



## (12) 发明专利申请

(10) 申请公布号 CN 104641615 A

(43) 申请公布日 2015. 05. 20

(21) 申请号 201380034264. 2

(22) 申请日 2013. 07. 16

(30) 优先权数据

13/550, 402 2012. 07. 16 US

(85) PCT国际申请进入国家阶段日

2014. 12. 26

(86) PCT国际申请的申请数据

PCT/US2013/050766 2013. 07. 16

(87) PCT国际申请的公布数据

W02014/014964 EN 2014. 01. 23

(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 张江 理查德·O·法利 丁刚

帕特里克·N·伦德奎斯特

(74) 专利代理机构 北京律盟知识产权代理有限公司 11287

代理人 宋献涛

(51) Int. Cl.

H04L 29/06(2006. 01)

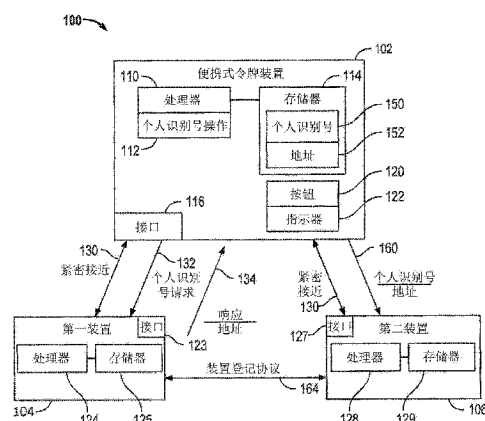
权利要求书4页 说明书8页 附图3页

### (54) 发明名称

用于配对两个装置的便携式令牌

### (57) 摘要

本发明揭示一种便携式令牌装置,其可用以辅助用户在一个装置处产生PIN且随后将所述PIN传递到另一装置以使得所述两个装置可安全地彼此通信。所述便携式令牌装置可包含:接口;和处理器。所述处理器可执行操作,包含:确定通过所述接口到第一装置的紧密接近耦合是否已发生;将PIN请求发射到所述第一装置;以及获得PIN。此外,所述处理器可确定通过所述接口到第二装置的紧密接近耦合是否已发生。如果是,那么所述处理器可命令将所述PIN发射到所述第二装置。所述第二装置可基于所述所接收PIN执行向所述第一装置的装置登记。



1. 一种便携式令牌装置,其包括:  
接口;以及  
处理器,其用以执行包含以下各项的操作:  
确定通过所述接口到第一装置的紧密接近耦合是否已发生;  
将 PIN 请求发射到所述第一装置;  
获得 PIN;  
确定通过所述接口到第二装置的紧密接近耦合是否已发生;以及  
将所述 PIN 发射到所述第二装置。
2. 根据权利要求 1 所述的便携式令牌装置,其中所述 PIN 是从所述第一装置接收。
3. 根据权利要求 1 所述的便携式令牌装置,其中所述 PIN 是基于来自所述第一装置的随机种子和在所述便携式令牌装置与所述第一装置之间共享的秘密而产生。
4. 根据权利要求 1 所述的便携式令牌装置,其中基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。
5. 根据权利要求 1 所述的便携式令牌装置,其中紧密接近耦合包括紧密接近无线耦合。
6. 根据权利要求 5 所述的便携式令牌装置,其中紧密接近无线耦合包括近场通信 NFC 耦合。
7. 根据权利要求 1 所述的便携式令牌装置,其中紧密接近耦合包括有线耦合。
8. 根据权利要求 1 所述的便携式令牌装置,其进一步包括按钮,其中所述按钮由用户推动以将所述 PIN 请求发射到所述第一装置且将所述 PIN 发射到所述第二装置。
9. 根据权利要求 1 所述的便携式令牌装置,其中所述 PIN 是随机 PIN。
10. 根据权利要求 1 所述的便携式令牌装置,其进一步包括用以存储所述 PIN 的存储器。
11. 根据权利要求 10 所述的便携式令牌装置,其中所述处理器在预定时间周期之后或在所述 PIN 已发射预定次数之后从所述存储器删除所述 PIN。
12. 根据权利要求 1 所述的便携式令牌装置,其进一步包括指示器,所述指示器用以警示用户所述 PIN 已在所述第一装置处获得且所述 PIN 已发射到所述第二装置。
13. 一种将 PIN 从第一装置传递到第二装置的方法,其包括:  
确定到所述第一装置的紧密接近耦合是否已发生;  
将 PIN 请求发射到所述第一装置;  
获得 PIN;  
确定到所述第二装置的紧密接近耦合是否已发生;以及  
将所述 PIN 发射到所述第二装置。
14. 根据权利要求 13 所述的方法,其中所述 PIN 是从所述第一装置接收。
15. 根据权利要求 13 所述的方法,其中所述 PIN 是基于来自所述第一装置的随机种子和在所述便携式令牌装置与所述第一装置之间共享的秘密而产生。
16. 根据权利要求 13 所述的方法,其中基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。
17. 根据权利要求 13 所述的方法,其中紧密接近耦合包括紧密接近无线耦合。

18. 根据权利要求 17 所述的方法,其中紧密接近无线耦合包括近场通信 NFC 耦合。
19. 根据权利要求 13 所述的方法,其中紧密接近耦合包括有线耦合。
20. 根据权利要求 13 所述的方法,其进一步包括:  
基于所接收按钮信号将所述 PIN 请求发射到所述第一装置;以及  
基于所接收按钮信号将所述 PIN 发射到所述第二装置。
21. 根据权利要求 13 所述的方法,其中所述 PIN 是随机 PIN。
22. 根据权利要求 13 所述的方法,其进一步包括警示用户所述 PIN 已在所述第一装置处获得且所述 PIN 已发射到所述第二装置。
23. 一种在便携式令牌装置处执行的计算机程序产品,其包括:  
计算机可读媒体,其包括用于以下操作的代码:  
确定到所述第一装置的紧密接近耦合是否已发生;  
将 PIN 请求发射到所述第一装置;  
获得 PIN;  
确定到所述第二装置的紧密接近耦合是否已发生;以及  
将所述 PIN 发射到所述第二装置。
24. 根据权利要求 22 所述的计算机程序产品,其中所述 PIN 是从所述第一装置接收。
25. 根据权利要求 23 所述的计算机程序产品,其中所述 PIN 是基于来自所述第一装置的随机种子和在所述便携式令牌装置与所述第一装置之间共享的秘密而产生。
26. 根据权利要求 23 所述的计算机程序产品,其中基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。
27. 根据权利要求 23 所述的计算机程序产品,其中紧密接近耦合包括紧密接近无线耦合。
28. 根据权利要求 27 所述的计算机程序产品,其中紧密接近无线耦合包括近场通信 NFC 耦合。
29. 根据权利要求 28 所述的计算机程序产品,其中紧密接近耦合包括有线耦合。
30. 根据权利要求 23 所述的计算机程序产品,其进一步包括用于以下操作的代码:  
命令基于所接收按钮信号将所述 PIN 请求发射到所述第一装置;以及  
命令基于所接收按钮信号将所述 PIN 发射到所述第二装置。
31. 根据权利要求 23 所述的计算机程序产品,其中所述 PIN 是随机 PIN。
32. 根据权利要求 23 所述的计算机程序产品,其进一步包括用于警示用户所述 PIN 已在所述第一装置处获得且所述 PIN 已发射到所述第二装置的代码。
33. 一种便携式令牌装置,其包括:  
用于确定到第一装置的紧密接近耦合是否已发生的装置;  
用于将 PIN 请求发射到所述第一装置的装置;  
用于获得 PIN 的装置;  
用于确定到第二装置的紧密接近耦合是否已发生的装置;以及  
用于将所述 PIN 发射到所述第二装置的装置。
34. 根据权利要求 33 所述的便携式令牌装置,其中所述 PIN 是从所述第一装置接收。
35. 根据权利要求 33 所述的便携式令牌装置,其中所述 PIN 是基于来自所述第一装置

