(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105224843 A
(43)申请公布日 2016.01.06

(21)申请号 201410260527.8

(22)申请日 2014.06.12

(71)申请人 西安中兴新软件有限责任公司
地址 710114 陕西省西安市高新区长安通讯产业园东西四号路1号

(72)发明人 张文博

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 张颖玲 孟桂超

(51)Int.Cl.
G06F 21/32(2013.01)

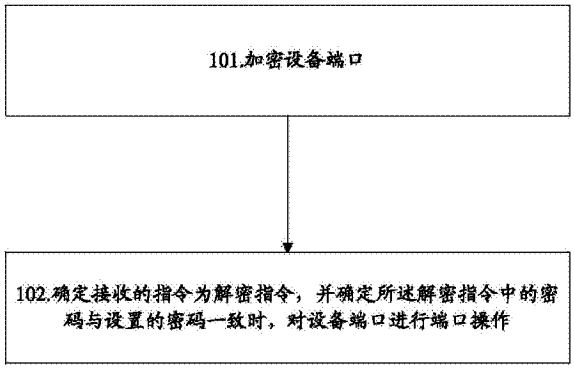
权利要求书1页 说明书7页 附图1页

(54)发明名称

一种保护信息安全的方法、装置及设备

(57)摘要

本发明公开了一种保护信息安全的方法，所述方法包括：加密设备端口，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。本发明同时还公开了一种保护信息安全的装置及设备。



CN 105224843 A

1. 一种保护信息安全的方法，其特征在于，所述方法包括：

加密设备端口，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。

2. 根据权利要求 1 所述的方法，其特征在于，所述加密设备端口包括：

预设所述设备端口的加密标识 flag；

将所述加密标识 flag 的状态设置为有效状态。

3. 根据权利要求 1 所述的方法，其特征在于，所述确定所述解密指令中的密码与设置的密码一致之前，所述方法还包括：提取所述解密指令中的密码，判断所述解密指令中的密码与设置的密码是否一致。

4. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码不一致时，所述设备端口保持加密状态。

5. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

确定接收的指令不是解密指令，判断所述设备端口是否为加密状态，确定所述设备端口为加密状态时，返回错误提示。

6. 根据权利要求 5 所述的方法，其特征在于，所述方法还包括：确定所述设备端口为非加密状态时，对所述设备端口进行端口操作。

7. 一种保护信息安全的装置，其特征在于，所述装置包括：加密模块、确定模块；其中，

所述加密模块，用于加密设备端口；

所述确定模块，用于确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。

8. 根据权利要求 7 所述的装置，其特征在于，所述加密模块，具体用于：

预设所述设备端口的加密标识 flag；

将所述加密标识 flag 的初始状态设置为有效状态。

9. 根据权利要求 7 所述的装置，其特征在于，所述确定模块，还用于：确定所述解密指令中的密码与设置的密码一致之前，提取所述解密指令中的密码，判断所述解密指令中的密码与设置的密码是否一致。

10. 根据权利要求 7 所述的装置，其特征在于，所述确定模块，还用于：

确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码不一致时，所述设备端口保持加密状态。

11. 根据权利要求 7 所述的装置，其特征在于，所述确定模块，还用于：

确定接收的指令不是解密指令，判断所述设备端口是否为加密状态，确定所述设备端口为加密状态时，返回错误提示。

12. 根据权利要求 11 所述的装置，其特征在于，所述确定模块，还用于：

确定所述设备端口为非加密状态时，对所述设备端口进行端口操作。

13. 一种设备，其特征在于，包括如权利要求 7-12 任一项所述的保护信息安全的装置。

一种保护信息安全的方法、装置及设备

技术领域

[0001] 本发明涉及数据卡及热点产品 hotspot 的信息安全领域，尤其涉及一种保护信息安全的方法、装置及设备。

背景技术

[0002] 目前，数据卡和热点产品的端口大部分是开放给用户的，比如，调试诊断 (diag，diagnosis) 端口；但也有一些热点产品的端口是隐藏的，但是这种隐藏可以通过特殊的指令将端口释放出来。因此，无论端口是开放的还是隐藏的，都很容易通过端口修改数据卡或热点产品中的关键信息。

