



(12) 发明专利申请

(10) 申请公布号 CN 104917753 A

(43) 申请公布日 2015. 09. 16

(21) 申请号 201510221865. 5

(22) 申请日 2015. 05. 04

(71) 申请人 北京奇艺世纪科技有限公司

地址 100080 北京市海淀区北一街2号鸿城  
拓展大厦10、11层

(72) 发明人 时斌

(74) 专利代理机构 北京润泽恒知识产权代理有  
限公司 11319

代理人 赵娟

(51) Int. Cl.

H04L 29/06(2006. 01)

H04W 12/04(2009. 01)

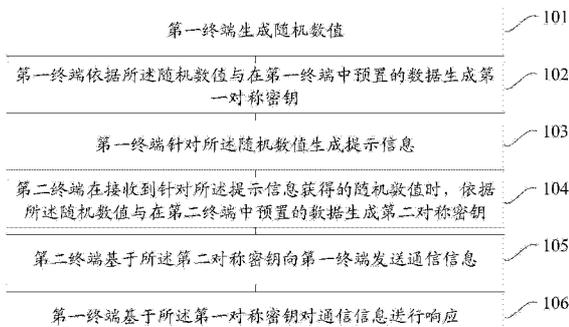
权利要求书2页 说明书8页 附图1页

(54) 发明名称

一种基于对称密钥进行通信的方法和系统

(57) 摘要

本发明实施例提供了一种基于对称密钥进行通信的方法和系统,该方法包括:第一终端生成随机数值;第一终端依据所述随机数值与在第一终端中预置的数据生成第一对称密钥;第一终端针对所述随机数值生成提示信息;第二终端在接收到针对所述提示信息获得的随机数值时,依据所述随机数值与在第二终端中预置的数据生成第二对称密钥;第二终端基于所述第二对称密钥向第一终端发送通信信息;第一终端基于所述第一对称密钥对通信信息进行响应。本发明实施例保证了每次通信的密钥的唯一性,提高了第一对称密钥和第二对称密钥的强度,进而提高了通信的安全性。



1. 一种基于对称密钥进行通信的方法,其特征在于,包括:
  - 第一终端生成随机数值;
  - 第一终端依据所述随机数值与在第一终端中预置的数据生成第一对称密钥;
  - 第一终端针对所述随机数值生成提示信息;
  - 第二终端在接收到针对所述提示信息获得的随机数值时,依据所述随机数值与在第二终端中预置的数据生成第二对称密钥;
  - 第二终端基于所述第二对称密钥向第一终端发送通信信息;
  - 第一终端基于所述第一对称密钥对通信信息进行响应。
2. 根据权利要求1所述的方法,其特征在于,所述第二终端基于所述第二对称密钥向第一终端发送通信信息的步骤包括:
  - 第二终端采用所述第二对称密钥对网络配置参数进行加密,以获得参数密文;
  - 第二终端将所述参数密文广播至第一终端。
3. 根据权利要求2所述的方法,其特征在于,所述第一终端基于所述第一对称密钥对所述通信信息进行响应的步骤包括:
  - 第一终端采用所述第一对称密钥对所述参数密文进行解密,以获得网络配置参数;
  - 第一终端采用所述网络配置参数进行设置,以接入网络。
4. 根据权利要求1或2或3所述的方法,其特征在于,所述第一终端生成随机数值的步骤包括:
  - 第一终端在第一次使用时或恢复出厂设置时,生成随机数值。
5. 根据权利要求1或2或3所述的方法,其特征在于,所述第一终端针对所述随机数值生成提示信息的步骤包括:
  - 第一终端驱动指示灯闪烁与所述随机数值相等的次数;
  - 和/或,
  - 第一终端驱动数码管显示所述随机数值。
6. 根据权利要求1或2或3所述的方法,其特征在于,所述第一终端为无用户界面的终端。
7. 一种基于对称密钥进行通信的系统,其特征在于,所述系统包括第一终端与第二终端;
  - 其中,所述第一终端包括:
    - 随机数值生成模块,用于生成随机数值;
    - 第一对称密钥生成模块,用于依据所述随机数值与在第一终端中预置的数据生成第一对称密钥;
    - 提示信息生成模块,用于针对所述随机数值生成提示信息;
    - 响应模块,用于基于所述第一对称密钥对通信信息进行响应;
  - 所述第二终端包括:
    - 第二对称密钥生成模块,用于在接收到针对所述提示信息获得的随机数值时,依据所述随机数值与在第二终端中预置的数据生成第二对称密钥;
    - 通信模块,用于基于所述第二对称密钥向第一终端发送通信信息。
8. 根据权利要求7所述的系统,其特征在于,所述通信模块包括:

