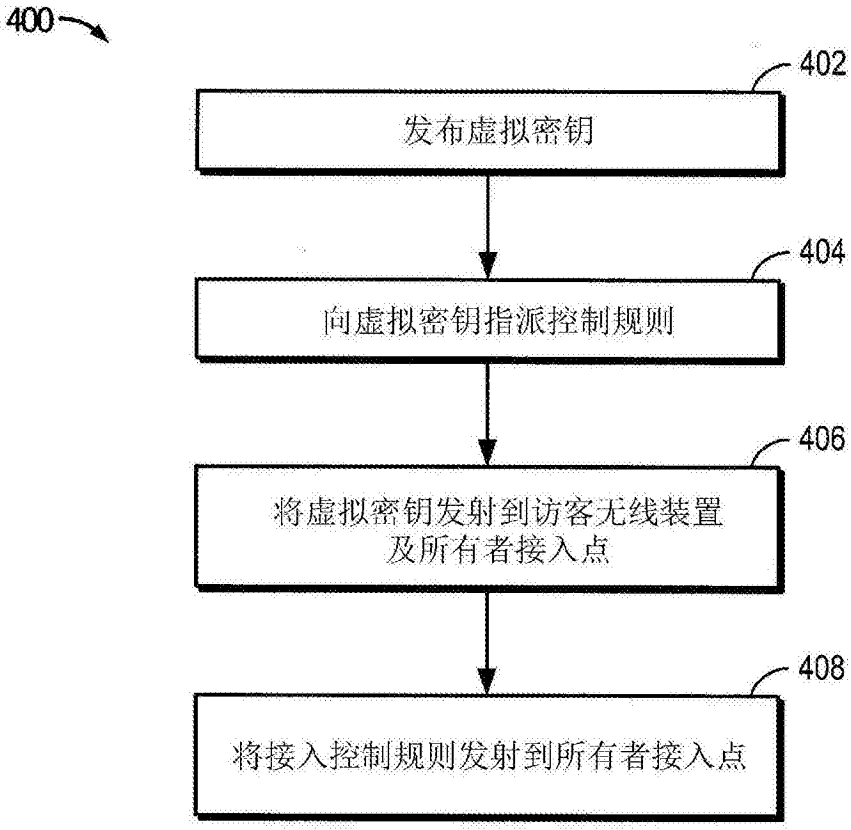

400
402
发布虚拟密钥
404
向虚拟密钥指派控制规则
406
将虚拟密钥发射到访客无线装置及所有者接入点
408
将接入控制规则发射到所有者接入点

图4