的随机种子和在所述便携式令牌装置与所述第一装置之间共享的秘密而产生。

36. 根据权利要求 33 所述的便携式令牌装置,其中基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。

37. 根据权利要求 33 所述的便携式令牌装置,其中紧密接近耦合包括紧密接近无线耦合。

38. 根据权利要求 37 所述的便携式令牌装置,其中紧密接近无线耦合包括近场通信 NFC 耦合。

39. 根据权利要求 33 所述的便携式令牌装置,其中紧密接近耦合包括有线耦合。

40. 根据权利要求 33 所述的便携式令牌装置,其中所述 PIN 是随机 PIN。

41. 一种第一装置,其包括:

接口;以及

处理器,其用以执行包含以下各项的操作:

当便携式令牌装置和所述第一装置紧密接近耦合时通过所述接口从所述便携式令牌装置接收 PIN 请求;以及

将响应发射到所述便携式令牌装置。

42. 根据权利要求 41 所述的第一装置,其中所述响应包含 PIN。

43. 根据权利要求 42 所述的第一装置,其中所述 PIN 是随机 PIN。

44. 根据权利要求 41 所述的第一装置,其中所述响应包含随机种子。

45. 根据权利要求 41 所述的第一装置,其中基于所述响应,所述便携式令牌装置获得发射到第二装置的 PIN,且基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。

46. 根据权利要求 45 所述的第一装置,其中所述处理器执行又一操作以在装置登记期间基于从所述第二装置接收的所述 PIN 或从所述 PIN 导出的检验数据来检验所述第二装置的授权。

47. 根据权利要求 41 所述的第一装置,其中紧密接近耦合包括紧密接近无线耦合。

48. 根据权利要求 47 所述的第一装置,其中紧密接近无线耦合包括近场通信 NFC 耦合。

49. 根据权利要求 41 所述的第一装置,其中所述第一装置不包含用于 PIN 的所述接收的输入机构。

50. 一种将响应从第一装置发射到便携式令牌装置的方法,其包括:

当所述便携式令牌装置和所述第一装置紧密接近耦合时从所述便携式令牌装置接收 PIN 请求;以及

将所述响应发射到所述便携式令牌装置。

51. 根据权利要求 50 所述的方法,其中所述响应包含 PIN。

52. 根据权利要求 51 所述的方法,其中所述 PIN 是随机 PIN。

53. 根据权利要求 50 所述的方法,其中所述响应包含随机种子。

54. 根据权利要求 50 所述的方法,其中基于所述响应,所述便携式令牌装置获得发射到第二装置的 PIN,且基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。

55. 根据权利要求 54 所述的方法,其进一步包括在装置登记期间基于从所述第二装置

接收的所述 PIN 或从所述 PIN 导出的检验数据来检验所述第二装置的授权。

56. 根据权利要求 50 所述的方法,其中紧密接近耦合包括紧密接近无线耦合。

57. 根据权利要求 56 所述的方法,其中紧密接近无线耦合包括近场通信 NFC 耦合。

58. 一种在第一装置处执行的计算机程序产品,其包括:

计算机可读媒体,其包括用于以下操作的代码:

当便携式令牌装置和所述第一装置紧密接近耦合时从所述便携式令牌装置接收 PIN 请求;以及

将响应发射到所述便携式令牌装置。

59. 根据权利要求 58 所述的计算机程序产品,其中所述响应包含 PIN。

60. 根据权利要求 59 所述的计算机程序产品,其中所述 PIN 是随机 PIN。

61. 根据权利要求 58 所述的计算机程序产品,其中所述响应包含随机种子。

62. 根据权利要求 58 所述的计算机程序产品,其中基于所述响应,所述便携式令牌装置获得发射到第二装置的 PIN,且基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。

63. 根据权利要求 62 所述的计算机程序产品,其进一步包括用于在装置登记期间基于从所述第二装置接收的所述 PIN 或从所述 PIN 导出的检验数据来检验所述第二装置的授权的代码。

64. 根据权利要求 58 所述的计算机程序产品,其中紧密接近耦合包括紧密接近无线耦合。

65. 根据权利要求 64 所述的计算机程序产品,其中紧密接近无线耦合包括近场通信 NFC 耦合。

66. 一种第一装置,其包括:

用于当便携式令牌装置和所述第一装置紧密接近耦合时从所述便携式令牌装置接收 PIN 请求的装置;以及

用于将响应发射到所述便携式令牌装置的装置。

67. 根据权利要求 66 所述的第一装置,其中所述响应包含 PIN。

68. 根据权利要求 67 所述的第一装置,其中所述 PIN 是随机 PIN。

69. 根据权利要求 66 所述的第一装置,其中所述响应包含随机种子。

70. 根据权利要求 66 所述的第一装置,其中基于所述响应,所述便携式令牌装置获得发射到第二装置的 PIN,且基于由所述第二装置接收的所述 PIN,所述第二装置执行向所述第一装置的装置登记。

71. 根据权利要求 70 所述的第一装置,其进一步包括用于在装置登记期间基于从所述第二装置接收的所述 PIN 或从所述 PIN 导出的检验数据来检验所述第二装置的授权的装置。

