(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104205899 B
(45)授权公告日 2018.06.08

(21)申请号 201380014931.0

(22)申请日 2013.03.20

(65)同一申请的已公布的文献号
申请公布号 CN 104205899 A

(43)申请公布日 2014.12.10

(30)优先权数据
61/613,438 2012.03.20 US
61/637,234 2012.04.23 US
13/843,395 2013.03.15 US

(85)PCT国际申请进入国家阶段日
2014.09.18

(86)PCT国际申请的申请数据
PCT/US2013/033161 2013.03.20

(87)PCT国际申请的公布数据
WO2013/142606 EN 2013.09.26

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 O·J·贝诺伊特
A·帕拉尼恭德尔 S·Y·D·何
A·佩雷斯 B·P·莫汉蒂
E·G·科恩

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
H04W 12/04(2009.01)
H04L 29/06(2006.01)
H04W 4/80(2018.01)
H04W 12/06(2009.01)
G06F 13/10(2006.01)

(56)对比文件
EP 181663 A1,2008.01.23,说明书第[0008]-[0042]段,图1-3.
EP 1993301 A1,2008.11.19,说明书第[0007]-[0011], [0052]-[0065]段.
US 2010318795 A1,2010.12.16,说明书第[0009]-[0054]段,图4.

审查员 李燕

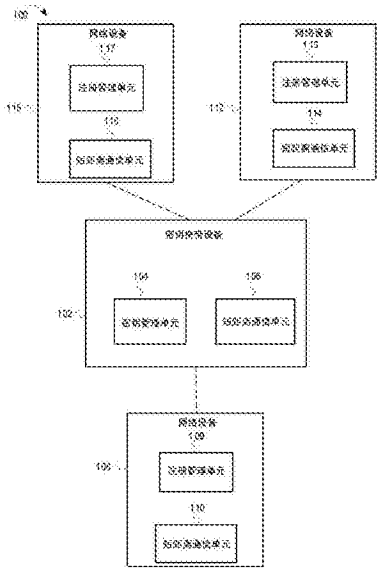
权利要求书8页 说明书43页 附图24页

(54)发明名称

使用短距离无线通信的网络安全配置

(57)摘要

本文公开了用于配置通信网络中的网络设备((109)、(113)、(117))的配置设备。该配置设备通过短距离通信连接发起与网络设备的配对操作(302)。该配置设备确定网络设备是处于注册状态还是未注册状态(304)。如果该配置设备确定网络设备处于未注册状态,则该配置设备在该配置设备与该网络设备之间建立安全短距离通信信道(306)。该配置设备通过安全短距离通信信道向网络设备发送网络密钥,以配置该网络设备通信地连接到所述通信网络(308)。如果该配置设备确定网络设备处于注册状态,则该配置设备确定是否将该网络设备注销(314)。



CN 104205899 B

1.一种用于使用配置设备来配置网络设备的方法，所述方法包括：

由所述配置设备通过与所述网络设备的短距离通信连接来发起与所述网络设备的配对操作；

由所述配置设备确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备处于所述未注册状态，则

在所述配置设备与所述网络设备之间建立短距离通信信道；以及

通过所述短距离通信信道向所述网络设备发送网络密钥，以便配置所述网络设备通信地连接到通信网络。

2.根据权利要求1所述的方法，还包括：

如果确定所述网络设备关于所述配置设备和其它配置设备处于未注册状态，则向所述配置设备注册所述网络设备。

3.根据权利要求1所述的方法，还包括如果确定所述网络设备处于所述已注册状态，则：

确定所述网络设备是向所述配置设备注册的；

确定是否将所述网络设备注销；并且

响应于确定所述网络设备是向所述配置设备注册的以及确定将所述网络设备注销，通过所述短距离通信信道向所述网络设备发送至少一个消息以将所述网络设备注销。

4.根据权利要求3所述的方法，其中发送至少一个消息以将所述网络设备注销包括：

发送至少一个指令，以删除在所述配对操作期间在所述网络设备处存储的数据。

5.根据权利要求1所述的方法，其中发起与所述网络设备的配对操作包括以下操作中的一项：

通过交换并存储所述网络设备的设备标识符和多个配对密钥来与所述网络设备配对；以及

使用非对称加密方案与所述网络设备进行配对。

6.根据权利要求5所述的方法，其中使用所述非对称加密方案与所述网络设备进行配对包括：

在所述网络设备处存储所述配置设备的公共密钥。

7.根据权利要求1所述的方法，其中确定所述网络设备是处于所述已注册状态还是所述未注册状态包括：

从所述配置设备向所述网络设备发送包含第一信息的第一消息；以及

基于响应于所述第一消息接收的第二消息来确定所述网络设备是处于所述已注册状态还是所述未注册状态。

8.根据权利要求1所述的方法，其中，所述短距离通信连接是近场通信(NFC)连接。

9.根据权利要求1所述的方法，其中所述短距离通信连接是以下各项中的一项：

蓝牙通信连接、ZigBee通信连接、和无线局域网(WLAN)通信连接。

10.根据权利要求1所述的方法，其中所述短距离通信信道包括支持完整性、加密和重放保护的安全的短距离通信信道。

11.根据权利要求1所述的方法，其中所述短距离通信信道是使用第一频带的带外通信

信道，其中通过所述短距离通信信道发送所述网络密钥给所述网络设备是为了配置所述网络设备使用与所述第一频带不同的第二频带通信地连接到所述通信网络。

12.根据权利要求1所述的方法，还包括：

提供所述配置设备的标识符给所述网络设备，以注册所述网络设备；以及

在所述配置设备处接收所述网络设备的标识符并保存所述网络设备的所述标识符。

13.一种用于配置网络设备的方法，所述方法包括：

在所述网络设备处，通过短距离通信连接接收来自配置设备的用以向所述配置设备进行注册的请求；

确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备处于所述未注册状态，则

向所述配置设备发送响应，以指示所述网络设备处于所述未注册状态；

在所述网络设备与所述配置设备之间建立短距离通信信道；

通过所述短距离通信信道从所述配置设备接收至少一个密钥，以向所述配置设备进行注册；

通过所述短距离通信信道从所述配置设备接收网络密钥，以便配置所述网络设备通过通信网络进行通信；以及

使用所述网络密钥通过所述通信网络进行通信。

14.根据权利要求13所述的方法，其中所述注册请求包括所述配置设备的标识符。

15.根据权利要求13所述的方法，其中所述注册请求包括所述配置设备的公共密钥。

16.根据权利要求13所述的方法，其中所述短距离通信信道是使用第一频带的带外通信信道，所述第一频带不同于通信网络使用的第二频带。

17.根据权利要求13所述的方法，其中，进行注册的所述请求包括随机数，并且响应于在所述网络设备处接收到所述随机数，计算在所述网络设备处存储的至少一个密钥的哈希值，并将所述哈希值发送给所述配置设备。

18.根据权利要求16所述的方法，其中，进行注册的所述请求包括对随机数的请求，并且响应于在所述网络设备处接收到针对所述随机数的所述请求，向所述配置设备发送随机数。

19.根据权利要求13所述的方法，其中确定所述网络设备是处于所述已注册状态还是所述未注册状态包括：

将存储在所述网络设备处的至少一个参数与从所述配置设备接收的参数进行比较。

20.根据权利要求13所述的方法，其中向所述配置设备发送所述响应还包括：

向所述配置设备发送存储在所述网络设备处的所述通信网络的网络密钥。

21.根据权利要求20所述的方法，其中发送存储在所述网络设备处的所述通信网络的所述网络密钥还包括：

向所述配置设备发送所述网络密钥的哈希值。

22.根据权利要求13所述的方法，其中所述通信网络包括一个或多个其它网络设备。

23.根据权利要求13所述的方法，还包括：

在所述网络设备处接收来自所述配置设备的注销请求；

确定所述网络设备是处于所述已注册状态还是所述未注册状态；

如果确定所述网络设备是处于所述已注册状态，则

确定所述网络设备是否是向发送所述注销请求的所述配置设备注册的；以及

如果确定所述网络设备是向发送所述注销请求的所述配置设备注册的，则删除存储在所述网络设备中的所述至少一个密钥。

24.根据权利要求23所述的方法，其中确定所述网络设备是向发送所述注销请求的所述配置设备注册的包括：

将在所述注销请求中接收的至少一个参数与在注册操作期间存储在所述网络设备中的参数进行比较。

25.根据权利要求23所述的方法，其中确定所述网络设备是向发送所述注销请求的所述配置设备注册的包括：

确定从所述配置设备接收的消息中包含的完整性字段是有效的还是无效的。

26.一种用于使用配置设备来配置网络设备的方法，所述方法包括：

由所述配置设备发送消息给所述网络设备以发起向所述网络设备的注册操作；

基于在从所述网络设备接收的响应中所接收的至少一个参数，确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备是处于所述未注册状态，则发送至少一个密钥，以将所述网络设备向所述配置设备进行注册；

确定通信网络的网络密钥是否存储在所述网络设备处；

如果确定所述网络密钥存储在所述网络设备处，则从所述网络设备接收所述网络密钥；以及

如果确定所述网络密钥不存储在所述网络设备处，则向所述网络设备发送所述网络密钥，以便配置所述网络设备通信地连接到所述通信网络。

27.根据权利要求26所述的方法，其中，来自所述网络设备的所述响应包括：

存储在所述网络设备处的至少一个密钥的哈希值。

28.根据权利要求26所述的方法，其中确定所述网络设备是处于所述已注册状态还是所述未注册状态包括以下操作中的一项或多项：

当从所述网络设备接收的至少一个密钥的哈希值为空时，确定所述网络设备处于所述未注册状态；

当从所述网络设备接收的至少一个密钥的所述哈希值不为空时，确定所述网络设备处于所述已注册状态；以及

当从所述网络设备接收的至少一个密钥的所述哈希值与存储在所述配置设备处的至少一个密钥的哈希值匹配时，确定所述网络设备是向所述配置设备注册的。

29.根据权利要求26所述的方法，还包括，

通过安全的短距离通信信道发送所述消息给所述网络设备。

30.根据权利要求26所述的方法，还包括：

由所述配置设备发送第二消息给所述网络设备，以确定是否将所述网络设备注销；

基于在来自所述网络设备的第二响应中接收的至少一个参数，确定所述网络设备是否是向所述配置设备注册的；以及

如果确定所述网络设备是向所述配置设备注册的，则发送至少一个指令以将所述网络设备注销。

31.根据权利要求30所述的方法，其中，来自所述网络设备的所述第二响应包括：

存储在所述网络设备处的至少一个参数的哈希值。

32.根据权利要求30所述的方法，其中来自所述网络设备的所述第二响应包括所述网络设备的状态，其中，所述状态指示所述网络设备是否是向所述配置设备注册的。

33.一种用于配置网络设备的配置设备，所述配置设备包括：

网络接口；

密钥管理单元，其配置成：

通过与所述网络设备的短距离通信连接来发起与所述网络设备的配对操作；

确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备处于所述未注册状态，则

在所述配置设备与所述网络设备之间建立短距离通信信道；以及

通过所述短距离通信信道向所述网络设备发送网络密钥，以便配置所述网络设备通信地连接到通信网络。

34.根据权利要求33所述的配置设备，其中所述密钥管理单元还配置成：

如果确定所述网络设备关于所述配置设备和其它配置设备处于未注册状态，则向所述配置设备注册所述网络设备。

35.根据权利要求33所述的配置设备，如果确定所述网络设备处于所述已注册状态，所述密钥管理单元进一步被配置成：

确定所述网络设备是向所述配置设备注册的还是向不同的配置设备注册的；

确定是否将所述网络设备注销；以及

响应于确定所述网络设备是向所述配置设备注册的以及确定将所述网络设备注销，通过所述短距离通信信道向所述网络设备发送至少一个消息以将所述网络设备注销。

36.根据权利要求35所述的配置设备，其中所述密钥管理单元配置成发送至少一个消息以将所述网络设备注销包括所述密钥管理单元配置成：

发送至少一个指令以删除在所述配对操作期间在所述网络设备处存储的数据。

37.根据权利要求33所述的配置设备，其中所述密钥管理单元配置成发起与所述网络设备的配对操作包括所述密钥管理单元配置成以下操作中的一项：

通过交换并存储所述网络设备的设备标识符和多个配对密钥来与所述网络设备配对；以及

使用非对称加密方案与所述网络设备进行配对。

38.根据权利要求37所述的配置设备，其中所述密钥管理单元配置成使用所述非对称加密方案与所述网络设备配对包括所述密钥管理单元配置成：

在所述网络设备存储所述配置设备的公共密钥。

39.根据权利要求33所述的配置设备，其中所述密钥管理单元配置成确定所述网络设备是处于所述已注册状态还是所述未注册状态包括所述密钥管理单元配置成：

从所述配置设备向所述网络设备发送包含第一信息的第一消息；以及

基于响应于所述第一消息接收的第二消息来确定所述网络设备是处于所述已注册状态还是所述未注册状态。

40.根据权利要求33所述的配置设备，其中所述短距离通信信道包括支持完整性、加密和重放保护的安全的短距离通信信道。

41.一种通信网络的网络设备，所述网络设备包括：

网络接口；

注册管理单元，其配置成：

通过短距离通信连接接收向配置设备注册的请求；

确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备处于所述未注册状态，则

向所述配置设备发送响应，以指示所述网络设备处于所述未注册状态；

在所述网络设备与所述配置设备之间建立短距离通信信道；

通过所述短距离通信信道从所述配置设备接收至少一个密钥，以向所述配置设备进行注册；

通过所述短距离通信信道从所述配置设备接收网络密钥，以便配置所述网络设备通过通信网络进行通信；以及

使用所述网络密钥通过所述通信网络进行通信。

42.根据权利要求41所述的网络设备，其中所述注册请求包括所述配置设备的标识符。

43.根据权利要求41所述的网络设备，其中所述注册请求包括所述配置设备的公共密钥。

44.根据权利要求41所述的网络设备，其中所述短距离通信信道是使用第一频带的带外通信信道，所述第一频带不同于通信网络使用的第二频带。

45.根据权利要求41所述的网络设备，其中进行注册的所述请求包括随机数，并且响应于在所述网络设备处接收到所述随机数，所述注册管理单元配置成：

计算在所述网络设备处存储的所述至少一个密钥的哈希值，并将所述哈希值发送给所述配置设备。

46.根据权利要求41所述的网络设备，其中，进行注册的所述请求包括对随机数的请求，并且响应于在所述网络设备处接收到针对所述随机数的所述请求，所述注册管理单元配置成向所述配置设备发送随机数。

47.根据权利要求41所述的网络设备，其中所述注册管理单元配置成确定所述网络设备是处于所述已注册状态还是所述未注册状态包括所述注册管理单元配置成：

将存储在所述网络设备处的至少一个参数与从所述配置设备接收的参数进行比较。

48.根据权利要求41所述的网络设备，其中所述注册管理单元配置成向所述配置设备发送所述响应还包括所述注册管理单元配置成：

向所述配置设备发送存储在所述网络设备处的所述通信网络的网络密钥。

49.根据权利要求48所述的网络设备，其中所述注册管理单元配置成发送存储在所述网络设备处的所述通信网络的所述网络密钥还包括所述注册管理单元配置成：

向所述配置设备发送所述网络密钥的哈希值。

50.根据权利要求41所述的网络设备，其中所述注册管理单元配置成建立所述短距离通信信道包括所述注册管理单元配置成：

执行密钥协商、密钥导出以及密钥确认过程，以建立安全的短距离通信信道。

51.根据权利要求41所述的网络设备，其中所述注册管理单元还配置成：

在所述网络设备处接收来自所述配置设备的注销请求；

确定所述网络设备是处于所述已注册状态还是所述未注册状态；

如果确定所述网络设备是处于所述已注册状态，则

确定所述网络设备是否是向发送所述注销请求的所述配置设备注册的；以及

如果确定所述网络设备是向发送所述注销请求的所述配置设备注册的，则删除存储在所述网络设备中的所述至少一个密钥。

52.根据权利要求51所述的网络设备，其中所述注册管理单元配置成确定所述网络设备是向发送所述注销请求的所述配置设备注册的包括所述注册管理单元配置成：

将在所述注销请求中接收的至少一个参数与在注册操作期间存储在所述网络设备中的参数进行比较。

53.根据权利要求51所述的网络设备，其中所述注册管理单元配置成确定所述网络设备是向发送所述注销请求的所述配置设备注册的包括所述注册管理单元配置成：

确定从所述配置设备接收的消息中包含的完整性字段是有效的还是无效的。

54.一种用于配置网络设备的配置设备，所述配置设备包括：

网络接口；

密钥管理单元，其配置成：

发送消息给所述网络设备以发起向所述网络设备的注册操作；

基于在从所述网络设备接收的响应中所接收的至少一个参数，确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备是处于所述未注册状态，则发送至少一个密钥，以将所述网络设备向所述配置设备进行注册；

确定通信网络的网络密钥是否存储在所述网络设备处；

如果确定所述网络密钥存储在所述网络设备处，则从所述网络设备接收所述网络密钥；以及

如果确定所述网络密钥不存储在所述网络设备处，则向所述网络设备发送网络密钥，以便配置所述网络设备通信地连接到所述通信网络。

55.根据权利要求54所述的配置设备，其中，来自所述网络设备的所述响应包括：

存储在所述网络设备处的至少一个密钥的哈希值。

56.根据权利要求54所述的配置设备，其中所述密钥管理单元配置成确定所述网络设备是处于所述已注册状态还是所述未注册状态包括所述密钥管理单元配置成进行以下操作中的一项或多项：

当从所述网络设备接收的至少一个密钥的哈希值为空时，确定所述网络设备处于所述未注册状态；

当从所述网络设备接收的至少一个密钥的所述哈希值不为空时，确定所述网络设备处于所述已注册状态；以及

当从所述网络设备接收的至少一个密钥的所述哈希值与存储在所述配置设备处的至少一个密钥的哈希值匹配时，确定所述网络设备是向所述配置设备注册的。

57.根据权利要求54所述的配置设备，其中所述密钥管理单元还配置成：

通过安全的短距离通信信道发送所述消息给所述网络设备。

58.根据权利要求54所述的配置设备，其中所述密钥管理单元还配置成：

由所述配置设备发送第二消息给所述网络设备，以确定是否将所述网络设备注销；

基于在来自所述网络设备的第二响应中接收的至少一个参数，确定所述网络设备是向所述配置设备注册的；以及

如果确定所述网络设备是向所述配置设备注册的，则发送至少一个指令以将所述网络设备注销。

59.一种具有存储在其中的机器可执行指令的非暂时性机器可读存储介质，所述机器可执行指令包括用于执行以下操作的指令：

由配置设备通过与网络设备的短距离通信连接来发起与所述网络设备的配对操作；

由所述配置设备确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备处于所述未注册状态，则

在所述配置设备与所述网络设备之间建立短距离通信信道；以及

通过所述短距离通信信道向所述网络设备发送网络密钥，以便配置所述网络设备通信地连接到通信网络。

60.根据权利要求59所述的非暂时性机器可读存储介质，其中所述指令还包括用于执行以下操作的指令：

如果确定所述网络设备关于所述配置设备和其它配置设备处于所述未注册状态，则向所述配置设备注册所述网络设备。

61.根据权利要求59所述的非暂时性机器可读存储介质，其中所述指令还包括如果确定所述网络设备处于所述已注册状态中用于执行以下操作的指令：

确定所述网络设备是向所述配置设备注册的还是向不同的配置设备注册的；

确定是否将所述网络设备注销；以及

响应于确定所述网络设备是向所述配置设备注册的以及确定将所述网络设备注销，通过所述短距离通信信道向所述网络设备发送至少一个消息以将所述网络设备注销。

62.根据权利要求61所述的非暂时性机器可读存储介质，其中用于发送至少一个消息以将所述网络设备注销的指令包括用于发送至少一个指令，以删除在所述配对操作期间在所述网络设备处存储的数据的指令。

63.一种具有存储在其中的机器可执行指令的非暂时性机器可读存储介质，所述机器可执行指令包括用于执行以下操作的指令：

由配置设备发送消息给网络设备，以发起向所述网络设备的注册操作；

基于在从所述网络设备接收的响应中所接收的至少一个参数，确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态；

如果确定所述网络设备是处于所述未注册状态，则发送至少一个密钥，以将所述网络设备向所述配置设备进行注册；

确定通信网络的网络密钥是否存储在所述网络设备处；

如果确定所述网络密钥存储在所述网络设备处，则从所述网络设备接收所述网络密钥；以及

如果确定所述网络密钥不存储在所述网络设备处，则向所述网络设备发送网络密钥，以便配置所述网络设备通信地连接到所述通信网络。

64.根据权利要求63所述的非暂时性机器可读存储介质，其中，来自所述网络设备的所述响应包括：

存储在所述网络设备处的至少一个密钥的哈希值。

65.根据权利要求63所述的非暂时性机器可读存储介质，其中用于确定所述网络设备是处于所述已注册状态还是所述未注册状态的指令包括以下各项中的一个或多个：

用于当从所述网络设备接收的至少一个密钥的哈希值为空时，确定所述网络设备处于所述未注册状态的指令；

用于当从所述网络设备接收的至少一个密钥的所述哈希值不为空时，确定所述网络设备处于所述已注册状态的指令；以及

用于当从所述网络设备接收的至少一个密钥的所述哈希值与存储在所述配置设备处的至少一个密钥的哈希值匹配时，确定所述网络设备是向所述配置设备注册的指令。

66.根据权利要求63所述的非暂时性机器可读存储介质，其中发送所述消息给所述网络设备来发起向所述网络设备的注册操作的指令还包括：

用于通过安全的短距离通信信道发送所述消息的指令。

67.根据权利要求63所述的非暂时性机器可读存储介质，其中所述指令还包括用于执行以下操作的指令：

由所述配置设备发送第二消息给所述网络设备以确定是否将所述网络设备注销；

基于在来自所述网络设备的第二响应中接收的至少一个参数，确定所述网络设备是否是向所述配置设备注册的；以及

如果确定所述网络设备是向所述配置设备注册的，则发送至少一个指令以将所述网络设备注销。

68.一种用于配置网络设备的配置设备，所述配置设备包括：

用于通过与所述网络设备的短距离通信连接来发起与所述网络设备的配对操作的单元；

用于确定所述网络设备关于所述配置设备和其它配置设备是处于已注册状态还是未注册状态的单元；

如果确定所述网络设备是处于所述未注册状态，则

用于在所述配置设备与所述网络设备之间建立短距离通信信道的单元；以及

用于通过所述短距离通信信道向所述网络设备发送网络密钥，以便配置所述网络设备通信地连接到通信网络的单元。

使用短距离无线通信的网络安全配置

[0001] 相关申请

[0002] 本申请要求享受于2012年3月20日提交的美国临时申请No.61/613,438、2012年4月23日提交的美国临时申请No.61/637,234以及2013年3月15日提交的美国申请No.13/843,395的优先权的权益。

背景技术

[0003] 概括的说，本发明主题的实施例涉及通信网络领域，更具体地说，涉及使用短距离无线通信的网络安全配置。

[0004] 在通信网络中，通信网络中设备之间的安全关联可以使用按钮配置和/或用户配置的密码/密钥等来完成。在按钮配置中，用户可以在特定时间内在每一设备上按下按钮，则这些设备可以彼此相关联。在用户配置的密码/密钥技术中，用户可以利用指定的规则输入经ASCII编码的密码，该经ASCII编码的密码可以被转换成通信网络密钥或直接地被配置作为网络密钥。然而，将用户配置的密码/密钥手动地输入多个网络设备是麻烦的。此外，用户配置的密码易受字典式攻击，且网络密钥经常太复杂而不能手动配置。按钮配置不是非常安全，且在物理地接入网络中的设备的情况下，能够触发按钮以在恶意用户控制下关联设备，以与网络中的设备相关联并从而获得与该网络相关联的安全设置。

发明内容

[0005] 公开了用于配置网络设备的各个实施例。在一些实施例中，一种用于使用中间配置设备来配置网络设备的方法包括：由配置设备通过与网络设备的短距离通信连接发起与通信网络的所述网络设备的配对操作；由所述配置设备确定所述网络设备是处于注册状态还是未注册状态；以及如果确定所述网络设备处于未注册状态，则在所述配置设备与所述网络设备之间建立短距离通信信道，以及通过所述短距离通信信道向所述网络设备发送网络密钥，以配置所述网络设备通信地连接到所述通信网络。

[0006] 在一些实施例中，所述方法还包括如果确定所述网络设备处于注册状态，则确定是否将所述网络设备注销。

[0007] 在一些实施例中，所述确定是否将所述网络设备注销包括：确定所述网络设备是向所述配置设备还是不同的配置设备注册了；以及响应于确定所述网络设备是向所述配置设备注册了并确定将所述网络设备注销，通过所述短距离通信信道向所述网络设备发送至少一个消息以将所述网络设备注销。

[0008] 在一些实施例中，所述发送至少一个消息以将所述网络设备注销包括发送至少一个指令，以删除在所述配对操作期间在所述网络设备上所存储的数据。

[0009] 在一些实施例中，所述发起与所述网络设备的配对操作包括以下各项中的一项：通过交换及存储所述网络设备的设备标识符和多个密钥来与网络设备配对；以及使用非对称加密方案与所述网络设备配对。

[0010] 在一些实施例中，所述使用所述非对称加密方案与所述网络设备进行所述配对包

括在所述网络设备处存储所述配置设备的公共密钥。

[0011] 在一些实施例中，所述确定所述网络设备是处于注册状态还是未注册状态包括：从所述配置设备向所述网络设备发送包含第一信息的第一消息；以及基于响应于所述第一消息而接收第二消息来确定所述网络设备是处于所述注册状态还是所述未注册状态。

[0012] 在一些实施例中，所述短距离通信连接是近场通信(NFC)连接。

[0013] 在一些实施例中，所述短距离通信连接是蓝牙通信连接、ZigBee通信连接、和无线局域网(WLAN)通信连接中的一个。

[0014] 在一些实施例中，所述短距离通信信道包括支持完整性、加密和重放保护的安全的短距离通信信道。

[0015] 在一些实施例中，所述重放保护是使用序列号来实现的。

[0016] 在一些实施例中，所述重放保护是使用时间戳来实现的。

[0017] 在一些实施例中，一种用于配置网络设备的方法包括：通过短距离通信连接，在通信网络的网络设备处接收来自配置设备的用于向所述配置设备注册的请求；确定所述网络设备是处于注册状态还是未注册状态；以及如果确定所述网络设备是处于未注册状态，则向所述配置设备发送响应，以指示所述网络设备处于未注册状态，在所述网络设备与所述配置设备之间建立短距离通信信道，以及通过所述短距离通信信道从所述配置设备接收至少一个密钥以向所述配置设备进行注册。

[0018] 在一些实施例中，所述注册的请求包括所述配置设备的标识符。

[0019] 在一些实施例中，所述注册的请求包括所述配置设备的公共密钥。

[0020] 在一些实施例中，所述注册的请求包括针对随机数的请求，或随机数。

[0021] 在一些实施例中，响应于在所述网络设备处接收所述随机数，计算在所述网络设备处存储的至少一个密钥的哈希值，并向所述配置设备发送所述哈希值。

[0022] 在一些实施例中，响应于在所述网络设备处接收针对所述随机数的请求，向所述配置设备发送随机数。

[0023] 在一些实施例中，所述确定所述网络设备是处于注册状态还是所述非注册状态包括将存储在所述网络设备处的至少一个参数与从所述配置设备接收的参数进行比较。

[0024] 在一些实施例中，所述向所述配置设备发送所述响应还包括向所述配置设备发送存储在所述网络设备处的所述通信网络的网络密钥。

[0025] 在一些实施例中，所述发送所述存储在所述网络设备处的所述通信网络的所述网络密钥还包括向所述配置设备发送所述网络密钥的哈希值。

[0026] 在一些实施例中，所述建立所述短距离通信信道包括执行密钥协商、密钥导出和密钥确认过程，以建立安全的短距离通信信道。

[0027] 在一些实施例中，所述方法还包括在所述网络设备处从所述配置设备接收注销请求；确定所述网络设备是处于所述注册状态还是所述非注册状态；如果确定所述网络设备是处于所述注册状态，则确定所述网络设备是否向发送所述注销请求的所述配置设备注册了；以及如果确定所述网络设备向发送所述注销请求的所述配置设备注册了，则删除存储在所述网络设备中的所述至少一个密钥。

[0028] 在一个实施例中，所述确定所述网络设备是向发送所述注销请求的所述配置设备注册了包括：将在所述注销请求中接收的至少一个参数与在注册操作期间存储在所述网络

设备中的参数进行比较。

[0029] 在一些实施例中，所述确定所述网络设备是向发送所述注销请求的所述配置设备注册了包括：确定从所述配置设备接收的信息中包含的完整性字段是有效的还是无效的。

[0030] 在一些实施例中，一种用于使用中间配置设备来配置网络设备的方法包括：在配置设备处发起与所述网络设备的消息交换，以注册所述网络设备；基于从所述网络设备接收的响应中所接收的至少一个参数确定所述网络设备是处于注册状态还是未注册状态；如果确定所述网络设备是处于所述未注册状态，则发送至少一个密钥，以将所述网络设备向所述配置设备进行注册；确定所述通信网络的网络密钥是否存储在所述网络设备处；如果确定所述网络密钥存储在所述网络设备处，则从所述网络设备接收所述网络密钥；以及如果确定所述网络密钥不存储在所述网络设备处，则向所述网络设备发送网络密钥。

[0031] 在一些实施例中，来自所述网络设备的所述响应包括存储在所述网络设备处的至少一个密钥的哈希值。

[0032] 在一些实施例中，所述确定所述网络设备是处于所述注册状态还是所述未注册状态包括以下各项中的一个或多个：当从所述网络设备接收的至少一个密钥的哈希值为空时，确定所述网络设备处于所述非注册状态；当从所述网络设备接收的至少一个密钥的所述哈希值不为空时，确定所述网络设备处于所述注册状态；以及当从所述网络设备接收的至少一个密钥的所述哈希值与存储在所述配置设备处的至少一个密钥的哈希值匹配时，确定所述网络设备向所述配置设备注册了。

[0033] 在一些实施例中，所述方法还包括发起与所述网络设备的消息交换，以通过安全的短距离通信信道注册所述网络设备。

[0034] 在一些实施例中，在所述配置设备处，发起与所述网络设备的第二消息交换以将所述网络设备注销；基于从所述网络设备接收的第二响应中的至少一个参数，确定所述网络设备是否向所述配置设备注册了；以及如果确定所述网络设备向所述配置设备注册了，则发送至少一个指令以将所述网络设备注销。

[0035] 在一些实施例中，来自所述网络设备的所述第二响应包括存储在所述网络设备处的至少一个参数的哈希值。

[0036] 在一些实施例中，来自所述网络设备的所述第二响应包括所述网络设备的状态，其中，所述状态指示所述网络设备是否向所述配置设备注册了。

[0037] 在一些实施例中，一种用于配置网络设备的配置设备，所述配置设备包括网络接口；以及密钥管理单元，配置成：通过与所述网络设备的短距离通信连接，发起与通信网络的所述网络设备的配对操作；确定所述网络设备是处于注册状态还是未注册状态；如果确定所述网络设备处于未注册状态，则在所述配置设备与所述网络设备之间建立短距离通信信道；以及通过所述短距离通信信道向所述网络设备发送网络密钥，以配置所述网络设备通信地连接到所述通信网络。

[0038] 在一些实施例中，所述密钥管理单元还配置成：如果确定所述网络设备处于注册状态，则确定是否将所述网络设备注销。

[0039] 在一些实施例中，所述密钥管理单元配置成确定是否将所述网络设备注销包括所述密钥管理单元配置成：确定所述网络设备是向所述配置设备还是向不同的配置设备注册了；以及响应于确定所述网络设备向所述配置设备注册了以及确定将所述网络设备注销，

通过所述短距离通信信道向所述网络设备发送至少一个消息以将所述网络设备注销。

[0040] 在一些实施例中，所述密钥管理单元配置成发送至少一个消息以将所述网络设备注销包括所述密钥管理单元配置成：发送至少一个指令以删除在所述配对操作期间在所述网络设备处存储的数据。

[0041] 在一些实施例中，所述密钥管理单元配置成发起与所述网络设备的配对操作包括所述密钥管理单元配置成如下各项中的一项：通过交换并存储所述网络设备的设备标识符和多个密钥来与所述网络设备配对；以及使用非对称加密方案与所述网络设备配对。

[0042] 在一些实施例中，所述密钥管理单元配置成使用所述非对称加密方案与所述网络设备配对包括所述密钥管理单元配置成在所述网络设备存储所述配置设备的公共密钥。

[0043] 在一些实施例中，所述密钥管理单元配置成确定所述网络设备是处于所述注册状态还是所述未注册状态包括所述密钥管理单元配置成从所述配置设备向所述网络设备发送包含第一信息的第一消息；以及基于响应于所述第一消息所接收的第二消息，确定所述网络设备是处于所述注册状态还是所述未注册状态。

[0044] 在一些实施例中，所述短距离通信信道包括支持完整性、加密和重放保护的安全短距离通信信道。

[0045] 在一些实施例中，一种通信网络的网络设备，所述网络设备包括：网络接口；以及注册管理单元配置成：通过短距离通信连接接收向配置设备注册的请求；确定所述网络设备是处于注册状态还是未注册状态；如果确定所述网络设备处于未注册状态，则向所述配置设备发送响应，以指示所述网络设备处于所述未注册状态；在所述网络设备和所述配置设备之间建立短距离通信信道；以及通过所述短距离通信信道从所述配置设备接收至少一个密钥，以向所述配置设备注册。