[0003] 所以，如何保护数据卡和热点产品等设备中的信息安全是目前亟待解决的问题。

发明内容

[0004] 为解决现有技术中存在的问题，本发明实施例提供了一种保护信息安全的方法、装置及设备。

[0005] 本发明实施例提供了一种保护信息安全的方法，所述方法包括：

[0006] 加密设备端口，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。

[0007] 上述方案中，所述加密设备端口包括：

[0008] 预设所述设备端口的加密标识 flag；

[0009] 将所述加密标识 flag 的状态设置为有效状态。

[0010] 上述方案中，所述确定所述解密指令中的密码与设置的密码一致之前，所述方法还包括：提取所述解密指令中的密码，判断所述解密指令中的密码与设置的密码是否一致。

[0011] 上述方案中，所述方法还包括：确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码不一致时，所述设备端口保持加密状态。

[0012] 上述方案中，所述方法还包括：

[0013] 确定接收的指令不是解密指令，判断所述设备端口是否为加密状态，确定所述设备端口为加密状态时，返回错误提示。

[0014] 上述方案中，所述方法还包括：确定所述设备端口为非加密状态时，对所述设备端口进行端口操作。

[0015] 本发明实施例还提供了一种保护信息安全的装置，所述装置包括：加密模块、确定模块；其中，

[0016] 所述加密模块，用于加密设备端口；

[0017] 所述确定模块，用于确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。

[0018] 上述方案中，所述加密模块，具体用于：

[0019] 预设所述设备端口的加密标识 flag；

[0020] 将所述加密标识 flag 的初始状态设置为有效状态。

[0021] 上述方案中，所述确定模块，还用于：确定所述解密指令中的密码与设置的密码一致之前，提取所述解密指令中的密码，判断所述解密指令中的密码与设置的密码是否一致。

[0022] 上述方案中，所述确定模块，还用于：

[0023] 确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码不一致时，所述设备端口保持加密状态。

[0024] 上述方案中，所述确定模块，还用于：

[0025] 确定接收的指令不是解密指令，判断所述设备端口是否为加密状态，确定所述设备端口为加密状态时，返回错误提示。

[0026] 上述方案中，所述确定模块，还用于：

[0027] 确定所述设备端口为非加密状态时，对所述设备端口进行端口操作。

[0028] 本发明实施例还提供了一种设备，包括所述的保护信息安全的装置。

[0029] 本发明实施例提供的保护信息安全的方法、装置及设备，加密设备端口，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。如此，通过加密设备端口，可以有效的防止用户获取并修改设备中的关键信息，也可以有效的防止竞争对手通过设备端口查看设备内部的配置信息等。

附图说明

[0030] 图 1 为本发明实施例一提供的保护信息安全的方法流程示意图；

[0031] 图 2 为本发明实施例二提供的保护信息安全的装置结构示意图。

具体实施方式

[0032] 本发明的各种实施例中：加密设备端口，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。

[0033] 下面通过附图及具体实施例对本发明的技术方案做进一步的详细说明。

[0034] 实施例一

[0035] 本发明实施例提供一种保护信息安全的方法，如图 1 所示，所述方法主要包括以下步骤：

[0036] 步骤 101，设备加密自身的设备端口；

[0037] 本步骤中，设备在启动前，可以预先设置设备端口的密码，所述设备端口的密码是按照加密算法生成的字符串，并通过设备端口指令写入设备中的、如写入设备的加密文件系统 (EFS，Encrypting File System) 中。

[0038] 设备在启动时，可以对自身的设备端口进行加密，所述设备端口可以包括：diag 端口、AT 端口以及调制 modem 端口等；所述设备可以包括：数据卡、热点产品等。所述设备加密自身的设备端口，包括：

[0039] 设备在启动时，预设所述设备端口的加密标识 flag，将所述加密标识 flag 的状态设置为有效状态。

[0040] 其中，所述加密标识 flag 的有效状态可以为：将加密标识 flag 的值设置为 1；相应地，所述加密标识 flag 的无效状态可以为：将加密标识 flag 的值设置为 0。

[0041] 具体地，比如，当所述设备端口为diag端口时，可预先设置所述diag端口的密码，所述diag端口的密码是按照加密算法生成的字符串，并通过diag指令写入设备中的、如写入设备的加密文件系统EFS中。