72. 根据权利要求 66 所述的第一装置,其中紧密接近耦合包括用于紧密接近无线耦合的装置。

73. 根据权利要求 72 所述的第一装置,其中所述用于紧密接近无线耦合的装置包括近场通信 NFC 耦合。

## 用于配对两个装置的便携式令牌

### 技术领域

[0001] 本发明大体上涉及便携式令牌装置,其可用以辅助用户在一个装置处产生 PIN 且随后将 PIN 传递到另一装置以使得所述两个装置可安全地彼此通信。

### 背景技术

[0002] 存在许多不同方式设置两个装置之间的安全无线通信。举例来说,为了连接两个 WiFi 装置,可在一个装置(例如,路由器)上设置口令/密钥,且可在另一装置(例如,膝上型计算机)中键入同一口令/密钥,使得所述装置可安全地彼此通信。然而,对于其它类型的装置,可能不存在输入口令/密钥的键盘。举例来说,在无线家庭数字接口(WHDI)环境中,可使用按钮按压序列来产生个人识别号(PIN)以安全地使两个家庭装置彼此登记且彼此交换登记密钥。然而,此按钮按压序列方法要求用户记住且输入长按钮序列,这可为困难的且不是用户友好的。

[0003] 又一问题在于许多类型的无线装置不具有键盘、按钮或任一类型的输入装置来输入 PIN、口令、密钥等等。这使得用户很难安全地连接这些类型的无线装置。

### 发明内容

[0004] 本发明的方面可涉及用于便携式令牌装置的设备和方法,所述便携式令牌装置可用以辅助用户在一个装置处产生 PIN 且随后将 PIN 传递到另一装置以使得所述两个装置可安全地彼此通信。所述便携式令牌装置可包含:接口;和处理器。所述处理器可执行操作,包含:确定通过所述接口到第一装置的紧密接近耦合是否已发生;将 PIN 请求发射到所述第一装置;以及获得 PIN。此外,所述处理器可确定通过所述接口到第二装置的紧密接近耦合是否已发生。如果是,那么所述处理器可命令将所述 PIN 发射到所述第二装置。所述第二装置可基于所述所接收 PIN 执行与所述第一装置的装置登记。

### 附图说明

[0005] 图 1 是其中可实践涉及便携式令牌装置的本发明的方面的系统的框图。

[0006] 图 2 是说明由便携式令牌装置实施的过程的流程图。

[0007] 图 3 是说明便携式令牌装置的使用的特定实例的图。

### 具体实施方式

[0008] 词语“示范性”或“实例”在本文用以表示“充当实例、例子或说明”。本文描述为“示范性”或“实例”的任一方面或实施例都不一定解释为比其它方面或实施例优选或有利。

[0009] 参见图 1,图 1 是其中可实践本发明的方面的系统 100 的框图。特定来说,系统 100 说明便携式令牌装置 102,所述便携式令牌装置可用以辅助用户在第一装置 104 处产生个人识别号(PIN)且随后将 PIN 传递到第二装置 106 以使得所述两个装置(例如,第一装置 104 和第二装置 106)可安全地彼此通信。特定来说,本发明的方面涉及便携式令牌装置

102,其允许第一装置 104 和第二装置 106 基于 PIN 而彼此验证且彼此登记,使得所述装置可安全地彼此通信。

[0010] 便携式令牌装置 102 可包含处理器 110、存储器 114 和接口 (I/F) 116。此外如将描述,便携式令牌装置 102 可包含例如按钮 120 和指示器 122 等其它特征。

[0011] 在一个方面中,处理器 110 可经配置以执行 PIN 操作程序 112(例如,从存储器 114 接收和存储在存储器 114 中),其产生 PIN 以在第一装置 104 与第二装置 106 之间共享,所述 PIN 允许第二装置 106 验证自身且向第一装置 104 登记,使得所述装置可安全地彼此通信,且执行装置登记协议以使得所述装置可彼此交互。下文将描述这些 PIN 操作。为了开始,处理器 110 执行第一操作以确定便携式令牌装置 102 通过 I/F 116 与第一装置 104 之间的紧密接近耦合 130 是否已发生。如果紧密接近耦合已发生,那么处理器 110 致使将 PIN 请求 132 通过 I/F 116 发射到第一装置 104。如将描述,基于来自第一装置 104 的响应 134,处理器 110 可获得 PIN。

[0012] 基于 PIN 请求 132,第一装置 104 可将可包含经预配置 PIN、随机 PIN 或随机种子的响应 134 发射到便携式令牌装置 102。任选地,第一装置 104 的装置地址 152 也可包含在响应 134 中。在一个方面中,处理器 110 可直接使用由第一装置 104 经由响应 134 接收的经预配置 PIN 或随机 PIN。在另一方面中,基于来自第一装置 104 的所接收随机种子以及在便携式令牌装置 102 与第一装置 104 之间共享的一或多个秘密,处理器 110 可产生经导出 PIN。例如经导出 PIN 的 PIN 150 可存储在存储器 114 中。在便携式令牌装置 102 与第一装置 104 之间共享的秘密可由便携式令牌装置 102、第一装置 104 或两者产生。其也可由第三方产生且设定到便携式令牌装置 102 和第一装置 104 两者中。此外,在一个实施例中,PIN 150 可为经预配置 PIN 或随机 PIN,且在下文中将称为 PIN 150。第一装置 104 的地址 152 也可存储在存储器 114 中。

[0013] 应了解,作为实例,基于响应 134 中的共享秘密和随机种子,经导出 PIN 可由便携式令牌装置 102 和第一装置 104 两者产生且知道,而第一装置 104 不必发射经导出 PIN 自身。这仅是产生 PIN 150 的一个实例,且也可利用其它方法。此外,虽然利用术语 PIN,但应了解,可使用任一识别符作为 PIN 150,包含经预配置 PIN、随机 PIN、密钥、口令等等,其可为数字的和 / 或字母数字的,且可用作第一装置 104 与第二装置 106 之间的验证和 / 或授权识别符。另外,在一个实施例中,地址 152 可为媒体接入控制 (MAC) 地址,且在下文中将作为 MAC 地址 152 来寻址。然而应了解,可利用其它类型的地址方法。

[0014] 接着,便携式令牌装置 102 的处理器 110 可执行操作以确定通过 I/F 116 的紧密接近 130 耦合是否已与第二装置 106 发生。如果是,那么处理器 110 可命令通过 I/F 116 且经由链路 160 将 PIN 150 和 MAC 地址 152 发射到第二装置 106。

[0015] 应了解,第一装置 104 可包含处理器 124、存储器 125 和接口 123,以及用以执行与第一装置 104 相关联的功能性的其它元件。举例来说,接口 123 可接收 PIN 请求 132 且在处理器 124 的控制下将响应 134 发射到便携式令牌装置 102。基于 PIN 请求 132 的接收,当便携式令牌装置 102 和第一装置 104 紧密接近时,处理器 124 可确定是否将经预配置 PIN、随机 PIN 或随机种子经由响应 134 发射到便携式令牌装置 102。类似地,第二装置 106 可包含处理器 128、存储器 129 和接口 127,以及用以执行与第二装置 106 相关联的功能性的其它元件。举例来说,I/F 127 可在来自便携式令牌装置 102 的消息 160 中接收 PIN 和 MAC