[0046] 在一些实施例中，所述注册的请求包括所述配置设备的标识符。

[0047] 在一些实施例中，所述注册的请求包括所述配置设备的公共密钥。

[0048] 在一些实施例中，所述注册的请求包括：对随机数的请求，或随机数。

[0049] 在一些实施例中，响应于在所述网络设备处接收所述随机数，所述注册管理单元配置成计算在所述网络设备处存储的至少一个密钥的哈希值以及向所述配上设备发送所述哈希值。

[0050] 在一些实施例中，响应于在所述网络设备处接收对所述随机数的所述请求，所述注册管理单元配置成向所述配置设备发送随机数。

[0051] 在一些实施例中，所述注册管理单元配置成确定所述网络设备是处于注册状态还是未注册状态包括所述注册管理单元配置成将存储在所述网络设备上的至少一个参数与从所述配置设备接收的参数进行比较。

[0052] 在一些实施例中，所述注册管理单元配置成向所述配置设备发送所述响应还包括所述注册管理单元配置成向所述配置设备发送存储在所述网络设备上的所述通信网络的网络密钥。

[0053] 在一些实施例中，所述注册管理单元配置成发送存储在所述网络设备上的所述通信网络的所述网络密钥还包括所述注册管理单元配置成向所述配置设备发送所述网络密钥的哈希值。

[0054] 在一些实施例中，所述注册管理单元配置成建立短距离通信信道包括所述注册管

理单元配置成执行密钥协商、密钥导出以及密钥确认过程，以建立安全短距离通信信道。

[0055] 在一些实施例中，所述注册管理单元还配置成：在所述网络设备处从所述配置设备接收注销的请求；确定所述网络设备是处于所述注册状态还是所述未注册状态；如果确定所述网络设备是处于所述注册状态，则确定所述网络设备是向发送所述注销请求的所述配置设备进行了注册，以及如果确定所述网络设备是向发送所述注销请求的所述配置设备注册了，则删除在所述网络设备中存储的所述至少一个密钥。

[0056] 在一些实施例中，所述注册管理单元配置成确定所述网络设备是向发送所述注销请求的所述配置设备注册了包括所述注册管理单元配置成将在所述注销请求中接收的至少一个参数与在注册操作期间在所述网络设备中存储的参数进行比较。

[0057] 在一些实施例中，所述注册管理单元配置成确定所述网络设备是向发送所述注销请求的所述配置设备注册了包括所述注册管理单元配置成确定在从所述配置设备接收的消息中包含的完整性字段是有效的还是无效的。

[0058] 在一些实施例中，一种用于配置网络设备的配置设备，所述配置设备包括：网络接口；以及密钥管理单元，配置成：发起与所述网络设备的消息交换，以注册所述网络设备；基于从所述网络设备接收的响应中的至少一个参数，确定所述网络设备是处于注册状态还是未注册状态；如果确定所述网络设备处于所述注册状态，则发送至少一个密钥，以向所述配置设备注册所述网络设备；确定所述通信网络的网络密钥是否存储在所述网络设备上；如果确定所述网络密钥存储在所述网络设备上，则从所述网络设备接收所述网络密钥；以及如果确定所述网络密钥不存储在所述网络设备上，则向所述网络设备发送网络密钥。

[0059] 在一些实施例中，来自所述网络设备的所述响应包括存储在所述网络设备上的至少一个密钥的哈希值。

[0060] 在一些实施例中，所述密钥管理单元配置成确定所述网络设备是处于注册状态还是未注册状态包括所述密钥管理单元配置成如下中的一项或多项：当从所述网络设备接收的至少一个密钥的哈希值为空时，确定所述网络设备处于未注册状态；当从所述网络设备接收的至少一个密钥的哈希值不为空时，确定所述网络设备处于注册状态；以及当从所述网络设备接收的至少一个密钥的哈希值与存储在所述配置设备上的至少一个密钥的哈希值匹配时，确定所述网络设备向所述配置设备注册了。

[0061] 在一些实施例中，所述密钥管理单元还配置成发起与所述网络设备的所述消息交换，以通过安全短距离通信信道注册所述网络设备。

[0062] 在一些实施例中，所述密钥管理单元还配置成：在所述配置设备处发起于所述网络设备的第二消息交换，以将所述网络设备注销；基于从所述网络设备接收的第二响应中的至少一个参数，确定所述网络设备向所述配置设备注册了；以及如果确定所述网络设备向所述配置设备注册了，则发送至少一个指令以将所述网络设备注销。

[0063] 在一些实施例中，一种非暂时性机器可读存储介质，其具有存储在其中的机器可执行指令，所述机器可执行指令包括用于执行以下操作的指令：由配置设备通过与网络设备的短距离通信连接发起与通信网络的所述网络设备的配对操作；由所述配置设备确定所述网络设备是处于注册状态还是未注册状态；如果确定所述网络设备处于未注册状态，则在所述配置设备与所述网络设备之间建立短距离通信信道；以及通过所述短距离通信信道向所述网络设备发送网络密钥，以配置所述网络设备通信地连接到所述通信网络。

[0064] 在一些实施例中，所述指令还包括用于如果确定所述网络设备处于注册状态，则确定是否将所述网络设备注销的指令。

[0065] 在一些实施例中，所述用于确定是否将所述网络设备注销包括用于执行以下操作的指令：确定所述网络设备是向所述配置设备还是不同的配置设备注册了；以及响应于确定所述网络设备是向所述配置设备注册了并确定将所述网络设备注销，通过所述短距离通信信道向所述网络设备发送至少一个消息以将所述网络设备注销。

[0066] 在一些实施例中，所述用于发送至少一个消息以将所述网络设备注销的指令包括用于发送至少一个指令，以删除在所述配对操作期间在所述网络设备上所存储的数据的指令。

[0067] 在一些实施例中，一种非暂时性机器可读存储介质，其具有存储在其中的机器可执行指令，所述机器可执行指令包括用于执行以下操作的指令：在配置设备处发起与所述网络设备的消息交换，以注册所述网络设备；基于从所述网络设备接收的响应中所接收的至少一个参数，确定所述网络设备是处于注册状态还是未注册状态；如果确定所述网络设备是处于所述未注册状态，则发送至少一个密钥，以将所述网络设备向所述配置设备进行注册；确定所述通信网络的网络密钥是否存储在所述网络设备处；如果确定所述网络密钥存储在所述网络设备处，则从所述网络设备接收所述网络密钥；以及如果确定所述网络密钥不存储在所述网络设备处，则向所述网络设备发送网络密钥。

[0068] 在一些实施例中，来自所述网络设备的所述响应包括存储在所述网络设备处的至少一个密钥的哈希值。

[0069] 在一些实施例中，所述用于确定所述网络设备是处于所述注册状态还是所述未注册状态的指令包括以下各项中的一个或多个：用于当从所述网络设备接收的至少一个密钥的哈希值为空时，确定所述网络设备处于所述非注册状态的指令；用于当从所述网络设备接收的至少一个密钥的所述哈希值不为空时，确定所述网络设备处于所述注册状态的指令；以及用于当从所述网络设备接收的至少一个密钥的所述哈希值与存储在所述配置设备处的至少一个密钥的哈希值匹配时，确定所述网络设备向所述配置设备注册了的指令。

[0070] 在一些实施例中，所述指令还包括用于发起与所述网络设备的所述消息交换以通过安全短距离通信信道注册所述网络设备的指令。

[0071] 在一些实施例中，所述指令还包括用于执行以下操作的指令：在所述配置设备处，发起与所述网络设备的第二消息交换以将所述网络设备注销；基于从所述网络设备接收的第二响应中的至少一个参数，确定所述网络设备是否向所述配置设备注册了；以及如果确定所述网络设备向所述配置设备注册了，则发送至少一个指令以将所述网络设备注销。

[0072] 在一些实施例中，一种用于配置网络设备的配置设备，所述配置设备包括：用于通过与所述网络设备的短距离通信连接，发起与通信网络的所述网络设备的配对操作的模块；用于确定所述网络设备是处于注册状态还是未注册状态的模块；如果确定所述网络设备是处于未注册状态，则用于在所述配置设备与所述网络设备之间建立短距离通信信道的模块；以及用于通过所述短距离通信信道向所述网络设备发送网络密钥，以配置所述网络设备通信地连接到所述通信网络的模块。

附图说明

[0073] 图1描绘了通信网络中的密钥携带设备和网络设备的示例性方框图。

[0074] 图2示出了用于配置网络设备的示例性操作的流程图。

[0075] 图3示出了用于使用第一和第二配置技术配置网络设备的示例性操作的流程图。

[0076] 图4示出了用于使用第三、第四和第五配置技术配置网络设备的示例性操作的流程图。

[0077] 图5示出了用于使用第一配置技术注册网络设备的示例性操作的顺序图。

[0078] 图6示出了用于使用第一配置技术注销网络设备的示例性操作的顺序图。

[0079] 图7示出了用于使用第二配置技术注册网络设备的示例性操作的顺序图。

[0080] 图8示出了用于使用第二配置技术注销网络设备的示例性操作的顺序图。

[0081] 图9、10、11和12示出了用于使用第三配置技术注册网络设备的示例性操作的顺序图。

[0082] 图13示出了用于使用第三配置技术注销网络设备的第一选项的示例性操作的顺序图。

[0083] 图14示出了用于使用第三配置技术注销网络设备的第二选项的示例性操作的顺序图。

[0084] 图15、16和17示出了用于使用第四配置技术注册网络设备的示例性操作的顺序图。

[0085] 图18和19示出了用于使用第四配置技术注销网络设备的第一选项的示例性操作的顺序图。

[0086] 图20示出了用于使用第四配置技术注销网络设备的第二选项的示例性操作的顺序图。

[0087] 图21和22示出了用于使用第五配置技术注册网络设备的示例性操作的顺序图。

[0088] 图23示出了用于使用第五配置技术注销网络设备的示例性操作的顺序图。

[0089] 图24示出了示例性的网络设备。

具体实施方式

[0090] 下文的描述包括体现本发明主题的技术的示例性的系统、方法、技术、指令序列和计算机程序产品。但是，应该理解的是，可以在没有这些具体细节的情况下实施所描述的实施例。例如，虽然示例涉及密钥携带设备安全地配置在通信网络中的网络设备，但是，在其它的实现中，密钥携带设备可以同时配置在一个或多个通信网络中的多个网络设备。在其它实例中，公知的指令实例、协议、结构和技术未详细示出以不混淆该描述。

[0091] 在一些实施例中，支持短距离通信的密钥携带设备可以通过在安全的通信信道上向网络设备发送网络密钥来安全地配置通信网络的网络设备。密钥携带设备可以通过交换配对数据并在网络设备和/或密钥携带设备上存储配对数据，来将网络设备向密钥携带设备注册。一旦将网络设备向密钥携带设备注册了，则密钥携带设备可以通过向该网络设备发送通信网络的网络密钥，来利用该通信网络安全地配置该网络设备。密钥携带设备还可以通过删除在网络设备和/或密钥携带设备上存储的配对数据和网络密钥，来将该网络设备从密钥携带设备注销。

[0092] 在一些实施例中，密钥携带设备可以利用一个或多个配置技术来安全地配置网络

设备。例如，在第一配置技术中，密钥携带设备可以通过将完整密钥、加密密钥和序列号作为配对数据存储在密钥携带设备和网络设备两者上，来将网络设备向密钥携带设备注册。此外，密钥携带设备可以存储网络设备的设备标识符作为配对数据的一部分，并且网络设备可以存储密钥携带设备的设备标识符作为配对数据的一部分。在第二配置技术中，密钥携带设备和网络设备可以通过将密钥携带设备的公共密钥作为配对数据存储在网络设备上来进行配对。在第一和第二两种配置技术中，密钥携带设备可以随后与网络设备交换一个或多个消息，以确定该网络设备是处于注册状态还是未注册状态，以及相应地注册或注销该网络设备(或维持当前配置)。在第三配置技术中，密钥携带设备和网络设备可以通过将私人密钥(例如，注册密钥)存储为配对数据来进行配对。密钥携带设备可以安全地交换一个或多个消息，以基于配对数据来确定网络设备是处于注册状态还是未注册状态。在一个示例中，密钥携带设备和网络设备可以利用哈希算法来安全地交换包含配对数据(例如，注册密钥)和/或网络密钥的消息。基于确定网络设备是处于未注册状态还是注册状态，密钥携带设备可以相应地注册或注销该网络设备(或维持当前配置)。在第四配置技术中，密钥携带设备和网络设备可以通过将私人密钥(例如，注册密钥)存储在密钥携带设备和网络设备两者上来进行配对，并且将状态字段存储在网络设备作为配对数据。在第四配置技术中，网络设备可以使用哈希算法，与密钥携带设备安全地交换包含配对数据(例如，注册密钥)和/或网络密钥的一个或多个消息。网络设备可以使用状态字段向密钥携带设备指示该网络设备是处于注册状态还是未注册状态，并且可以相应地确定是注册还是注销该网络设备。在第五配置技术中，除了网络设备和密钥携带设备可以在交换包含配对数据和/或网络密钥的任何消息之前建立安全的通信信道之外，其可以类似于第四配置技术。网络设备和密钥携带设备可以通过安全的通信信道来安全地交换包含配对数据和/或网络密钥的消息。下文将参考图1-24来进一步描述利用密钥携带设备来安全地配置网络设备的配置技术。

[0093] 图1描绘了通信网络中的密钥携带设备和网络设备的示例性方框图。图1描绘了通信网络100。例如，通信网络100可以是使用一个或多个网络通信标准的家庭或企业网络系统(例如，基于IEEE 802.3、IEEE 802.11或Wi-Fi®、IEEE P1905.1、电力线宽带网络标准、同轴电缆以太网、ZigBee®或IEEE 802.15.4等中的一个或多个的网络系统)。通信网络100包括具有密钥管理单元104和短距离通信单元106的密钥携带设备102。通信网络100还包括：具有注册管理单元109和短距离通信单元110的网络设备108，具有注册管理单元117和短距离通信单元118的网络设备116，以及具有注册管理单元113和短距离通信单元114的网络设备112。在一种实现中，密钥携带设备102可以包括通信单元(例如，集成电路、片上系统、或电路板)，该通信单元包括密钥管理单元104和短距离通信单元106。

[0094] 密钥携带设备102可以是支持短距离通信并管理通信网络100的各种类型的网络设备中的一种，例如，移动电话、平板计算机、笔记本计算机、智能远程控制设备等。密钥携带设备102典型地包括显示单元，用以向用户显示网络设备的状态、注册确认、注销确认等。密钥携带设备中的短距离通信单元106可以与网络设备108、116和112建立带外通信链路(即，在与由通信网络100所使用的频带不同的频带中的通信链路)。在一种实现中，短距离通信单元106可以建立近场通信(NFC)链路作为带外通信链路，并利用近场通信接口和协议

(例如,NFCIP)。在其它实现中,短距离通信单元106可以使用短距离通信技术/协议(例如,Bluetooth®等)来建立通信。

[0095] 密钥携带设备102的密钥管理单元104可以与网络设备(例如,网络设备116、112或108)交换一个或多个消息,以安全地配置该网络设备。在一些实现中,密钥携带设备102可以具有同时配置多个通信网络系统中的网络设备的能力。密钥管理单元104可以与网络设备建立安全的通信信道。例如,该安全的通信信道可以支持消息的加密、对消息的完整性保护和防止由恶意的密钥携带设备进行的重放攻击。在一种实现中,当短距离通信单元106建立NFC链路时,密钥管理单元104建立安全的通信信道(例如,通过使用椭圆曲线Diffie-赫尔曼(ECDH)和高级加密标准的NFC-SEC密码标准(NFC-SEC-01))。然而,应该注意的是,在其它的实现中,可以利用其它的安全信道技术(例如,Wi-Fi简单配置(WSC)中指定的注册协议)。在一些实现中,密钥管理单元104可以使用安全信道密钥和序列号(例如,使用序列号计数器生成的),来建立具有完整性和重放保护的安全通信信道。该序列号允许密钥携带设备102和网络设备(例如,网络设备120)保持对交换的消息的追踪并提供抵抗重放攻击的保护。例如,每个交换的消息可以包括由序列号计数器生成的序列号,并且在发送/接收消息之后,该序列号计数器可以递增。密钥携带设备102和网络设备112可以确定所接收的消息是否与小于或等于序列号计数器的当前值的序列号相关联。如果所接收的消息与小于或等于序列号计数器的当前值的序列号相关联,则该陈旧的序列号可以指示由恶意设备进行的重放攻击。然后,密钥管理单元104可以忽视所接收的具有陈旧的序列号的消息,以便避免重放攻击。密钥携带设备102和网络设备112并不受限于利用序列号来检测重放攻击。在一些实现中,密钥携带102和网络设备112可以利用时间戳来检测重放攻击。

[0096] 密钥携带设备102的密钥管理单元104包括用于生成并存储一个或多个网络密钥的能力,并且能够向/从网络设备发送/接收网络密钥。例如,当网络设备与通信网络100进行配置,并且用户使用密钥携带设备102首次注册该网络设备时,密钥管理单元104可以从该网络设备接收通信网络100的网络密钥并存储该网络密钥。在一种实现中,用户可以将与通信网络100进行配置的一个或多个网络设备向密钥携带设备102注册,并且网络密钥可以不在该网络设备和密钥管理单元104之间进行传送。在另一实现中,用户可以将(未与通信网络100进行配置的)网络设备向密钥携带设备102注册,并且密钥管理单元104可以向该网络设备发送通信网络100的网络密钥。在一些实现中,在缺少通信网络100的情况下,密钥携带设备102或网络设备中的任何一个可以均不具有网络密钥,而用户可以将一个或多个网络设备向密钥携带设备102注册。密钥管理单元104可以生成新的随机网络密钥,并将该网络密钥发送至向密钥携带设备102注册的每个网络设备并建立通信网络。在一些实现中,密钥管理单元104可以从网络管理员或通过另一带外通信链路从网络设备接收网络密钥,而不是生成新的随机网络密钥。密钥管理单元104可以存储关于向密钥携带设备102注册的网络设备的信息。此外,密钥管理单元104可以针对向密钥携带设备102注册的每个网络设备,存储配对信息以及关于安全通信信道的信息(例如,安全信道密钥)。例如,密钥管理单元104可以存储与密钥携带设备102的存储器处的表格中的网络设备的设备标识符相对应的安全信道密钥。在一些实现中,密钥携带设备102可以支持将密钥携带设备102的设置和信息导出、导入和备份到第二密钥携带设备或网络中的服务器的功能。然后,可以使用该第二密钥携带设备来配置一个或多个网络设备。下文将参考图2-23进一步针对各种网络配置技

术来描述密钥携带设备102的另外的特征和操作。

[0097] 网络设备108、112和116可以是通信网络100中的各种类型的网络设备，例如，膝上型计算机、电视机、照相机、游戏机、数字温控器、电子门锁等。在一些实现中，网络设备108、112和116可以是多归属设备并且可以同时与多个通信网络进行配置。在一个示例中，网络设备108、112、和116可以是IEEE P1905.1通信网络中的设备。在一些实现中，网络设备116、112和108的短距离通信单元118、114和110可以利用密钥携带设备102的短距离通信单元106分别建立短距离通信链路(例如，NFC链路)。网络设备108、112和116包括从密钥管理单元104接收网络密钥并向密钥携带设备102注册的能力，如下文将详细描述的。例如，网络设备116、112和108中的注册管理单元117、113和109可以分别向密钥携带设备102注册，并从密钥携带设备102接收网络密钥。在一些实现中，密钥携带设备102中的密钥管理单元104可以向网络设备116、112和108请求网络密钥。当密钥携带设备请求网络密钥时，相应的网络设备116、112和108中的注册管理单元117、113和109可以向密钥管理单元104发送网络密钥。可以通过删除与密钥携带设备102相对应的配对数据并从而从密钥携带设备102注销，来重置网络设备108、112和116。例如，网络设备108、112和116可以通过硬件(例如，重置按钮等)或通过软件(例如，程序指令等)来进行重置。在一些实现中，网络设备108、112和116可以包括发光二极管(LED)，用以通过不同的颜色来显示其状态(例如，红色针对未注册的状态，绿色针对注册的状态，而当注册过程正在进行中时为黄色)。下文将参考图2-23进一步针对各种网络配置技术来描述网络设备108、112和116的另外的特征和操作。

[0098] 图2示出了用于配置网络设备的示例性操作的流程图。例如，图2示出了一旦与网络设备112建立了短距离通信链路，在密钥携带设备102处执行的操作(如上文参考图1所描述的)。为了简化，图2未示出用于在密钥携带设备102与网络设备112之间建立安全通信信道的过程，并且未示出各种配置技术的其它细节，这些细节将在下文参考图3-23详细描述。

[0099] 在方框202，确定是要注册还是注销网络设备。例如，密钥携带设备102的密钥管理单元104确定是要注册还是注销网络设备112。在一种实现中，密钥管理单元104可以从用户接收输入，以注册或注销网络设备112。在其它的实现中，用户可以将密钥携带设备102放置在网络设备112的预定的邻近距离内，以通过短距离通信联络(例如，NFC)来自动地触发对网络设备112(其处于未注册的状态)的注册。类似地，当密钥携带设备102被放置在网络设备112的预定的邻近距离之内时，密钥管理单元104可以自动地注销网络设备112(其处于注册状态)。如果确定要注册网络设备112，则控制流程去往方框214。如果确定要将网络设备112注销，则控制流程去往方框204。

[0100] 在方框204，响应于确定要将网络设备注销，密钥携带设备102确定网络设备112是否处于注册状态。例如，密钥管理单元104可以与网络设备112交换一个或多个消息，以确定网络设备112是否处于注册状态。在一些实现中，密钥管理单元104可以处理在消息交换期间从网络设备112接收的信息，以便确定网络设备112是否处于注册状态。在其它实现中，密钥管理单元104可以在消息交换期间接收关于网络设备112的状态的信息。例如，网络设备112的状态可以指示网络设备112是否处于注册状态。如果网络设备112处于注册状态，则控制流程去往方框208。如果网络设备不处于注册状态，则控制流程去往方框206。

[0101] 在方框206，显示网络设备的未注册状态。在一种实现中，密钥携带设备102中的显示单元可以显示网络设备是未注册的。例如，在方框204处在确定网络设备112不处于注册

状态后，密钥管理单元104可以指令密钥携带设备102的显示单元显示网络设备112是未注册的。在一些实现中，网络设备112也可以具有显示能力并显示其是未注册的。

[0102] 在方框208，确定网络设备是否向密钥携带设备注册了。在一种实现中，密钥管理单元104确定网络设备112是否向密钥携带设备102注册了。例如，密钥管理单元104可以通过处理在初始消息交换期间从网络设备112接收的信息，来确定网络设备112是否向密钥携带设备102注册了。在一些实现中，密钥管理单元104可以基于所接收的关于网络设备112的状态的信息，来确定网络设备112是否向密钥携带设备102注册了。如果网络设备112向密钥携带设备102注册了，则控制流程去往方框210。如果网络设备未向密钥携带设备注册，则控制流程去往方框212。

[0103] 在方框210，发送指令以将网络设备注销。在一种实现中，密钥管理单元104发送指令以将网络设备112注销。例如，密钥管理单元104可以向网络设备112发送指令，以删除(与密钥携带设备102相对应的)网络密钥和配对数据。在一些实现中，密钥管理单元104还可以删除存储在密钥携带设备102处的用于与网络设备112进行配对的配对数据。在一些实现中，将网络设备112注销可能仅在密钥携带设备102能够安全地向网络设备112认证其自身时是有效的。例如，密钥携带设备102可以与网络设备112交换一个或多个消息，以证明其不是恶意设备，并且在认证之后可以继续注销过程。

[0104] 在方框212，显示指示网络设备未向密钥携带设备注册的状态。在一种实现中，密钥携带设备102中的显示单元显示网络设备112未向密钥携带设备102注册。例如，密钥管理单元104可以指令显示单元显示网络设备112未向密钥携带设备102注册的消息(这取决于在方框208进行的确定)。在一些实现中，网络设备112也可以具有显示能力，并显示其未向密钥携带设备102注册以指示不允许进行注销。

[0105] 在方框214，响应于确定要注册网络设备，密钥携带设备102确定网络设备112是否已经处于注册状态。例如，密钥管理单元104可以与网络设备112交换一个或多个消息，以确定网络设备112是否处于注册状态。在一些实现中，密钥管理单元104可以处理在消息交换期间从网络设备112接收的信息，以便确定网络设备112是否处于注册状态。在其它的实现中，密钥管理单元104可以在消息交换期间接收关于网络设备112的状态的信息。例如，网络设备112的状态可以指示网络设备112是否处于注册状态。如果网络设备112处于注册状态，则控制流程去往方框216。如果网络设备112不处于注册状态，则控制流程去往方框218。

[0106] 在方框216，显示网络设备的注册状态。在一种实现中，密钥携带设备102的显示单元显示网络设备112是注册的。例如，密钥管理单元104可以指令显示单元显示网络设备112是注册的(基于在方框214做出的确定)。在一些实现中，网络设备也可以具有显示能力并显示注册状态。

[0107] 在方框218，确定网络设备是否包括网络密钥。在一种实现中，密钥管理单元104确定网络设备112是否包括网络密钥。例如，网络设备112基于在与网络设备112的消息交换期间所接收的信息，来确定网络设备112是否包括网络密钥。如果网络设备112包括网络密钥，则控制流程去往方框220。如果网络设备不包括网络密钥，则控制流程去往方框222。

[0108] 在方框220，如果网络设备包括网络密钥，则发送指令以注册该网络设备，并且从该网络设备接收网络密钥。在一种实现中，密钥管理单元104发送指令以注册网络设备112，并从网络设备112接收网络密钥。例如，密钥管理单元104发送指令以更新存储在网络设备

112处的配对数据。密钥管理单元104可以与网络设备112建立安全通信信道，并通过该安全通信信道发送指令以更新网络设备112处的配对数据。密钥管理单元104也可以通过安全通信信道向网络设备112请求通信网络100的网络密钥。例如，网络设备112可能已经与通信网络100进行了配置，并且通信网络100的网络密钥可以存储在网络设备112处。密钥管理单元104可以通过安全通信信道，从网络设备112接收通信网络100的网络密钥，并且可以将该网络密钥存储在密钥携带设备102处。

[0109] 在方框222，如果网络设备包括网络密钥，则发送指令以注册网络设备，并且向网络设备发送网络密钥。在一种实现中，密钥管理单元104发送指令以注册网络设备112，并向网络设备112发送通信网络100的网络密钥。例如，密钥管理单元104发送指令以更新网络设备112处的配对数据。密钥管理单元104可以与网络设备112建立安全通信信道，并通过安全通信信道发送指令以更新网络设备112处的配对数据。密钥管理单元也可以通过安全通信信道向网络设备112发送通信网络100的网络密钥。例如，密钥携带设备102可以与通信网络100进行配置，并且通信网络100的网络密钥可以存储在密钥携带设备102处。密钥携带设备102可以向网络设备112发送通信网络100的网络密钥。在一些实现中，密钥携带设备102可能未与通信网络100进行配置，并且通信网络100的网络密钥可能未存储在密钥携带设备102处。密钥携带设备102可以生成新的随机网络密钥，并向网络设备112发送该网络密钥。

[0110] 应该注意的是，在图2的流程图中描述的过程在本质上是示例性的，且为了简化起见，在图2的流程图中未描述全部的过程。还应该注意的是，可以以不同的顺序执行一个或多个过程。例如，可以在确定网络设备112是否包括网络密钥之前发送用以注册网络设备112的指令(在方框220和222)。

[0111] 图3示出了用于使用第一和第二配置技术配置网络设备的示例性操作的流程图。图3描述了对第一配置技术(其在下文在图5-6中描述)和第二配置技术(其在下文在图7-8中描述)是共同的、用于使用通信设备配置网络设备的示例性操作。在一个示例中，通信设备可以被称为本文中描述的通信网络的密钥携带设备(例如，在图1中示出的通信网络100的密钥携带设备102)。通信设备(或密钥携带设备)也可以被称为通信网络(例如，通信网络100)的配置设备。

[0112] 在方框302，在通信设备处通过短距离通信连接发起与网络设备的配对操作。在一种实现中，密钥携带设备102通过NFC发起与网络设备112的配对操作。例如，密钥携带设备102的密钥管理单元104可以发起与网络设备112的注册管理单元113的配对操作，以注册或注销该网络设备。在一些实现中，密钥管理单元104可以基于用户输入来发起与注册管理单元113的配对操作。在其它实现中，当密钥携带设备102位于网络设备112的附近时，并且一建立短距离通信链路，则密钥管理单元104就可以发起与注册管理单元113的配对操作。流程继续进行到方框304。

[0113] 在方框304，确定网络设备是处于注册状态还是未注册状态。在一种实现中，在密钥携带设备102向网络设备112发送注册或注销请求之后，密钥管理单元104基于从网络设备112接收的一个或多个响应消息，确定网络设备112是处于注册状态还是未注册状态。例如，密钥管理单元104可以与网络设备112的注册管理单元113交换一个或多个注册或注销请求及响应消息，以确定网络设备112是处于注册状态还是未注册状态。图5、6、7和8在阶段A-D2示出了这种消息交换，如将在下文详细描述的。如果网络设备112处于未注册状态，则

控制流程去往方框306，并且密钥管理单元104可以执行注册过程。如果网络设备112处于注册状态，则控制流程去往方框312，并且密钥管理单元104可以执行注销过程。

[0114] 在方框306，与网络设备112建立安全通信信道。在一种实现中，密钥管理单元104与网络设备112的注册管理单元113建立安全通信信道。例如，密钥管理单元104可以通过执行密钥协商、密钥导出和密钥确认过程来建立安全通信信道。密钥管理单元104和网络设备112可以为安全通信信道确定一个或多个安全信道密钥(例如，完整性密钥、加密密钥和序列号计数器)，并保存该安全信道密钥。例如，密钥管理单元104和网络设备112在图5和7中的阶段E执行密钥协商、密钥导出和密钥确认过程。流程继续进行到方框308。

[0115] 在方框308，向网络设备发送网络密钥。在一种实现中，密钥管理单元104通过在方框306建立的安全通信信道，向网络设备112的注册管理单元113发送通信网络的网络密钥。例如，在图5和7中，密钥管理单元104在阶段F向注册管理单元113发送网络密钥。在接收到网络密钥之后，注册管理单元113可以保存该网络密钥，并将网络设备112与通信网络100进行配置(例如，加入通信网络100)。此外，在完成注册过程之后，密钥管理单元104和注册管理单元113可以更新分别存储在密钥携带设备102和网络设备112的配对数据(例如，图5中的设备标识符和安全信道密钥，以及图7中的公共密钥)。

[0116] 在方框312，确定网络设备是否向通信设备注册了。在一种实现中，密钥管理单元104确定网络设备112是否向密钥携带设备102注册了。例如，密钥管理单元104可以基于在图6和8中的阶段D1和D2的消息交换，来确定网络设备112是否向密钥携带设备102注册了。当网络设备112向密钥携带设备102注册了时，密钥管理单元104可以仅进行注销过程。如果网络设备112向密钥携带设备102注册了，则控制流程去往方框314。如果网络设备112未向密钥携带设备102注册，则密钥管理单元104可以停止注销过程。

[0117] 在方框314，向网络设备发送至少一个消息以将该网络设备注销。在一种实现中，密钥管理单元104向网络设备112中的注册管理单元113发送至少一个消息，以将网络设备112注销。在一种实现中，密钥管理单元104可以通过安全通信信道发送指令，以将网络设备112注销。例如，在图6中，网络设备112和密钥携带设备102将安全信道密钥存储作为配对数据的一部分。如在图6中的阶段E1-F处所示出的，密钥管理单元104可以利用该安全信道密钥来建立安全通信信道，并通过该安全通信信道发送指令以将网络设备112注销。在接收到该注销的指令之后，网络设备112中的注册管理单元113可以确定该注销指令是否是从密钥携带设备102接收的。如果该注销指令不是从密钥携带设备102接收的，则注册管理单元113可以标记错误。在另一实现中，如在图8中的阶段E所示出的，密钥管理单元104可以执行密钥协商、密钥导出和密钥确认过程，以向网络设备112证明其身份。如果密钥协商、密钥导出和密钥确认过程不成功，则注册管理单元113可以终止注销过程。

[0118] 应该注意的是，在图3的流程图中描述的过程在本质上是示例性，且为了简化起见，图3未示出当执行第一和第二配置技术时所执行的所有操作的所有细节。下文将参考图5-8进一步描述针对第一和第二配置技术在密钥携带设备102和网络设备102处执行的示例性操作的另外细节。

[0119] 图4示出了用于使用第三、第四和第五配置技术来配置网络设备的示例性操作的流程图。图4描述了对第三配置技术(下文在图9-14中描述的)、第四配置技术(下文在图15-20中描述的)、以及第五配置技术(下文在图21-23中描述的)共同的、用于使用通信设备来

配置网络设备的示例性操作。在一个示例中，通信设备可以被称为本申请中描述的通信网络的密钥携带设备(例如，图1中示出的通信网络100的密钥携带设备102)。通信设备(或密钥携带设备)也可以被称为通信网络的配置设备(例如，通信网络100)。

