[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/06
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 03814830.7

[43] 公开日 2005 年 8 月 31 日

[11] 公开号 CN 1663219A

[22] 申请日 2003.5.30 [21] 申请号 03814830.7
[30] 优先权
[32] 2002. 6.26 [33] US [31] 10/183,152
[86] 国际申请 PCT/US2003/017224 2003.5.30
[87] 国际公布 WO2004/004279 英 2004.1.8
[85] 进入国家阶段日期 2004.12.24
[71] 申请人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 D·基琴

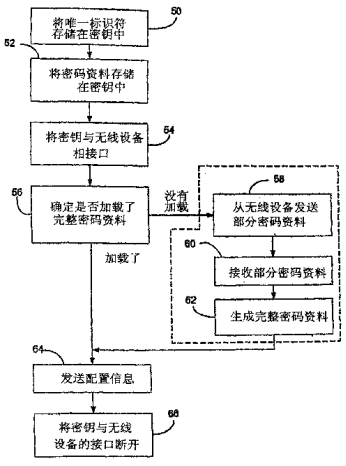
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 火惠颖

权利要求书 4 页 说明书 4 页 附图 3 页

[54] 发明名称 用于无线设备配置的活动密钥

[57] 摘要

一种配置无线设备的密钥，包括：存储包括唯一网络标识符在内的网络配置信息的非易失性存储器。一种与非易失性存储器相耦合的电路，对网络配置信息进行管理。一种接口，与无线设备进行包括网络配置信息在内的数据的通信。