[0042] 所述设备加密diag端口包括：

[0043] 设备在启动时，预设所述diag端口的加密标识flag，将所述加密标识flag的状态设置为有效状态。

[0044] 这里，所述设备对AT端口及modem端口的加密流程与对所述diag端口的加密流程相同，在此不在赘述。其中，

[0045] 当设备运行出现问题时，用户可通过所述diag端口抓取设备的运行日志，从而分析解决问题；或当用户想要查看或修改设备内部参数时，也可通过所述diag端口实现。

[0046] 所述用户可以通过AT端口发送AT指令进行呼叫、短信、电话本、数据业务、传真等方面的控制。

[0047] 所述用户还可以通过modem端口进行拨号建立虚拟网卡。

[0048] 步骤102，设备确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作；

[0049] 本步骤中，设备启动后，接收到用户通过人机接口输入的指令时，判断所述指令是否为解密指令，确定所述指令为解密指令时，提取所述解密指令中的密码，将所述解密指令中的密码与设置的密码进行匹配，判断所述解密指令中的密码与设置的密码是否一致，当确定所述解密指令中的密码与设置的密码一致时，将所述加密标识flag的状态设置为无效状态，对所述设备端口进行端口操作；其中，所述对所述设备端口进行端口操作包括：通过所述diag端口查看或修改设备中的信息、抓取设备的运行日志；或通过所述AT端口进行呼叫、短信、数据传输等方面的控制；或通过所述modem端口拨号建立虚拟网卡。所述设置的密码可以为：设备的加密文件系统EFS中预先存储的密码。

[0050] 另外，当所述设备确定所述解密指令中的密码与设置的密码不一致时，则通过人机界面向用户提示密码错误，所述设备端口仍保持加密状态，以防止被修改信息。

[0051] 这里，当设备确定接收的指令不是解密指令时，判断设备端口是否处于加密状态；

[0052] 具体地，当确定所述指令不是解密指令时，判断设备端口是否处于加密状态包括：判断所述加密标识flag的状态是否为有效状态，确定所述加密标识flag的状态为有效状态时，即代表此时设备端口为加密状态。

[0053] 相应地，当确定所述加密标识flag的状态为无效状态时，即代表此时设备端口为非加密状态，可直接对所述设备端口进行端口操作；

[0054] 当设备确定所述设备端口为加密状态时，则通过人机界面向用户返回错误提示。

[0055] 这里，当所述设备端口为所述diag端口时，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述diag端口进行diag操作。

[0056] 具体地，当用户想查看或修改设备内部信息时，则通过人机接口、即diag端口向设备输入diag指令；设备接收到用户输入的diag指令，检测接收到的diag指令中的字段判断所述diag指令是否为解密指令，确定所述diag指令为解密指令时，根据diag指令中的字段提取所述解密指令中的密码，将所述解密指令中的密码与设置的密码进行匹配，判

断所述解密指令中的密码与设置的密码是否一致，当确定所述解密指令中的密码与设置的密码一致时，将所述加密标识 flag 的状态设置为无效状态，即完成所述 diag 端口的解密过程，对所述 diag 端口进行 diag 操作。

[0057] 其中，所述 diag 指令是具有固定格式的，是根据所述 diag 指令规定的写法生成的，比如，send data75370300 ；这里，可以根据实际情况自定义所述 diag 指令中的数字部分。所述对所述 diag 端口进行 diag 操作包括 ：通过所述 diag 端口查看或修改设备内部的配置信息及重要参数 ；或者查看设备中关键模块的处理流程等。

[0058] 所述设备内部的配置信息及重要参数包括 ：设备的拨号参数、锁网参数、锁卡参数等 ；

[0059] 所述设备中关键模块的处理流程包括 ：自主研发模块中的数据处理流程。

[0060] 另外，当所述设备确定所述解密指令中的密码与设置的密码不一致时，则通过人机界面向用户提示密码错误，所述 diag 端口仍保持加密状态，以防止被修改信息。