[0120] 在方框402，在通信设备处发起与网络设备的第一消息交换。在一种实现中，密钥管理单元104发起与网络设备112的第一消息交换。例如，该第一消息交换可以包括随机数和(使用该随机数加密的)加密数据。在第三、第四和第五配置技术中，配对数据包括存储在密钥携带设备102中的注册密钥(RKk)和存储在网络设备112中的注册密钥(RKn)。密钥携带设备102和网络设备112也可以分别将网络密钥存储为NK和NK'。在第一消息交换期间，密钥携带设备102可以利用随机数N1发送“你好”请求(在本申请中，其也可以称为注册或注销请求)，并且网络设备112可以以加密的RKn、加密的NK'和另一随机数N2来响应(例如，如在图9和13中在阶段A-C中所示出的)。网络设备112可以使用密钥携带设备102已知的哈希算法和随机数N1来加密RKn。网络设备112也可以使用密钥携带设备102已知的哈希算法来加密NK'。密钥携带设备102可以利用随机数N2来在一个或多个消息交换中向网络设备112发送加密的数据。在一些实现中，第一消息交换可以是向密钥携带设备102请求随机数，以及具有来自网络设备112的随机数的响应(如在图14和20中在阶段A-C、以及在图15和18中在阶段A1-A2中所示出的)。在一些实现中，第一消息交换可以是在密钥携带设备102与网络设备112之间建立安全通信信道(例如，如在图21和23中在阶段A所描述的)。流程继续进行到方框404。

[0121] 在阶段404，确定网络设备是处于注册状态还是未注册状态。在一种实现中，密钥管理单元104通过对在第一消息交换中从网络设备112接收的数据进行处理，来确定网络设备112是处于注册状态还是未注册状态。例如，图9和图10在阶段D和K示出了用于确定网络设备112是处于注册状态还是未注册状态的操作。图13在阶段D和E示出了用于确定网络设备112是处于注册状态还是未注册状态。在一些实现中，密钥管理单元104可以基于在第一消息交换之后后续的消息交换来确定网络设备112是处于注册状态还是未注册状态。例如，密钥管理单元104可以从网络设备112接收网络设备112的状态(如在图15、18和23中在阶段H、以及在图21中在阶段I所示出的)。在一些实现中，密钥管理单元104可以不确定网络设备112是处于注册状态还是未注册状态，而是密钥管理单元104可以基于来自用户的输入来继续注册或注销网络设备112。例如，在图14和20中，不是确定网络设备112是处于注册还是未注册状态，而是在阶段E向网络设备112发送注销请求。如果确定网络设备是处于注册状态，则控制流程去往方框414，并且可以执行注销网络设备112的注销过程。如果确定网络设备112处于未注册状态，则控制流程去往方框406并且可以执行注册网络设备112的注册过程。

[0122] 在方框406，向网络设备发送至少一个注册密钥以注册该网络设备。在一种实现中，密钥管理单元104向网络设备112发送至少一个注册密钥，以注册网络设备112。例如，密钥管理单元104可以向网络设备112发送RKk。密钥管理单元104可以建立安全通信信道(例如，使用密钥协商、密钥导出和密钥确认过程)，并通过该安全通信信道发送RKk(例如，如在图9中在阶段H、在图16中在阶段N2、以及在图21中在阶段B中所示出的)。在一些实现中，当存储在密钥携带设备102处的RKk为空时，密钥管理单元104可以生成新的随机RKk并向网络设备112发送该RKk。流程继续进行到方框408。

[0123] 在方框408，确定网络密钥是否存储在网络设备。在一种实现中，密钥管理单元104

通过对在第一消息交换中从网络设备112接收的数据进行处理，来确定网络密钥是否存储在网络设备112。例如，密钥管理单元104确定从网络设备112接收的加密的NK'是否为空(例如，如在图10中在阶段M、在图16中在阶段Q所示出的)。在一些实现中，由网络设备112在第一消息交换之后的后继的消息交换中发送的状态可以指示网络密钥是否存储在网络设备112(例如，如在图22中在阶段L所示出的)。在确定网络密钥存储在网络设备112之后，密钥管理单元104可以确定利用存储在网络设备112的该网络密钥，并控制流程去往方框410。如果网络密钥不存储在网络设备112，则控制流程去往方框412。

[0124] 在方框410，从网络设备112接收网络密钥。在一种实现中，密钥管理单元104从网络设备112中的注册管理单元113接收网络密钥。例如，密钥管理单元104可以向注册管理单元113发送“获取”网络密钥请求，以接收网络密钥。在一些实现中，该获取网络密钥请求可以包括加密的RKk(例如，如在图11中在阶段O2和在图16中在阶段T所示出的)。RKk可以是使用网络设备112已知的哈希算法并使用从网络设备112所接收的N2来加密的。在一些实现中，可以通过安全通信信道来发送获取网络密钥请求，并且获取网络密钥请求可以不包括加密的RKk(如在图22中在阶段N所示出的)。响应于该获得网络密钥请求，密钥管理单元104可以接收存储在网络设备112的网络密钥并保存该网络密钥。

[0125] 在方框412，向网络设备发送网络密钥。在一种实现中，密钥管理单元104向网络设备112中的注册管理单元113发送存储在密钥携带设备102的网络密钥。例如，密钥管理单元104可以向网络设备112发送“设置”网络密钥请求。该设置网络密钥请求可以包括网络密钥和加密的RKk(例如，如在图12中在阶段Y和在图17中阶段AD所示出的)。RKk可以是使用网络设备112已知的哈希算法和使用从网络设备112接收的N2来加密的。在一些实现中，该设置网络密钥请求可以通过安全通信信道来发送并且可以不包括加密的RKk(例如，如在图22中在阶段U中所示出的)。响应于该设置网络密钥请求，密钥管理单元104可以从网络设备112接收设置网络密钥响应，该设置网络密钥响应可以包括网络密钥被存储在网络设备112的确认。

[0126] 在方框414，确定网络设备是否向通信设备注册了。在一种实现中，密钥管理单元104通过对在第一消息交换期间接收的数据进行处理，来确定网络设备112是否向密钥携带设备102注册了。在另一实现中，密钥管理单元104可以不确定网络设备112是否向密钥携带设备102注册了，而是密钥管理单元104可以向网络设备112发送注销请求。网络设备112可以基于该注销请求确定网络设备112是否向密钥携带设备102注册了(如在方框416中所描述的)。在一些实现中，密钥管理单元104可以验证从网络设备112接收的加密的RKn(在第一消息交换期间接收的)与加密的RKk(使用由网络设备112加密RKn所利用的相同的随机数和哈希算法加密的)是否匹配，以确定网络设备112是否向密钥携带设备102注册了(例如，如在图13中在阶段E所示出的)。在其它实现中，密钥管理单元104可以基于从网络设备112接收的网络设备112的状态，来确定网络设备112是否向密钥携带设备102注册了(例如，在图18中在阶段I)。如果网络设备112向密钥携带设备102注册了，则控制流程去往方框416。如果网络设备112未向密钥携带设备102进行注册，则密钥携带设备102可能无法将网络设备112注销。

[0127] 在方框416，发送至少一个指令以将网络设备注销。在一种实现中，密钥管理单元104发送指令以将网络设备112注销。例如，密钥管理单元104可以向网络设备112中的注册

管理单元113发送注销请求。该注销请求可以包括加密的RKk(如在图13中在阶段G、在图14中在阶段E、在图19中在阶段L、以及在图20中在阶段E所示出的)。RKk可以是使用网络设备112已知的哈希算法和使用从网络设备接收的随机数来加密的。在一些实现中,密钥管理单元104可以不必发送具有加密的RKk的注销请求,而是该注销请求可以包括RKk而不是加密的RKk(例如,如在图23中在阶段B所示出的)。在一些实现中,在接收到注销请求之后,注册管理单元113可以确定网络设备112是否向密钥携带设备102注册了(例如,如在图14中在阶段F、在图19中在阶段M、在图20中在阶段F、以及在图23中在阶段E所示出的)。如果网络设备112向密钥携带设备102注册了,则注册管理单元113可以执行一个或多个操作以将网络设备112注销,并向密钥管理单元104发送注销响应。如果网络设备112未向密钥携带设备102注册,则注册管理单元113可以向密钥管理单元104指示网络设备112未向密钥携带设备102注册。

[0128] 应该注意的是,在图4的流程图中示出的过程在本质上是示例性的,且为了简化起见,图4未示出当实现第三、第四和第五配置技术时所执行的所有操作的所有细节。下文将参考图9-23进一步描述针对第三、第四和第五配置技术,在密钥携带设备102和网络设备112处执行的示例性操作的另外细节。

[0129] 图5示出了用于使用第一配置技术来注册网络设备的示例性操作的顺序图。图5包括密钥携带设备102和网络设备112(如上文参考图1所描述的)。当存储在密钥携带设备102处的配对数据包括网络设备的设备标识符(IDY)、完整性密钥(KI)、加密密钥(KE)、以及序列号计数器(SN)时,密钥携带设备102可以利用第一配置技术。存储在网络设备112处的配对数据可以包括密钥携带设备的设备标识符(IDB)、完整性密钥(KI')、加密密钥(KE')、以及序列号计数器(SN')。应该注意的是,IDY、KI、KE、SN、IDB、KI'、KE'和SN'代表用于在密钥携带设备102和网络设备112存储配对数据的示例性变量。还应该注意的是,密钥携带设备102的设备标识符是IDA,而网络设备112的设备标识符是IDX。还应该注意的是,密钥携带设备102能够存储与向密钥携带设备102注册的多个网络设备相对于的多组配对数据(即,IDY、KI、KE和SN)。图5在一系列的阶段A-I2中示出了在密钥携带设备102和网络设备112之间用于注册网络设备112的交互。虽然图5示出了由密钥管理单元104和注册管理单元113执行的操作,但是在一些实现中,上述操作可以分别由密钥携带设备102和网络设备112的其它单元来执行。

[0130] 在阶段A,向网络设备112发送注册请求。在一种实现中,密钥携带设备102中的密钥管理单元104向注册管理单元113发送注册请求。例如,注册请求可以包括IDA和用于更新网络设备112处的配对数据的指令。

[0131] 在阶段B,确定IDB是否为空。在一种实现中,注册管理单元113确定存储在网络设备112处IDB的值是否为空则。如果IDB为空,则注册管理单元113在阶段C2向密钥管理单元104发送响应。如果IDB不为空,则注册管理单元113可以在阶段C1确定IDB是否等于IDA。

[0132] 在阶段C1,确定IDB是否等于IDA。在一种实现中,注册管理单元113确定IDB是否等于IDA。如果IDB等于IDA,则注册管理单元113在阶段D1向密钥管理单元104发送响应。如果IDB不等于IDA,则注册管理单元113在阶段D2向密钥管理单元104发送响应。

[0133] 在阶段C2,向网络设备112发送响应。在一种实现中,注册管理单元113向密钥管理单元104发送OK响应。例如,OK响应可以包括网络设备112准备好进行注册的确认,并且还可

以包括IDX。

[0134] 在阶段D1，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应，以指示网络设备112已经向密钥携带设备102注册。

[0135] 在阶段D2，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应，以指示网络设备112向另一密钥携带设备注册了。

[0136] 在阶段E，执行密钥协商、密钥导出和密钥确认操作以建立安全通信信道。在一种实现中，密钥管理单元104和注册管理单元113执行密钥协商、密钥导出和密钥确认操作，以建立安全通信信道。例如，密钥管理单元104和注册管理单元113可以确定安全信道密钥(例如，加密密钥、完整性密钥和序列号计数器)。密钥管理单元104和注册管理单元113可以使用该安全信道密钥来建立安全通信信道。该安全通信信道可以确保针对在密钥携带设备102和网络设备112之间的交换的任何消息的完整性以及重放保护。只要在密钥携带设备102和网络设备112之间存在安全通信信道，密钥管理单元104和注册管理单元113就可以存储加密密钥、完整性密钥和序列号计数器。如下文在阶段I1和I2所描述的，密钥管理单元104和注册管理单元113也可以将安全信道密钥存储为配对数据。

[0137] 在阶段F，通过安全通信信道来发送网络密钥。在一种实现中，密钥管理单元104通过安全通信信道向注册管理单元113发送存储在密钥携带设备102的通信网络100的网络密钥。例如，密钥管理单元104可以在消息(例如，使用加密密钥加密的消息)中发送网络密钥连同在消息生成时序列号计数器(SN)的值。应该注意的是，每次生成消息，存储在网络设备112和密钥携带设备102的序列号计数器可以递增。

[0138] 在阶段G，确定网络密钥是否是从密钥携带设备102接收的。在一种实现中，注册管理单元113确定网络密钥是否是从密钥携带设备102接收的。例如，注册管理单元113可以利用在阶段F接收的消息中的序列号计数器的值，来确定网络密钥是否是从密钥携带设备102接收的。注册管理单元113可以通过验证在阶段G在所接收的消息中的序列号计数器的值在顺序上依次在从密钥携带设备102接收到最后的消息之后，来确定网络密钥是否是从密钥携带设备102接收的。如果网络密钥不是从密钥携带设备102接收的，则注册管理单元113可以在阶段H1向密钥管理单元104发送错误消息。如果网络密钥是从密钥携带设备102接收的，则注册管理单元113可以在阶段H2通过安全通信信道向密钥管理单元104发送注册确认消息。

[0139] 在阶段H1，向密钥携带设备102发送错误消息。在一种实现中，注册管理单元113向密钥管理单元发送错误消息，以指示在阶段F向网络设备112发送的网络密钥不是从密钥携带设备102发送的。在一些实现中，在阶段H1接收到错误消息之后，密钥管理单元104可以在阶段F重复上述操作，以向注册管理单元113发送网络密钥。

[0140] 在阶段H2，通过安全通信信道向密钥携带设备102发送注册确认消息。在一种实现中，注册管理单元113通过安全通信信道发送注册确认消息(例如，使用加密密钥加密的消息)，以向密钥管理单元104指示NK在网络设备112处被成功接收。

[0141] 在阶段I1，更新密钥携带设备102处的配对数据。在一种实现中，密钥管理单元104更新存储在密钥携带设备102的配对数据(与网络设备112相对应的)。例如，密钥管理单元104可以设置IDY等于IDX(在阶段C2接收的)、KI等于安全通信信道的完整性密钥、KE等于安全通信信道的加密密钥、以及SN等于安全通信信道的序列号计数器。

[0142] 在阶段I2，更新网络设备112处的配对数据。在一种实现中，注册管理单元113更新存储在网络设备112的配对数据。例如，注册管理单元113可以设置IDB等于IDA(在阶段A接收的)、KI'等于安全通信信道的完整性密钥，KE'等于安全通信信道的加密密钥、以及SN'等于安全通信信道的序列号计数器。

[0143] 图6示出了使用第一配置技术来注销网络设备的示例性操作的顺序图。图6包括密钥携带设备102和网络设备112(如上文参考图5所描述的)。当存储在密钥携带设备102和网络设备112处的配对数据与图5中描述的配对数据类似时，密钥携带设备102可以利用第一配置技术来注销网络设备112。当网络设备112向密钥携带设备102注册了时，密钥携带设备102可以仅注销网络设备112。应该注意的是，当网络设备112向密钥携带设备102注册时，IDY等于IDX，IDB等于IDA，KI'等于KI(其中KI等于在注册期间所建立的安全通信信道的完整性密钥)，KE'等于KE(其中KE等于安全通信信道的加密密钥)，并且SN'等于SN(其中SN等于安全通信信道的序列号)。图6示出了在一系列的阶段A-I2中，在密钥携带设备102和网络设备112之间用于注销网络设备112的交互。虽然图6示出了由密钥管理单元104和注册管理单元113执行的操作，在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执行。

[0144] 在阶段A，向网络设备112发送注销请求。在一种实现中，密钥携带设备102中的密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求可以包括用于注销的指令(例如，清除配对数据)和IDA。

[0145] 在阶段B，确定IDB是否为空。在一种实现中，注册管理单元113确定存储在网络设备112处的IDB的值是否为空。如果IDB为空，则注册管理单元113在阶段C1向密钥管理单元104发送响应。如果IDB不为空，则注册管理单元113可以在阶段C2确定IDB是否等于IDA。

[0146] 在阶段C1，向密钥携带设备102发送响应。在一种实现中，注册管理单元113向密钥管理单元102发送响应。例如，该响应可以向密钥管理单元104指示网络设备102未注册(即，未向任何密钥携带设备注册)。

[0147] 在阶段C2，确定IDB是否等于IDA。在一种实现中，注册管理单元113确定IDB是否等于IDA。如果IDB等于IDA，则注册管理单元113在阶段D2向密钥管理单元104发送响应。如果IDB不等于IDA，则注册管理单元113在阶段D1向密钥管理单元104发送响应。

[0148] 在阶段D1，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应，以指示网络设备112向另一密钥携带设备注册了。

[0149] 在阶段D2，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送OK响应。例如，OK响应可以包括网络设备112准备好被注销的确认。OK响应也可以包括IDX。

[0150] 在阶段E1，确定针对网络设备112的安全信道密钥。在一种实现中，密钥管理单元104确定针对网络设备112的安全信道密钥。例如，密钥管理单元104基于在阶段D2接收的IDX来确定安全信道密钥。密钥管理单元104可以在网络设备112的注册期间查找存储在密钥携带设备102处的安全信道密钥(例如，完整性密钥、加密密钥、以及序列号计数器)。

[0151] 在阶段E2，建立安全通信信道。在一种实现中，密钥管理单元104使用在阶段E1确定的安全信道密钥与注册管理单元113建立安全通信信道。安全通信信道可以确保针对在密钥携带设备102和网络设备112之间交换的消息的完整性和重放保护。

[0152] 在阶段F，在安全通信信道上发送一个或多个指令，以将网络设备112注销。在一种实现中，密钥管理单元104可以向注册管理单元113发送具有一个或多个指令的消息(例如，使用加密密钥加密的消息)，以将网络设备112注销。例如，该消息可以包括用于清除在网络设备112处存储的配对数据和网络密钥的指令。该消息也可以包括在消息生成时序列号计数器(SN)的值。应该注意的是，每次生成消息时，存储在网络设备112和密钥携带设备102处的序列号计数器可以递增。

[0153] 在阶段G，确定上述指令是否是从密钥携带设备102接收的。在一种实现中，注册管理单元113确定上述指令是否是从密钥携带设备102接收的。例如，注册管理单元113可以利用在阶段F所接收的消息中的序列号计数器(SN)的值来确定上述指令是否是从密钥携带设备102接收的。注册管理单元113可以通过验证在阶段F接收的消息中的序列号计数器的值在顺序上依次在从密钥携带设备102接收的最后的消息之后，来确定上述指令是否是从密钥携带设备102接收的。如果上述指令不是从密钥携带设备102接收的，则注册管理单元113可以在阶段H1向密钥管理单元104发送错误消息。如果上述指令是从密钥携带设备102接收的，则注册管理单元113可以在阶段H2通过安全通信信道向密钥管理单元104发送注销确认消息。

[0154] 在阶段H1，向密钥携带设备102发送错误消息。在一种实现中，注册管理单元113向密钥管理单元104发送错误消息，以指示在阶段F接收的指令不是从密钥携带设备102发送的。在一些实现中，在阶段H1接收到错误消息之后，密钥管理单元104可以重发指令以将网络设备112注销。

[0155] 在阶段H2，通过安全通信信道向密钥携带设备102发送注销确认消息。在一种实现中，注册管理单元113通过安全通信信道发送注销确认消息(例如，使用加密密钥加密的消息)，以向密钥管理单元104指示在网络设备112处从密钥携带设备102成功接收用于注销的指令。

[0156] 在阶段I1，清除在密钥携带设备102处的配对数据。在一种实现中，密钥管理单元104清除存储在密钥携带设备102处的配对数据(与网络设备112相对应)。例如，密钥管理单元104可以将IDY、KI、KE和SN设置等于空。

[0157] 在阶段I2，清除存储在网络设备112处的配对数据和网络密钥。在一种实现中，注册管理单元113清除存储在网络设备112处的配对数据。例如，注册管理单元113可以将IDB、KI’、KE’、和SN’设置等于空。注册管理单元113也可以删除存储在网络设备112处的网络密钥(其是在向密钥携带设备102注册期间接收的)。

[0158] 图7示出了用于使用第二配置技术注册网络设备的示例性操作的顺序图。图7包括密钥携带设备102和网络设备112(如上文参考图1所描述的)。当存储在网络设备112处的配对数据包括密钥携带设备的公共密钥时，密钥携带设备102可以利用第二配置技术。例如，网络设备112可以以变量QB存储公共密钥。应该注意的是，密钥携带设备102的公共密钥是QA，并且当网络设备112向密钥携带设备102注册时，QB可以被设置为QA。还应该注意的是，在第二配置技术中，密钥携带设备102不存储针对与密钥携带设备102配对的网络设备的配对数据。图7在一系列的阶段A-I中示出了在密钥携带设备102和网络设备112之间用于注册网络设备112的交互。虽然图7示出了由密钥管理单元104和注册管理单元113执行的操作，但是在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执

行。

[0159] 在阶段A，向网络设备112发送注册请求。在一种实现中，密钥携带设备102中的密钥管理单元104向注册管理单元113发送注册请求。例如，注册请求可以包括用于注册的指令和QA。

[0160] 在阶段B，确定QB是否为空。在一种实现中，注册管理单元113确定存储在网络设备112处的QB的值是否为空。如果QB为空，则注册管理单元113在阶段C2向密钥管理单元104发送响应。如果QB不为空，则注册管理单元113可以在阶段C1确定QB是否等于QA。

[0161] 在阶段C1，确定QB是否等于QA。在一种实现中，注册管理单元113确定QB是否等于QA。如果QB等于QA，则注册管理单元113在阶段D1向密钥管理单元104发送响应。如果QB不等于QA，则注册管理单元113在阶段D2向密钥管理单元104发送响应。

[0162] 在阶段C2，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应。例如，响应可以包括网络设备112准备好要向密钥携带设备102注册的确认。

[0163] 在阶段D1，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应，以指示网络设备112以及向密钥携带设备102注册了。

[0164] 在阶段D2，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应，以指示网络设备112向另一密钥携带设备注册了。

[0165] 在阶段E，执行密钥协商、密钥导出以及密钥确认操作以建立安全通信信道。在一种实现中，密钥管理单元104和注册管理单元113执行密钥协商、密钥导出和密钥确认操作以建立安全通信信道。例如，密钥管理单元104和注册管理单元113可以确定安全信道密钥(例如，加密密钥、完整性密钥以及序列号计数器)。密钥管理单元104和注册管理单元113可以使用该安全信道密钥来建立安全通信信道。该安全通信信道可以针对在密钥携带设备102和网络设备112之间交换的消息确保完整性和重放保护。只要在密钥携带设备102和网络设备112之间存在安全通信信道，密钥管理单元104和注册管理单元113就可以存储加密密钥、完整性密钥和序列号计数器。

[0166] 在阶段F，通过安全通信信道发送网络密钥。在一种实现中，密钥管理单元104通过安全通信信道向注册管理单元113发送存储在密钥携带设备102处的通信网络100的网络密钥。例如，密钥管理单元104可以在消息中发送网络密钥(例如，使用加密密钥加密的消息)连同在消息生成时序列号计数器的值。应该注意的是，每一次消息生成时，在网络设备112和密钥携带设备102处存储的序列号计数器可以递增。

[0167] 在阶段G，确定网络密钥是否是从密钥携带设备102接收的。在一种实现中，注册管理单元113确定网络密钥是否是从密钥携带设备102接收的。例如，注册管理单元113可以利用在阶段F所接收的消息中的序列号计数器的值，来确定网络密钥是否是从密钥携带设备102接收的。注册管理单元113可以通过验证该消息中的序列号计数器的值在顺序上依次在从密钥携带设备102接收的最后的消息之后，来确定网络密钥是否是从密钥携带设备102接收的。如果网络密钥不是从密钥携带设备102接收的，则注册管理单元113可以在阶段H1向密钥管理单元104发送错误消息。如果网络密钥是从密钥携带设备102接收的，则注册管理单元113可以在阶段H2通过安全通信信道向密钥管理单元104发送注册确认消息。

[0168] 在阶段H1，向密钥携带设备102发送错误消息。在一种实现中，注册管理单元113向

密钥管理单元104发送错误消息，以指示网络设备112在阶段F接收的网络密钥不是从密钥携带设备102发送的。在一些实现中，在阶段1接收错误消息之后，密钥管理单元104可以向注册管理单元113重发网络密钥。

[0169] 在阶段H2，通过安全通信信道向密钥携带设备102发送注册确认消息。在一种实现中，注册管理单元113通过安全通信信道发送注册确认消息(例如，使用加密密钥加密的消息)，以向密钥管理单元104指示网络密钥在网络设备112处被成功接收。

[0170] 在阶段I，更新网络设备112处的配对数据并存储网络密钥。在一种实现中，注册管理单元113更新存储在网络设备112处的配对数据。例如，注册管理单元113可以设置QB等于QA(在阶段A所接收的)以更新配对数据。注册管理单元113也可以将在阶段F从密钥管理单元104接收的网络密钥存储在网络设备112处。

[0171] 图8示出了用于使用第二配置技术来将网络设备注销的示例性操作的顺序图。图8包括密钥携带设备102和网络设备112(如上文参考图7所描述的)。当存储在网络设备112处的配对数据与在图7中所描述的配对数据类似时，密钥携带设备102可以利用第二配置技术来将网络设备112注销。当网络设备112向密钥携带设备102注册了时，密钥携带设备102可以仅将网络设备112注销。应该注意的是，当网络设备112向密钥携带设备102注册时，QB等于QA。图8在一系列的阶段A-G中示出了密钥携带设备102和网络设备112之间的交互以将网络设备112注销。虽然图8示出了由密钥管理单元104和注册管理单元113所执行的操作，但是，在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执行。

[0172] 在阶段A，向网络设备112发送注销请求。在一种实现中，密钥携带设备102中的密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求可以包括用于注销的指令(即，清除配对数据)和QA。

[0173] 在阶段B，确定QB是否为空。在一种实现中，注册管理单元113确定存储在网络设备112处的QB的值是否为空。如果QB为空，则注册管理单元113在阶段C1向密钥管理单元104发送响应。如果QB不为空，则注册管理单元113可以在阶段C2确定QB是否等于QA。

[0174] 在阶段C1，向网络设备112发送响应。在一种实现中，注册管理单元113向网络设备112发送响应。例如，该响应可以向密钥管理单元104指示网络设备102是未注册的(即，未向任何密钥携带设备注册)。

[0175] 在阶段C2，确定QB是否等于QA。在一种实现中，注册管理单元113确定QB是否等于QA。如果QB等于QA，则注册管理单元113在阶段D1向密钥管理单元104发送响应。如果QB不等于QA，则注册管理单元113在阶段D2向密钥管理单元104发送响应。

[0176] 在阶段D1，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应，以指示网络设备112是否向另一密钥携带设备注册了。

[0177] 在阶段D2，向网络设备112发送响应。在一种实现中，注册管理单元113向密钥管理单元104发送响应。例如，该响应可以包括网络设备112准备好被注销的确认。

[0178] 在阶段E，执行密钥协商、密钥导出和密钥确认操作。在一种实现中，密钥管理单元104和注册管理单元113执行密钥协商、密钥导出和密钥确认过程。例如，密钥管理单元104单元可以发起密钥协商、密钥导出和密钥确认操作，以向网络设备112证明其身份(例如，成功的密钥确认将指示密钥携带设备102知道与QB相关联的私人密钥(例如，加密密钥))。在

一些实现中，当密钥携带设备102知道与QB相关联的私人密钥时，密钥管理单元104可以(在向注册管理单元113发送的消息中)将完整性密钥(例如，MAC)设置为有效。在密钥携带设备102与网络设备112之间的密钥协商、密钥导出和密钥确认操作的成功可以使网络设备112识别密钥携带设备102。

[0179] 在阶段F1，确定密钥协商、密钥导出和密钥确认操作是否成功。在一种实现中，注册管理单元113确定与密钥携带设备102的密钥协商、密钥导出和密钥确认操作是否成功。密钥协商、密钥导出和密钥确认操作的成功可以允许注册管理单元113确定在阶段A从密钥携带设备102接收到注销请求。在一些实现中，注册管理单元113确定在从密钥管理单元104接收的消息中的完整性密钥是否有效，以确定在阶段A从密钥携带设备102接收到注销请求。如果密钥协商、密钥导出和密钥确认操作成功，则注册管理单元113在阶段F2清除配对数据和网络密钥(在注册期间从密钥携带设备102接收的)。如果密钥协商、密钥导出和密钥确认操作不成功，则注册管理单元113在阶段G终止网络设备112的注销。

[0180] 在阶段F2，清除在网络设备112处存储的配对数据和网络密钥。在一种实现中，注册管理单元113清除在网络设备112处存储的配对数据和网络密钥。例如，注册管理单元113可以删除网络密钥并将QB设置为空。在一些实现中，在清除配对数据和网络密钥之后，网络设备112可以向密钥携带设备102发送确认消息。

[0181] 在阶段G，终止注销。在一种实现中，注册管理单元113终止网络设备112的注销。例如，当在阶段F1中密钥协商、密钥导出和密钥确认操作不成功时，注册管理单元113可以终止网络设备112的注销。在一些实现中，注册管理单元113可以在终止注销之后向密钥管理单元104发送错误消息。

[0182] 图9、10、11和12示出了用于使用第三配置技术注册网络设备的示例性操作的顺序图。图9、10、11和12包括密钥携带设备102和网络设备112(如上文参考图1所描述的)。当存储在密钥携带设备102处的配对数据包括注册密钥(RKk)，并且存储在网络设备112处的配对数据包括注册密钥(RKn)时，密钥携带设备102可以利用第三配置技术。密钥携带设备102和网络设备112也可以存储网络密钥(NK)和网络密钥(NK')。密钥携带设备102和网络设备112可以对用于加密和安全地交换RKk和RKn的哈希算法达成一致。哈希算法可以利用随机数来加密RKk和RKn。例如，可以将随机数与注册密钥串联(即，随机数的比特可以添加到注册密钥以确定串联值)，并且然后可以将串联值的哈希值计算为注册密钥的加密值。可以在没有任何加密的情况下在网络设备112和密钥携带设备102之间交换随机值，并允许网络设备112和密钥携带设备102加密其注册密钥。应该注意的是，RKk和RKn分别代表用于在密钥携带设备102和网络设备112处存储注册密钥的示例性变量。类似地，NK和NK'分别代表用于在密钥携带设备102和网络设备112处存储网络密钥的示例性变量。还应该注意的是，当网络设备112向密钥携带设备102注册了时，RKk和RKn的值相等。此外，当网络设备112被配置具有由密钥携带设备102管理的通信网络(即，通信网络100)时，NK和NK'的值相等。还应该注意的是，当网络设备112未向任何密钥携带设备注册时，RKn和NK'可以为空。在一些实现中，RKk和NK也可以为空(例如，当密钥携带设备102不具有通信网络100的网络密钥时)。但是，当RKk和/或NK的值为空时，密钥携带设备102包括用于生成RKk和NK的随机值的能力。图9、10、11和12示出了在一系列的阶段A-AD中在密钥携带设备102和网络设备112之间用于注册网络设备112的交互。虽然图9、10、11和12示出了由密钥管理单元104和注册管理单元113

所执行的操作，在一些实现中，可以分别由密钥携带设备102和网络设备112中的其它单元来执行上述操作。

[0183] 在阶段A，向网络设备112发送你好(hello)请求。在一种实现中，密钥携带设备102中的密钥管理单元104向注册管理单元113发送你好请求。例如，你好请求可以包括随机数N1。随机数N1可以由注册管理单元113在阶段B用来加密RKn。

[0184] 在阶段B，计算RKn和NK'的加密值。在一种实现中，注册管理单元113计算RKn和NK'的加密值。例如，注册管理单元113可以使用与密钥携带设备102达成一致意见的哈希算法计算与N1串联的RKn的哈希值，以及NK'的哈希值。应该注意的是，当RKn和/或NK'为空时，RKn和/或NK'的加密值也可以为空。

[0185] 在阶段C，向密钥携带设备102发送你好(hello)响应。在一种实现中，注册管理单元113向密钥管理设备104发送你好响应。例如，你好响应可以包括RKn和NK'(在阶段B计算的)的加密值以及随机数N2。密钥管理单元104可以利用随机数N2来加密RKk(如下文将在阶段O1中所描述的)。

[0186] 在阶段D，确定RK n的加密值为空。在一种实现中，密钥管理单元104确定RKn的加密值(在阶段C接收的)是否为空。如果RKn的加密值为空，则密钥管理单元104可以确定网络设备未向任何密钥携带设备注册，且密钥管理单元104可以注册网络设备112。例如，如果RKn的加密值为空，则密钥管理单元104可以在阶段E执行操作。如果RKn的加密值不为空，则密钥管理单元104可以确定网络设备112向密钥携带设备注册了且控制流程去往链接2.1，在该链接中密钥管理单元104可以执行在阶段K的操作。

[0187] 在阶段E，确定RKk是否为空。在一种实现中，密钥管理单元104确定在密钥携带设备102处存储的RKk是否为空。如果RKk为空，则密钥管理单元104可以执行在阶段F的操作。如果RKk不为空，则密钥管理单元104可以执行在阶段G的操作。

[0188] 在阶段F，生成随机的RKk。在一种实现中，密钥管理单元104使用伪随机数算法生成随机的RKk。例如，当注册密钥在密钥携带设备102处不存在时，密钥管理单元104可以生成可以向注册管理单元113发送的、用以向密钥携带设备102注册网络设备112的、新的随机注册密钥。在一些实现中，密钥管理单元104将随机的RKk保存为存储在密钥携带设备102处的RKk。