地址,且在处理器 128 的控制下可执行装置登记协议 164 以向第一装置 104 登记,使得第一装置 104 和第二装置 106 可检验其是否经授权以彼此登记且因此其可安全地彼此通信。如稍后将更详细描述,第一装置 104 和第二装置 106 可为执行各种类型的功能的广泛多种不同类型的装置。

[0016] 基于由第二装置 106 接收的 PIN 150,第二装置 106 在处理器 128 的控制下可执行装置登记协议 164 以向第一装置 104 登记,使得第一装置 104 和第二装置 106 可安全地彼此通信且经其相应接口 123 和 127 彼此链接。第二装置 106 可基于第一装置 104 已知且由便携式令牌装置 102 传送到第二装置 106 的 PIN 150,通过装置登记协议 164 向第一装置 104 验证自身。特定来说,第一装置 104 在处理器 124 的控制下可检验第二装置 106 是否经授权以基于 PIN 150 向第一装置 104 登记。而且,在一个实施例中,关于授权,第一装置 104 可利用从 PIN 导出的检验数据。基于 MAC 地址和其它数据的装置登记协议 164 是此项技术中众所周知的。

[0017] 在一个方面中,紧密接近耦合 130 可包含经由 I/F 116 以及第一装置 104 和第二装置 106 的对应 I/F 123 和 127 的紧密接近无线耦合。在此方面中,便携式令牌装置 102 可触碰或可非常靠近第一装置 104 和第二装置 106 以便实施紧密接近无线耦合。作为实例,紧密接近无线耦合可为近场通信 (NFC) 耦合。其它类型的紧密无线耦合可包含:蓝牙、紫蜂 (ZIGBEE) 等等。

[0018] 作为另一实例,紧密接近耦合 130 可包含与便携式令牌装置 102 的有线耦合,其经由配合的物理接口物理地耦合到第一装置 104 和第二装置 106。可使用此情况的实例,通用串行总线 (USB) 耦合,其中便携式令牌装置 102 的 I/F 116 是 USB 接口,且第一装置 104 和第二装置 106 类似地包含 USB 端口或接口 123 和 127 以用于与便携式令牌装置 102 物理地连接。应了解,可使用广泛多种不同的配合物理接口来形成便携式令牌装置 102 与第一装置 104 和第二装置 106 之间的物理或有线连接。

[0019] 此外,在一个方面中,作为实例,便携式令牌装置 102 可包含按钮 120。按钮 120 可由用户按下以将 PIN 请求 132 发射到第一装置 104,且随后将 PIN 150 和 MAC 地址 152 发射到第二装置 106。而且,可使用指示器 122 来警示用户便携式令牌装置 102 已成功地与第一装置 104 通信。举例来说,指示器 122 可警示用户已获得与第一装置 104 相关联的 PIN。此外,指示器 122 可用以警示用户便携式令牌装置 102 已成功地与第二装置 106 通信,使得 PIN 150 已发射到第二装置。可使用不同类型的指示器向用户展示此情况。作为实例,指示器 122 可为产生声音 (例如,蜂鸣或嘟嘟声) 的声音装置,或指示器 122 可为产生光来向用户指示这些事件已发生的发光装置 (例如,LED)。所述光可为白色或有色的,且可经定时或闪光等等。应了解,按钮和指示器是便携式令牌装置 102 上的任选实施方案。

[0020] 另外,在一个方面中,便携式令牌装置 102 的存储器 114 可用以临时存储在 PIN 150 和 MAC 地址 152 正从第一装置 104 递送到第二装置 106 时对其进行存储。这可增强便携式令牌装置 102 的安全性特性。作为实例,处理器 110 可在预定时间周期之后 (例如,在 5 或 10 分钟之后) 或在 PIN 150 和随机地址 152 被递送一或多次 (例如,到第二、第三、第四装置等等) 之后从存储器 114 删除 PIN 150 和 MAC 地址 152。PIN 150 和 MAC 地址 152 可被递送的预定时间的长度和次数可为可配置的,且可针对便携式令牌装置 102 来选择。

[0021] 作为一个实例,便携式令牌装置 102 可与第一非便携式装置 104 和第二非便携式

装置 106 一起使用。非便携式装置大体上指代虽然可为固定的或可为可移动的但仍大体上驻留于一个位置处的装置。非便携式装置的实例可包含家庭装置（例如，TV、CD、DVD 播放器、机顶盒、立体声系统、厨房电器、个人计算机等等）、能量监视装置、加热装置、安全性装置、机器到机器（M2M）装置、医疗装置或不容易便携的任一类型的装置。显然，存在可彼此无线通信的广泛多种非便携式装置且此列表不是穷尽的。

[0022] 特定来说，例如第一装置 104 和第二装置 106 等便携式和非便携式无线装置经常不包含用以输入名称、PIN、口令、密钥等等来彼此验证和登记的输入机构（例如，键盘）。便携式令牌装置 102 可用以辅助用户在第一装置 104 处产生 PIN 150 且随后将 PIN 150 传递到另一第二装置 106 以使得所述两个装置（例如，第一装置 104 和第二装置 106）可检验其是否经授权以彼此登记且因此安全地彼此通信。特定来说，通过传递 PIN 150，便携式令牌装置 102 允许第一装置 104 和第二装置 106 基于 PIN 而彼此验证且彼此登记，使得所述装置可链接且安全地彼此通信。这可在不需要用户输入名称、PIN、密钥、口令等等的情况下实现。

[0023] 因此，在便携式令牌装置 102 的实例中，可能不存在键盘、小键盘、显示装置等等。这是因为不需要这些元件。便携式令牌装置的所利用的仅有组件可为：处理器 110、存储器 114 和接口 116。此外，取决于设计考虑，在需要时便携式令牌装置 102 也可利用（或不利用）按钮 120 和指示器 122。因此，本发明的方面提供的益处在于便携式令牌装置 102 在电子组件方面的需要很少。举例来说，不需要或不使用键盘、小键盘、显示装置等等。本质上，便携式令牌装置 102 需要的全部可为处理器、存储器和接口。因此，便携式令牌装置 102 可为将制造和利用的极简单且低成本装置。

[0024] 另外应了解，因为第一非便携式装置 104 和第二非便携式装置 106 经常不包含用以输入名称、口令、PIN、密钥等等的输入机构（例如，键盘、小键盘、显示装置），所以便携式令牌装置 102 使得很容易使第一装置 104 和第二装置 106 彼此通信，而不必记住或键入这些项目。