ISSN1008-4274

1．一种密钥，其特征在于，包括：

非易失性存储器，用于存储网络上的无线设备的网络配置信息，该网络配置信息包括唯一网络标识符；

与非易失性存储器相耦合的配置管理电路，用于管理网络配置信息；和

接口，用于与无线设备进行包括网络配置信息在内的数据通信。

2. 如权利要求 1 所述的密钥，其特征在于，所述配置管理电路包括处理器。

3. 如权利要求 1 所述的密钥，其特征在于，还包括用于管理网络配置信息的密钥管理器；和

所述非易失性存储器包括可编程存储器。

4. 如权利要求 3 所述的密钥，其特征在于，非易失性存储器包括第一部分密码资料；和

密钥管理器，操作该管理器从无线设备接收第二部分密码资料，从第一部分密码资料和第二部分密码资料生成完整的密码资料，并将完整的资料存储在可编程存储器中。

5. 如权利要求 4 所述的密钥，其特征在于，所述第二部分密码资料存储在非易失性存储器中。

6. 如权利要求 3 所述的密钥，其特征在于，还包括密钥接收器，用于从无线设备接收完整的密钥并将其存储在可编程存储器中。

7. 一种方法，其特征在于，包括：

将密钥设备与无线设备相接口；

将网络配置信息从密钥设备发送至无线设备，该网络配置信息包括唯一标识符；和

在所述发送之后，将密钥设备从无线设备断开接口。

8. 如权利要求 7 所述的方法，其特征在于，所述发送网络配置信息包括发送完整的密码资料。

9. 如权利要求 7 所述的方法，其特征在于，还包括确定所述密钥设备是否包括完整的密码资料。

10. 如权利要求 9 所述的方法，其特征在于，还包括：响应于确定密钥设备

是否包括第一部分密码资料；

从无线设备请求第二部分密码资料；和

接收第二部分密码资料；和

从第二部分密码资料生成完整的密码资料。

11. 如权利要求 10 所述的方法，其特征在于，所述生成完整的密码资料包括将第一部分密码资料与第二部分密码资料相结合。

12. 如权利要求 11 所述的方法，其特征在于，所述发送网络配置信息包括发送完整的密码资料。

13. 如权利要求 9 所述的方法，其特征在于，包括响应于确定密钥设备不包括完整的密码资料：

从无线设备将第一密码资料发送至密钥设备；

接收第一密码资料；和

将接收到的第一密码资料存储在非易失性存储器中。

14. 如权利要求 13 所述的方法，其特征在于，所述发送网络配置信息包括发送第一密码资料。

15. 一种方法，其特征在于，包括：

将密钥设备与无线设备相接口；

确定所述密钥设备是否包括完整的密码资料；

响应于确定密钥设备不包括完整的密码资料，生成完整的密钥资料；

将网络配置信息从密钥设备发送至无线设备，该网络配置信息包括完整密钥资料；和

在所述发送之后，将密钥设备从无线设备断开接口。

16. 如权利要求 15 所述的方法，其特征在于，所述生成完整的密码材料包括：

从无线设备接收第二部分密码资料；和

从第二部分密码资料生成完整的密码资料。

17. 如权利要求 16 所述的方法，其特征在于，所述生成完整的密码资料包括从无线设备请求第二部分密码资料。

18. 如权利要求 16 所述的方法，其特征在于，所述生成完整的密码资料包括

将存储在非易失性存储器中的第二部分密码资料与第一密码资料相结合。

19. 如权利要求 18 所述的方法，其特征在于，还包括将完整的密码资料存储在非易失性存储器中。

20. 如权利要求 19 所述的方法，其特征在于，所述存储还包括盖写所述第一部分密码资料。

21. 一种无线设备，其特征在于，包括：

端口，与包括完整的密码资料在内的网络配置信息的指定类型的密钥相接口；和

与密钥通信的密钥管理器，该密钥管理器从密钥接收网络配置信息。

22. 如权利要求 21 所述的无线设备，其特征在于，所述端口为串行接口。

23. 如权利要求 21 所述的无线设备，其特征在于，所述密钥管理器传送部分密码资料至密钥，以形成密钥中的完整的密码资料。

24. 如权利要求 21 所述的无线设备，其特征在于，还包括：存储完整的密码资料的非易失性存储器。

25. 如权利要求 24 所述的无线设备，其特征在于，所述完整的密码资料为加密密钥。

26. 如权利要求 24 所述的无线设备，其特征在于，所述密钥管理器用完整的密码资料来协商加密密钥。

27. 如权利要求 21 所述的无线设备，其特征在于，所述网络配置信息还包括唯一网络标识符。

28. 一种网络，其特征在于，包括：

密钥，该密钥包括：

存储包括唯一网络标识符在内的网络配置信息的非易失性存储器；

与非易失性存储器相耦合的用于管理网络配置信息的电路；和

与无线设备进行包括网络配置信息在内的数据通信的接口；和

可由密钥配置的在网络上运行的无线设备，该无线设备包括：

与密钥相连的接口；和

与密钥通信的密钥管理器，该密钥管理器从密钥接收网络配置信息。

29. 如权利要求 28 所述的网络，其特征在于，所述无线设备端口是串行端口。