加密子模块,用于采用所述第二对称密钥对网络配置参数进行加密,以获得参数密文;

广播子模块,用于将所述参数密文广播至第一终端。

9. 根据权利要求 8 所述的系统,其特征在于,所述响应模块包括:

解密子模块,用于采用所述第一对称密钥对所述参数密文进行解密,以获得网络配置参数;

配置子模块,用于采用所述网络配置参数进行设置,以接入网络。

10. 根据权利要求 7 或 8 或 9 所述的系统,其特征在于,所述随机数值生成模块包括:

初始生成子模块,用于在第一次使用时或恢复出厂设置时,生成随机数值。

11. 根据权利要求 7 或 8 或 9 所述的系统,其特征在于,所述提示信息生成模块包括:

第一驱动子模块,用于驱动指示灯闪烁与所述随机数值相等的次数;

和/或,

第二驱动子模块,用于驱动数码管显示所述随机数值。

12. 根据权利要求 7 或 8 或 9 所述的系统,其特征在于,所述第一终端为无用户界面的终端。

## 一种基于对称密钥进行通信的方法和系统

### 技术领域

[0001] 本发明涉及通信的技术领域,特别是涉及一种基于对称密钥进行通信的方法和一种基于对称密钥进行通信的系统。

### 背景技术

[0002] 随着物联网(Internet of Things, IOT)技术的迅速发展,各种智能设备也迅速普及到人们的生活中,例如,智能家具、智能厨具、智能穿戴设备等等。

[0003] 物联网一般为无线网,一般需要通过联网才能实现其功能,因此,需要将其接入网络。

[0004] 但是,诸如手环等智能穿戴设备、无线摄像头、无线音箱、智能插座等智能设备,需要无线连接,但一般没有用户界面(User Interface, UI)可供用户进行设置。

[0005] 此时,往往通过手机等控制设备告诉其入网的设置。

[0006] 例如,用户新添加的Wi-Fi(无线抱枕)摄像头,若接入自己家的Wi-Fi环境,则需要输入Wi-Fi的名称和密码,但这个摄像头本身并没有提供可视的用户界面进行设置,需要用手机、平板电脑等其他设备告诉其Wi-Fi的名称和密码。

[0007] 为了避免密码泄漏,事先将密钥存入设备中,在广播过程中大多使用对称密钥对通信过程进行加密,该密钥存在被逆向破解的风险,造成设置过程中易受到监听或攻击,通信的安全性较差。

### 发明内容

[0008] 鉴于上述问题,提出了本发明实施例以便提供一种克服上述问题或者至少部分地解决上述问题的一种基于对称密钥进行通信的方法和相应的一种基于对称密钥进行通信的系统。

[0009] 为了解决上述问题,本发明实施例公开了一种基于对称密钥进行通信的方法,包括:

[0010] 第一终端生成随机数值;

[0011] 第一终端依据所述随机数值与在第一终端中预置的数据生成第一对称密钥;

[0012] 第一终端针对所述随机数值生成提示信息;

[0013] 第二终端在接收到针对所述提示信息获得的随机数值时,依据所述随机数值与在第二终端中预置的数据生成第二对称密钥;

[0014] 第二终端基于所述第二对称密钥向第一终端发送通信信息;

[0015] 第一终端基于所述第一对称密钥对通信信息进行响应。

[0016] 优选地,所述第二终端基于所述第二对称密钥向第一终端发送通信信息的步骤包括:

[0017] 第二终端采用所述第二对称密钥对网络配置参数进行加密,以获得参数密文;