[0189] 在阶段G，与网络设备112建立安全通信信道。在一种实现中，密钥管理单元104可以通过与注册管理单元113执行密钥协商、密钥导出、以及密钥确认操作来建立安全通信信道。安全通信信道可以允许在没有加密RKk的情况下，密钥管理单元104向注册管理单元113发送RKk(在阶段H)。

[0190] 在阶段H，向网络设备112发送注册请求。在一种实现中，密钥管理单元104通过安全通信信道向注册管理单元113发送注册请求。例如，注册请求可以包括RKk。

[0191] 在阶段I，在网络设备112处保存RKk。在一种实现中，在阶段H注册管理单元113保存从密钥管理单元104接收的、在注册请求中的RKk。例如，注册管理单元113可以将RKn设置为等于RKk，以保存RKk，并向密钥携带设备102进行注册。

[0192] 在阶段J，向密钥携带设备102发送注册响应。在一种实现中，注册管理单元113向密钥管理单元104发送注册响应。例如，注册响应可以向密钥管理单元104指示网络设备112向密钥携带设备102注册了。在阶段J接收到注册响应之后，控制流程去往链接2.2，在该链

接中密钥管理单元104可以执行在阶段M的操作。

[0193] 在阶段K，确定RKn的加密值是否等于RKk的加密值。在一种实现中，密钥管理单元104确定RKn的加密值(在阶段C接收的)是否等于RKk的加密值。密钥管理单元104可以通过使用与网络设备112达成一致意见的哈希算法计算与N1串联的RKk的哈希值来计算RKk的加密值。如果RKn的加密值等于RKk的加密值，则密钥管理单元104可以确定网络设备112向密钥携带设备102注册了，且密钥管理单元104可以执行在阶段M的操作。如果RKn的加密值不等于RKk的加密值，则密钥管理单元104可以确定网络设备112向另一密钥携带设备(不同于密钥携带设备102)注册了，并且密钥管理单元104可以在阶段L停止注册操作。

[0194] 在阶段L，停止注册操作。在一种实现中，密钥管理单元104可以停止网络设备112向密钥携带设备102注册的操作。

[0195] 在阶段M，确定NK'的加密值是否为空。在一种实现中，密钥管理单元104确定NK'的加密值(在阶段C接收的)是否为空。如果NK'的加密值为空，则密钥管理单元104可以确定网络密钥未存储在网络设备112处，且控制流程去往链接4，在该链接中密钥管理单元104可以执行在阶段V的操作。如果NK'的加密值不为空，则密钥管理单元104可以执行在阶段N的操作。

[0196] 在阶段N，确定是否使用网络设备112的网络密钥。在一种实现中，密钥管理单元104确定是否使用网络设备112的网络密钥。例如，当通信网络100的网络密钥未存储在密钥携带设备102处时，密钥管理单元104可以确定使用(例如，接收并保存)存储在网络设备112处的网络密钥。如果密钥管理单元104确定使用网络设备112的网络密钥，则控制流程去往链接3，在该链接中密钥管理单元104可以执行在阶段O1的操作。如果密钥管理单元104确定不使用网络设备112的网络密钥，则控制流程去往链接4，在该链接中密钥管理单元104可以执行在阶段V的操作。

[0197] 在阶段O1，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104使用与网络设备112达成一致意见的哈希算法来计算与N2(即，在阶段C所接收的N2)串联的RKk的哈希值。

[0198] 在阶段O2，向网络设备112发送获取网络密钥请求。在一种实现中，密钥管理单元104向注册管理单元113发送获取网络密钥请求。例如，获取网络密钥请求包括RKk的加密值(在阶段O1所计算的)。获取网络密钥请求可以包括对存储在网络设备112处的NK'的请求。

[0199] 在阶段P，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段O2所接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N2串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以验证获取网络密钥请求是从密钥携带设备102(而不是从恶意设备)接收的，并且注册管理单元113可以在阶段R发送获取网络密钥响应。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以在阶段O2确定获取网络密钥请求是由恶意设备发送的，且注册管理单元113可以在阶段Q检测到错误。

[0200] 在阶段Q，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为获取网络密钥请求由恶意设备发送的结果，注册管理单元113可以检测到发生了错误。

[0201] 在阶段R，向网络设备112发送获取网络密钥响应。在一种实现中，注册管理单元

113向密钥管理单元104发送获取网络密钥响应。例如，当注册管理单元113在阶段P确定RKk的加密值等于RKn的加密值时，获取网络密钥响应可以包括NK'。当在阶段P RKk的加密值不等于RKn的加密值时，获取网络密钥响应可以包含在阶段Q检测到的错误。在一些实现中，注册管理单元113可以与密钥管理单元104建立安全信道(例如，通过执行密钥协商、密钥导出和密钥确认操作)，并且可以通过安全通信信道发送获取网络密钥响应。

[0202] 在阶段S，确定获取网络密钥响应包含错误。在一种实现中，密钥管理单元104确定获取网络密钥响应是否包含错误。例如，密钥管理单元104可以确定获取网络密钥响应包含由注册管理单元113在阶段Q所检测到的错误。如果获取网络密钥响应包含错误，则密钥管理单元104可以在阶段U停止注册操作。如果获取网络密钥响应不包含错误，则密钥管理单元104可以执行在阶段T的操作。

[0203] 在阶段T，保存NK'。在一种实现中，密钥管理单元104保存在阶段R从注册管理单元113接收的注册响应中的NK'。例如，密钥管理单元104可以将NK设置等于NK'以保存NK'。

[0204] 在阶段U，停止注册操作。在一种实现中，密钥管理单元104停止用于向密钥携带设备102注册网络设备112的注册操作。

[0205] 在阶段V，确定NK是否为空。在一种实现中，密钥管理单元104确定在密钥携带设备102中存储的NK是否为空。如果NK为空，则密钥管理单元104可以执行在阶段W的操作。如果NK不为空，则密钥管理单元104可以执行在阶段X的操作。

[0206] 在阶段W，生成随机的NK。在一种实现中，密钥管理单元104生成随机的NK。例如，密钥管理单元104可以使用为随机数算法来生成随机的NK。在一些实现中，密钥管理单元104将随机的NK保存为在密钥携带设备102中存储的NK。在阶段W之后，密钥管理单元104可以执行在阶段X的操作。

[0207] 在阶段X，计算RKk的加密值。在一种实现中，密钥管理单元104计算机RKk的加密值。例如，密钥管理单元104可以使用与网络设备112达成一致意见的哈希算法来计算与N2(即，在阶段C接收的N2)串联的RKk的哈希值。

[0208] 在阶段Y，向网络设备112发送设置网络密钥请求。在一种实现中，密钥管理单元104向注册管理单元113发送设置网络请求。例如，设置网络密钥请求可以包含NK和RKk的加密值(在阶段X计算的)。在一些实现中，密钥管理单元104可以与注册管理单元113建立安全的通信信道并且通过安全的通信信道发送设置网络密钥请求。

[0209] 在阶段Z，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段Y接收的)是否等于RKn的加密值。注册管理单元113可以使用与密钥携带设备102达成一致意见的哈希算法计算与N2串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以验证在阶段Y的设置网络密钥请求是从密钥携带设备102(而不是从恶意设备)接收的，并且注册管理单元113可以在阶段AB保存NK。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定在阶段Y的设置网络密钥请求时由恶意设备发送的，并且注册管理单元可以在阶段AA检测到错误。

[0210] 在阶段AA，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为设置网络密钥请求由恶意设备发送的结果，注册管理单元113可以检测到发生了错误。

[0211] 在阶段AB，保存NK。在一种实现中，注册管理单元113在阶段Y保存在设置网络密钥

请求中接收的NK。例如，注册管理单元113可以将NK’设置等于NK以在网络设备112处保存NK。

[0212] 在阶段AC，向密钥携带设备102发送设置网络密钥响应。在一种实现中，注册管理单元113向密钥管理单元104发送设置网络密钥响应。例如，设置网络密钥响应可以包括当注册管理单元113在阶段AB保存NK时的确认。当注册管理单元113在阶段AA检测到错误时，设置网络密钥响应可以包含错误。

[0213] 在阶段AD，停止注册操作。在一种实现中，密钥管理单元104停止用于注册网络设备112的注册操作。例如，密钥管理单元104可以在从注册管理单元113接收到设置网络密钥响应之后，停止注册操作。在一些实现中，当设置网络密钥响应包含错误时，密钥管理单元104可以执行一个或多个操作以向注册管理单元113重发设置网络密钥请求。

[0214] 图13示出了用于使用第三配置技术将网络设备注销的第一选项的示例性操作的顺序图。图13包括密钥携带设备102和网络设备112(如上文参考图9、10、11和12所描述的)。当存储在密钥携带设备102和网络设备112处的配对数据与在图9、10、11和12中所描述的配对数据类似时，密钥携带设备102可以使用第三配置技术利用第一选项来将网络设备112注销。在使用第三配置技术用于将网络设备112注销的第一选项中，密钥携带设备102执行操作以确定网络设备112是否向密钥携带设备102注册了。仅当网络设备112向密钥携带设备102注册了时，密钥携带设备102才将网络设备112注销。应该注意的是，当网络设备112向密钥携带设备102注册了时，RKn等于RKk。图13在一系列的阶段A-L中示出了在密钥携带设备102和网络设备112之间用于将网络设备112注销的交互。如果图13示出了由密钥管理单元104和注册管理单元113所执行的操作，但是在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执行。

[0215] 在阶段A，向网络设备112发送你好请求。在一种实现中，密钥管理单元104向注册管理单元113发送你好请求。例如，你好请求可以包括随机数N1。随机数N1可以由注册管理单元113利用来在阶段B对RKn进行加密。

[0216] 在阶段B，计算RKn和NK’的加密值。在一种实现中，注册管理单元113计算RKn和NK’的加密值。例如，注册管理单元113可以使用与密钥携带设备102达成一致的哈希算法计算与N1串联的RKn的哈希值和NK’的哈希值。应该注意的是，当RKn和/或NK’为空时，RKn和/或NK’的加密值也可以为空。

[0217] 在阶段C，向密钥携带设备102发送你好响应。在一种实现中，注册管理单元113向密钥管理单元104发送你好响应。例如，你好响应可以包括RKn和NK’的加密值(在阶段B计算的)以及随机数N2。随机数N2可以由密钥管理单元104利用来加密RKk(如下文将在阶段F描述的)。

[0218] 在阶段D，确定RKn的加密值是否为空。在一种实现中，注册管理单元113确定RKn的加密值(在阶段C接收的)是否为空。如果RKn的加密值为空，则密钥管理单元104可以确定网络设备112未向任何密钥携带设备进行注册，并且密钥管理单元104可以在阶段L停止注销操作。如果RKn的加密值不为空，则密钥管理单元104可以确定网络设备112向密钥携带设备注册了，且密钥管理单元104可以在阶段E执行操作。

[0219] 在阶段E，确定RKn的加密值是否等RKk的加密值。在一种实现中，密钥管理单元104确定RKn的加密值(在阶段C接收的)等于RKk的加密值。密钥管理单元104可以使用与网络设

备112达成一致意见的哈希算法计算与N1串联的RKk的哈希值来计算RKk的加密值。如果RKn的加密值等于RKk的加密值，则密钥管理单元104可以确定网络设备112向密钥携带设备102注册了，且密钥管理单元104可以将网络设备112注销。如果RKn的加密值不等于RKk的加密值，则密钥管理单元104可以确定网络设备112向另一密钥携带设备(不同于密钥携带设备102)注册了，且密钥管理单元104可以在阶段L停止注销操作。

[0220] 在阶段F，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104使用与网络设备112达成一致意见的哈希算法来计算与N2(即，在阶段C所接收的N2)串联的RKk的哈希值。

[0221] 在阶段G，向网络设备112发送注销请求。在一种实现中，密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求可以包括RKk的加密值(在阶段F计算的)和用于删除RKn和NK'的值的请求。

[0222] 在阶段H，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段G所接收的)是否等于RK的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N2串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以验证注销请求是从密钥携带设备102(而不是从恶意设备)接收的，并且注册管理单元113可以在阶段I删除RKn和NK'的值。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定在阶段G的注销请求时由恶意设备发送的，并且注册管理单元113可以在阶段J检测到错误。

[0223] 在阶段I，删除RKn和NK'的值。在一种实现中，注册管理单元113删除RKn和NK'的值。一旦删除了RKn和NK'的值，则网络设备112不再是向密钥携带设备102注册的，注册管理单元113可以向密钥管理单元104发送确认以确认网络设备112的注销(如下文在阶段K所描述的)。

[0224] 在阶段J，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为注销请求由恶意设备发送的结果，注册管理单元113可以检测到发生了错误。

[0225] 在阶段K，向密钥携带设备102发送注销请求。在一种实现中，注册管理单元113向密钥管理单元104发送注销响应。例如，注销响应可以包括当注册管理单元113在阶段I删除了RKn和NK'的值时的确认。当注册管理单元113在阶段J检测到错误时，注销响应可以包括错误。

[0226] 在阶段L，停止注销操作。在一种实现中，密钥管理单元104停止用于将网络设备112注销的注销操作。在一些实现中，当注销响应(在阶段K接收的)包含错误时，密钥管理单元104可以向注册管理单元113重发注销请求。

[0227] 图14示出了用于使用第三配置技术将网络设备注销的第二选项的示例性操作的顺序图。图14包括密钥携带设备102和网络设备112(如上文参考图9、10、11和12所描述的)。当在密钥携带设备102和网络设备112处存储的配对数据与在图9、10、11和12中所描述的配对数据类似时，密钥携带设备102可以使用第三配置技术利用第二选项来将网络设备112注销。在使用第三配置技术用于将网络设备112注销的第二选项中，网络设备112执行操作以确定操作以确定网络设备112是否向密钥携带设备102注册了。在从密钥携带设备102接收注销请求之后，仅当网络设备112确定网络设备112向密钥携带设备102注册了时，网络设备112才可以执行注销操作。应该注意的是，当网络设备112向密钥携带设备102注册了时，RKn

等于RKk。图14在一系列的阶段A-J中示出了在密钥携带设备102和网络设备112之间的、用于将网络设备112注销的交互。虽然图14示出了由密钥管理单元102和注册管理单元13执行的操作，但是在一些实现中，可以分别由密钥携带设备102和网络设备112中的其它单元执行操作。

[0228] 在阶段A，向网络设备112发送随机数请求。在一种实现中，密钥管理单元104向注册请求单元113发送随机数请求。例如，随机数请求包括从注册管理单元113请求随机数。

[0229] 在阶段B，生成随机数。在一种实现中，注册管理单元113生成随机数(即，N1)。例如，注册管理单元113可以生成N1，使得可以使用在密钥携带设备102和网络设备112之间达成一致意见的哈希算法利用N1来加密注册密钥。

[0230] 在阶段C，向网络设备112发送随机数响应。在一种实现中，注册管理单元113向密钥管理单元104发送随机数响应。例如，随机数响应可以包括N1(在阶段B生成的)。

[0231] 在阶段D，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104可以使用与网络设备112达成一致意见的哈希算法计算与N1(即，在阶段C接收的N1)串联的RKk的哈希值。

[0232] 在阶段E，向网络设备112发送注销请求。在一种实现中，密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求可以包括RKk的加密值(在阶段D计算的)以及用于删除RKn和NK'的值的请求。

[0233] 在阶段F，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段E接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N1串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以确定注销请求(在阶段E接收的)是从密钥携带设备102接收的，并且注册管理单元113可以在阶段G删除RKn和NK'的值。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定注销请求不是从密钥携带设备102接收的(而是从恶意设备接收的)，则注册管理单元113可以在阶段H检测到错误。

[0234] 在阶段G，删除RKn和NK'的值。在一种实现中，注册管理单元113删除RKn和NK'的值。一旦删除了RKn和NK'的值，则网络设备112不再是向密钥携带设备102注册的，并且注册管理单元113可以向密钥管理单元104发送用于确认网络设备112的注销的确认(如下文在阶段I所描述的)。

[0235] 在阶段H，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为从恶意设备接收到注销请求的结果，注册管理单元113可以检测到发生了错误。

[0236] 在阶段I，向密钥携带设备102发送注销响应。在一种实现中，注册管理单元113向密钥管理单元104发送注销响应。例如，注销响应可以包括当注册管理单元113在阶段G删除RKn和NK'的值时的确认。当注册管理单元113在阶段H检测到错误时，注销响应可以包括错误。

[0237] 在阶段J，停止注销操作。在一种实现中，密钥管理单元104停止用于将网络设备112注销的注销操作。在一些实现中，当注销响应(在阶段I接收的)包括错误时，密钥管理单元104可以向注册管理单元113重发注销请求。

[0238] 图15、16和17示出了用于使用第四配置技术注册网络设备的示例性操作的顺序

图。图15、16和17包括密钥携带设备102和网络设备112(如上文参考图1所描述的)。当在密钥携带设备102处存储的配对数据包括注册密钥(RKk)意见在网络设备112处存储的配对数据包括注册密钥(RKn)以及网络设备112的状态(状态)时,密钥携带设备102可以利用第四配置技术。在第四配置技术中,网络设备112执行操作以确定网络设备112的状态(例如,网络设备112向密钥携带设备102注册了、向另一密钥携带设备注册了或未注册)。网络设备112可以向密钥携带设备102发送其状态(例如,通过发送状态)。密钥携带设备102和网络设备112也可以存储网络密钥(NK)和网络密钥(NK')。密钥携带设备102和网络设备112可以对用于加密和安全交换RKk和RKn的哈希算法达成一致意见。哈希算法可以利用随机数来加密RKk和RKn。例如,随机数可以与注册密钥串联(例如,可以将随机数的比特添加到注册密钥上以确定串联值),并且任何可以将串联值的哈希值计算为注册密钥的加密值。可以在不加密的情况下,在网络设备112和密钥携带设备102之间交换随机数,并允许网络设备112和密钥携带设备102对其注册密钥进行加密。应该注意的是,RKk和RKn、以及状态分别代表用于在密钥携带设备102处存储注册密钥、在网络设备112处存储注册密钥以及网络设备112的状态的示例性变量。类似地,NK和NK'分别代表用于在密钥携带设备102处存储网络密钥、以及在网络设备112处存储网络密钥的示例性变量。还应用注意的是,当网络设备112向密钥携带设备102注册了时,状态被设置为"注册的",且RKk和RKn的值相等。此外,当网络设备112被配置具有由密钥携带设备102管理的通信网络(即,通信网络100)时,NK和NK'的值相等。还应该注意的是,当网络设备112未向任何密钥携带设备注册时,状态可以被设置为"未注册的",且RKn和NK'可以为空。在一些实现中,RKn和NK也可以为空(例如,当密钥携带设备102不具有通信网络100的网络密钥时)。但是,当RKk和/或NK的值为空时,密钥携带设备102包括用于生成RKk和NK的随机值的能力。图15、16和17在一系列的阶段A1-AI中示出了在密钥携带设备102和网络设备112之间用于注册网络设备112的交互。虽然图15、16和17示出了由密钥管理单元104和注册管理单元113执行的操作,但是在一些实现中,上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执行。

[0239] 在阶段A1,向网络设备112发送随机数请求。在一种实现中,密钥管理单元104向注册管理单元113发送随机数请求。例如,随机数请求包括从网络设备112请求随机数。

[0240] 在阶段A2,向网络设备112发送随机数响应。在一种实现中,注册管理单元113向密钥管理单元104发送随机数响应。例如,随机数响应可以包括N1(由注册管理单元113生成的随机数)。使用在密钥携带设备102和网络设备112之间达成一致意见的哈希算法可以利用N1来加密注册密钥。

[0241] 在阶段B,向网络设备112发送你好请求。在一种实现中,密钥管理单元104向注册管理单元113发送你好请求。例如,你好请求可以包括RKk的加密值和对状态的请求。密钥管理单元104可以通过使用与网络设备112达成一致意见的哈希算法计算与N1(即,在阶段A2接收的N1)串联的RKk的哈希值来计算RKk的加密值。

[0242] 在阶段C,确定RKn是否为空。在一种实现中,注册管理单元113确定RKn是否为空。例如,注册管理单元113可以通过检查在阶段B所接收的RKn的加密值是否为空来确定RKn为空。如果RKn为空,则注册管理单元113可以在阶段D将状态设置为'未注册的'。如果RKn不为空,则注册管理单元113可以在阶段E确定RKk的加密值是否等于RKn的加密值。

[0243] 在阶段D,将状态设置为"未注册的"。在一种实现中,注册管理单元113将状态设置

为“未注册的”，并且注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0244] 在阶段E，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKn的加密值(在阶段B接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N1串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以确定网络设备112向密钥携带设备102注册了，且注册管理单元113可以在阶段G将状态设置为‘注册的’。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定网络设备112向另一密钥携带设备(不同于密钥携带设备102)注册了，且注册管理单元113可以将状态设置为‘向不同的KCD注册了’。

[0245] 在阶段F，将状态设置为‘向不同的KCD注册了’。在一种实现中，注册管理单元113将在网络设备112处存储的状态设置为‘向不同的KCD注册了’。注册管理单元113可以在阶段H向密钥管理单元发送状态。

[0246] 在状态G，将状态设置为‘注册的’。在一种实现中，注册管理单元113将状态设置为‘注册的’。注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0247] 在阶段H，向密钥携带设备102发送你好响应。在一种实现中，注册管理单元113向密钥管理单元104发送你好响应。例如，你好响应可以包括状态、NK’的加密值、以及随机数(N2)。注册管理单元113可以使用与密钥携带设备102达成一致意见的哈希算法计算NK’的加密值。使用在密钥携带设备102与网络设备112之间达成一致意见的哈希算法，密钥携带设备102可以利用N2来加密RKk(如下文在步骤S描述的)。

[0248] 在阶段I，确定所接收的状态是否为‘未注册的’。在一种实现中，密钥管理单元104确定在阶段H接收的状态是否为‘未注册的’。如果状态为‘未注册的’，则控制流程去往链接2，并且密钥管理单元104可以在阶段L执行操作。如果状态时‘未注册的’，则密钥管理单元104可以在阶段J执行操作。

[0249] 在阶段J，确定状态是否为‘向不同的KCD注册了’。在一种实现中，密钥管理单元104确定状态是否为‘向不同的KCD注册了’。如果状态是‘向不同的KCD注册了’，则密钥管理单元104可以确定网络设备112未向密钥携带设备102进行注册，且密钥管理单元104可以在阶段K停止注册操作。如果状态不是‘向不同的KCD注册了’，则控制流程去往链接3，并且密钥管理单元104可以执行阶段AA的操作。

[0250] 在阶段K，停止注册操作。在一种实现中，密钥管理单元104停止用于将网络设备112向密钥携带设备102注册的注册操作。

[0251] 在阶段L，确定RKk是否为空。在一种实现中，密钥管理单元104确定在密钥携带设备102处存储的RKk是否为空。如果RKk为空，则密钥管理单元104在阶段M生成随机的RKk。如果RKk不为空，则密钥管理单元104在阶段N1建立安全的通信信道。

[0252] 在阶段M，生成随机的RKk。在一种实现中，密钥管理单元104使用伪随机数算法生成随机的RKk。例如，当在密钥携带设备102处不存在注册密钥时，密钥管理单元104可以生成可以向网络设备发送以将网络设备向密钥携带设备102注册的新的随机注册密钥。在一些实现中，密钥管理单元104将随机的RKk保存为在密钥携带设备102处存储的RKk。

[0253] 在阶段N1，与网络设备112建立安全通信信道。在一种实现中，密钥管理单元104可以通过与注册管理单元113执行密钥协商、密钥导出、以及密钥确认操作来建立安全通信信

道。安全通信信道可以在不使用哈希算法加密RKk的情况下，允许密钥管理单元104向注册管理单元113发送RKk。

[0254] 在阶段N2，向网络设备112发送注册请求。在一种实现中，密钥管理单元104向注册管理单元113发送注册请求。注册请求可以包括RKk。

[0255] 在阶段O，在网络设备112保存RKk。在一种实现中，注册管理单元113在阶段N1保存从密钥管理单元104接收的RKk。例如，注册管理单元113可以将RKn设置为RKk以保存RKk以及将状态设置为‘注册的’。在保存RKk之后，网络设备112向密钥携带设备102注册，并且注册管理单元113可以在阶段P向密钥管理单元104发送确认。

[0256] 在阶段P，向密钥携带设备102发送注册响应。在一种实现中，注册管理单元113向密钥管理单元104发送注册响应。例如，注册响应可以包括网络设备112向密钥携带设备102注册了的确认。在一些实现中，注册响应可以包括在网络设备112处存储的状态。

[0257] 在阶段Q，确定NK’的加密值是否为空。在一种实现中，密钥管理单元104确定在阶段H接收的NK’的加密值是否为空。如果NK’的加密值为空，则密钥管理单元104确定网络设备112不具有网络密钥，则控制流程去往链接3，在该链接中密钥管理单元104可以执行阶段AA的操作。如果NK’的加密值不为空，则密钥管理单元104确定网络设备112具有存储在网络设备112处的网络密钥，且密钥管理单元104可以执行在阶段R的操作。

[0258] 在阶段R，确定是否使用网络设备112的网络密钥。在一种实现中，密钥管理单元104确定是否使用网络设备112的网络密钥。例如，当通信网络100的网络密钥不存在在密钥携带设备102处时，密钥管理单元104可以确定使用(例如，接收及保存)存储在网络设备112处的网络密钥。如果密钥管理单元104确定不使用网络设备112的网络密钥，则控制流程去往链接3，在该链接中，密钥管理单元104可以执行在阶段AA的操作。如果密钥管理单元104确定使用网络设备112的网络密钥，则密钥管理单元104可以执行在阶段S的操作。

[0259] 在阶段S，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104使用与网络设备112达成一致意见的哈希算法计算与N2(即，在阶段H接收的N2)串联的RKk的哈希值。

[0260] 在阶段T，向网络设备112发送获取网络密钥请求。在一种实现中，密钥管理单元104向注册管理单元113发送获取网络密钥请求。例如，获取网络密钥请求包括RKk的加密值(在阶段S计算的)。获取网络密钥请求可以包括对存储在网络设备112处的NK’的请求。

[0261] 在阶段U，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段T接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N2串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以验证获取网络密钥请求是从密钥携带设备102(而不是从恶意设备)接收的，且注册管理单元113可以在阶段W发送获取网络密钥响应。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定在阶段T的获取网络请求时由恶意设备发送的，且注册管理单元113可以在阶段V检测到错误。

[0262] 在阶段V，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为获取网络密钥请求由恶意设备发送的结果，注册管理单元113可以检测到发生了错误。

[0263] 在阶段W，向网络设备112发送获取网络密钥响应。在一种实现中，注册管理单元

113向密钥管理单元104发送获取网络密钥响应。例如，当在阶段U注册管理单元113确定RKk的加密值等于RKn的加密值时，获取网络密钥响应可以包括NK'。当在阶段U RKk的加密值不等于RKn的加密值时，获取网络密钥响应可以包括在阶段V检测到的错误。在一些实现中，获取网络密钥响应可以包括NK'的加密值而不是NK'。在其它实现中，注册管理单元113可以与密钥管理单元104建立安全通信信道，并通过安全通信信道发送获取网络密钥响应。

[0264] 在阶段X，确定获取网络密钥响应是否包括错误。在一种实现中，密钥管理单元104确定获取网络密钥响应是否包含错误。例如，密钥管理单元104可以确定获取网络密钥响应包括注册管理单元113在阶段V所检测到的错误。如果获取网络密钥响应包括错误，则密钥管理单元104可以在阶段Z停止注册操作。如果获取网络密钥响应不包括错误，则密钥管理单元104可以执行阶段Y的操作。

[0265] 在阶段Y，保存NK'。在一种实现中，密钥管理单元104保存在阶段W从注册管理单元113接收的注册响应中的NK'。例如，密钥管理单元104可以设置NK等于NK'以保持NK'。

[0266] 在阶段Z，停止注册操作。在一种实现中，密钥管理单元104停止用于将网络设备112向密钥携带设备102注册的注册操作。

[0267] 在阶段AA，确定NK为空。在一种实现中，密钥管理单元104确定存储在密钥携带设备102处的NK是否为空。如果NK为空，密钥管理单元104可以执行在阶段AB的操作。如果NK不为空，则密钥管理单元104可以执行在阶段AC的操作。

[0268] 在阶段AB，生成随机的NK。在一种实现中，密钥管理单元104生成随机的NK。例如，密钥管理单元104可以使用伪随机数算法来生成随机的NK。在一些实现中，密钥管理单元104将随机的NK保存为在密钥携带设备102处存储的NK。在阶段AB之后，密钥管理单元104可以执行在阶段AC的操作。

[0269] 在阶段AC，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104可以使用与网络设备112达成一致意见的哈希算法计算与N2(即，在阶段H接收的N2)串联的RKk的哈希值。

[0270] 在阶段AD，向网络设备112发送设置网络密钥请求。在一种实现中，密钥管理单元104向注册管理单元113发送设置网络请求。例如，设置网络密钥请求包括NK和RKk的加密值(在阶段AC所计算的)。在一些实现中，设置网络密钥请求可以包括NK的加密值而不是NK。在其它实现中，密钥管理单元104可以建立与注册管理单元113的安全通信信道，并通过安全通信信道发送设置网络密钥请求。

[0271] 在阶段AE，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段AD接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N2串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以验证在阶段AD的设置网络密钥请求是从密钥携带设备102(而不是从恶意设备)接收的，并且注册管理单元113可以在阶段AF保存NK。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定在阶段AD的设置网络密钥请求是由恶意设备发送的，请求注册管理单元113可以在阶段AG检测到错误。

[0272] 在阶段AF，保存NK。在一种实现中，注册管理单元113保存在阶段AD在设置网络密钥请求中接收的NK。例如，注册管理单元113可以设置NK'等于NK以在网络设备112处保存

NK。

[0273] 在阶段AG，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为设置网络密钥请求是由恶意设备发送的结果，注册管理单元113可以检测到发生了错误。

[0274] 在阶段AH，向密钥携带设备102发送设置网络密钥响应。在一种实现中，注册管理单元113向密钥管理单元104发送设置网络密钥响应。例如，设置网络密钥响应可以包括当注册管理单元113在阶段AF保存NK时的确认。当注册管理单元113在阶段AG检测到错误时，设置网络响应可以包括错误。

[0275] 在阶段AI，停止注册操作。在一种实现中，密钥管理单元104停止用于将网络设备112向钥携带设备102注册的注册操作。例如，密钥管理单元104可以在从注册管理单元113接收设置网络密钥响应之后停止注册操作。在一些实现中，当设置网络密钥响应包括错误时，密钥管理单元104可以执行一个或多个操作以向注册管理单元113重发设置网络密钥请求。

[0276] 图18和19示出了用于使用第四配置技术以将网络设备注销的第一选项的示例性操作的顺序图。图18和19包括密钥携带设备102和网络设备112(如参考图15、16和17所描述的)。当存储在密钥携带设备102和网络设备112处的配对数据与图15、16和17中描述的配对数据类似时，密钥携带设备102可以使用第四配置技术利用第一选项来将网络设备112注销。在使用第四配置技术用于将网络设备112注销的第一选项中，密钥携带设备102可以在确定网络设备112向密钥携带设备102注册了之后发送注销请求。密钥携带设备102可以从网络设备112接收网络设备112向密钥携带设备102注册了的信息。仅当网络设备112向密钥携带设备102注册了时，密钥携带设备102才可以将网络设备112注销。应该注意的是，当网络设备112向密钥携带设备102注册了时，状态被设置为‘注册的’，且RKn等于RKk。图18和19在一系列的阶段A1-Q中示出了在密钥携带设备102和网络设备112之间用于将网络设备112注销的交互。虽然图18和19示出了由密钥管理单元104和注册管理单元113执行的操作，但是在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元来执行。

[0277] 在阶段A1，向网络设备112发送随机数请求。在一种实现中，密钥管理单元104向注册管理单元113发送随机数请求。例如，随机数请求包括对来自网络设备112的随机数的请求。

[0278] 在阶段A2，向网络设备112发送随机数响应。在一种实现中，注册管理单元113向密钥管理单元104发送随机数响应。例如，随机数响应可以包括N1(由注册管理单元113生成的随机数)。使用在密钥携带设备102和网络设备112之间达成一致意见的哈希算法可以利用N1来加密注册密钥。

[0279] 在阶段B，向网络设备112发送你好请求。在一种实现中，密钥管理单元104向注册管理单元113发送你好请求。例如，你好请求可以包括RKk的加密值和对状态的请求。密钥管理单元104可以通过使用与网络设备112达成一致意见的哈希算法计算与N1(即，在阶段A2接收的N1)串联的RKk的哈希值来计算RKk的加密值。

[0280] 在阶段C，确定RKn是否为空。在一种实现中，注册管理单元113确定RKn是否为空。例如，注册管理单元113可以通过检查在网络设备112处存储的RKn是否为空来确定RKn为空。如果RKn为空，则注册管理单元113可以在阶段D将状态设置为‘未注册的’。如果RKn不为

空，则注册管理单元113可以确定RKk的加密值是否等于在阶段E的RKn的加密值。

[0281] 在阶段D，将状态设置为‘未注册的’。在一种实现中，注册管理单元113将状态设置为‘未注册的’，并且注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0282] 在阶段E，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKn的加密值(在阶段B接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N1串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以确定网络设备112向密钥携带设备102注册了，且注册管理单元113可以在阶段G将状态设置为‘注册的’。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定网络设备112向另一密钥携带设备(不同于密钥携带设备102)注册了，且注册管理单元113可以在阶段F将状态设置为‘向不同的KCD注册了’。