[0061] 这里，当所述设备接收到 diag 指令，确定接收的 diag 指令不是解密指令时，判断所述 diag 端口是否处于加密状态 ；

[0062] 具体地，当设备确定接收的 diag 指令不是解密指令时，判断所述加密标识 flag 的状态是否为有效状态，确定所述加密标识 flag 的状态为有效状态时，即代表此时 diag 端口为加密状态 ；

[0063] 相应地，当确定所述加密标识 flag 的状态为无效状态时，即代表此时 diag 端口为非加密状态，可直接对所述 diag 端口进行 diag 端口操作。

[0064] 当设备确定所述 diag 端口为加密状态时，则通过人机界面向用户返回错误提示。

[0065] 另外，当所述设备端口为所述 AT 端口时，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述 AT 端口进行 AT 操作。

[0066] 具体地，当用户想对设备的功能进行控制，或查看设备的注册信息时，则通过人机接口、即 AT 端口向设备输入 AT 指令即可实现 ；比如，当用户输入 AT+CMUT 指令时，则代表控制设备的麦克风静音 ；当用户输入 AT+CREG 指令时，则代表获取设备的注册状态。其中，所述 AT 指令的格式为 ：指令中前两个字符必须是 AT，可以根据 AT 标准指令集选择想要输入的指令 ；如果 AT 标准指令集不包括想要选择的指令时，可根据实际情况进行研发。

[0067] 当所述设备端口为所述 modem 端口时，确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述 modem 端口进行 modem 操作。

[0068] 当用户想通过拨号建立虚拟网卡时，可通过人机接口、即 modem 端口向设备输入相应的 modem 指令，所述 modem 端口根据所述 modem 指令即可建立虚拟网卡。

[0069] 这里，所述设备对 AT 端口及 modem 端口的解密流程与对所述 diag 端口的解密流程相同。

[0070] 本实施例提供的保护信息安全的方法，通过加密 diag 端口，可以有效的防止用户获取并修改设备的锁网、锁卡信息，也可以避免机卡绑定的用户转网。

[0071] 另外，还可以有效避免黑客通过 diag 端口对设备进行攻击，获取并非法篡改设备中的重要信息等。

[0072] 实施例二

[0073] 相应于实施例一，本发明实施例还提供了一种保护信息安全的装置，如图 2 所示，

所述装置包括：加密模块21、确定模块22；其中，

[0074] 所述加密模块21，用于加密设备端口；

[0075] 所述确定模块22，用于确定接收的指令为所述解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述设备端口进行端口操作。

[0076] 设备在启动前，可以预先设置设备端口的密码，所述设备端口的密码是按照加密算法生成的字符串，并通过设备端口指令写入设备中的、如写入设备的加密文件系统EFS中。

[0077] 设备在启动时，所述加密模块21，具体用于：预设所述设备端口的加密标识flag，将所述加密标识flag的状态设置为有效状态。

[0078] 其中，所述加密标识flag的有效状态可以为：所述加密模块21将加密标识flag的值设置为1；相应地，所述加密标识flag的无效状态可以为：所述加密模块21将加密标识flag的值设置为0。

[0079] 所述设备端口可以包括：diag端口、AT端口及modem端口等；所述设备包括如图2所示的保护信息安全的装置的基本结构；具体地，所述设备可以包括：数据卡、热点产品等。

[0080] 比如，当所述设备端口为diag端口时，可预先设置所述diag端口的密码，所述diag端口的密码是按照加密算法生成的字符串，并通过diag指令写入设备中的、如写入设备的加密文件系统EFS中。这时，所述加密模块21，还用于：加密所述diag端口；具体地，设备在启动时，所述加密模块21预设所述diag端口的加密标识flag，将所述加密标识flag的初始状态设置为有效状态。

[0081] 这里，所述加密模块21对AT端口及modem端口的加密流程与对所述diag端口的加密流程相同，在此不在赘述。其中，

[0082] 当设备运行出现问题时，用户可通过所述diag端口抓取设备的运行日志，从而分析解决问题；或当用户想要查看或修改设备内部参数时，也可通过所述diag端口实现。