30. 如权利要求 28 所述的网络，其特征在于，所述密钥管理器将部分密码资料传送至密钥以形成密钥中的完整的密码资料。

31. 一种物品，其特征在于，包括机器可读媒体，该媒体中包括的机器可读指令在由机器执行时，使机器：

确定与无线设备相接口的密钥设备是否包括完整的密码资料；

响应于确定密钥设备不包括完整的密码资料，生成完整的密码资料；和

将网络配置信息从密钥设备发送到无线设备，该网络配置信息包括完整的密码资料。

32. 如权利要求 31 所述的物品，其特征在于，所述生成完整的密码资料包括：

从无线设备接收第二部分密码资料；和

从第二部分密码资料生成完整的密码资料。

33. 如权利要求 31 所述的物品，其特征在于，所述生成完整的密码资料包括从无线设备请求第二部分密码资料。

34. 如权利要求 31 所述的物品，其特征在于，所述生成完整的密码资料包括将存储在非易失性存储器中的第二部分密码资料和第一密码资料相结合。

35. 如权利要求 34 所述的物品，其特征在于，还包括：将完整的密码资料存储在非易失性存储器中。

36. 如权利要求 35 所述的物品，其特征在于，所述存储还包括盖写第一部分密码资料。

用于无线设备配置的活动密钥

技术领域

本发明涉及和无线网络一起使用的配置设备。

背景技术

随着诸如膝上电脑、个人数字助理、照相机、电子邮件终端、VCR 和摄录象机之类的移动设备的增长对局域网无线访问的需求也持续增长。随着无线 LAN 的日益增长，与那些无线 LAN（特别是涉及安全的）相关的配置也考虑相应增加。符合 IEEE 802.11 标准、IEEE 802.11-1999 无线分组的当前无线设备的配置信息包括唯一标识符、加密密钥及其它几个参数的输入。通常可以通过用键盘、菜单系统、触摸屏或一些其它的键盘设备手工键入配置信息。该信息可包括一个长字符串，以提供充分的安全程度。手工输入配置信息会不方便。

附图说明

图 1 为无线局域网的方框图。

图 2 为与无线设备接口的密钥的方框图。

图 3 为另一与无线设备接口的密钥的方框图。

图 4 为密钥操作的流程图。

在各图中，同样的标号指示同样的元件。

具体说明

图 1 示出与接入点 14 和几个无线设备 12a-12d 互连的无线局域网（LAN）10。接入点 14 和各无线设备 12a－12d 包括配置信息，以提供在 WLAN 上的安全通信。配置信息可包括标识符、加密密钥和用作协商加密密钥的起点的密码资料。接入点 14 可以通过硬连线连接 16 将 WLAN10 与诸如因特网或以太网之类的另一网络 18 相连。WLAN10 是允许无线设备 12a－12d 经空中传送数据的，使得对有线连接的需求最小化的灵活的通信系统。任何可用的通信机构或方法包括码分多址（CDMA）、跳频、正交频分多路复用（OFDM）、红外的、和窄带单频，也可以使用其它方法

而不限制本发明。可以将 WLAN10 用于各种功能，包括：家庭互联、制造、仓库贮存、卫生保健、零售和学术界等。

各无线设备 12a-12d 和接入点 14 可包括用于接收存储在密钥 30 内的密码资料 35 的端口 20a－20e。密钥 30 适于与端口 20a-20e 连接，并可以用于将密码资料传送至无线设备 12a－12d 和接入点 14。

图 2 示出密钥 30 的方框图。密钥 30 可包括诸如处理器 32 之类的数字电路，以传送密码资料。非易失性存储器 34 可以存储要传送至无线设备 12a-12d 的密码资料 35 和可由处理器 32 执行的设备程序。

密码资料 35 可以直接用作加密密钥或被设备 12 或 14（图 1）用作起点来协商加密密钥。密码资料 35 可以是固定的、可编程的或部分固定/部分可编程的。固定密码资料被永久地存储在非易失性存储器 34 中。固定信息可以在制作密钥 30 期间被存储，或通过将密钥 30 与无线设备 12a－12d 和接入点 14 接口来编程。固定密码资料是一次性存储在密钥 30 中的并且不可以重新编程。相反，可编程密码资料是可以改变的。部分固定/部分可编程密码资料可包括可改变的部分，及余下的固定密码资料。

加密密钥管理器可包括在设备程序中以在密钥 30 和无线设备 12 或接入点 14 之间传送密码资料 35。另选地，加密密钥管理器还可以包括在接入点 14 和无线设备 12a-12d 中。

密钥 30 可包括与对应于 WLAN 上的设备的端口 20 连接的连接器 31。可以将任何类型的传送信息的接口用于与端口 20a-20e 相连，包括：串行接口、通用串行总线（USB）和红外线（IR）。例如：可以用配置成具有连接器的门锁和带有附加连接器的“智能卡”的设备来实施串行端口接口。“智能卡”可以具有与具有卡内电子电路的信用卡类似的形状因数。密钥 30 被插入与设备相对应的端口 20a-20e，以将密码资料 35 传送至 WLAN 上的设备。WLAN 设备可以将密码资料 35 用作起点以与另一 WLAN 设备协商加密密钥。