[0018] 第二终端将所述参数密文广播至第一终端。

- [0019] 优选地,所述第一终端基于所述第一对称密钥对所述通信信息进行响应的步骤包括:
- [0020] 第一终端采用所述第一对称密钥对所述参数密文进行解密,以获得网络配置参数;
- [0021] 第一终端采用所述网络配置参数进行设置,以接入网络。
- [0022] 优选地,所述第一终端生成随机数值的步骤包括:
- [0023] 第一终端在第一次使用时或恢复出厂设置时,生成随机数值。
- [0024] 优选地,所述第一终端针对所述随机数值生成提示信息的步骤包括:
- [0025] 第一终端驱动指示灯闪烁与所述随机数值相等的次数;
- [0026] 和/或,
- [0027] 第一终端驱动数码管显示所述随机数值。
- [0028] 优选地,所述第一终端为无用户界面的终端。
- [0029] 本发明实施例还公开了一种基于对称密钥进行通信的系统,所述系统包括第一终端与第二终端;
- [0030] 其中,所述第一终端包括:
- [0031] 随机数值生成模块,用于生成随机数值;
- [0032] 第一对称密钥生成模块,用于依据所述随机数值与在第一终端中预置的数据生成第一对称密钥;
- [0033] 提示信息生成模块,用于针对所述随机数值生成提示信息;
- [0034] 响应模块,用于基于所述第一对称密钥对通信信息进行响应;
- [0035] 所述第二终端包括:
- [0036] 第二对称密钥生成模块,用于在接收到针对所述提示信息获得的随机数值时,依据所述随机数值与在第二终端中预置的数据生成第二对称密钥;
- [0037] 通信模块,用于基于所述第二对称密钥向第一终端发送通信信息。
- [0038] 优选地,所述通信模块包括:
- [0039] 加密子模块,用于采用所述第二对称密钥对网络配置参数进行加密,以获得参数密文;
- [0040] 广播子模块,用于将所述参数密文广播至第一终端。
- [0041] 优选地,所述响应模块包括:
- [0042] 解密子模块,用于采用所述第一对称密钥对所述参数密文进行解密,以获得网络配置参数;
- [0043] 配置子模块,用于采用所述网络配置参数进行设置,以接入网络。
- [0044] 优选地,所述随机数值生成模块包括:
- [0045] 初始生成子模块,用于在第一次使用时或恢复出厂设置时,生成随机数值。
- [0046] 优选地,所述提示信息生成模块包括:
- [0047] 第一驱动子模块,用于驱动指示灯闪烁与所述随机数值相等的次数;
- [0048] 和/或,
- [0049] 第二驱动子模块,用于驱动数码管显示所述随机数值。
- [0050] 优选地,所述第一终端为无用户界面的终端。

[0051] 本发明实施例包括以下优点：

[0052] 本发明实施例在第一终端与第二终端中，基于随机数值和阈值的数据动态生成第一对称密钥和第二对称密钥，并基于该第一对称密钥和第二对称密钥进行通信，保证了每次通信的密钥的唯一性，提高了第一对称密钥和第二对称密钥的强度，进而提高了通信的安全性。

## 附图说明

[0053] 图 1 是本发明的一种基于对称密钥进行通信的方法实施例的步骤流程图；

[0054] 图 2 是本发明的一种基于对称密钥进行通信的系统实施例的结构框图。

## 具体实施方式

[0055] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0056] 由于手机等控制设备一般使用无线通信告诉无 UI 的智能设备要连接的 Wi-Fi 的名称和密码，而手机等控制设备发射的无线信号具有一定覆盖范围（7-8 米或更远），因此，在此过程中，手机等控制设备发射的无线信号可能被其他设备接收，存在 Wi-Fi 密码被窃取的问题，此问题在独栋住宅并不是十分明显，但在商品房或群租等用户密集的环境中比较明显。

[0057] 同理，在手机等控制设备的无线信号能够覆盖的区域内，如果存在一台待添加和绑定用户的设备，那么这台设备就有可能被恶意设置连接到攻击者指定的 Wi-Fi 上，然后添加到攻击者的账户，导致隐私泄露。

[0058] 由于密码等信息容易被窃听，如果不加密，任意设备都能听到，用户在设置网络配置参数时，如果有攻击者用一个 Wi-Fi 设备进行监听，就能获得密码等信息。

[0059] 如果加密，加密使用的密钥需要保存在设备内部，容易被分析破解。一旦某个厂商的设备密钥被破解，那么所有的设备在配置时就可能被监听并分析用户密码等关键信息。

[0060] 因此，提出了本发明实施例的核心构思之一，基于动态生成的对称密钥进行网络配置参数的设置，提高安全性。

[0061] 参照图 1，示出了本发明的一种基于对称密钥进行通信的方法实施例的步骤流程图，具体可以包括如下步骤：

[0062] 步骤 101，第一终端生成随机数值；

[0063] 在具体实现中，第一终端可以为无用户界面的终端，例如，智能插座、智能音响、智能家具、智能厨具等等。

[0064] 其中，用户界面可以指用户（User）与机器（Machine）进行交互操作的界面，用户可以通过该界面对机器进行操作。

[0065] 在本发明实施例中，可以生成一个随机数值，如执行 rand() 等随机算法计算一个随机数值、指定某个数字作为随机数值，基于该随机数值进行网络配置参数的设置。

[0066] 在本发明的一种优选实施例中，步骤 101 可以包括如下子步骤：

[0067] 子步骤 S11，第一终端在第一次使用时或恢复出厂设置时，生成随机数值。

[0068] 一般情况下，第一终端在第一次使用时或恢复出厂设置时，处于初始化状态，设置

的参数是默认的参数。

[0069] 其中,网络配置参数为空,无法接入网络,如无线局域网(Wireless Local Area Networks, WLAN)。此时,可以触发网络配置参数的设置流程。