[0283] 在阶段F，将状态设置为‘向不同的KCD注册了’。在一种实现中，注册管理单元113将在网络设备112处存储的状态设置为‘向不同的KCD注册了’。注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0284] 在状态G，将状态设置为‘注册的’。在一种实现中，注册管理单元113将状态设置为‘注册的’。注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0285] 在阶段H，向密钥携带设备102发送你好响应。在一种实现中，注册管理单元113向密钥管理单元104发送你好响应。例如，你好响应可以包括状态、NK’的加密值、以及随机数(N2)。注册管理单元113可以使用与密钥携带设备102达成一致意见的哈希算法计算NK’的加密值。使用在密钥携带设备102与网络设备112之间达成一致意见的哈希算法，密钥携带设备102可以利用N2来加密RKk(如下文在步骤K描述的)。

[0286] 在阶段I，确定所接收的状态是否为‘注册的’。在一种实现中，密钥管理单元104确定在阶段H接收的状态是否为‘注册的’。如果状态为‘注册的’，则密钥管理单元104确定网络设备112向密钥携带设备102注册了，且控制流程去往链接5，在该链接中密钥管理单元104可以执行在阶段K的操作。如果状态不是‘注册的’，则密钥管理单元104可以停止在阶段J的注销操作。

[0287] 在阶段J，停止注销操作。在一种实现中，密钥管理单元104停止用于将网络设备112注销的注销操作。

[0288] 在阶段K，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104使用与网络设备112达成一致意见的哈希算法计算与N2(即，在阶段H接收的N2)串联的RKk的哈希值。

[0289] 在阶段L，向网络设备112发送注销请求。在一种实现中，密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求可以包括RKk的加密值(在阶段K计算的)以及用于删除RKn和NK’的值的请求。

[0290] 在阶段M，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段L接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N2串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以验证注销请求是从密钥携带设备102(而不是从恶意设备)接收的，且注册管理单元113可以在阶段N删除RKn和

NK'的值。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定在阶段L的注销请求是由恶意设备发送的，并且注册管理单元113可以在阶段O检测到错误。

[0291] 在阶段N，删除RKn和NK'的值。在一种实现中，注册管理单元113删除RKn和NK'的值。一旦删除了RKn和NK'的值，网络设备112不再是向密钥携带设备102注册的，且注册管理单元113可以向密钥管理单元104发送用于确认将网络设备112注销的确认(如下文在阶段P所描述的)。

[0292] 在阶段O，检测到错误。在一种实现中注册管理单元113检测到错误。例如，作为注销请求由恶意设备发送的结果，注册管理单元113可以检测到发生了错误。

[0293] 在阶段P，向密钥携带设备102发送注销请求。在一种实现中，注册管理单元113向密钥管理单元104发送注销响应。例如，注销响应可以包括当注册管理单元113在阶段N删除了RKn和NK'的值时的确认。当注册管理单元113在阶段O检测到错误时，注销响应可以包括错误。

[0294] 在阶段Q，停止注销操作。在一种实现中，密钥管理单元104停止用于将网络设备112注销的注销操作。在一些实现中，当注销响应(在阶段P接收的)包括错误时，密钥管理单元104可以向注册管理单元113重发注销请求。

[0295] 图20示出了用于使用第四配置技术以将网络设备注销的第二选项的示例性操作的顺序图。图20包括密钥携带设备102和网络设备112(如参考图15、16和17所描述的)。当存储在密钥携带设备102和网络设备112处的配对数据与在图15、16和17中描述的配对数据类似时，密钥携带设备102可以使用第四配置技术利用第二选项来将网络设备112注销。在使用第四配置技术用于将网络设备112注销的第二选项中，密钥携带设备102可以在不确定网络设备112向密钥携带设备102注册了的情况下发送注销请求。网络设备112可以确定网络设备112是否向密钥携带设备102注册了并执行一个或多个操作以删除RKn和NK'以注销。仅当网络设备112向密钥携带设备102注册了时，密钥携带设备102才可以将网络设备112注销。应该注意的是，当网络设备112向密钥携带设备102注册了时，状态被设置为'注册的'，且RKn等于RKk。图20在一系列的阶段A-J中示出了在密钥携带设备102和网络设备112之间用于将网络设备112注销的交互。虽然图20示出了由密钥管理单元104和注册管理单元113执行的操作，但是在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元来执行。

[0296] 在阶段A，向网络设备112发送随机数请求。在一种实现中，密钥管理单元104向注册管理单元113发送随机数请求。例如，随机数请求包括对来自网络设备112的随机数的请求。

[0297] 在阶段B，生成随机数。在一种实现中，注册管理单元113生成随机数(即，N1)。例如，注册管理单元113可以生成N1，使得可以使用在密钥携带设备102和网络设备112之间达成一致意见的哈希算法利用N1来加密注册密钥。

[0298] 在阶段C，向网络设备112发送你好响应。在一种实现中，注册管理单元113向密钥管理单元104发送你好响应。例如，你好响应可以包括N1(在阶段B生成的)。

[0299] 在阶段D，计算RKk的加密值。在一种实现中，密钥管理单元104计算RKk的加密值。例如，密钥管理单元104可以使用与网络设备112达成一致意见的哈希算法计算与N1(即，在阶段C接收的N1)串联的RKk的哈希值。

[0300] 在阶段E，向网络设备112发送注销请求。在一种实现中，密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求可以包括RKk的加密值(在阶段D计算的)以及用于删除RKn和NK'的值的请求。

[0301] 在阶段F，确定RKk的加密值是否等于RKn的加密值。在一种实现中，注册管理单元113确定RKk的加密值(在阶段E接收的)是否等于RKn的加密值。注册管理单元113可以通过使用与密钥携带设备102达成一致意见的哈希算法计算与N1串联的RKn的哈希值来计算RKn的加密值。如果RKk的加密值等于RKn的加密值，则注册管理单元113可以确定注销请求(在阶段E接收的)是从密钥携带设备102接收的，且注册管理单元113可以在阶段G删除RKn和NK'的值。如果RKk的加密值不等于RKn的加密值，则注册管理单元113可以确定注销请求不是从密钥携带设备102(而是从恶意设备接收的)，并且注册管理单元113可以在阶段H检测到错误。

[0302] 在阶段G，删除RKn和NK'的值。在一种实现中，注册管理单元113删除RKn和NK'的值。一旦删除了RKn和NK'的值，网络设备112不再是向密钥携带设备102注册的，且注册管理单元113可以向密钥管理单元104发送用于确认将网络设备112注销的确认(如下文在阶段I所描述的)。

[0303] 在阶段H，检测到错误。在一种实现中，注册管理单元113检测到错误。例如，作为从恶意设备接收到注销请求的结果，注册管理单元113可以检测到发生了错误。

[0304] 在阶段I，向密钥携带设备102发送注销响应。在一种实现中，注册管理单元113向密钥管理单元104发送注销响应。例如，注销响应可以包括当注册管理单元113在阶段G删除了RKn和NK'的值时的确认。当注册管理单元113在阶段H检测到错误时，注销响应可以包括错误。

[0305] 在阶段J，停止注销操作。在一种实现中，密钥管理单元104停止用于将网络设备112注销的注销操作。在一些实现中，当注销响应(在阶段I接收的)包括错误时，密钥管理单元104可以向注册管理单元113重发注销请求。

[0306] 图21和22示出了用于使用第五配置技术注册网络设备的示例性操作的顺序图。图21和22包括密钥携带设备102和网络设备112(如上文参考图1所描述的)。当存储在密钥携带设备102处的配对数据包括注册密钥(RKk)且存储在网络设备112处的配对数据包括注册密钥(RKn)以及网络设备112的状态(状态)时，密钥携带设备102可以利用第五配置技术。在第五配置技术中，密钥携带设备102在密钥携带设备102开始用于配置网络设备112的操作之前，与网络设备112建立安全通信信道。密钥携带设备102和网络设备112可以在不对配对数据执行加密操作的情况下，通过安全通信信道，交换包括在密钥携带设备102和网络设备112处存储的配置数据的所有消息。密钥携带设备102和网络设备112也可以存储网络密钥(NK)和网络密钥(NK')。应该注意的是，RKk和RKn、以及状态分别代表用于在密钥携带设备102处存储注册密钥、在网络设备112处存储注册密钥以及网络设备112的状态的示例性变量。类似地，NK和NK'分别代表用于在密钥携带设备102以及网络设备112处存储网络密钥的示例性变量。还应用注意的是，当从密钥携带设备102接收到注册请求且网络设备112已经向密钥携带设备102注册了时，可以将状态设置为指示网络密钥(例如，通信网络100的网络密钥)是否存储在网络设备112处。当网络设备112向密钥携带设备102注册了时，RKk和RKn的值是相等的。当网络设备被配置具有由密钥携带设备102管理的通信网络(即，通信网络

100)时,NK和NK'的值也是相等的。还应该注意的是,当网络设备112未向任何密钥携带设备注册时,状态可以被设置为'未注册的',且RKn和NK'可以为空。在一些实现中,RKn和NK也可以为空(例如,当密钥携带设备102不具有通信网络100的网络密钥时)。但是,当RKk和/或NK的值为空时,密钥携带设备102包括用于生成RKk和NK的随机值的能力。图21和22在一系列的阶段A-X中示出了在密钥携带设备102和网络设备112之间用于注册网络设备112的交互。虽然图21和22示出了由密钥管理单元104和注册管理单元113执行的操作,但是在一些实现中,上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执行。

[0307] 在阶段A,与网络设备112建立安全通信信道。在一种实现中,密钥管理单元104可以通过执行与注册管理单元113的密钥协商、密钥到处和密钥确认操作来进行安全通信信道。安全通信信道可以允许密钥管理单元104和注册管理单元113在不对配对数据执行加密操作的情况下交换配对数据(例如,RKk、NK、NK'、和状态等。在密钥携带设备102和网络设备112之间的安全通信信道可以继续存在直到注册操作完成。

[0308] 在阶段B,向网络设备112发送注册请求。在一种实现中,密钥管理单元104向注册管理单元113发送注册请求。例如,注册请求包括RKk和对将RKk保存在网络设备112处的请求。

[0309] 在阶段C1,确定RKn是否为空。在一种实现中,注册管理单元113确定在网络设备112处存储的RKn是否为空。如果RKn为空,则注册管理单元113可以在阶段C2保存RKk。如果RKn不为空,则注册管理单元113可以在阶段D确定RKn是否等于RKk。

[0310] 在阶段C2,保存RKk。在一种实现中,注册管理单元113保存在阶段B接收的RKk。例如,注册管理单元113可以设置RKn等于RKk以保存RKk。一旦注册管理单元113保存了RKk,则网络设备112向密钥携带设备102注册了。在阶段C2之后,注册管理单元113可以在阶段F确定NK'是否为空。

[0311] 在阶段D,确定RKn是否等于RKk。在一种实现中,注册管理单元113确定RKn是否等于RKk(在阶段B接收的)。如果RKn等于RKk,则注册管理单元113可以在阶段F确定NK'是否为空。如果RKn不等于RKk,则注册管理单元113可以确定网络设备112向不同于密钥携带设备102的密钥携带设备注册了,并执行在阶段E的操作。

[0312] 在阶段E,将状态设置为'向不同的KCD注册了'。在一种实现中,注册管理单元113将状态设置为'向不同的KCD注册了'。注册管理单元113可以在阶段I向密钥携带设备102发送状态。

[0313] 在阶段F,确定NK'是否为空。在一种实现中,注册管理单元113确定存储在网络设备112处的NK'是否为空。如果NK'为空,则注册管理单元113可以确定网络密钥不存储在网络设备112处并执行在阶段H的操作。如果NK'不为空,则注册管理单元113可以确定网络密钥存储在网络设备112处,并执行在阶段G的操作。

[0314] 在阶段G,将状态设置为'具有NK'。在一种实现中,注册管理单元113将状态设置为'具有NK'。注册管理单元113可以在阶段I在注册响应中发送状态。

[0315] 在阶段H,将状态设置为'不具有NK'。在一种实现中,注册管理单元113将状态设置为'不具有NK'。注册管理单元113可以在阶段I在注册响应中发送状态。

[0316] 在阶段I,向密钥携带设备102发送注册响应。在一种实现中,注册管理单元113向密钥管理单元104发送注册响应。例如,注册响应可以包括存储在网络设备112处的状态。

[0317] 在状态J，确定状态是否为‘向不同的KCD注册了’。在一种实现中，密钥管理单元104确定状态(在阶段I接收的)是否为‘向不同的KCD注册了’。如果状态是‘向不同的KCD注册了’，则密钥管理单元104可以确定网络设备112向另一密钥携带设备注册了(不同于密钥携带设备102)，并且密钥管理单元104可以在阶段K停止注册操作。如果状态不是‘向不同的KCD注册了’，则控制流程去往链接6，且注册管理单元113可以执行在阶段L的操作。

[0318] 在阶段K，停止注册操作。在一种实现中，密钥管理单元104停止用于注册网络设备112的注册操作。

[0319] 在阶段L，确定状态是否为‘具有NK’。在一种实现中，密钥管理单元104确定状态(在阶段I接收的)是否为‘具有NK’。如果状态是‘具有NK’，则密钥管理单元104可以确定网络密钥存储在网络设备112处，且密钥管理单元104可以执行在阶段M的操作。如果状态不是‘具有NK’，则密钥管理单元104可以确定在网络设备112处未存储网络密钥，且密钥管理单元104可以执行在阶段R的操作。

[0320] 在阶段M，确定是否使用网络设备112的网络密钥。在一种实现中，密钥管理单元104确定是否使用网络设备112的网络密钥。例如，当通信网络100的网络密钥未存储在密钥携带设备102处时，密钥管理单元104可以确定使用(例如，接收和保存)存储在网络设备112处的网络密钥。如果密钥管理单元104确定使用网络设备112的网络密钥，则密钥管理单元104可以在阶段N发送获取网络密钥请求。如果密钥管理单元104确定不使用网络设备112的网络密钥，则密钥管理单元104可以执行在阶段R的操作。

[0321] 在阶段N，向网络设备112发送获取网络密钥请求。在一种实现中，密钥管理单元104向注册管理单元113发送获取网络密钥请求。例如，获取网络密钥请求包括对NK’的请求。

[0322] 在阶段O，从网络设备112接收获取网络密钥响应。在一种实现中，密钥管理单元104从注册管理单元113接收获取网络密钥响应。例如，获取网络密钥响应包括存储在网络设备112处的NK’。应该注意的是，由于在第五配置技术中，安全通信信道确保避免了来自恶意设备的任何消息，所以在发送获取网络密钥响应之前，注册管理单元113可能不执行用于确定获取网络密钥请求是从密钥携带设备102接收的操作。

[0323] 在阶段P，保存NK’。在一种实现中，密钥管理单元104保存在阶段O接收的NK’。例如，密钥管理单元104可以设置NK等于NK’以保存NK’。在保存NK’之后，密钥管理单元104可以停止在阶段Q的注册操作。

[0324] 在阶段Q，停止注册操作。在一种实现中，密钥管理单元104停止用于注册网络设备112的注册操作。

[0325] 在阶段R，确定NK是否为空。在一种实现中，密钥管理单元104确定存储在密钥携带设备102处的NK是否为空。如果NK为空，则密钥管理单元104可以在阶段S生成随机的NK。如果NK不为空，则密钥管理单元104可以执行在阶段T的操作。

[0326] 在阶段S，生成随机的NK。在一种实现中，密钥管理单元104生成随机的NK。例如，密钥管理单元104可以使用伪随机数算法生成随机的NK。在一些实现中，密钥管理单元104将随机的NK保存为在密钥携带设备102处存储的NK。在阶段S，密钥管理单元104可以执行在阶段T的操作。

[0327] 在阶段T，生成设置网络密钥请求。在一种实现中，密钥管理单元104生成设置网络

密钥请求。例如，设置网络密钥请求可以包括在密钥携带设备102处存储的NK。

[0328] 在阶段U，向网络设备112发送设置网络密钥请求。在一种实现中，密钥管理单元104向注册管理单元113发送设置网络密钥请求(在阶段T生成的)。

[0329] 在阶段V，保存NK。在一种实现中，注册管理单元113保存在设置网络密钥请求中接收的NK。例如，注册管理单元113可以设置NK'等于NK以保存NK。在保存NK之后，注册管理单元113可以向密钥管理单元104发送NK被保存在网络设备112处的确认。应该注意的是，由于在第五配置技术中，安全通信信道确保避免了来自恶意设备的任何消息，所以在保存NK之前，注册管理单元113可能不执行用于确定设置网络密钥请求是从密钥携带设备102接收的操作。

[0330] 在阶段W，向密钥携带设备102发送设置网络密钥响应。在一种实现中，注册管理单元113向密钥管理单元104发送设置网络密钥响应。例如，设置网络密钥响应包括NK被存储在网络设备112处的确认。在一些实现中，设置网络密钥响应也可以在NK未成功保存在网络设备112处时包括错误。

[0331] 在阶段X，停止注册操作。在一种实现中，密钥管理单元104停止用于注册网络设备112的操作。在一些实现中，在接收设置网络密钥响应中的错误(在阶段W接收的)之后，密钥管理单元104可以向注册管理单元113重发NK。

[0332] 图23示出了用于使用第五配置技术将网络设备注销的示例性操作的顺序图。图23包括密钥携带设备102和网络设备112(如上文参考图21和22所描述的)。当存储在密钥携带设备102和网络设备112处的配对数据类似于在图21和22中描述的配对数据时，密钥携带设备102可以使用第五配置技术将网络设备112注销。在第五配置技术中，密钥携带设备102在密钥携带设备102开始配置网络设备112的操作之前与网络设备112建立安全通信信道。密钥携带设备102和网络设备112可以在不对配对数据执行加密操作的情况下，通过安全通信信道交换包括在密钥携带设备102和网络设备112处存储的配对数据的所有消息。网络设备112可以在从密钥携带设备102接收注销请求之后确定网络设备112是否向密钥携带设备102注册了，并执行一个或多个操作以删除RKn和NK'以注销。仅当网络设备向密钥携带设备102注册了时，密钥携带设备102才可以将网络设备112注销。应该注意的是，当网络设备112向密钥携带设备102注册了时，RKn等于RKk。图23在一系列的阶段A-I中示出了在密钥携带设备102和网络设备112之间用于将网络设备112注销的交互。虽然图23示出了由密钥管理单元104和注册管理单元113执行的操作，但是在一些实现中，上述操作可以分别由密钥携带设备102和网络设备112中的其它单元执行。

[0333] 在阶段A，与网络设备112建立安全通信信道。在一种实现中，密钥管理单元104可以通过与注册管理单元113执行密钥协商、密钥到处和密钥确认操作来建立安全通信信道。安全通信信道可以允许密钥管理单元104和注册管理单元113在不对配对数据执行加密操作的情况下交换配对数据(例如，RKk、状态等)。密钥携带设备102和网络设备112之间的安全通信信道可以继续存在直到完成注销操作。

[0334] 在阶段B，向网络设备112发送注销请求。在一种实现中，密钥管理单元104向注册管理单元113发送注销请求。例如，注销请求包括RKk和对删除存储在网络设备112处的RKn和NK'的请求。

[0335] 在阶段C，确定RKn是否为空。在一种实现中，注册管理单元113确定存储在网络设

备112处的RKn是否为空。如果RKn为空，则注册管理单元113可以执行在阶段D的操作。如果RKn不为空，则注册管理单元113可以在阶段E确定RKn是否等于RKk。

[0336] 在阶段D，将状态设置为‘未注册的’。在一种实现中，注册管理单元113将状态设置为‘未注册的’。注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0337] 在阶段E，确定RKn是否等于RKk。在一种实现中，注册管理单元113确定RKn是否等于RKk(在阶段B接收的)。如果RKn等于RKk，则注册管理单元113可以确定网络设备112向密钥携带设备102注册了，且注册管理单元113可以执行在阶段G的操作。如果RKn不等于RKk，则注册管理单元113可以确定网络设备112未向密钥携带设备102进行注册，且注册管理单元113可以执行在阶段F的操作。在一些实现中，注册管理单元113可以通过将包括注销请求的消息中包含的一个或多个安全信道密钥与在网络设备112处存储的安全信道密钥(与在阶段A建立的安全信道相对应)进行比较来确定网络设备112是否向密钥携带设备102注册了。如果包含在消息中的安全信道密钥与存储在网络设备112处的安全信道密钥匹配，则注册管理单元113可以确定网络设备112向密钥携带设备102注册了。如果包含在消息中的安全信道密钥与存储在网络设备112处的安全信道密钥不匹配，则注册管理单元113可以确定网络设备112未向密钥携带设备102进行注册。

[0338] 在阶段F，将状态设置为‘向不同的KCD注册了’。在一种实现中，注册管理单元113将状态设置为‘向不同的KCD注册了’。注册管理单元113可以在阶段H向密钥管理单元104发送状态。

[0339] 在阶段G，删除RKn和NK’，且将状态设置为‘未注册的’。在一种实现中，注册管理单元113删除存储在网络设备112处的RKn和NK’的值，并状态设置为‘未注册的’。应该注意的是，由于在第五配置技术中，安全通信信道确保避免了来自恶意设备的任何消息，所以在删除RKn和NK’的值之前，注册管理单元113可能不执行用于确定注销请求是从密钥携带设备102接收的操作。

[0340] 在阶段H，向密钥携带设备102发送注销响应。在一种实现中，注册管理单元113向密钥管理单元104发送注销响应。例如，注销响应可以包括状态，该状态用于向密钥管理单元104指示网络设备112未注册或网络设备112向另一密钥携带设备(不同于密钥携带设备102)注册了。在一些实现中，注销响应也可以包括当一个或多个注销操作在网络设备112处不成功时的错误。

[0341] 在阶段I，停止注销操作。在一种实现中，密钥管理单元104停止用于将网络设备112注销的注销操作。在一些实现中，当密钥管理单元104在阶段H接收到在注销响应中的错误时，密钥管理单元104可以向注册管理单元113重发注销请求。

[0342] 应该注意的是，在图5-23中描述的配置技术在本质上是示例性的，且为了简化起见，图5-23不一定示出了由密钥携带设备102和网络设备112所执行的全部操作。例如，第一配置技术(上文在图5和6中描述的)和第二配置技术(上文在图7和8中描述的)不包括当网络密钥未存储在密钥携带设备102处时用于接收网络密钥或生成随机的网络密钥的操作。但是，应该注意的是，密钥携带设备102包括当网络密钥为存储在密钥携带设备102处时用于执行这样的操作的能力。还应该注意的是，在图5-23中示出的操作可以在密钥携带设备102和网络设备112处以不同的顺序执行、并行执行等。此外，密钥携带设备102不受限于一次利用一个配置技术来配置网络设备。在一些实现中，密钥携带设备102可以利用两个或更

多个配置技术来配置同一个或不同的通信网络中的网络设备。

[0343] 应当理解的是，本申请中描述的图1-23和操作时意在帮助理解实施例的示例，其不应该用于限制实施例或限制权利要求书的保护范围。实施例可以执行另外的操作、更少的操作、按照不同顺序的操作、并行的操作以及一些不同的操作。例如，可以利用不同的决策步骤来修改或替换图2-4和/或图5-23中的一些操作，以实现在图2-4中描述的过程。图13和14示出了用于将网络设备112注销的第三配置技术的可供选择的实现。类似地，图18和19，以及图20示出了用于将网络设备112注销的第四配置技术。应该注意的是，第二、第三、第四、和第五配置技术可以符合NFC-SEC-01标准。此外，在第二、第三、第四和第五配置技术中，配对数据不存储在密钥携带设备102处，这允许利用多个密钥携带设备来配置通信网络100中的网络设备，而无需与密钥携带设备102重新同步。

[0344] 如将由本领域的技术人员明白的，本发明主题的方面可以实施为系统、方法或计算机程序产品。因此，本发明主题的方面可以表现为完全硬件实施例、软件实施例(包括固件、常驻软件、微代码等)或在本申请中通常可以被称为“电路”、“模块”或“系统”的将软件和硬件方面进行组合的实施例。此外，本发明主题的方面可以表现为在一个或多个计算机可读介质中实施的计算机程序产品，上述一个或多个计算机可读介质在其上包含有计算机可读程序代码。

[0345] 可以利用一个或多个计算机可读介质的任何组合。计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可以是，例如，但不限于，电子的、磁的、光学的、电磁的、红外线的或半导体系统、装置或设备、或前述的任何适当的组合。计算机可读存储介质的更具体的示例(非详尽的列表)将包括下列：具有一个或多个线的电子连接、便携计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦写可编程只读存储器(EPROM或闪存)、光纤、便携压缩光盘只读存储器(CD-ROM)、光存储设备、磁存储设备、或前述的任何适当组合。在本文档的上下文中，计算机可读存储介质可以是任何可以包含、或存储以由指令执行系统、装置或设备使用或与指令执行系统、装置或设备连接的程序的有形介质。

[0346] 计算机可读信号介质可以包括在其中包含有计算机可读程序代码的传播数据信号，例如，在基带中或作为载波的一部分。这样的传播信号可以表现为各种形式，包括但不限于电磁的、光学的或其任何适当的组合。计算机可读信号介质可以是不是计算机可读存储介质、且可以传送、传播或传输用于由指令执行系统、装置或设备使用的或与指令执行系统、装置或设备连接的任何计算机可读介质。

[0347] 可以使用任何适当的介质，包括但不限于无线、有线、光纤线缆、RF等或前述的任何适当的组合来发送计算机可读介质上包含的程序代码。

[0348] 用于执行针对本发明主题的方面的计算机程序代码可以以一个或多个程序语言的任何组合写入，上述语言包括诸如Java、Smalltalk、C++等之类的面向对象的编程语言和诸如“C”编程语言或类似的编程语言之类的常规过程编程语言。程序代码可以完全在用户的计算机上、部分在用户的计算机上、作为独立的软件包、部分在用户的计算机以及部分在远程计算机上或完全在远程计算机或服务器上执行。在较后的场景中，包括局域网(LAN)或广域网(WAN)、或到外部计算机的连接(例如，通过使用互联网服务提供商的互联网)。

[0349] 本发明主题的方面是参考根据本发明主题的实施例的方法、装置(系统)和计算机

程序产品的流程图和/或方框图来描述的。将可以理解的是，流程图和/或方框图中的每一个方框，以及流程图和/或方框图中的方框的组合可以通过计算机程序指令来实现。这些计算机程序指令可以提供给通用计算机、专用计算机、或用于产生机器的其它可编程数据处理装置的处理器，使得通过计算机或其它可编程数据处理装置的处理器执行的指令创建用于实现在流程图和/或方框图方框中指定的功能/动作的模块。

[0350] 这些计算机程序指令也可以存储在能够指导计算机、其它可编程数据处理装置、或其它设备以特定方式作用的计算机可读介质中，使得存储在计算机可读介质中的指令产生包括实现在流程图和/或方框图方框中指定的功能/动作的指令的制品。

[0351] 计算机程序指令也可以上载到计算机、其它可编程数据处理装置、或其它设备上，以使得一系列操作步骤在计算机、其它可编程设备或其它设备上执行以产生计算机实现的过程，使得在计算机或其它可编程装置上执行的指令提供用于实现在流程图和/或方框图方框中指定的功能/动作的过程。

[0352] 图24示出了示例性的网络设备2400。在一些实现中，网络设备2400可以是支持短距离通信(例如，NFC、蓝牙、ZigBee等)的通信设备。网络设备2400包括处理器单元2401(可能包括多个处理器、多个内核、多个节点、和/或执行多线程等)。网络设备2400包括存储器2403。存储器2403可以是系统存储器(例如，一个或多个高速缓存、SRAM、DRAM、零电容RAM、双晶体管RAM、eDRAM、EDO RAM、DDR RAM、EEPROM、NRAM、RRAM、SONOS、PRAM等)或上文已经描述的机器可读介质的可能的实现中的任何一个或多个。网络设备2400也可以包括总线2411(PCI、串行总线、AHB™、AXI™、NoC等)、存储设备2409(例如，SD卡、SIM卡、光存储器、磁存储器等)、通信单元2405(例如，GSM单元、CDMA单元、FM单元、Wi-Fi单元等)、I/O设备2407(例如，触摸屏、照相机、麦克风、扬声器等)以及网络接口2420(例如，蓝牙接口、NFC接口、Wi-Fi接口、电源线接口、以太网接口、帧中继接口、SONET接口等)。通信单元2405包括短距离通信单元2413和管理单元2415。短距离通信单元2413包括用于实现一个或多个短距离通信技术(例如，NFC、ZigBee、蓝牙等)的组件。管理单元2415可以是注册管理单元或密钥管理单元(如上文在图1-23中所描述的)。管理单元2415包含用于实现上文在图1-23中所描述的实施例中的一些的功能。管理单元2415可以包括便于使用上文在图5-23中描述的至少五种配置技术来安全配置网络设备的一个或多个功能。

[0353] 这些功能中的任何一个可以部分地(或完全地)以在硬件中和/或在处理单元2401上或在存储器2403中实现。例如，上述功能可以利用专用集成电路、在处理器单元2401中实现的逻辑中、在外围设备或卡上的协处理器中等实现。此外，实现可以包括更少的或在图24中未示出的另外的组件(例如，视频卡、音频卡、另外的网络接口、外围设备等)。处理器单元2401、存储设备2409、I/O设备2407、网络接口2420以及通信单元2405耦合到总线2411。虽然被示出为耦合到总线2411，但是，存储器2403可以耦合到处理器单元2401。

[0354] 虽然参考各种实现和开发描述了实施例，但是将理解的是，这些实施例是说明性的，且本发明主题的保护范围不受限于它们。通常，用于使用如本申请中描述的短距离无线通信安全配置网络设备的技术可以利用与任何硬件系统一致的设施来实现。许多改变、修改、添加和改进是可能的。

[0355] 可以针对本申请中描述为单个实例的组件、操作或结构提供多个实例。最终，各个组件、操作和数据存储器之间的界限是有点随意的，且在具体的说明性配置的上下文中描

述了具体的操作。功能的其它分配可以预想且其可以落入本发明主题的保护范围中。通常，在示例性配置中呈现为单独组件的结构和功能可以被实现为组合的结构或功能。类似地，呈现为单个组件的结构和功能可以被实现成单独的组件。这些和其它的改变、修改、添加和改进可以落入本发明主题的保护范围之内。

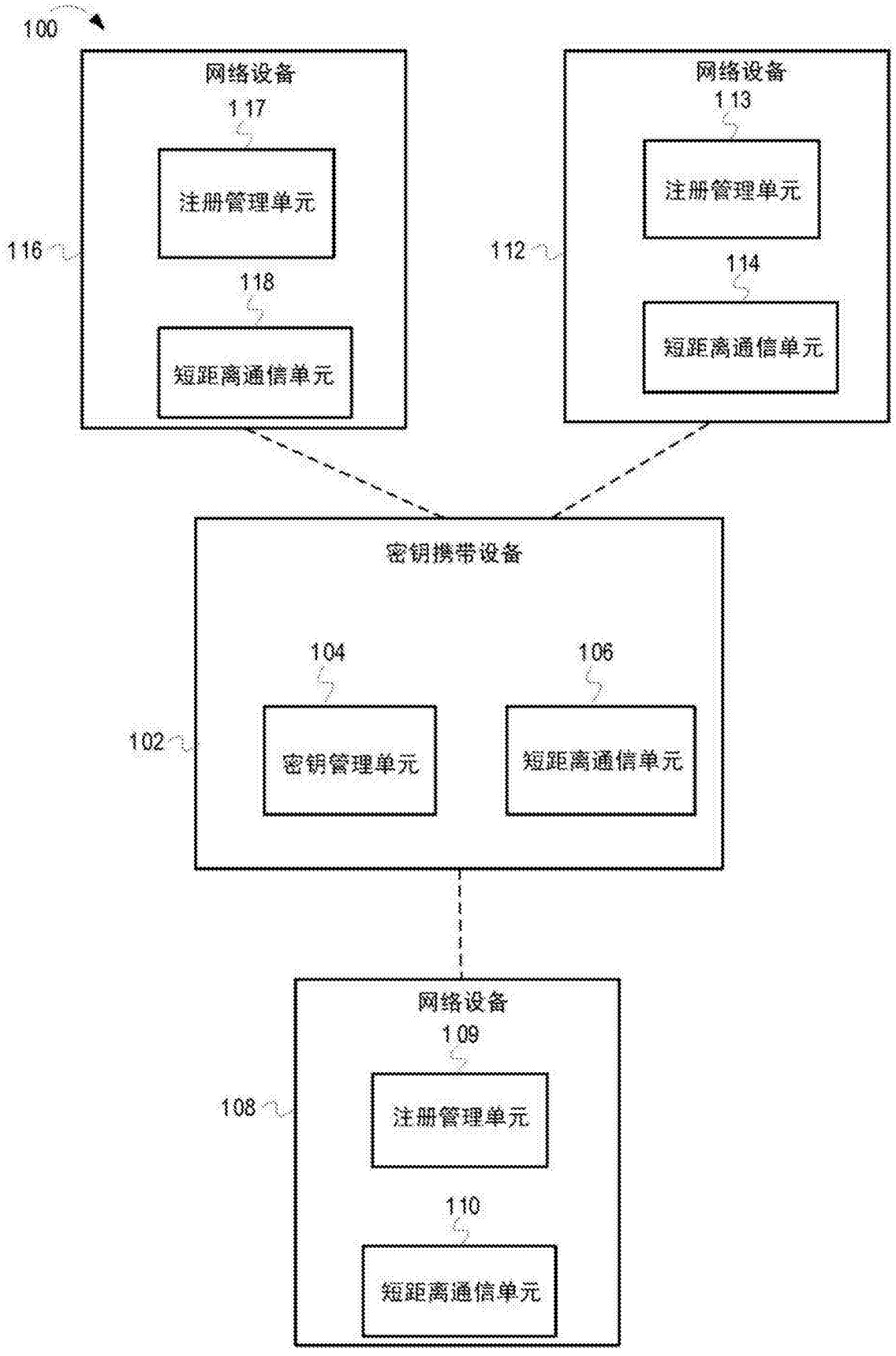

100
网络设备
117
注册管理单元
116
118
短距离通信单元
网络设备
113
注册管理单元
112
114
短距离通信单元
密钥携带设备
104
106
102
密钥管理单元
短距离通信单元
网络设备
109
108
注册管理单元
110
短距离通信单元