图 3 示出与另一密钥 72 相耦合的无线设备 70，以在它们之间传送配置信息。无线设备 70 可以被包括在 WLAN 中。密钥 72 包括与无线设备 70 的端口 78 相耦合的接口 74。接口 74 可以是任何类型的用于在无线设备端口 78 和密钥 72 之间传送信息的接口。接口 74 与可存储固定或可编程的密码资料或两者都可存储的非易

失性存储器 76 相连。

无线设备 70 包括处理器 80 和与端口 78 耦合的非易失性存储器 82。处理器 80 可包括用于在密钥 72 和无线设备 70 之间传送密码资料的加密密钥管理器。例如：如果密钥 72 包括完整的密码资料、加密密钥管理器可以对将密码资料传送至无线设备 70 进行管理。如果密钥 72 包括部分密码资料或无密码资料，加密密钥管理器可以将密码资料从无线设备 70 传送至密钥 72 以生成密钥 30 中完整的密码资料。无线设备密码资料可以存储在无线设备非易失性存储器 76 中。与处理器相耦合的无线接口 82 便于与 WLAN 上的其它无线设备通信。

图 4 示出密钥过程的一个方面的流程图。在制作密钥期间可以将唯一标识符存储在 50 处的非易失性存储器中。该唯一标识符可以是与由在该 WLAN 上所有设备使用的的特定 WLAN 相对应的序列号或名字。在 52 处，可以将完整的密码资料编程到密钥的密钥存储部分。在另选的实施中，可以将部分密码资料或无密码资料编程到密钥存储部分。

密钥存储部分可包括可重编程序的存储器和/或固定存储器。一方面，可以将完整的固定密钥编程到密钥的固定存储器中。第二方面，可以将部分密码资料编程到固定存储器中，而余下的部分可以编程。第三方面，可以将所有的密码资料编程到可重编程的存储器。

当用固定存储器中的完整的固定密钥配置密钥时，密钥变成一个简单、廉价的设备。固定密钥是不可以重新编程的。因此，新的加密密钥需要新的密钥设备。

当用在可重新编的存储器中的部分密码资料或无密码资料配置密钥时，可以提高该密钥的安全性，因为最终用户可以对加密密钥重新编程以提高对唯一标识符和加密密钥的独立性。

在方框 54，可以将密钥与无线设备相接口，以将配置信息发送至无线设备。接口最好包括双线串行接口，以在密钥和无线设备之间传导信号。

方框 56 确定密码材料的加载状态。加载状态包括存储设备的类型和密码资料的数量。密码资料加载状态可以由无线设备和无线密钥确定。方框 58 检测是否加载了完整的密码资料。如果没有，则无线设备将部分密码资料或完整的密码资料发送至无线密钥。在 60 和 62 处，密钥接收密码资料并生成完整的密码资料。在 64 处，密钥 30 将包含完整的密码资料和唯一网络标识符在内的配置信息发送