[0025] 简单另外参考图 2，图 2 展示说明用于由便携式令牌装置 102 实施令牌辅助通信协议的过程 200 的流程图。在决策框 202 处，便携式令牌装置 102 可确定与第一装置 104 的紧密接近耦合是否已发生。如果为否，那么过程结束（或过程可周期性重复）。然而，如果紧密接近耦合已发生，那么可将 PIN 请求发射到第一装置 104（框 204）。接着，便携式令牌装置 102 可获得 PIN（框 208），如先前详细描述。第一装置 104 确定经预配置 PIN、随机 PIN 或随机种子以包含于响应 134 中的可能方式可基于使用情况来界定。作为实例，如果存在设定的经预配置 PIN，那么可发送经预配置 PIN；如果存在第一装置 104 与便携式令牌装置 102 之间的预共享秘密，那么可使用随机种子；或可使用随机 PIN。如果接收到随机种子，那么便携式令牌装置的处理器和第一装置两者可使用随机种子和共享秘密来产生相同的经导出 PIN。

[0026] 接着，在决策框 210 处，便携式令牌装置 102 确定紧密接近耦合是否已与第二装置 106 发生。如果为否，那么过程结束（或过程可周期性重复）。然而，如果紧密接近耦合已与第二装置 106 发生，那么便携式令牌装置 102 将 PIN 发射到第二装置 106（框 212），且第二装置 106 与第一装置 104 之间的装置登记可发生（框 214），如先前所述。

[0027] 另外参见图 3，将说明便携式令牌装置 102 的使用的特定实例。举例来说，在房屋

或建筑结构 300 中,房间 A 中的用户 302 可能希望开始装置登记过程以安全地连接和无线地链接两个装置以彼此交互。在此实例中,便携式令牌装置 102 可为遥控器 312,且第一装置 104 可为机顶盒 320,且第二装置 106 可为电视机 (TV) 322。应注意,在此实例中,先前描述的便携式令牌装置 102 的组件和功能性集成到遥控器 312 中。便携式令牌装置 102 的先前描述的功能性同样适用于此遥控器 312 实例中,且可返回参见图 1。

[0028] 在此实例中,在房间 A 中,用户 302 可首先将遥控器 312 带到机顶盒 320。无线耦合可通过紧密接近无线耦合 130(例如,经由 NFC 耦合)实现,其中用户 302 可用遥控器 312 触碰机顶盒 320。此外,用户 302 也可按下遥控器 312 上的按钮 120 以启用 PIN 请求 132。

[0029] 假定机顶盒 320 和遥控器 312 已经具有用于 PIN 导出的共享秘密,一旦机顶盒 320 通过 NFC 耦合检测到遥控器 312,且接收到 PIN 请求 132,机顶盒 320 便可产生随机种子且可将随机种子连同其 MAC 地址以及其它信息一起发送到遥控器 312。如先前描述,遥控器 312 可基于所接收随机种子和与机顶盒 312 共享的秘密来产生经导出 PIN 150,且可将此 PIN 150 和 MAC 地址 152 局部地存储在存储器 114 中。PIN 150 可用于单次使用,且可仅在短时间周期(例如,5 到 10 分钟)中有效。在此之后,遥控器 312 可将其丢弃。

[0030] 在遥控器 312 已产生 PIN 150 之后,用户 312 可将遥控器 312 带到第二装置,例如 TV 322。用户也可按下遥控器 312 上的按钮 120 以开始将 PIN 150 发射到 TV 322。一旦 TV 322 通过 NFC 检测到遥控器 312,TV 322 便可获取 PIN 150 和 MAC 地址 152 来使用地址 152 起始与机顶盒 320 的装置登记协议 164。以此方式,通过传递 PIN 150 和 MAC 地址 152,遥控器 312 允许机顶盒 320 和 TV 322 开始彼此的安全装置登记通信且检验彼此的验证,使得它们可彼此登记且安全地彼此通信以实现安全 TV 内容发射。这可在不需要用户输入名称、PIN、密钥、口令等等的情况下通过便携式令牌装置增强来实现。

[0031] 特定来说,应了解,PIN 150 可由 TV 322 用作授权令牌以证实与机顶盒 320 的此装置登记由用户批准。作为实例,在家庭网络内,通常仅家庭成员可在短时间周期(例如,5 到 10 分钟)内物理地接近所述两个装置。任选地,TV 322 还可在起始装置登记协议之前请求用户的确认。举例来说,机顶盒 320 信息(例如,装置类型和名称)可在 TV 322 上向用户显示以通过按下遥控器 312 上的适当按钮来确认。

[0032] 在另一实例中,用户 302 可首先将便携式令牌装置 102 带到热控制器 330。无线耦合可通过紧密接近无线耦合 130(例如,经由 NFC 耦合)实现,其中用户 302 可用便携式令牌装置 102 触碰热控制器 330。此外,用户 302 也可按下便携式令牌装置 102 上的按钮 120 以启用 PIN 请求 132。

[0033] 一旦热控制器 330 通过 NFC 耦合检测到便携式令牌装置 102,且接收到 PIN 请求 132,热控制器 330 便可产生随机种子且可将随机种子连同其 MAC 地址以及其它信息一起发送到便携式令牌装置 102。如先前描述,便携式令牌装置 102 可基于所接收随机种子和(与热控制器 330 共享的)秘密来产生 PIN 150,且可将此 PIN 150 和 MAC 地址 152 局部地存储在存储器 114 中。PIN 150 可用于单次使用,且可仅在短时间周期(例如,5 到 10 分钟)中有效。在此之后,便携式令牌装置 102 可将其丢弃。

[0034] 在便携式令牌装置 102 已产生 PIN 150 之后,用户 312 可将遥控器 312 带到房屋 300 的另一区域(例如,房间 B)中的第二装置,例如热传感器 332。用户也可按下便携式令牌装置 102 上的按钮 120 以开始将 PIN 150 发射到热传感器 332。一旦热传感器 332 通过

NFC 检测到便携式令牌装置 102, 热传感器 332 便可获取 PIN 150 和 MAC 地址 152 来使用地址 152 起始与热控制器 330 的装置登记协议 164。以此方式, 通过传递 PIN 150 和 MAC 地址 152, 便携式令牌装置 102 允许热控制器 330 和热传感器 332 检验彼此的授权且安全地彼此登记, 使得它们可关于加热功能性安全地彼此通信。这可在不需要用户输入名称、PIN、密钥、口令等等的情况下实现。此外, 便携式令牌装置 102 还可以相同方式用以检验授权且针对加热功能性登记其它热传感器 332 (例如, 在房间 C 和 D 中)。因此, 便携式令牌装置 102 可用以授权和登记多个装置。

[0035] 应了解, 先前描述的机顶盒、TV、热控制器、热传感器等等仅为实例。其它非便携式装置的实例可包含家庭装置 (例如, TV、CD、DVD 播放器、机顶盒、立体声系统、厨房电器、个人计算机等等)、能量监视装置、加热装置、安全性装置、机器到机器 (M2M) 装置、医疗装置或不可容易便携的任一类型的装置。显然, 存在可彼此无线通信的广泛多种非便携式装置 (例如 M2M 装置) 且此列表不是穷尽的。