图1

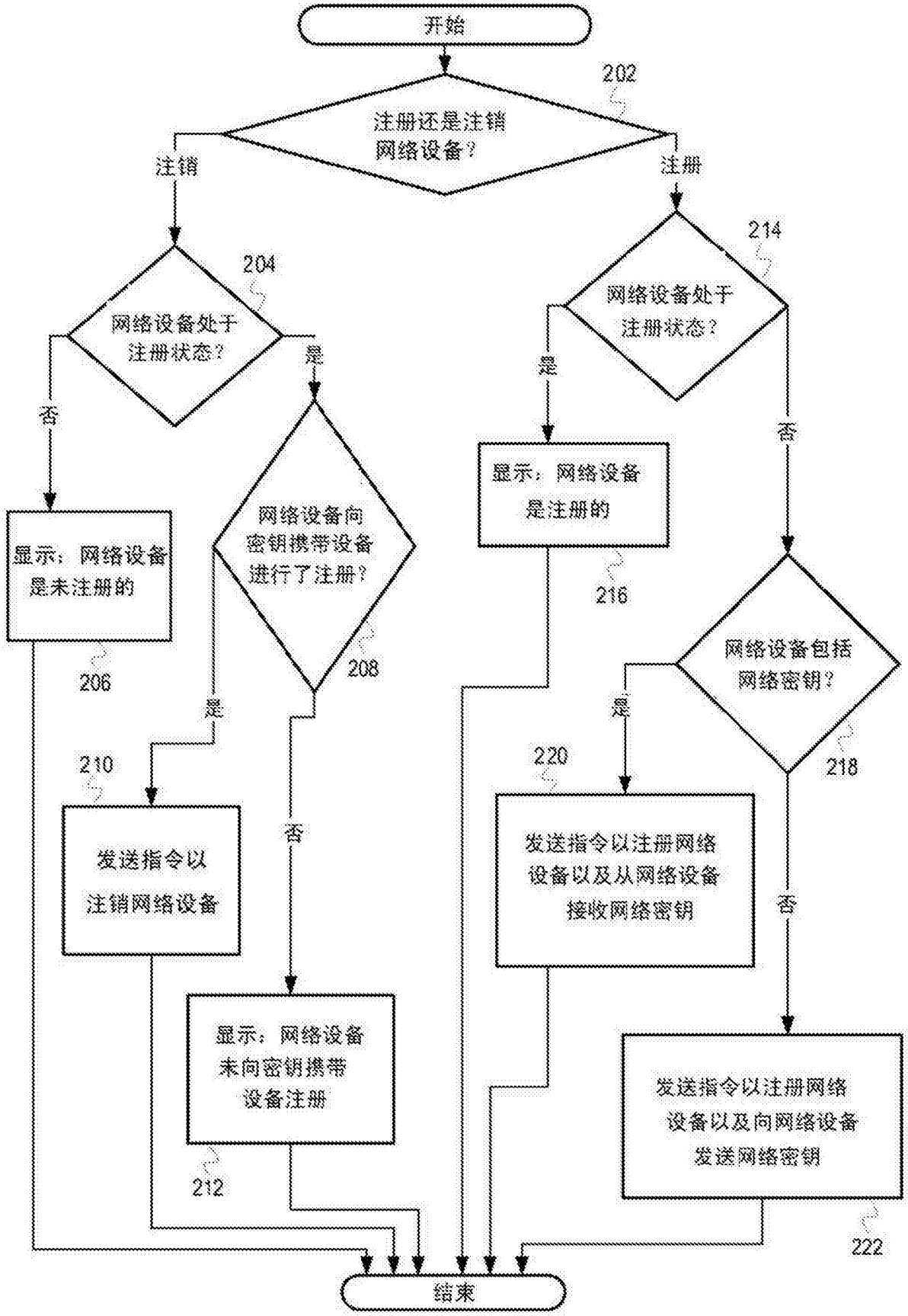

开始
202
注册还是注销网络设备？
注销
注册
204
网络设备处于注册状态？
否
是
显示：网络设备是未注册的
206
网络设备向密钥携带设备进行了注册？
208
是
否
210
发送指令以注销网络设备
显示：网络设备未向密钥携带设备注册
212
214
网络设备处于注册状态？
是
否
显示：网络设备是注册的
216
网络设备包括网络密钥？
是
否
218
220
发送指令以注册网络设备以及从网络设备接收网络密钥
发送指令以注册网络设备以及向网络设备发送网络密钥
222
结束

图2

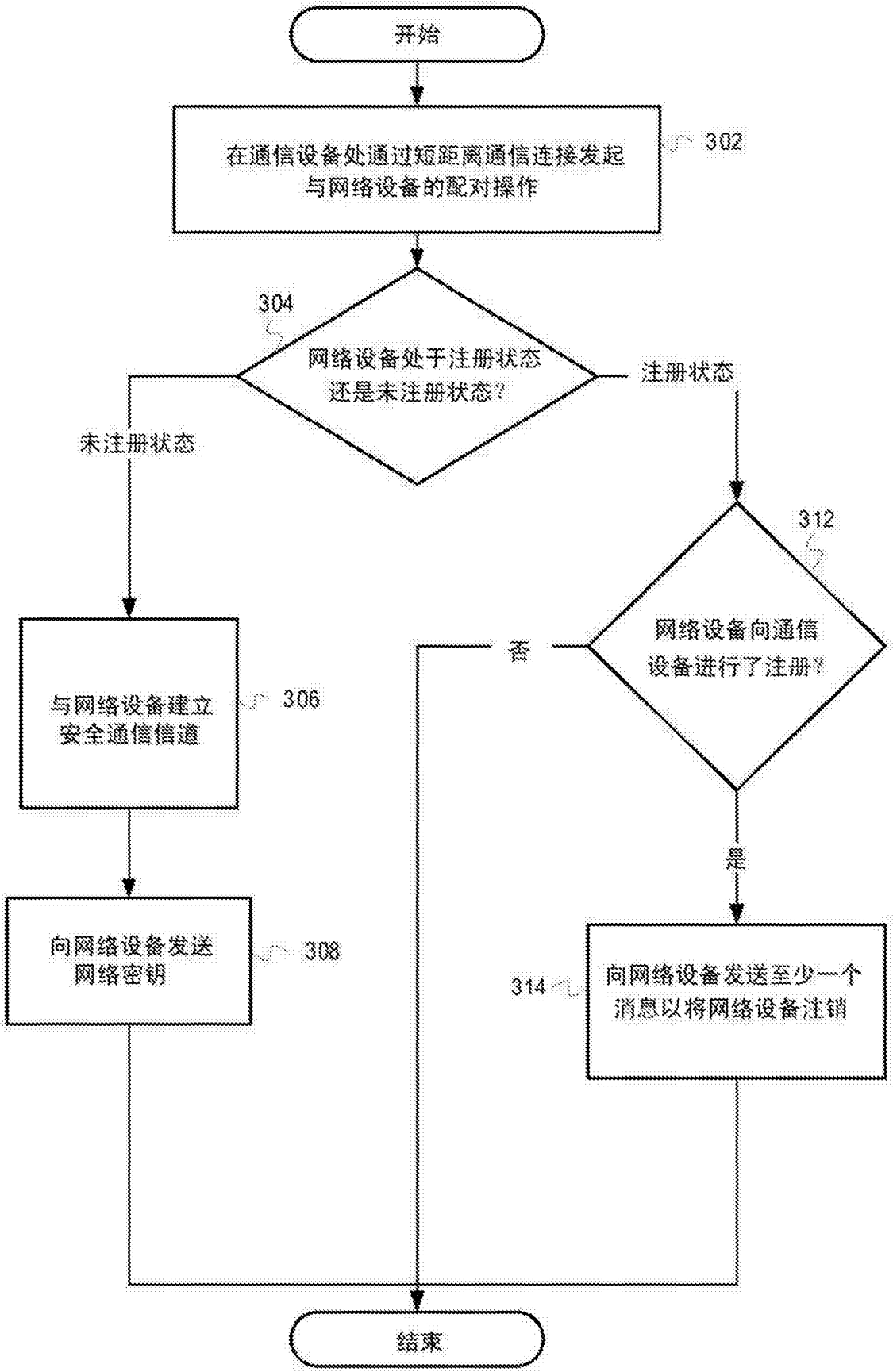

开始
在通信设备处通过短距离通信连接发起与网络设备的配对操作
302
304
网络设备处于注册状态还是未注册状态？
注册状态
未注册状态
312
网络设备向通信设备进行了注册？
否
是
与网络设备建立安全通信信道
306
向网络设备发送网络密钥
308
314
向网络设备发送至少一个消息以将网络设备注销
结束

图3

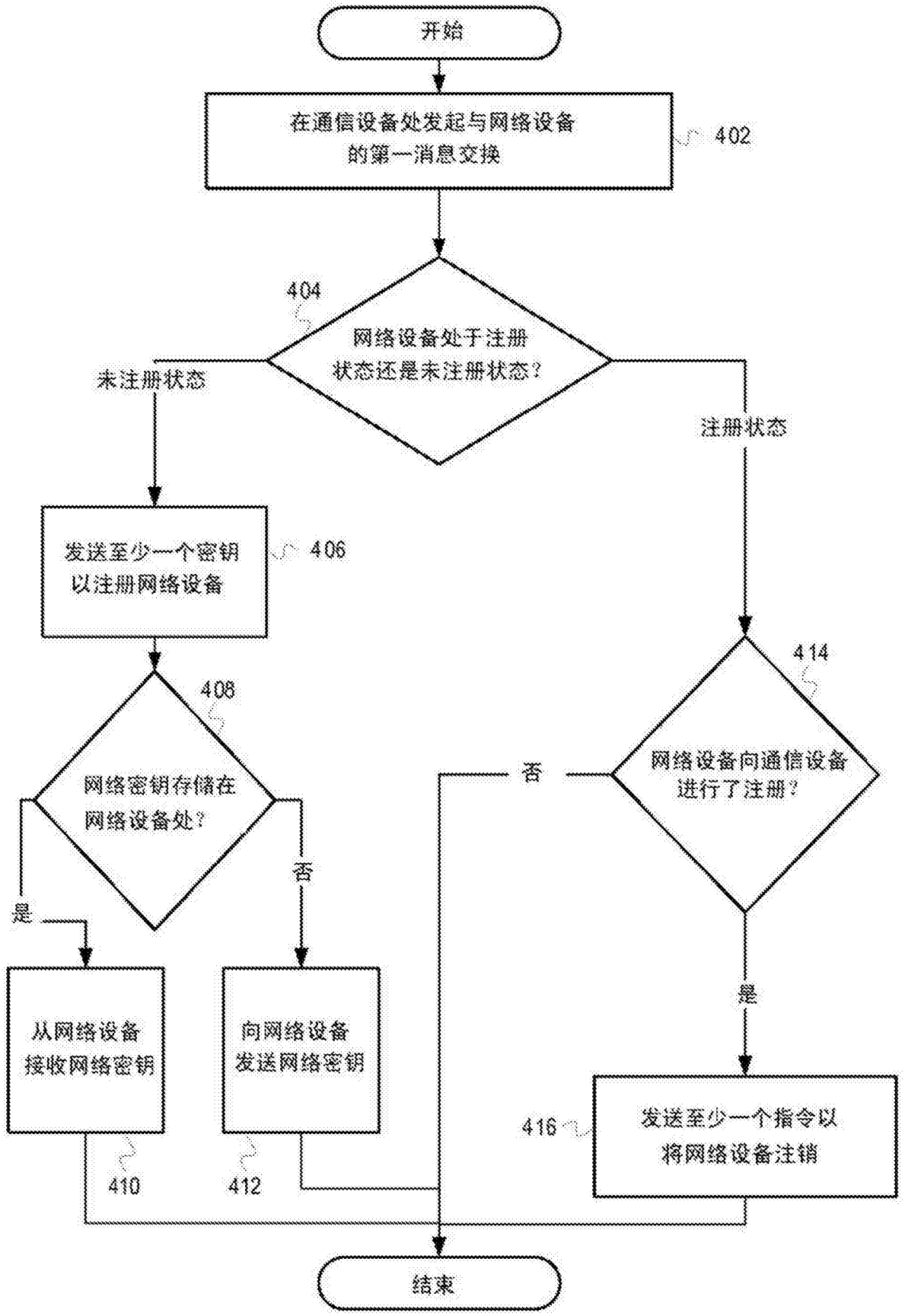

开始
在通信设备处发起与网络设备的第一消息交换
402
404
网络设备处于注册状态还是未注册状态？
未注册状态
注册状态
发送至少一个密钥以注册网络设备
406
408
网络密钥存储在网络设备处？
是
否
从网络设备接收网络密钥
向网络设备发送网络密钥
410
412
414
网络设备向通信设备进行了注册？
否
是
416
发送至少一个指令以将网络设备注销
结束

图4

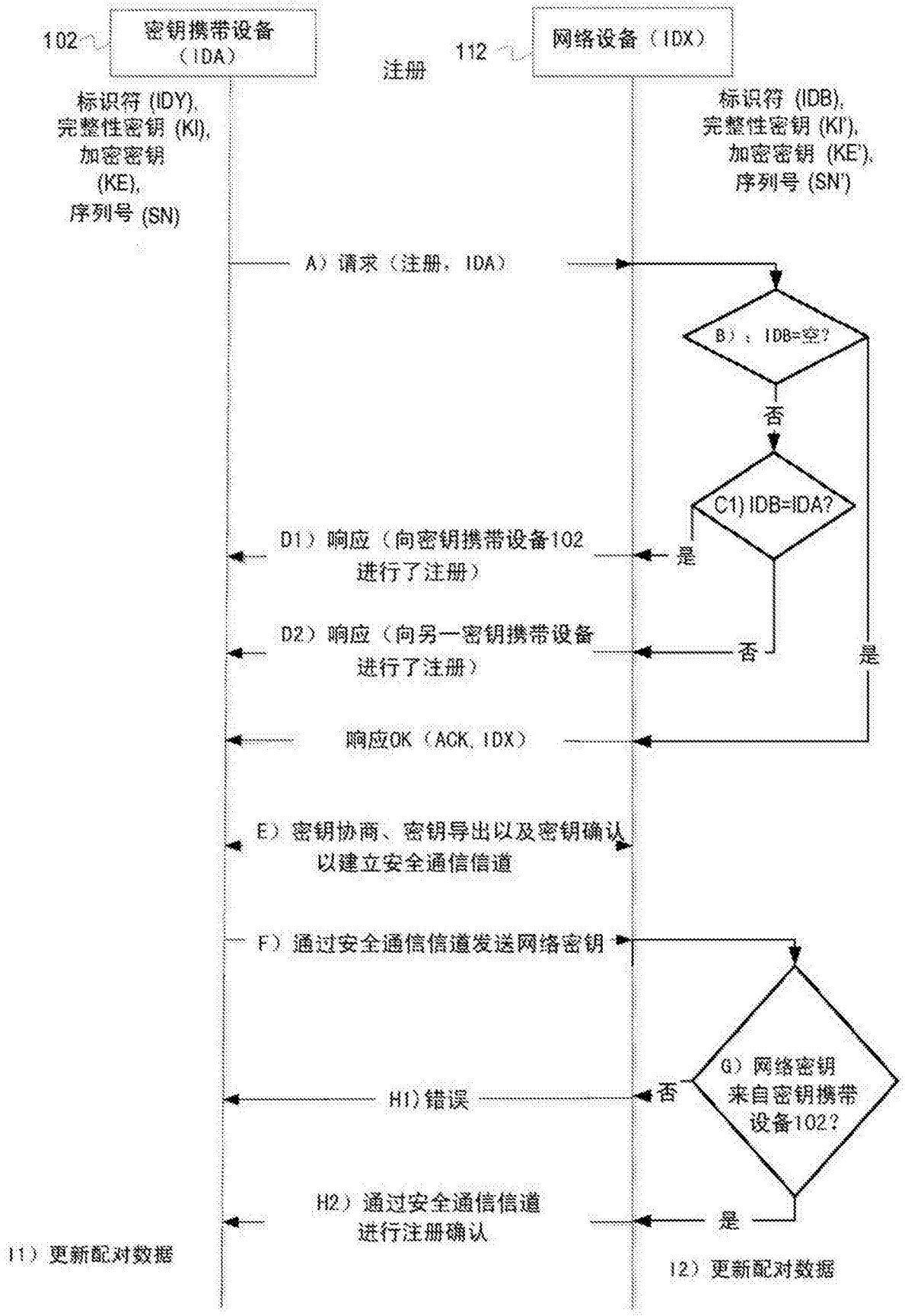

102
密钥携带设备（IDA）
注册
112
网络设备（IDX）
标识符（IDY），
完整性密钥（KI），
加密密钥（KE），
序列号（SN）
标识符（IDB），
完整性密钥（KI'），
加密密钥（KE'），
序列号（SN'）
A）请求（注册，IDA）
B），IDB=空？
否
C1）IDB=IDA？
是
D1）响应（向密钥携带设备102进行了注册）
否
D2）响应（向另一密钥携带设备进行了注册）
是
响应OK（ACK，IDX）
E）密钥协商、密钥导出以及密钥确认以建立安全通信信道
F）通过安全通信信道发送网络密钥
G）网络密钥来自密钥携带设备102？
否
H1）错误
是
H2）通过安全通信信道进行注册确认
I1）更新配对数据
I2）更新配对数据

图5

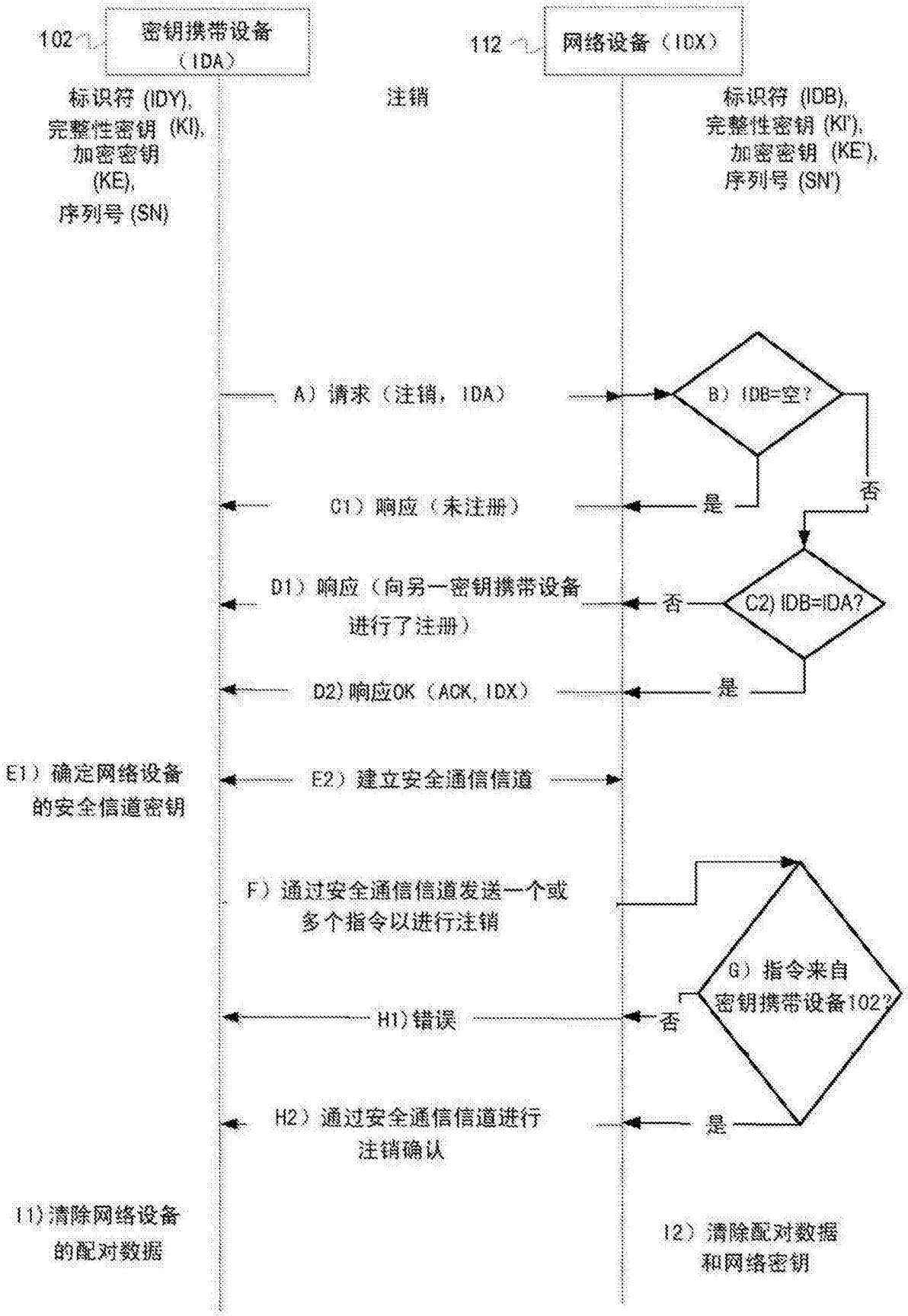

102
密钥携带设备（IDA）
112
网络设备（IDX）
标识符 (IDY)，
完整性密钥 (KI)，
加密密钥 (KE)，
序列号 (SN)
注销
标识符 (IDB)，
完整性密钥 (KI')，
加密密钥 (KE')，
序列号 (SN')
A）请求（注销，IDA）
B）IDB=空？
是
否
C1）响应（未注册）
D1）响应（向另一密钥携带设备进行了注册）
否
C2) IDB=IDA?
D2) 响应OK（ACK，IDX）
是
E1）确定网络设备的安全信道密钥
E2）建立安全通信信道
F）通过安全通信信道发送一个或多个指令以进行注销
G）指令来自密钥携带设备102？
H1）错误
否
H2）通过安全通信信道进行注销确认
是
I1）清除网络设备的配对数据
I2）清除配对数据和网络密钥

图6

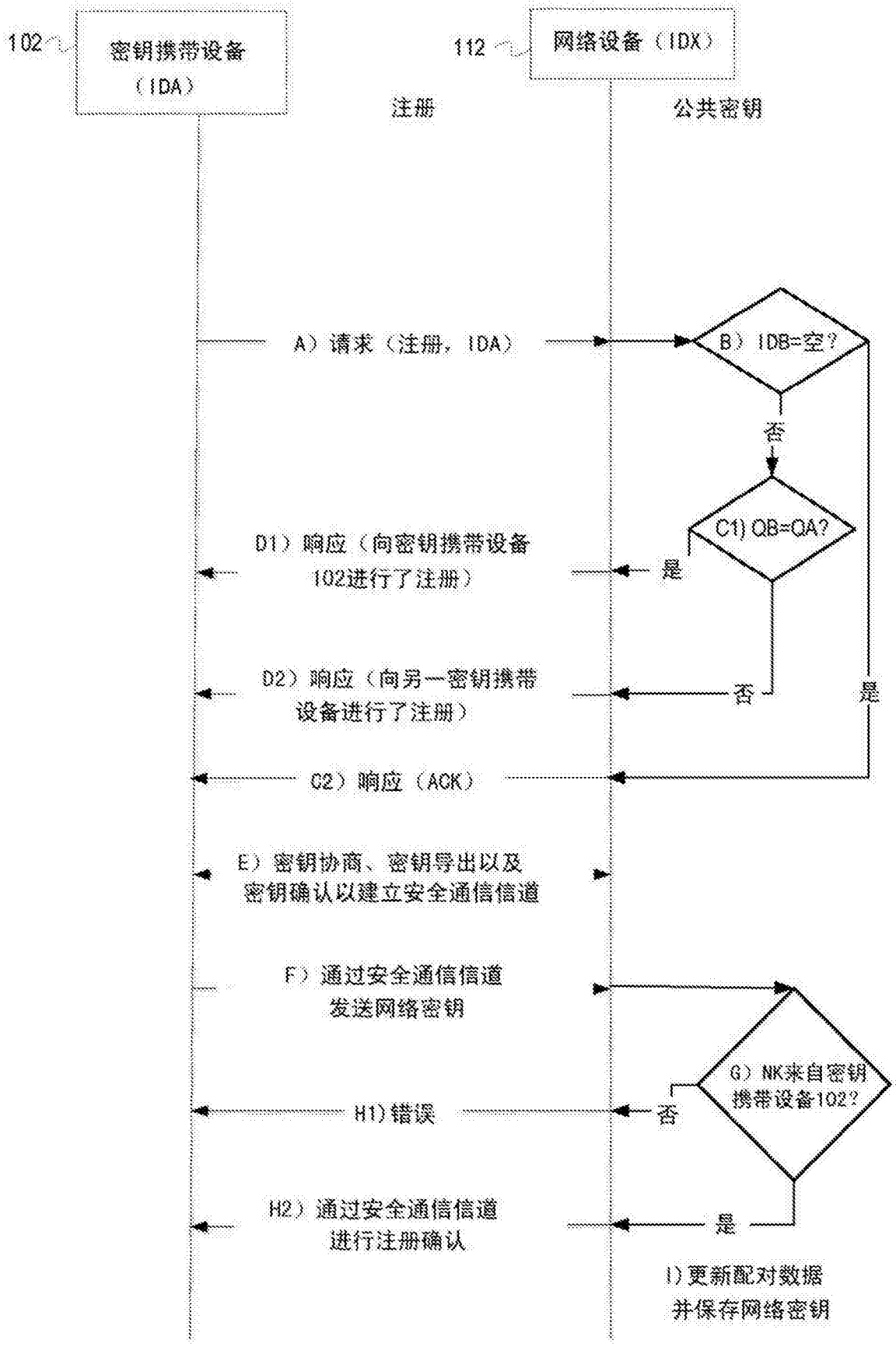

102
密钥携带设备
（IDA）
112
网络设备（IDX）
注册
公共密钥
A）请求（注册，IDA）
B）IDB=空？
否
C1) QB=QA?
是
D1）响应（向密钥携带设备
102进行了注册）
否
是
D2）响应（向另一密钥携带
设备进行了注册）
C2）响应（ACK）
E）密钥协商、密钥导出以及
密钥确认以建立安全通信信道
F）通过安全通信信道
发送网络密钥
G）NK来自密钥
携带设备102？
否
H1)错误
是
H2）通过安全通信信道
进行注册确认
I)更新配对数据
并保存网络密钥

图7

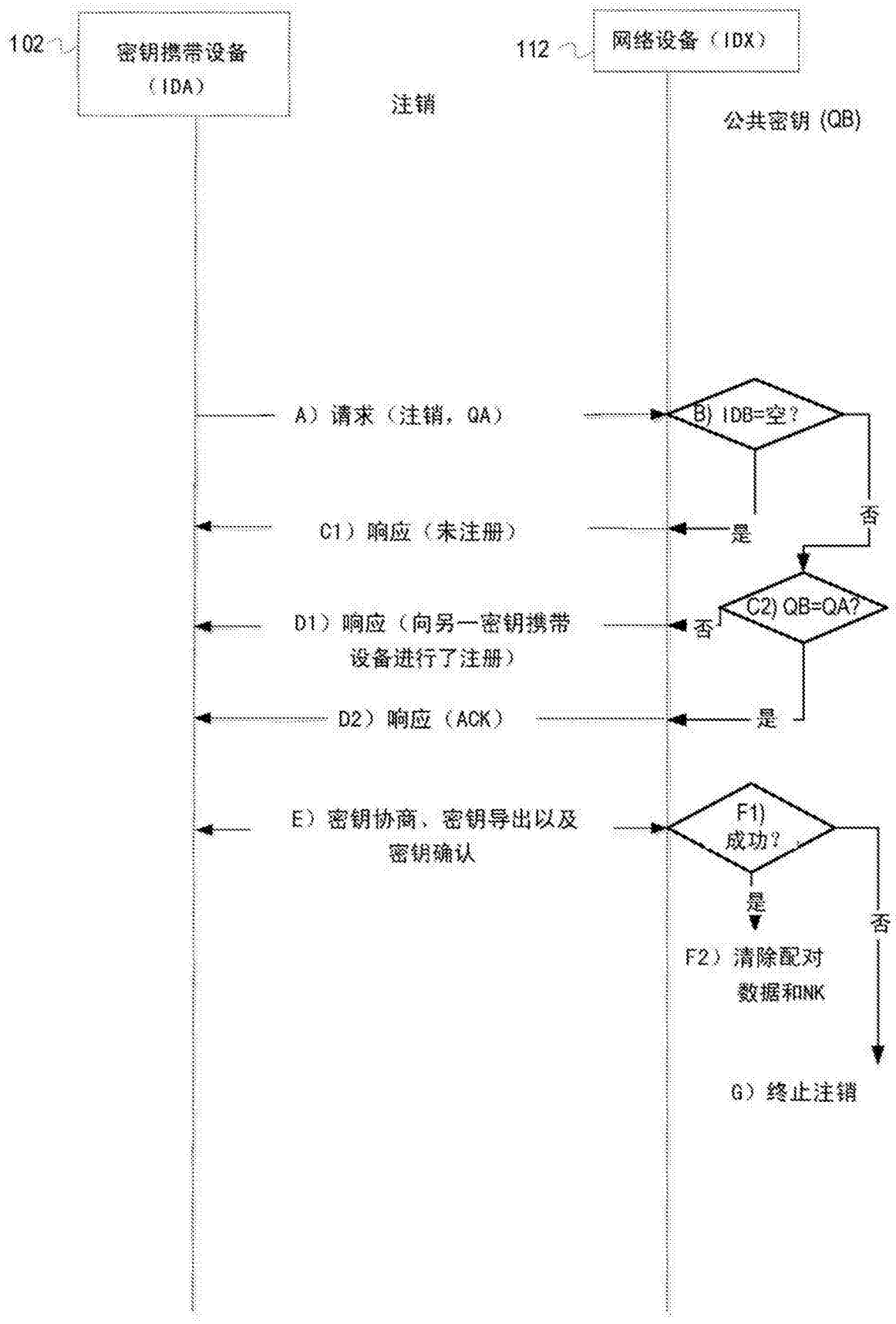

102
密钥携带设备
（IDA）
112
网络设备（IDX）
注销
公共密钥 (QB)
A）请求（注销，QA）
B) IDB=空？
否
是
C1）响应（未注册）
C2) QB=QA?
否
D1）响应（向另一密钥携带
设备进行了注册）
是
D2）响应（ACK）
E）密钥协商、密钥导出以及
密钥确认
F1)
成功？
是
否
F2）清除配对
数据和NK
G）终止注销