至无线设备。在 66 处，密钥被从无线设备断开接口。

对本发明的若干实施例进行的描述。然而，我们将理解可以作出各种变体而不偏离本发明的精神和范围。因此，其它实施例在下列权利要求的范围内。

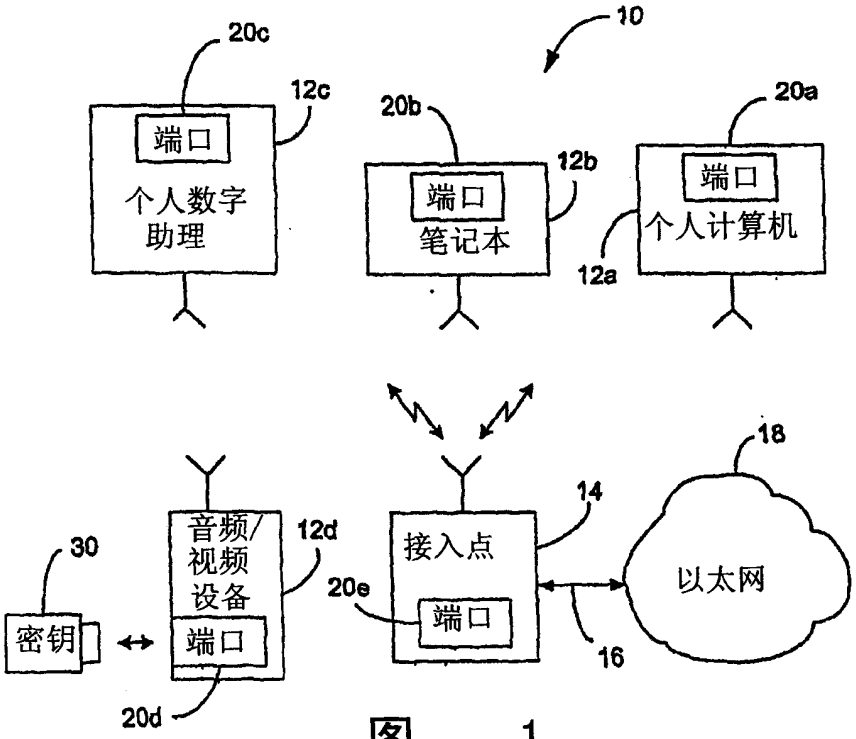

10
20c
12c
端口
个人数字助理
20b
端口
笔记本
12b
20a
端口
个人计算机
12a
18
14
音频/视频设备
12d
接入点
以太网
30
密钥
端口
20e
端口
16
20d