[0036] 如先前描述, 无线装置 (便携式和非便携式) 经常不包含用以输入名称、PIN、口令、密钥等等来彼此验证和登记的输入机构 (例如, 键盘)。便携式令牌装置 102 可用以辅助用户在第一装置处产生 PIN 且随后将 PIN 传递到另一第二装置以使得所述两个装置可安全地彼此通信。特定来说, 通过传递 PIN, 便携式令牌装置 102 允许第一装置、第二装置以及其它多个装置检验彼此的授权且彼此登记以使得它们可链接且安全地彼此通信。这可在不需要用户输入名称、PIN、密钥、口令等等的情况下实现。有利地, 如先前所述, 此方法可由不具有用以输入 PIN、口令、密钥名称等等的按钮或键盘的装置使用。此外, 这些实施方案还通过不要求用户记住任何 PIN 或按钮序列而改善了用户体验。这些方法还可由 M2M 装置广泛使用, 因为许多 M2M 装置不具有任何 PIN 插入机构。而且应了解, 便携式令牌装置 102 的方面可在其它装置中实施, 例如遥控器、M2M 装置、移动计算机、移动装置、个人数字助理、无线电话、无线装置、手机、智能电话、平板计算机、膝上型计算机, 或任一类型的便携式计算装置。

[0037] 应了解, 先前描述的本发明的方面可结合便携式令牌装置 102 的处理器 110 以及第一装置 104 和第二装置 106 的处理器 124 和 128 和 / 或其它装置的指令执行来实施。特定来说, 便携式令牌装置的电路以及第一和第二装置 (包含但不限于处理器) 可在用以执行根据本发明实施例的方法或过程的程序、例程或指令执行的控制下操作。举例来说, 此程序可以固件或软件实施 (例如, 存储在存储器和 / 或其它位置中), 且可由便携式令牌装置以及第一和第二装置的处理器和 / 或其它电路实施。此外应了解, 术语处理器、微处理器、电路、控制器等等指代能够执行逻辑、命令、指令、软件、固件、功能性等等的任一类型的逻辑或电路。

[0038] 应了解, 当便携式令牌装置和其它装置为移动或无线装置时, 其可通过无线网络经由基于或另外支持任何合适无线通信技术的一或多个无线通信链路通信。举例来说, 在一些方面中, 便携式令牌装置和其它装置可与包含无线网络的网络相关联。在一些方面中, 网络可包括人体区域网络或个域网 (例如, 超宽带网络)。在一些方面中, 网络可包括局域网或广域网。无线装置可支持或另外使用多种无线通信技术、协议或标准中的一或多者, 例如 CDMA、TDMA、OFDM、OFDMA、WiMAX 和 Wi-Fi。类似地, 无线装置可支持或另外使用多种对应调制或多路复用方案中的一或多者。无线装置可因此包含适当组件 (例如, 空中接口)

以使用上述或其它无线通信技术建立一或多个无线通信链路和经由所述一或多个无线通信链路通信。举例来说,装置可包括具有相关联发射器和接收器组件(例如,发射器和接收器)的无线收发器,所述组件可包含促进经由无线媒体的通信的各种组件(例如,信号产生器和信号处理器)。众所周知,移动无线装置可因此与其它移动装置、手机、其它有线和无线计算机、因特网网站等等无线地通信。

[0039] 本文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)和其它系统。术语“系统”和“网络”经常可互换地使用。CDMA系统可实施例如通用陆地无线电接入(UTRA)、CDMA2000等等无线电技术。UTRA包含宽带CDMA(W-CDMA)和CDMA的其它变体。CDMA2000涵盖暂行标准(IS)-2000、IS-95和IS-856标准。TDMA系统可实施例如全球移动通信系统(GSM)等无线电技术。OFDMA系统可实施例如以下无线电技术:演进型通用陆地无线电接入(演进型UTRA或E-UTRA),超移动宽带(UMB),电气电子工程师协会(IEEE)802.11(Wi-Fi),IEEE 802.16(WiMAX),IEEE 802.20,快闪OFDM,RTM等等。通用陆地无线电接入(UTRA)和E-UTRA是通用移动通信系统(UMTS)的部分。3GPP长期演进(LTE)是UMTS的使用E-UTRA的即将到来的版本,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在来自名为“第三代合作伙伴计划”(3GPP)的组织的文献中描述。CDMA2000和UMB在来自名为“第三代合作伙伴计划2”(3GPP2)的组织的文献中描述。

[0040] 本文的教导可并入到多种设备(例如,装置)中(例如,在其内实施或由其执行)。举例来说,本文教导的一或多个方面可并入到以下装置中:电话(例如,蜂窝式电话)、个人数据助理(“PDA”)、平板计算机、移动计算机、膝上型计算机、平板计算机、娱乐装置(例如,音乐或视频装置)、头戴式耳机(例如,头戴受话器、耳机等等)、医疗装置(例如,生物计量传感器、心率监视器、计步器、EKG装置等等)、用户I/O装置、计算机、服务器、销售点装置、娱乐装置、机顶盒,或任一其它合适装置。这些装置可具有不同的电力和数据要求。

[0041] 在一些方面中,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)。此接入装置可提供例如经由有线或无线通信链路到另一网络(例如,例如因特网或蜂窝式网络等广域网)的连接性。因此,接入装置可使得另一装置(例如,Wi-Fi站)能够接入另一网络或某种其它功能性。另外应了解,所述装置中的一者或两者可为便携式的,或在一些情况下为相对非便携的。

[0042] 所属领域的技术人员将了解,可使用多种不同技艺和技术中的任一者来表示信息和信号。举例来说,贯穿以上描述可参考的数据、指令、命令、信息、信号、位、符号和码片可通过电压、电流、电磁波、磁场或磁粒子、光场或光粒子或其任一组合来表示。

[0043] 所属领域的技术人员将进一步了解,结合本文揭示的实施例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、计算机软件或两者的组合。为了清楚地说明硬件与软件的此可互换性,上文已大体在其功能性方面描述了各种说明性组件、块、模块、电路和步骤。此功能性实施为硬件还是软件取决于特定应用和强加于总体系统的设计约束。所属领域的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,但此些实施方案决策不应解释为造成脱离本发明的范围。

[0044] 结合本文揭示的实施例描述的各种说明性逻辑块、模块和电路可以通用处理器、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、离散硬件组件或其经设计以执行本文描述的功能的任一组合来实施或执行。通用处理器可为微处理器,但在替代例中,处理器可为任何常规处理器、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 与微处理器的组合、多个微处理器、结合 DSP 核心的一或多个微处理器,或任何其它此类配置。