图8

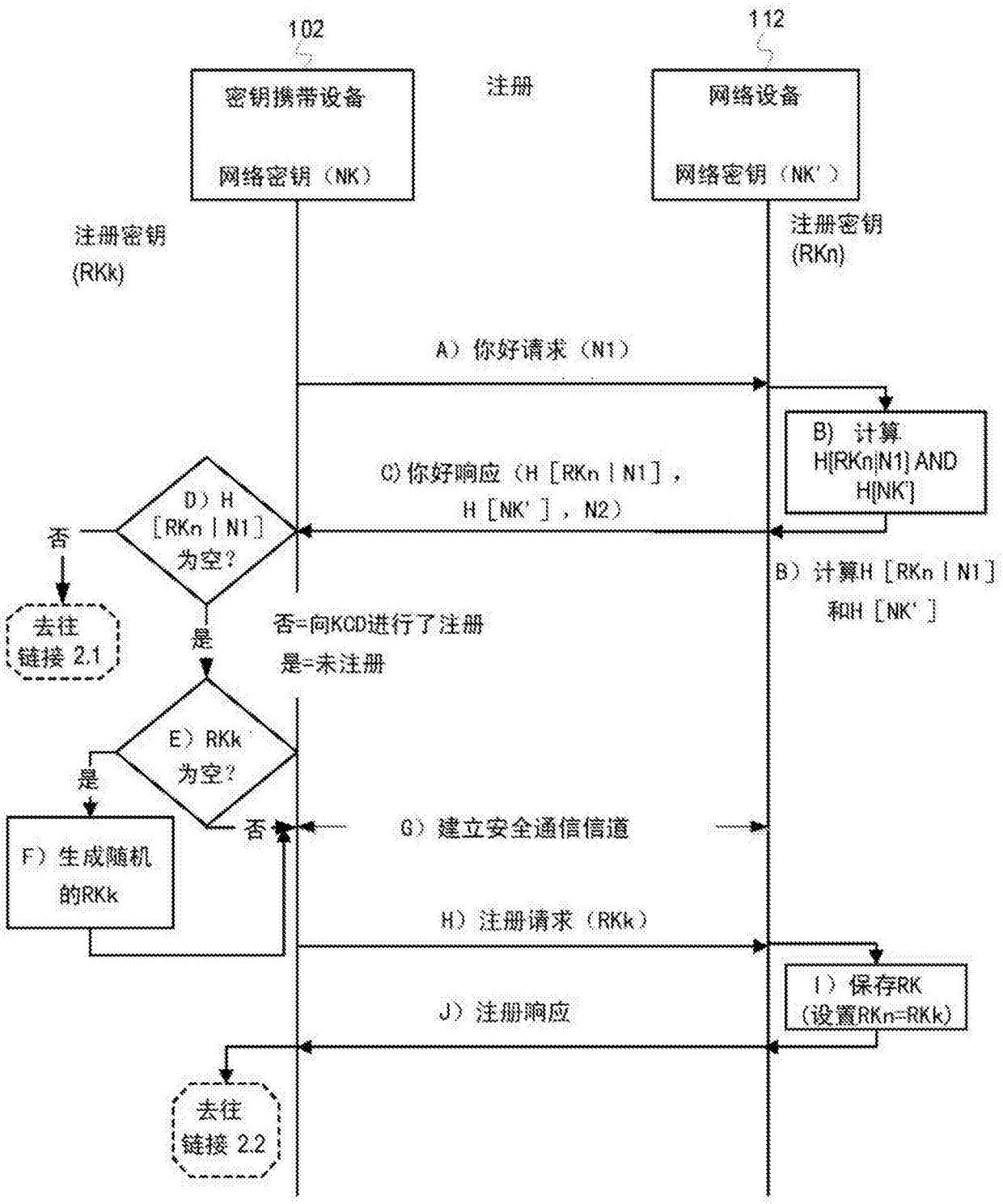

102
112
密钥携带设备
网络密钥（NK）
注册
网络设备
网络密钥（NK'）
注册密钥
(RKk)
注册密钥
(RKn)
A）你好请求（N1）
B）计算
H[RKn|N1]AND
H[NK']
C）你好响应（H［RKn｜N1］，
H［NK'］，N2）
D）H
［RKn｜N1］
为空？
否
是
去往
链接 2.1
否=向KCD进行了注册
是=未注册
B）计算H［RKn｜N1］
和H［NK'］
E）RKk
为空？
是
否
F）生成随机
的RKk
G）建立安全通信信道
H）注册请求（RKk）
I）保存RK
（设置RKn=RKk）
J）注册响应
去往
链接 2.2

图9

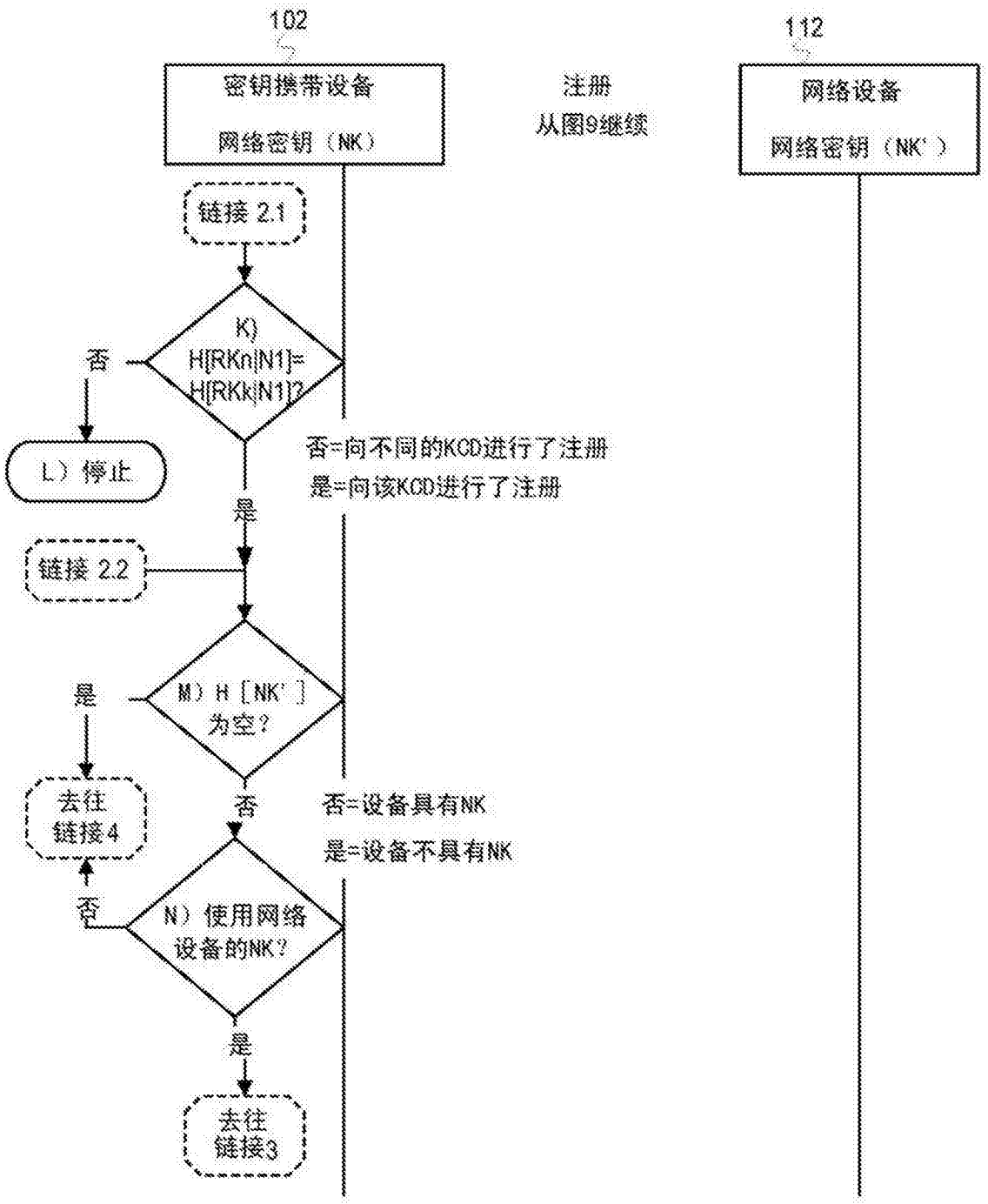

102
密钥携带设备
网络密钥（NK）
注册
从图9继续
112
网络设备
网络密钥（NK'）
链接 2.1
K)
H[RKn|N1]=
H[RKk|N1]?
否
L）停止
否=向不同的KCD进行了注册
是=向该KCD进行了注册
是
链接 2.2
M）H［NK'］
为空？
是
去往
链接4
否
否=设备具有NK
是=设备不具有NK
否
N）使用网络
设备的NK？
是
去往
链接3

图10

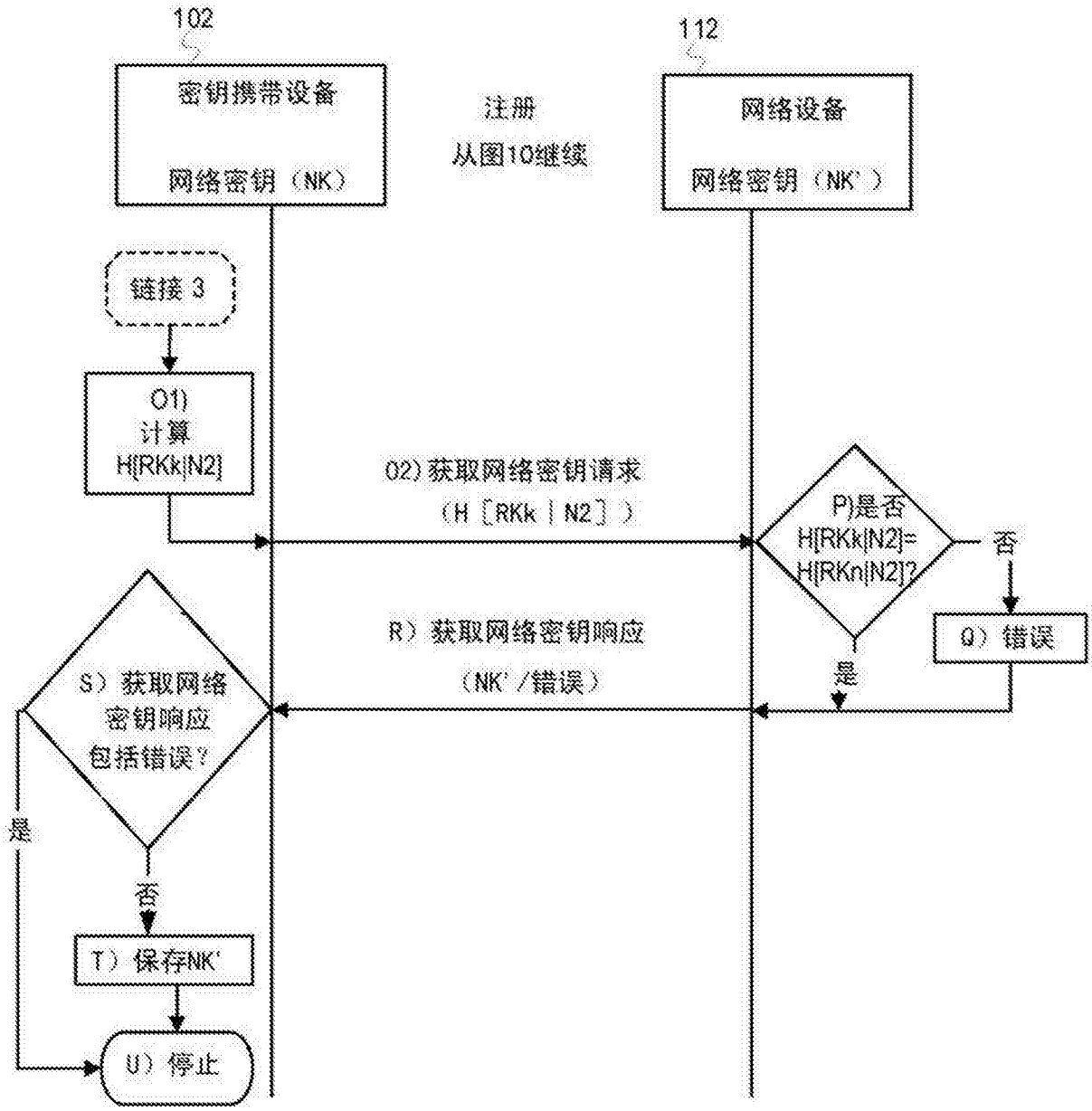

102
密钥携带设备
网络密钥（NK）
注册
从图10继续
112
网络设备
网络密钥（NK'）
链接 3
O1)
计算
H[RKk|N2]
O2)获取网络密钥请求
（H［RKk | N2］）
P)是否
H[RKk|N2]=
H[RKn|N2]?
否
Q）错误
是
R）获取网络密钥响应
（NK'/错误）
S）获取网络
密钥响应
包括错误?
是
否
T）保存NK'
U）停止

图11

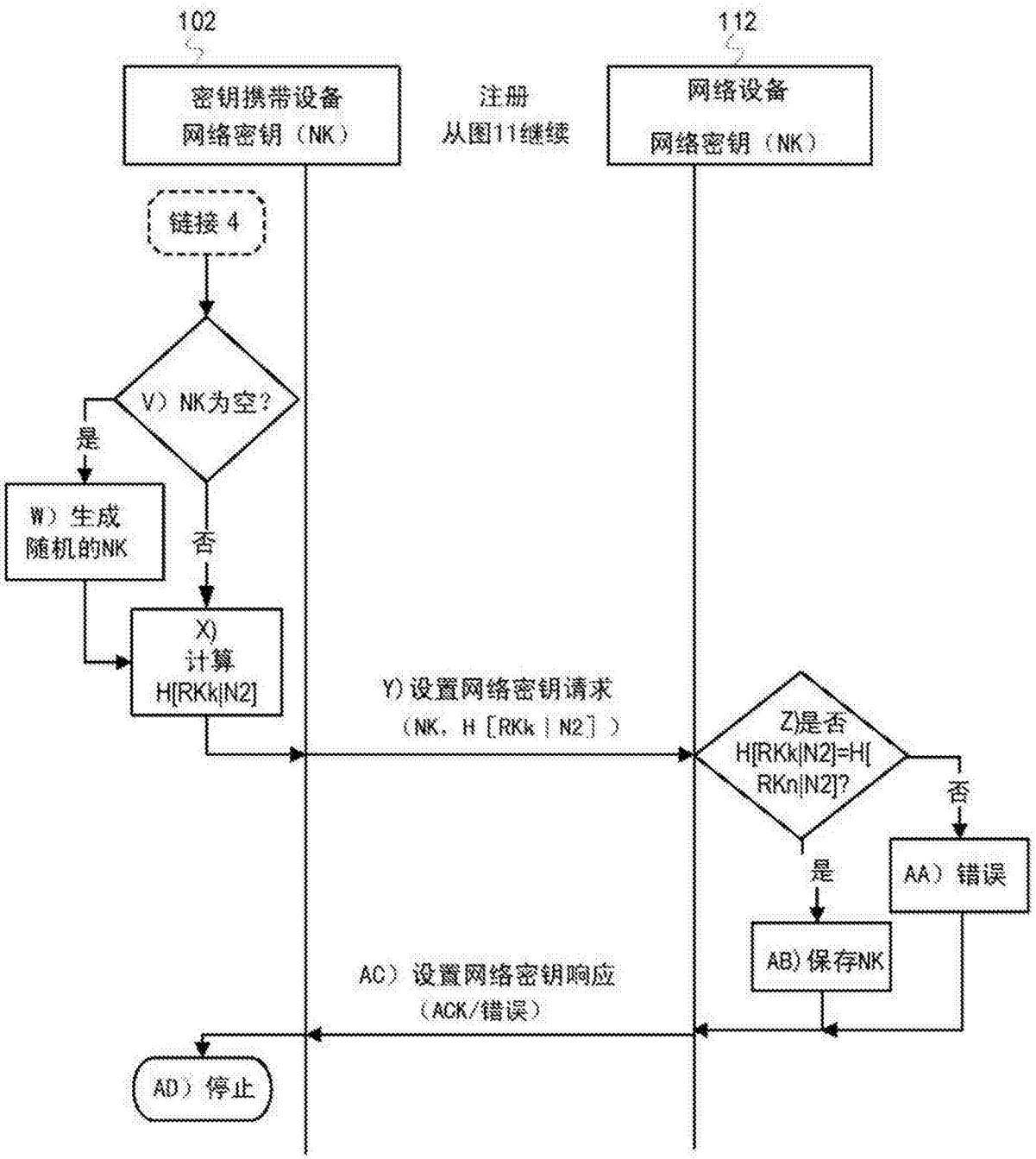

102
112
密钥携带设备
网络密钥（NK）
注册
从图11继续
网络设备
网络密钥（NK）
链接 4
V）NK为空？
是
否
W）生成
随机的NK
X)
计算
H[RKk|N2]
Y)设置网络密钥请求
（NK，H［RKk｜N2］）
Z)是否
H[RKk|N2]=H[
RKn|N2]?
否
是
AA）错误
AB)保存NK
AC）设置网络密钥响应
（ACK/错误）
AD）停止

图12

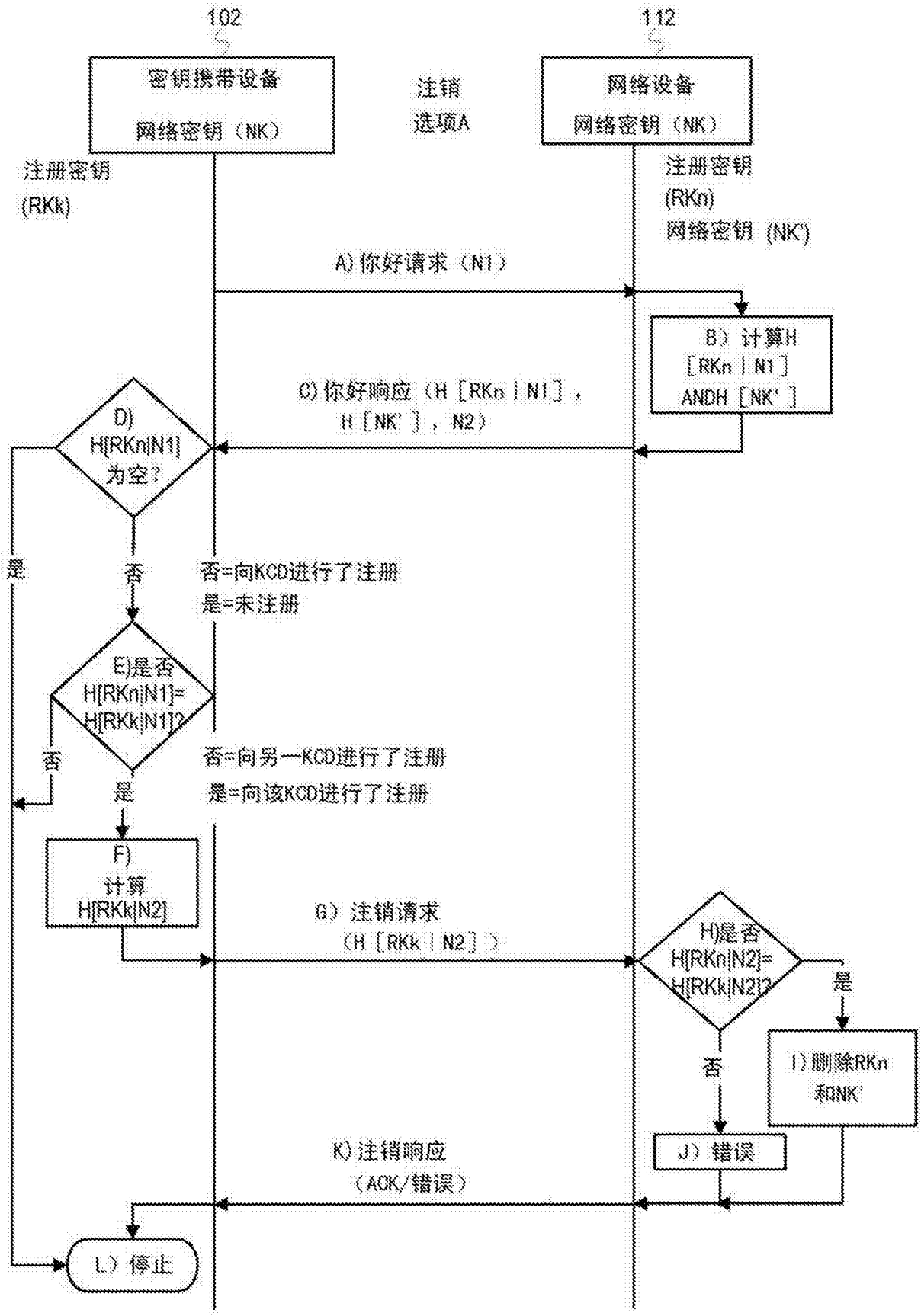

102
112
密钥携带设备
网络密钥（NK）
注销
选项A
网络设备
网络密钥（NK）
注册密钥
(RKk)
注册密钥
(RKn)
网络密钥 (NK')
A)你好请求（N1）
B）计算H
[RKn | N1]
ANDH [NK']
C)你好响应（H [RKn | N1]，
H [NK']，N2）
D)
H[RKn|N1]
为空?
是
否
否=向KCD进行了注册
是=未注册
E)是否
H[RKn|N1]=
H[RKk|N1]?
否
是
否=向另一KCD进行了注册
是=向该KCD进行了注册
F)
计算
H[RKk|N2]
G）注销请求
（H [RKk | N2]）
H)是否
H[RKn|N2]=
H[RKk|N2]?
是
否
I)删除RKn
和NK'
J）错误
K)注销响应
（ACK/错误）
L）停止

图13

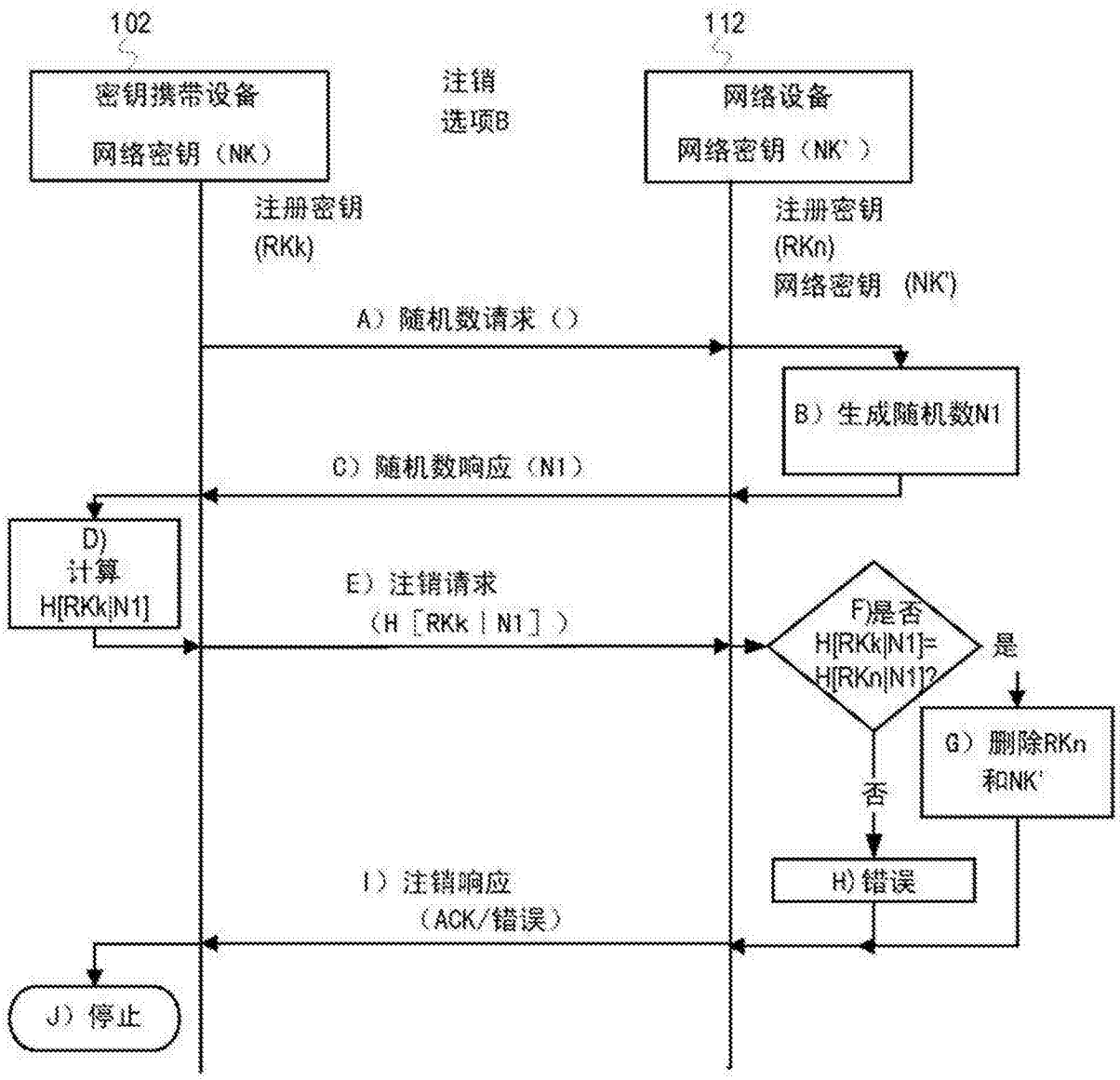

102
112
密钥携带设备
网络密钥（NK）
注销
选项B
网络设备
网络密钥（NK'）
注册密钥
(RKk)
注册密钥
(RKn)
网络密钥 (NK')
A）随机数请求（）
B）生成随机数N1
C）随机数响应（N1）
D)
计算
H[RKk|N1]
E）注销请求
（H［RKk｜N1］）
F)是否
H[RKk|N1]=
H[RKn|N1]?
是
G）删除RKn
和NK'
否
H)错误
I）注销响应
（ACK/错误）
J）停止

图14

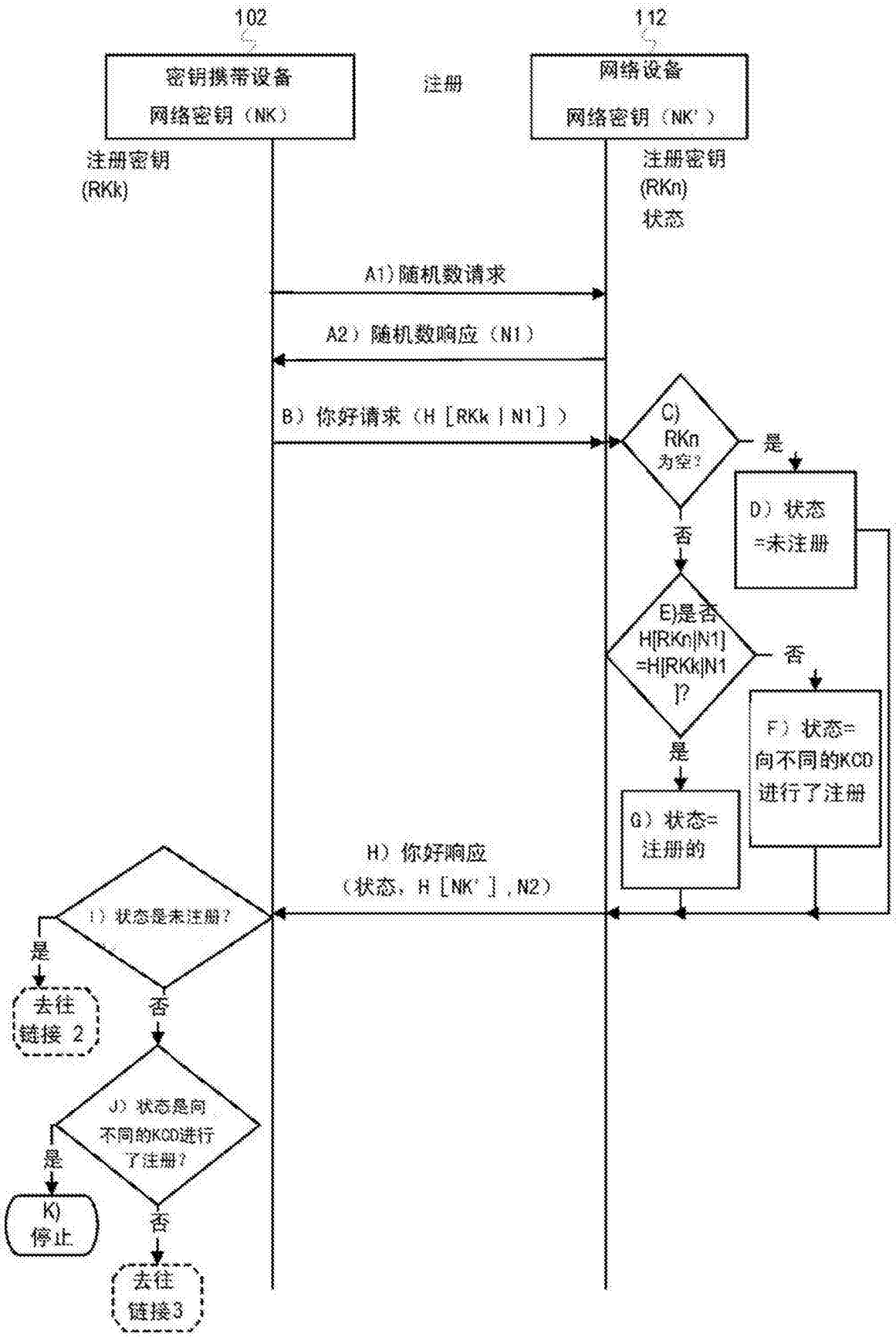

102
112
密钥携带设备
网络密钥（NK）
注册
网络设备
网络密钥（NK'）
注册密钥
(RKk)
注册密钥
(RKn)
状态
A1）随机数请求
A2）随机数响应（N1）
B）你好请求（H［RKk｜N1］）
C)
RKn
为空?
是
D）状态
=未注册
否
E)是否
H[RKn|N1]
=H[RKk|N1
]?
否
F）状态=
向不同的KCD
进行了注册
是
G）状态=
注册的
H）你好响应
（状态，H［NK'］，N2）
I）状态是未注册?
是
去往
链接 2
否
J）状态是向
不同的KCD进行
了注册?
是
K)
停止
否
去往
链接3

图15

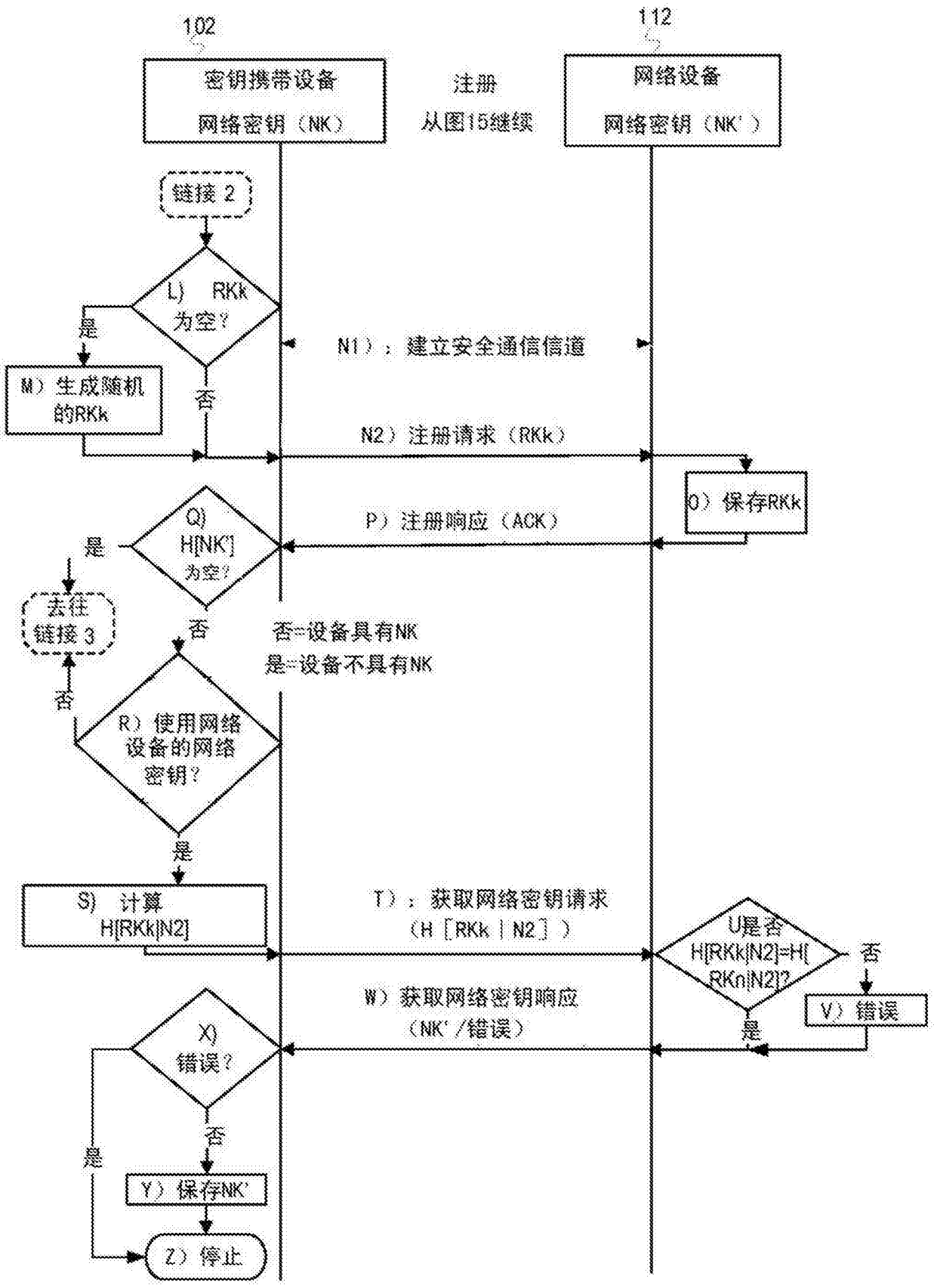

102
112
密钥携带设备
网络密钥（NK）
注册
从图15继续
网络设备
网络密钥（NK'）
链接 2
L） RKk为空？
是
否
M）生成随机的RKk
N1）：建立安全通信信道
N2）注册请求（RKk）
O）保存RKk
P）注册响应（ACK）
Q） H[NK']为空？
是
去往链接 3
否
否=设备具有NK
是=设备不具有NK
否
R）使用网络设备的网络密钥？
是
S） 计算H[RKk|N2]
T）：获取网络密钥请求（H［RKk | N2］）
U是否H[RKk|N2]=H[RKn|N2]?
否
V）错误
是
W）获取网络密钥响应（NK'/错误）
X） 错误？
否
是
Y）保存NK'
Z）停止