[0083] 所述用户可以通过AT端口发送AT指令进行呼叫、短信、电话本、数据业务、传真等方面的控制。

[0084] 所述用户还可以通过modem端口进行拨号建立虚拟网卡。

[0085] 设备在启动后，所述确定模块22接收到用户通过人机接口输入的指令时，判断所述指令是否为解密指令，确定所述指令为解密指令时，提取所述解密指令中的密码，将所述解密指令中的密码与设置的密码进行匹配，判断所述解密指令中的密码与设置的密码是否一致，当确定所述解密指令中的密码与设置的密码一致时，将所述加密标识flag的状态设置为无效状态，对所述设备端口进行端口操作；其中，所述设置的密码可以为：设备的加密文件系统EFS中预先存储的密码；所述对所述设备端口进行端口操作包括：通过所述diag端口查看或修改设备中的信息等、抓取设备的运行日志；或通过所述AT端口进行呼叫、短信、数据传输等方面的控制；或通过所述modem端口拨号建立虚拟网卡。

[0086] 另外，当所述确定模块22确定所述解密指令中的密码与设置的密码不一致时，则通过人机界面向用户提示密码错误，所述设备端口仍保持加密状态，以防止被修改信息。

[0087] 这里，当所述确定模块22确定接收的指令不是解密指令时，判断设备端口是否处于加密状态；

[0088] 具体地，当所述确定模块 22 确定所述指令不是解密指令时，判断设备端口是否处于加密状态包括：判断所述加密标识 flag 的状态是否为有效状态，确定所述加密标识 flag 的状态为有效状态时，即代表此时设备端口为加密状态。

[0089] 相应地，当所述确定模块 22 确定所述加密标识 flag 的状态为无效状态时，即代表此时设备端口为非加密状态。

[0090] 当确定模块 22 确定所述设备端口为加密状态时，则通过人机界面向用户返回错误提示；

[0091] 当确定模块 22 确定所述设备端口为非加密状态时，可直接对所述设备端口进行端口操作。

[0092] 比如，当所述设备端口为所述 diag 端口时，所述确定模块 22 确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述 diag 端口进行 diag 操作。

[0093] 具体地，当用户想查看或修改设备内部信息时，则通过人机接口、即 diag 端口向设备输入 diag 指令，所述确定模块 22 接收到用户输入的 diag 指令，检测接收到的 diag 指令中的字段判断所述 diag 指令是否为解密指令，确定所述 diag 指令为解密指令时，根据 diag 指令中的字段提取所述解密指令中的密码，将所述解密指令中的密码与设置的密码进行匹配，判断所述解密指令中的密码与设置的密码是否一致，当确定所述解密指令中的密码与设置的密码一致时，将所述加密标识 flag 的状态设置为无效状态，即完成所述 diag 端口的解密过程，对所述 diag 端口进行 diag 操作。

[0094] 其中，所述 diag 指令是具有固定格式的，是根据所述 diag 指令规定的写法生成的，比如，send data75370300；这里，可以根据实际情况自定义所述 diag 指令中的数字部分。所述对所述 diag 端口进行 diag 操作包括：通过所述 diag 端口查看或修改设备内部的配置信息及重要参数；或者查看设备中关键模块的处理流程等。

[0095] 所述设备内部的配置信息及重要参数包括：设备的拨号参数、锁网参数、锁卡参数等；

[0096] 所述设备中关键模块的处理流程包括：自主研发模块中的数据处理流程。

[0097] 另外，当所述确定模块 22 确定所述解密指令中的密码与设置的密码不一致时，则通过人机界面向用户提示密码错误，所述 diag 端口仍保持加密状态，以防止被修改信息。

[0098] 这里，当所述确定模块 22 确定接收的 diag 指令不是解密指令时，判断所述 diag 端口是否处于加密状态；

[0099] 具体地，当确定模块 22 确定接收的 diag 指令不是解密指令时，判断所述加密标识 flag 的状态是否为有效状态，确定所述加密标识 flag 的状态为有效状态时，即代表此时 diag 端口为加密状态；

[0100] 相应地，当所述确定模块 22 确定所述加密标识 flag 的状态为无效状态时，即代表此时 diag 端口为非加密状态，可直接对所述 diag 端口进行 diag 端口操作。

[0101] 当所述确定模块 22 确定所述 diag 端口为加密状态时，则通过人机界面向用户返回错误提示。

[0102] 另外，当所述设备端口为所述 AT 端口时，所述确定模块 22 确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述 AT 端口进行 AT 操作。