[0045] 结合本文揭示的实施例描述的方法或算法的步骤可直接以硬件、以由处理器执行的软件模块或以两者的组合来体现。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、可装卸式磁盘、CD-ROM 或此项技术中已知的任一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和向存储媒体写入信息。在替代方案中,存储器媒体可与处理器成一体式。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。

[0046] 在一或多个示范性实施例,所描述功能可以硬件、软件、固件或其任一组合实施。如果以软件实施为计算机程序产品,那么功能可作为一或多个指令或代码存储于计算机可读媒体上或经由计算机可读媒体传输。计算机可读媒体包含计算机存储媒体和通信媒体两者,所述通信媒体包含促进计算机程序从一处转移到另一处的任何媒体。存储媒体可为可由计算机存取的任何可用媒体。举例来说且并非限制,计算机可读媒体可包括 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储装置、磁盘存储装置或其它磁性存储装置,或可用以载运或存储呈指令或数据结构形式的所要程序代码且可由计算机存取的任何其它媒体。而且,将任何连接恰当地称为计算机可读媒体。举例来说,如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或例如红外线、无线电和微波等无线技术从网站、服务器或其它远程源发射软件,那么同轴电缆、光纤电缆、双绞线、DSL 或例如红外线、无线电和微波等无线技术包含于媒体的定义中。如本文所使用,磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软磁盘和蓝光光盘,其中磁盘通常以磁性方式再生数据,而光盘用激光以光学方式再生数据。以上各项的组合也应包含在计算机可读媒体的范围内。

[0047] 提供所揭示实施例的先前描述以使得所属领域的技术人员能够制作或使用本发明。所属领域的技术人员将容易明了对这些实施例的各种修改,且在不脱离本发明的精神或范围的情况下可将本文界定的一般原理应用于其它实施例。因此,本发明既定不限于本文展示的实施例,而是应被赋予与本文揭示的原理和新颖特征一致的最广范围。