图 1

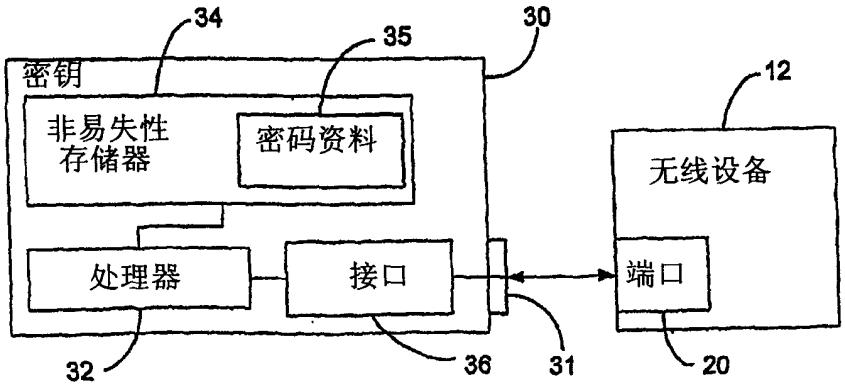

34
35
30
密钥
非易失性存储器
密码资料
12
无线设备
处理器
接口
端口
32
36
31
20

图 2

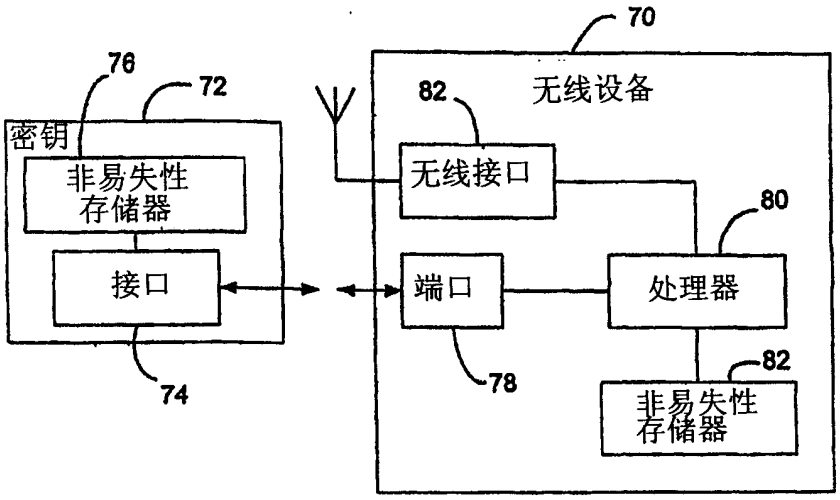


图 3

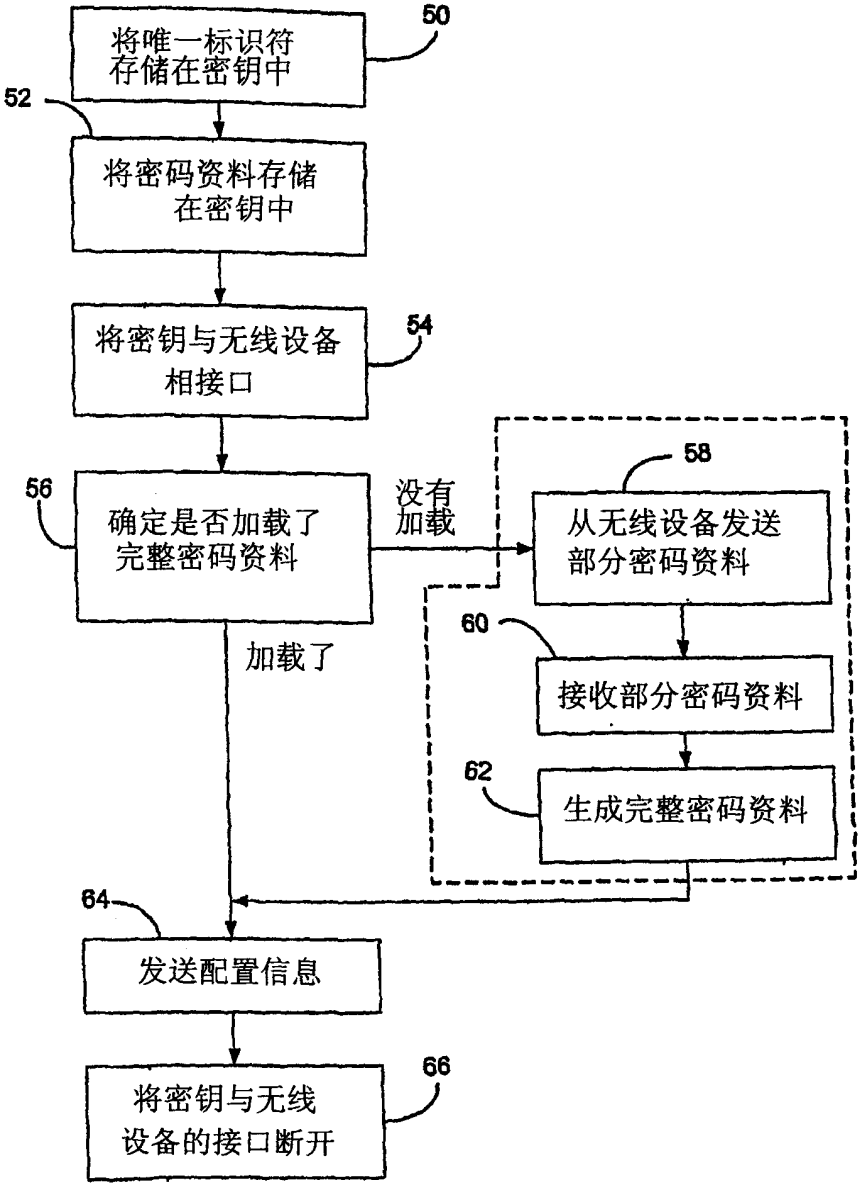

将唯一标识符
存储在密钥中
50
52
将密码资料存储
在密钥中
将密钥与无线设备
相接口
54
56
确定是否加载了
完整密码资料
没有
加载
58
从无线设备发送
部分密码资料
60
接收部分密码资料
62
生成完整密码资料
加载了
64
发送配置信息
将密钥与无线
设备的接口断开
66

图 4