[0103] 具体地，当用户想对设备的功能进行控制，或查看设备的注册信息时，则通过人机接口、即 AT 端口向设备输入 AT 指令即可实现；比如，当用户输入 AT+CMUT 指令时，则代表控制设备的麦克风静音；当用户输入 AT+CREG 指令时，则代表获取设备的注册状态。其中，所述 AT 指令的格式为：指令中前两个字符必须是 AT，可以根据 AT 标准指令集选择想要输入的指令；如果 AT 标准指令集不包括想要选择的指令时，可根据实际情况进行研发。

[0104] 当所述设备端口为所述 modem 端口时，所述确定模块 22 确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对所述 modem 端口进行 modem 操作。

[0105] 具体地，当用户想通过拨号建立虚拟网卡时，可通过人机接口、即 modem 端口向设备输入相应的 modem 指令，所述 modem 端口根据所述 modem 指令即可建立虚拟网卡。

[0106] 这里，所述确定模块 22 对 AT 端口及 modem 端口的解密流程与对所述 diag 端口的解密流程相同。

[0107] 实际应用时，本发明实施例提供的加密模块 21 及确定模块 22 可由保护信息安全装置中的中央处理器 (CPU，Central Processing Unit)、数字信号处理器 (DSP，Digital Signal Processor) 或可编程逻辑阵列 (FPGA，Field － Programmable Gate Array) 实现。

[0108] 基于上述保护信息安全的装置，本发明实施例还提供了一种设备，包括图 2 所示的保护信息安全装置的基本结构及其各种变形和等同替换，不做赘述。

[0109] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

[0110] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

[0111] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

[0112] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

[0113] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

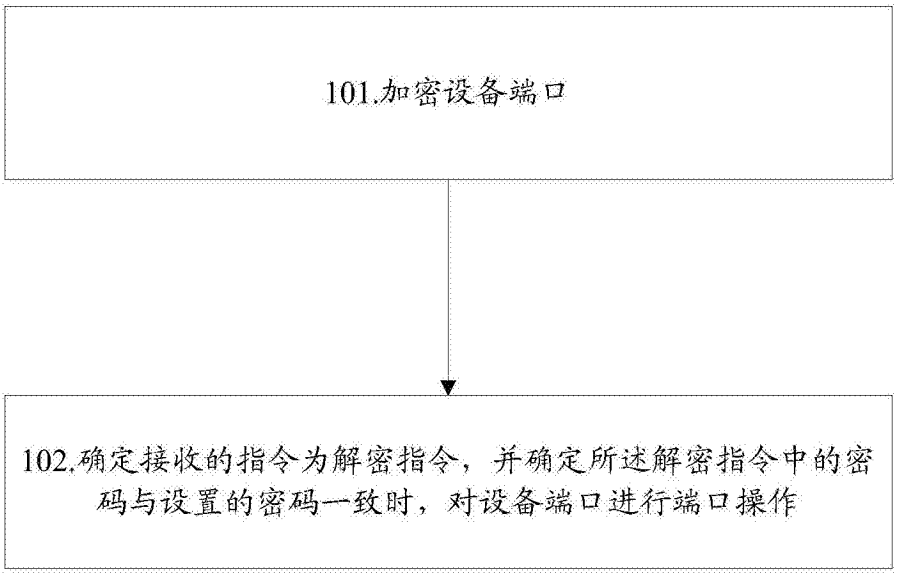

101.加密设备端口
102.确定接收的指令为解密指令，并确定所述解密指令中的密码与设置的密码一致时，对设备端口进行端口操作

图 1

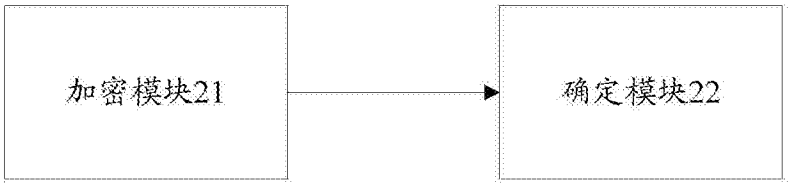

加密模块21
确定模块22

图 2