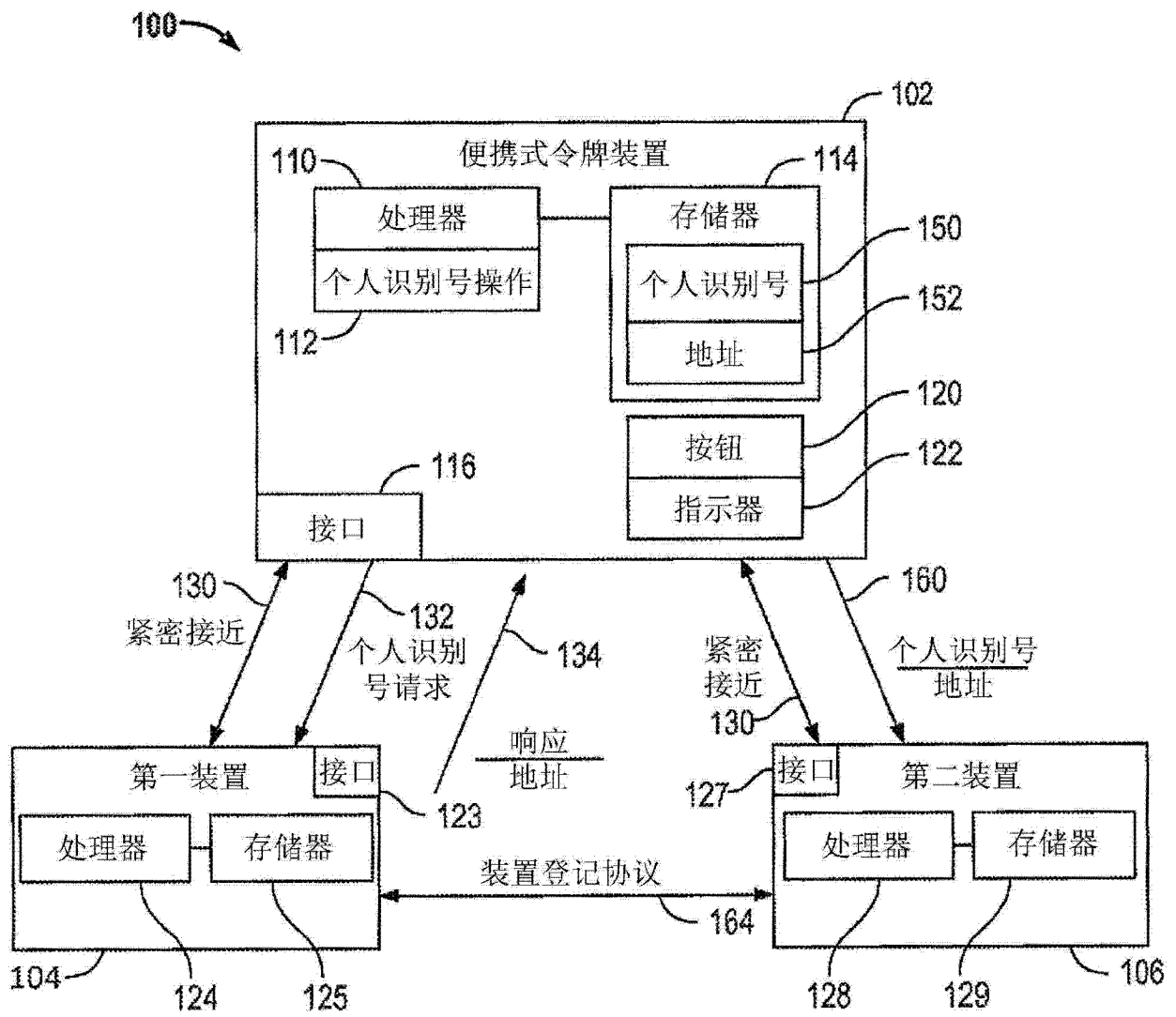


图 1

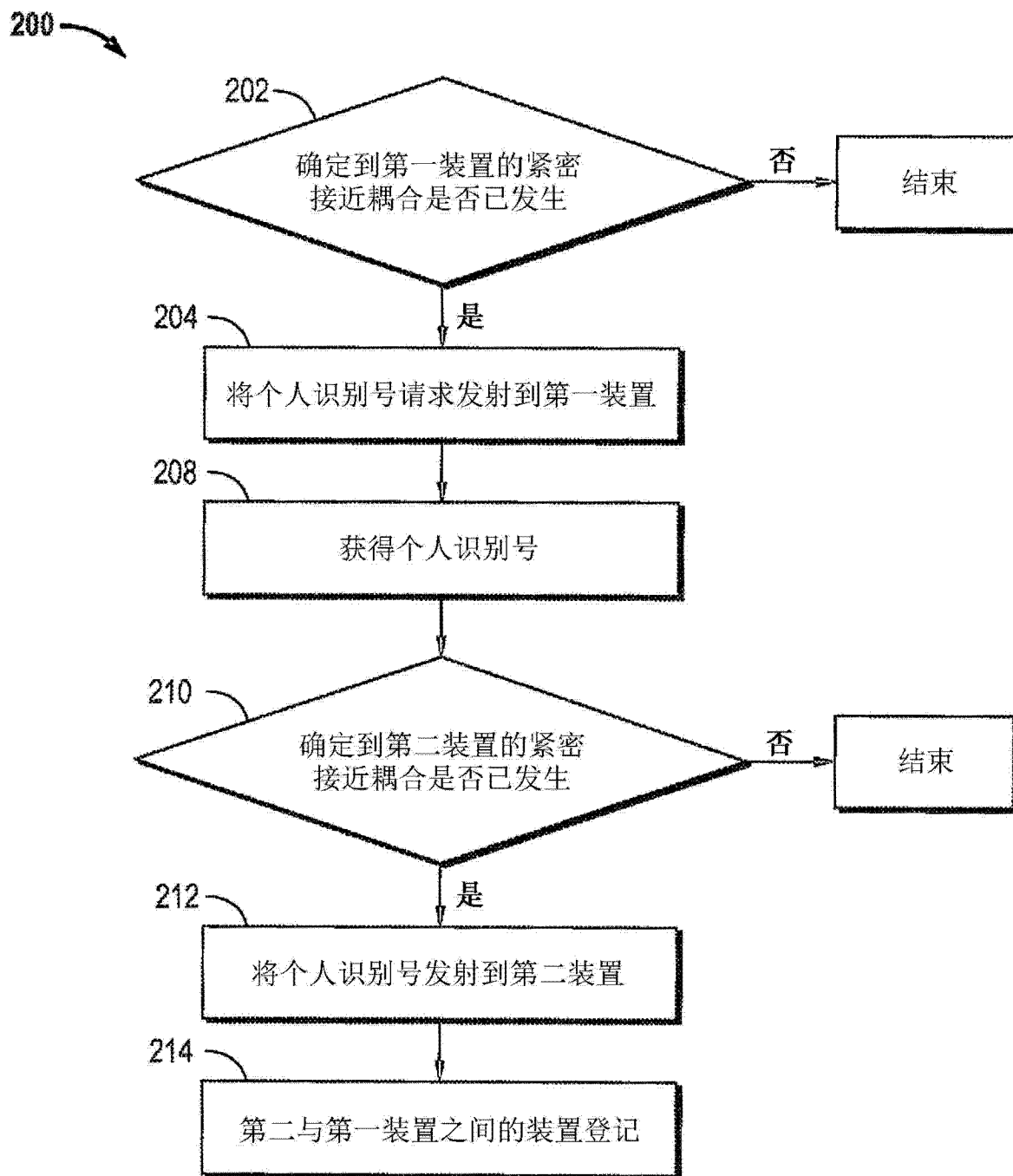


图 2

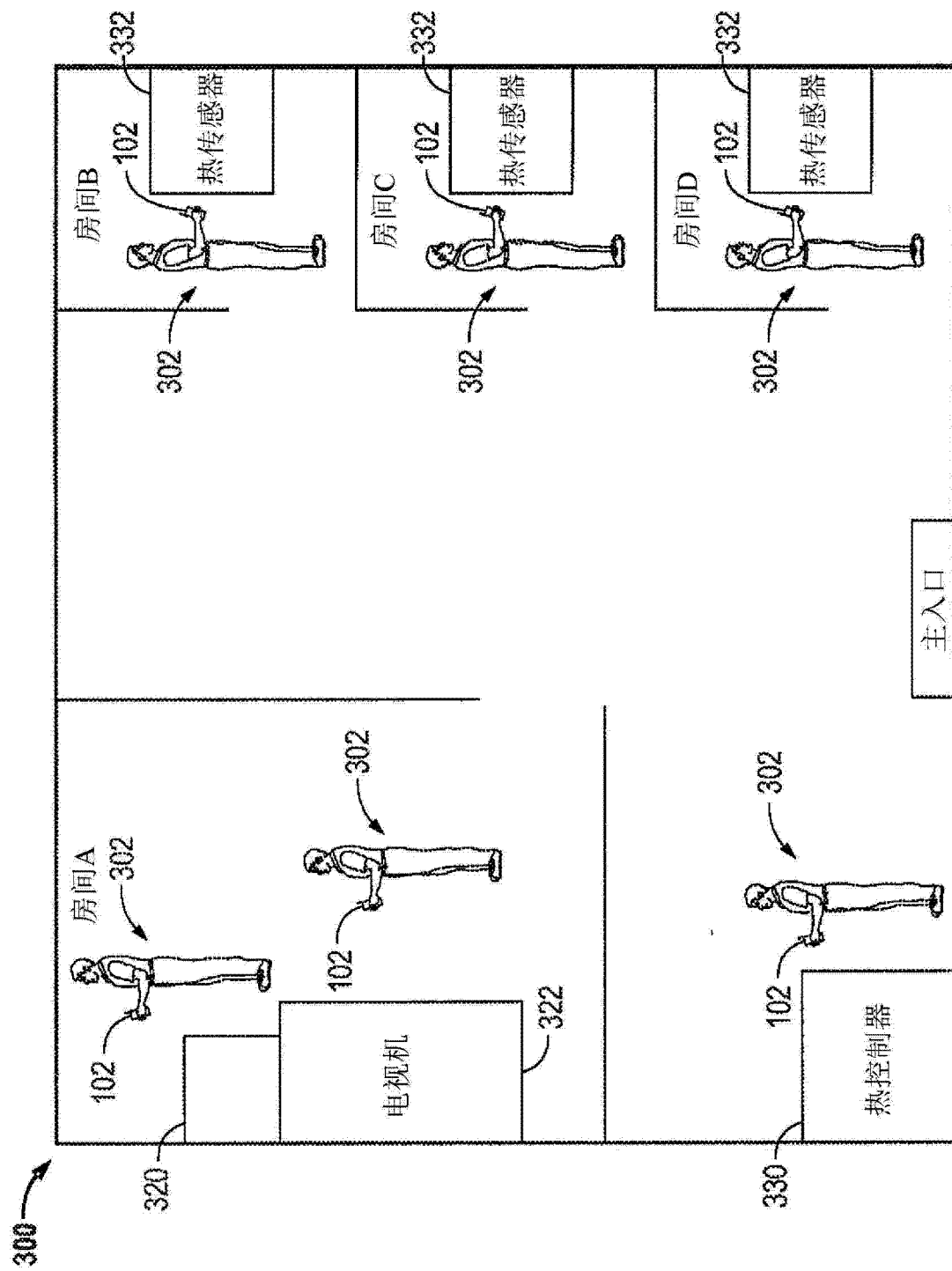


图 3