图16

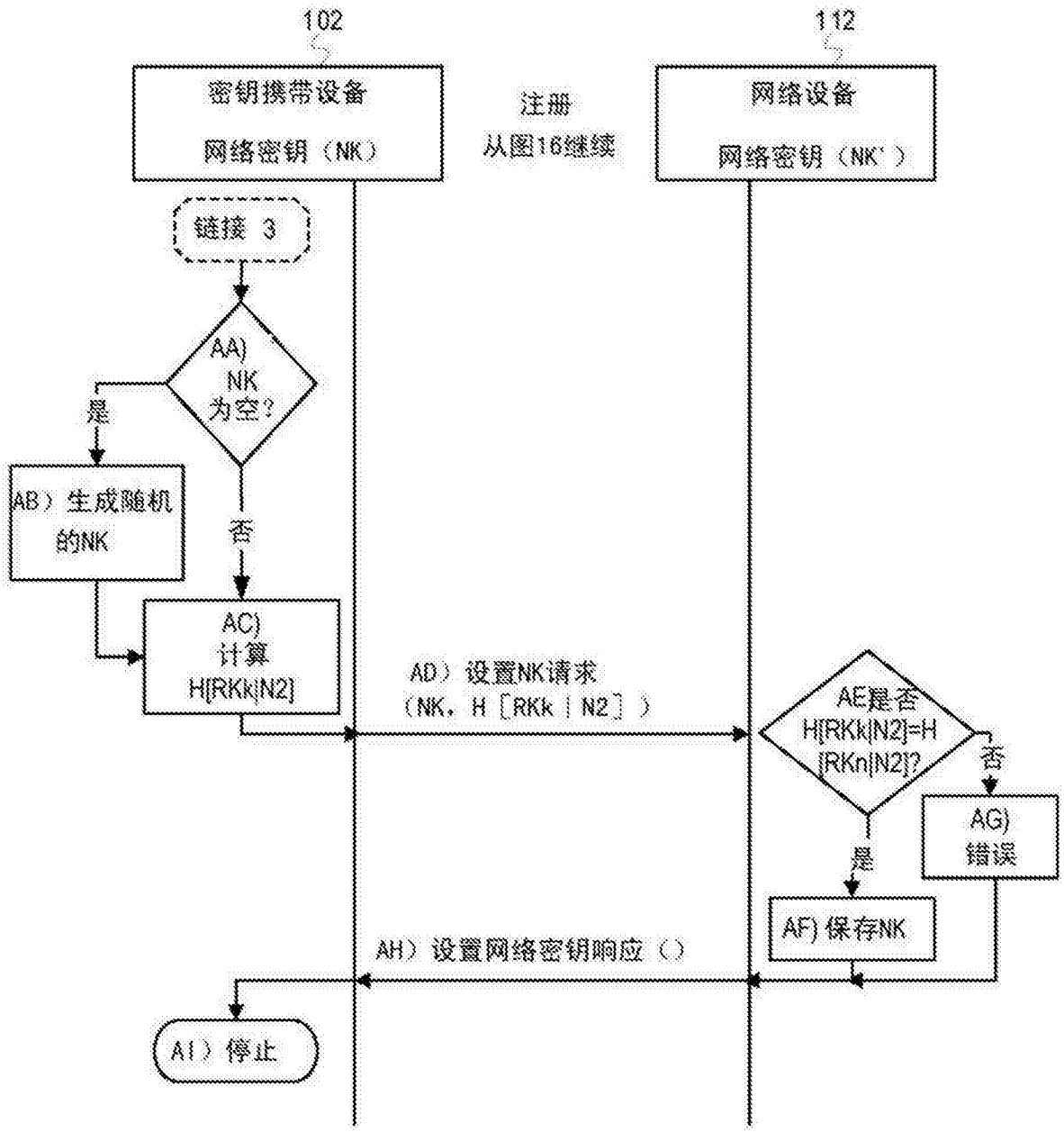

102
112
密钥携带设备
网络密钥（NK）
注册
从图16继续
网络设备
网络密钥（NK'）
链接 3
AA)
NK
为空?
是
否
AB）生成随机
的NK
AC)
计算
H[RKk|N2]
AD）设置NK请求
（NK，H［RKk｜N2］）
AE)是否
H[RKk|N2]=H
[RKn|N2]?
否
是
AG)
错误
AF) 保存NK
AH）设置网络密钥响应（）
AI）停止

图17

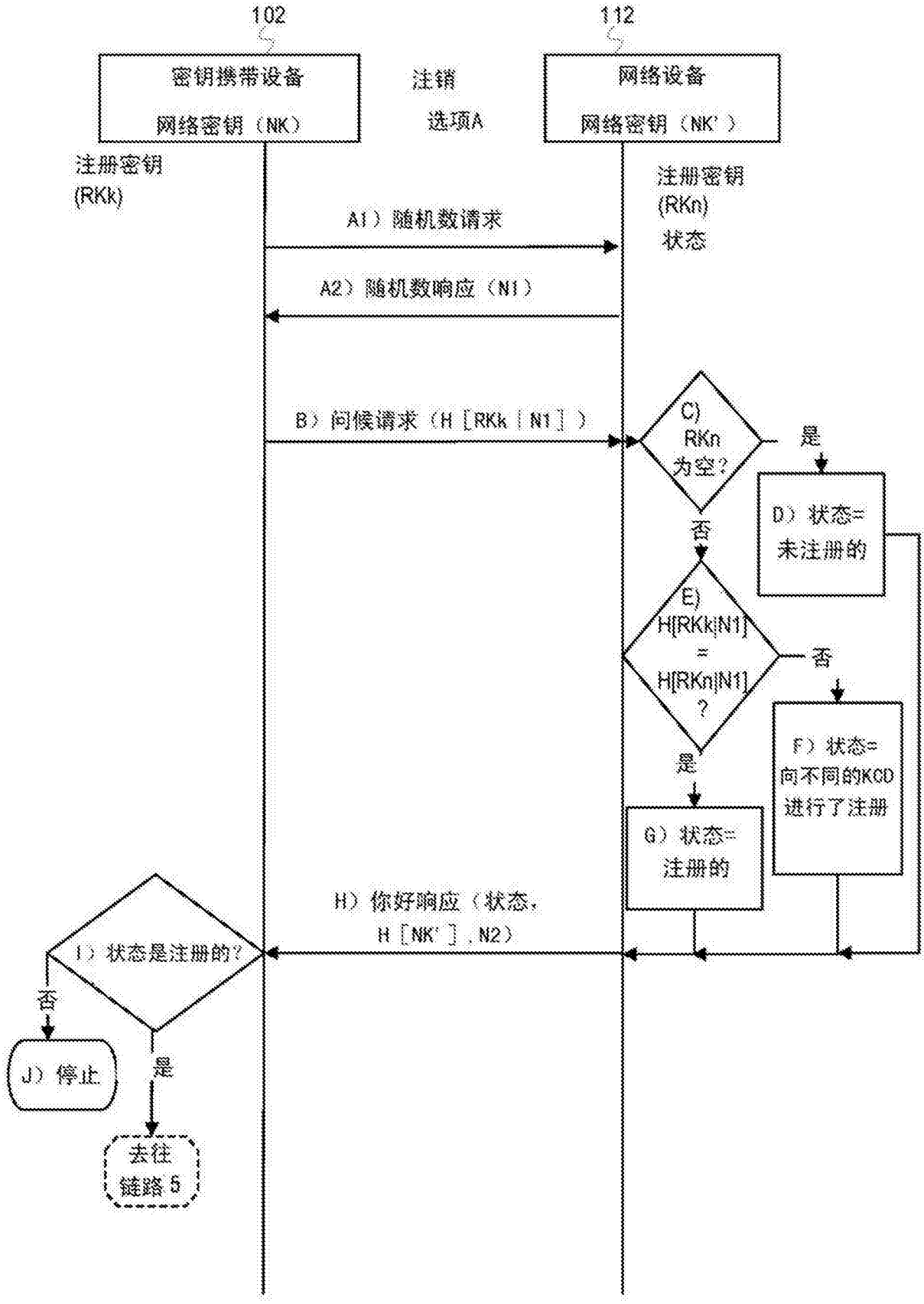

102
112
密钥携带设备
网络密钥（NK）
注销
选项A
网络设备
网络密钥（NK'）
注册密钥
(RKk)
注册密钥
(RKn)
状态
A1）随机数请求
A2）随机数响应（N1）
B）问候请求（H［RKk｜N1］）
C)
RKn
为空？
是
D）状态=
未注册的
否
E)
H[RKk|N1]
=
H[RKn|N1]
？
否
F）状态=
向不同的KCD
进行了注册
是
G）状态=
注册的
H）你好响应（状态，
H［NK'］，N2）
I）状态是注册的？
否
J）停止
是
去往
链路5

图18

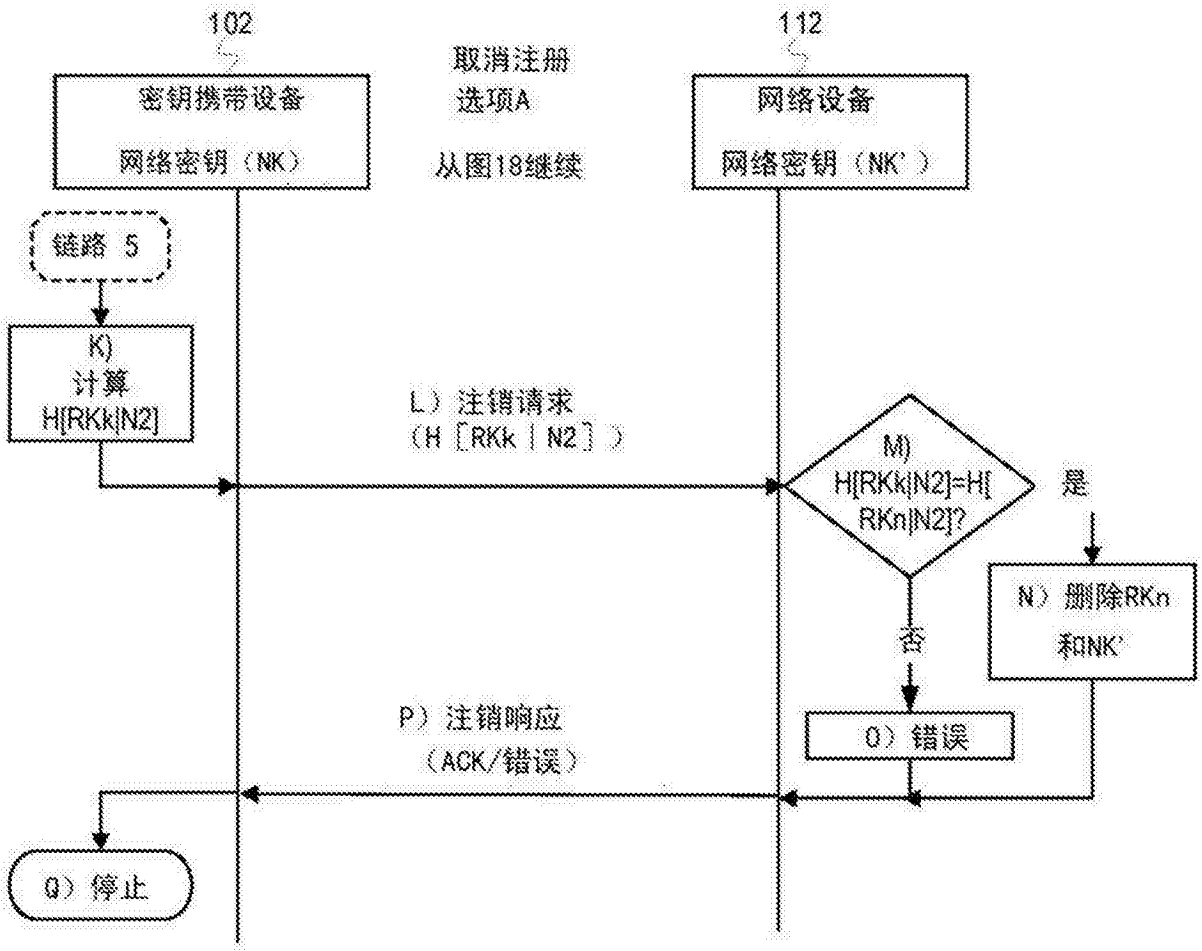

102
112
取消注册
选项A
从图18继续
密钥携带设备
网络密钥（NK）
网络设备
网络密钥（NK'）
链路 5
K)
计算
H[RKk|N2]
L）注销请求
（H［RKk｜N2］）
M)
H[RKk|N2]=H[
RKn|N2]?
是
否
N）删除RKn
和NK'
O）错误
P）注销响应
（ACK/错误）
Q）停止

图19

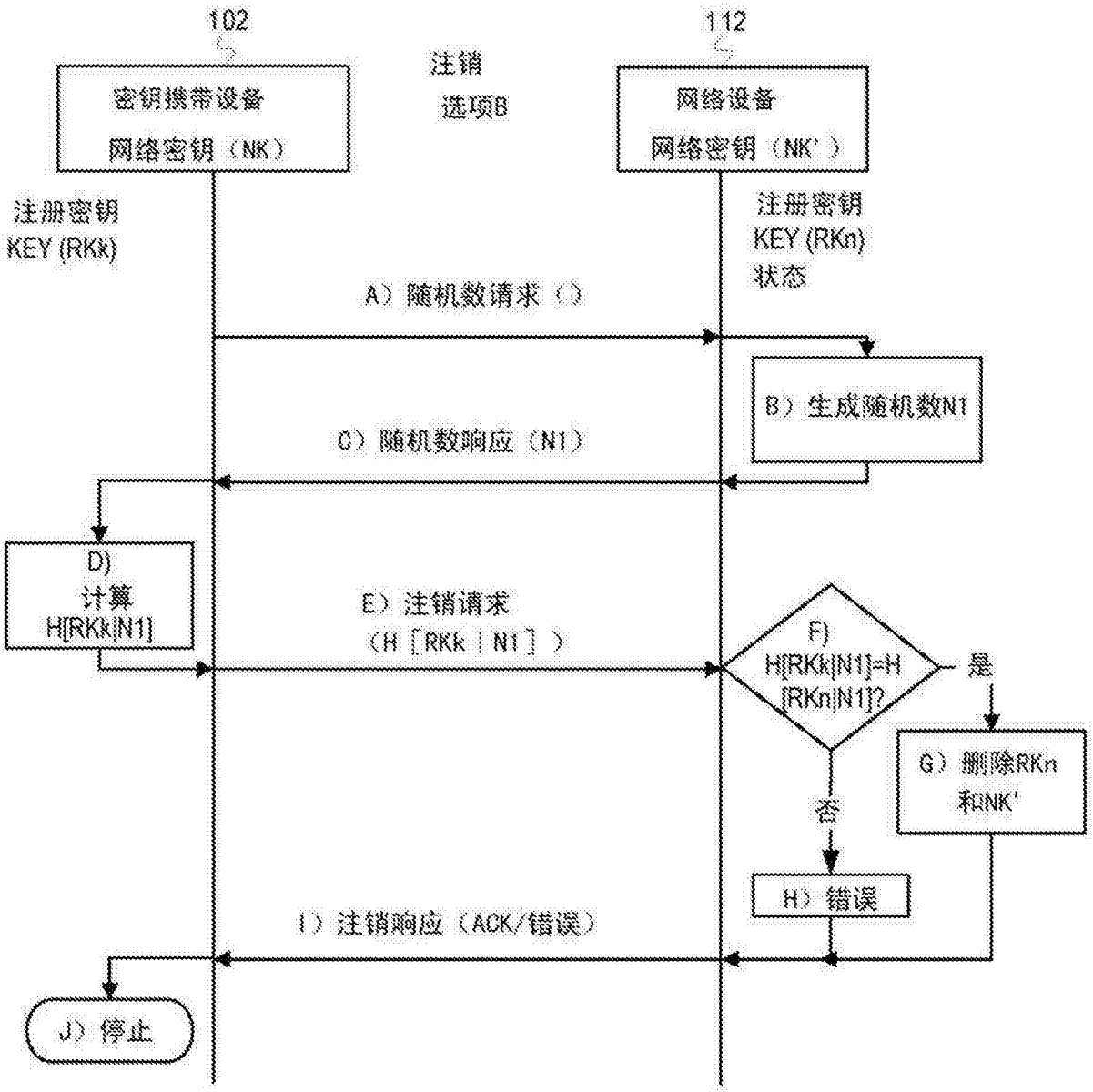

102
112
注销
选项B
密钥携带设备
网络密钥（NK）
网络设备
网络密钥（NK'）
注册密钥
KEY (RKk)
注册密钥
KEY (RKn)
状态
A）随机数请求（）
B）生成随机数N1
C）随机数响应（N1）
D)
计算
H[RKk|N1]
E）注销请求
（H［RKk｜N1］）
F)
H[RKk|N1]=H
[RKn|N1]?
是
G）删除RKn
和NK'
否
H）错误
I）注销响应（ACK/错误）
J）停止

图20

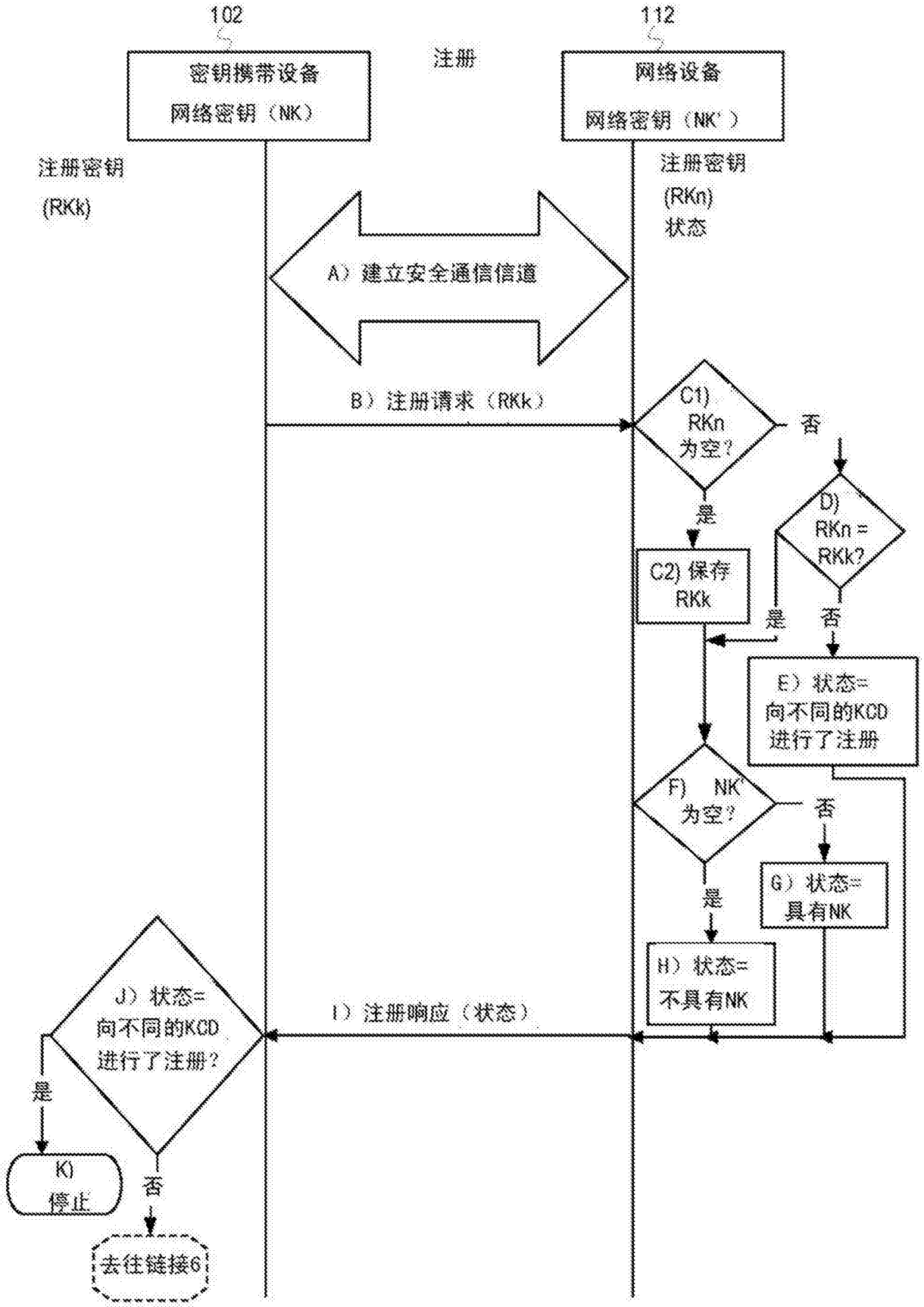

102
112
注册
密钥携带设备
网络密钥（NK）
网络设备
网络密钥（NK'）
注册密钥
(RKk)
注册密钥
(RKn)
状态
A）建立安全通信信道
B）注册请求（RKk）
C1)
RKn
为空?
否
是
C2) 保存
RKk
D)
RKn =
RKk?
是
否
E）状态=
向不同的KCD
进行了注册
F) NK'
为空?
否
是
G）状态=
具有NK
H）状态=
不具有NK
I）注册响应（状态）
J）状态=
向不同的KCD
进行了注册?
是
否
K)
停止
去往链接6

图21

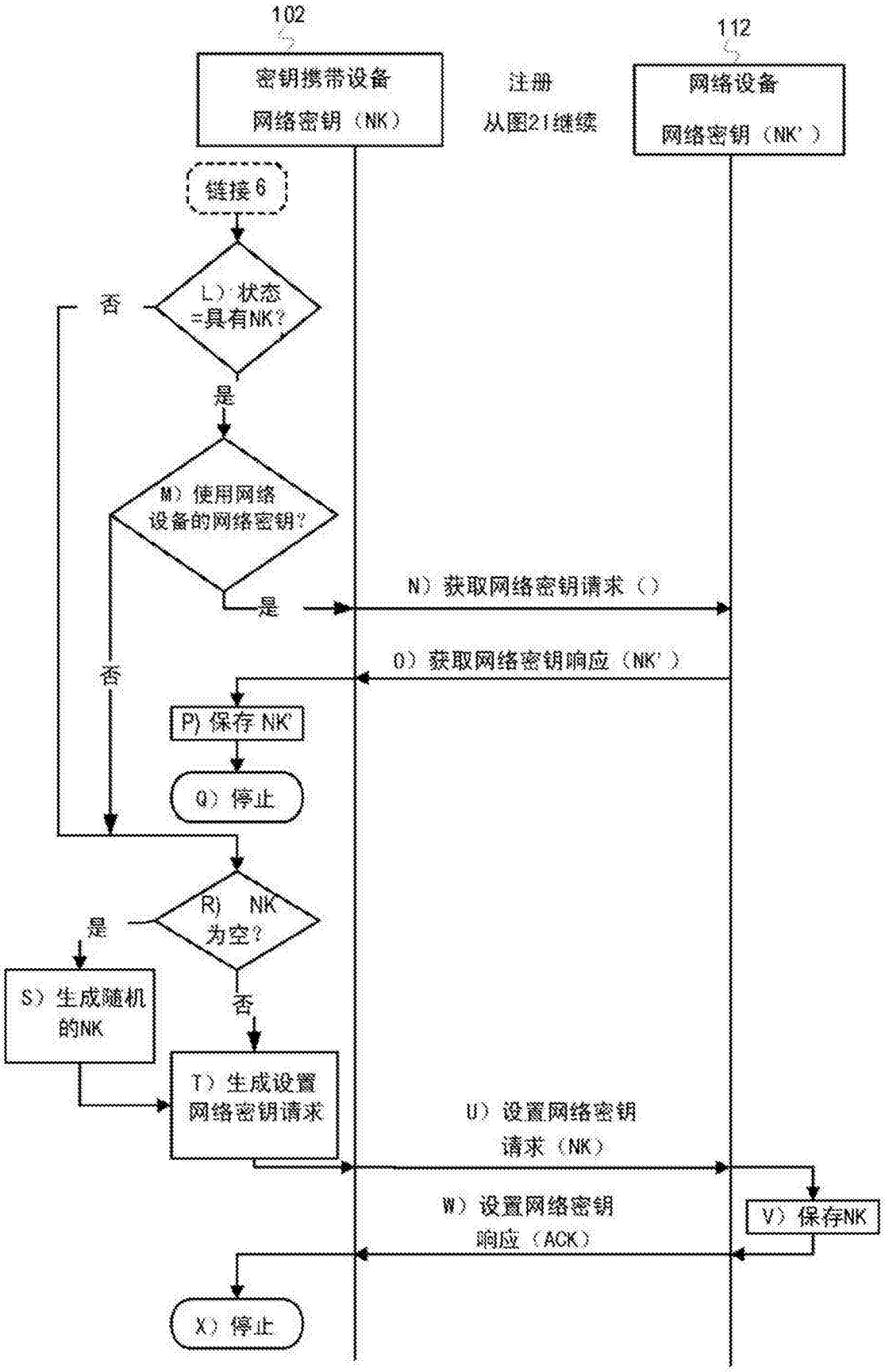

102
密钥携带设备
网络密钥（NK）
注册
从图21继续
112
网络设备
网络密钥（NK'）
链接 6
L）状态=具有NK？
否
是
M）使用网络设备的网络密钥？
是
N）获取网络密钥请求（）
O）获取网络密钥响应（NK'）
否
P）保存 NK'
Q）停止
R） NK为空？
是
否
S）生成随机的NK
T）生成设置网络密钥请求
U）设置网络密钥请求（NK）
W）设置网络密钥响应（ACK）
V）保存NK
X）停止

图22

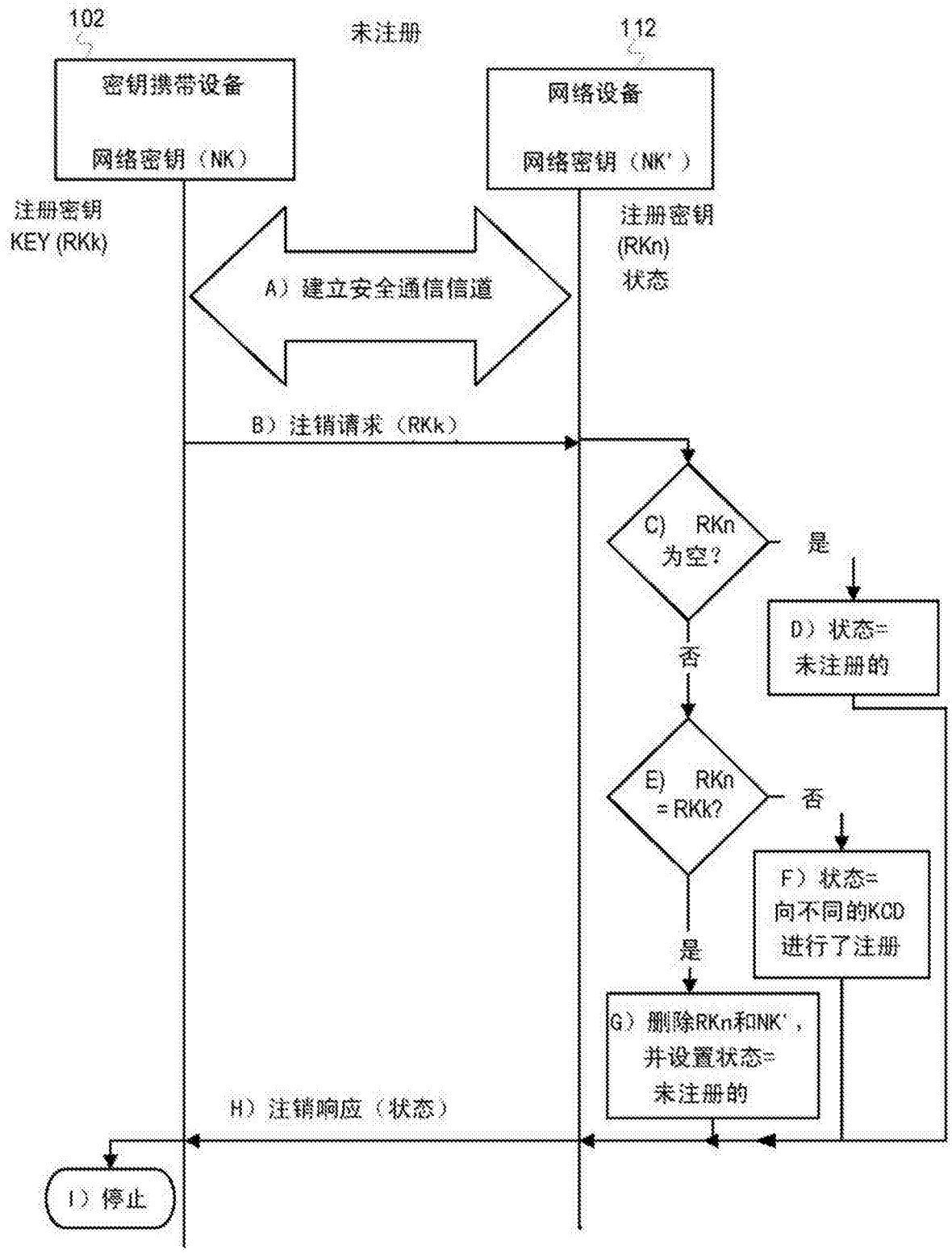

102
未注册
112
密钥携带设备
网络密钥（NK）
网络设备
网络密钥（NK'）
注册密钥
KEY (RKk)
注册密钥
(RKn)
状态
A）建立安全通信信道
B）注销请求（RKk）
C） RKn
为空？
是
D）状态=
未注册的
否
E） RKn
= RKk?
否
F）状态=
向不同的KCD
进行了注册
是
G）删除RKn和NK'，
并设置状态=
未注册的
H）注销响应（状态）
I）停止

图23

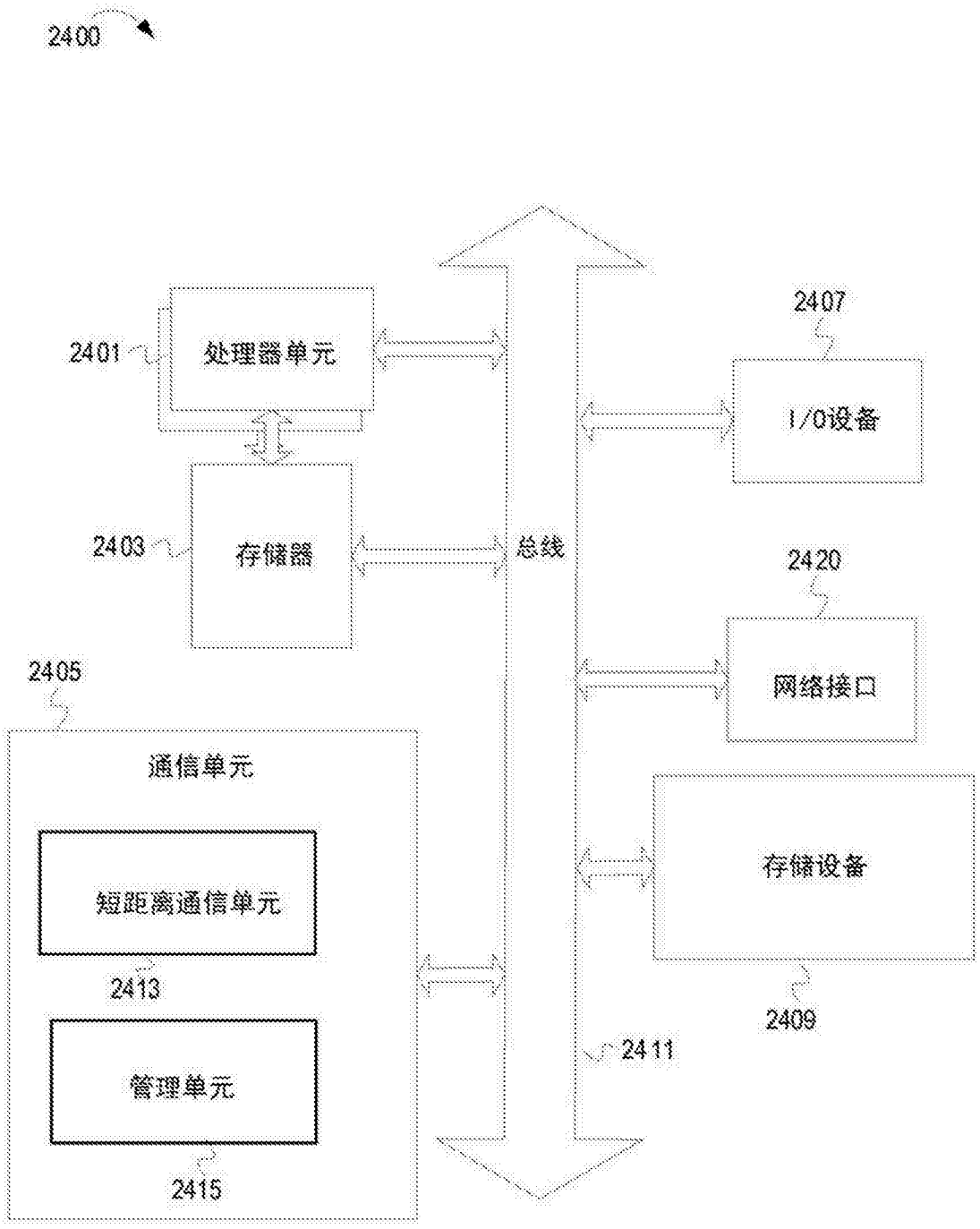

2400
2401
处理器单元
2407
I/O设备
2403
存储器
总线
2420
网络接口
2405
通信单元
短距离通信单元
2413
管理单元
2415
存储设备
2409
2411

图24