[0070] 当然,上述生成随机数值的时机只是作为示例,在实施本发明实施例时,可以根据实际情况设置其他生成随机数值的时机,例如,上电时按下某个按键本发明实施例对此不加以限制。另外,除了上述生成随机数值的时机外,本领域技术人员还可以根据实际需要采用其它生成随机数值的时机,本发明实施例对此也不加以限制。

[0071] 步骤 102,第一终端依据所述随机数值与在第一终端中预置的数据生成第一对称密钥;

[0072] 应用本发明实施例,可以预先在第一终端中设置数据,该数据可以包括一组或多组字符,可以为任意长度、任意字符,如二进制数据。

[0073] 在本发明实施例中,可以动态生成一随机数值,引入第一终端独有的特殊因素,基于该随机数值按照预设的组合规则对该一组或多组字符进行组合,现场生成新的对称密钥(如第一对称密钥)。

[0074] 其中,对称密钥加密又可以叫专用密钥加密,即发送和接收数据的双方使用相同的密钥对明文进行加密和解密运算。

[0075] 在一个示例中,在数据中某个位置,添加随机数值,获得第一对称密钥。

[0076] 在另一个示例中,可以将数据移位,该移位的值为随机数值,获得第一对称密钥。

[0077] 在另一个示例中,将数据中每个数字与随机数值相加,获得第一对称密钥。

[0078] 当然,上述第一对称密钥的生成方式只是作为示例,在实施本发明实施例时,可以根据实际情况设置其他第一对称密钥的生成方式,本发明实施例对此不加以限制。另外,除了上述第一对称密钥的生成方式外,本领域技术人员还可以根据实际需要采用其它第一对称密钥的生成方式,本发明实施例对此也不加以限制。

[0079] 步骤 103,第一终端针对所述随机数值生成提示信息;

[0080] 在本发明实施例中,第一终端可以在生成随机数值之后,生成相应的提示信息。

[0081] 需要说明的是,该提示信息可以为非用户界面的提示信息。

[0082] 在本发明实施例的一种优选示例中,步骤 103 可以包括如下子步骤:

[0083] 子步骤 S21,第一终端驱动指示灯闪烁与所述随机数值相等的次数;

[0084] 在本示例中,若第一终端中具有指示灯,如电源指示灯、信号指示灯等,则可以以基于指示灯提示用户该数值,即驱动指示灯闪烁与随机数值相等的次数。

[0085] 和/或,

[0086] 子步骤 S22,第一终端驱动数码管显示所述随机数值。

[0087] 在本示例中,若第一终端中具有数码管,如智能电饭煲、智能电炖锅等智能家具用于显示时间的数码管等,则可以以基于数码管提示用户该数值,即驱动数码管显示随机数值。

[0088] 当然,上述提示信息只是作为示例,在实施本发明实施例时,可以根据实际情况设置其他提示信息,本发明实施例对此不加以限制。另外,除了上述提示信息外,本领域技术人员还可以根据实际需要采用其它提示信息,本发明实施例对此也不加以限制。

[0089] 需要说明的是,该提示信息也可以是携带有随机数值的广播,本发明实施例对此

不加以限制。

[0090] 步骤 104, 第二终端在接收到针对所述提示信息获得的随机数值时, 依据所述随机数值与在第二终端中预置的数据生成第二对称密钥;

[0091] 在一种情形中, 用户可以在观察提示信息后, 在第二终端中输入随机数值。

[0092] 在另一种情形中, 第二终端可以监听到携带有随机数值的广播, 从中提取相应的随机数值

[0093] 应用本发明实施例, 可以预先在第二终端中设置与第一终端中的数据相同的数据, 该数据也可以包括一组或多组字符, 也可以为任意长度、任意字符。

[0094] 在本发明实施例中, 可以引入第一终端独有的特殊因素, 基于该随机数值按照预设的组合规则对该一组或多组字符进行组合, 现场生成新的对称密钥 (如第二对称密钥)。

[0095] 在一个示例中, 在数据中某个位置, 添加随机数值, 获得第二对称密钥。

[0096] 在另一个示例中, 可以将数据移位, 该移位的值为随机数值, 获得第二对称密钥。

[0097] 在另一个示例中, 将数据中每个数字与随机数值相加, 获得第二对称密钥。

[0098] 当然, 上述第二对称密钥的生成方式只是作为示例, 在实施本发明实施例时, 可以根据实际情况设置其他第二对称密钥的生成方式, 本发明实施例对此不加以限制。另外, 除了上述第二对称密钥的生成方式外, 本领域技术人员还可以根据实际需要采用其它第二对称密钥的生成方式, 本发明实施例对此也不加以限制。

[0099] 需要说明的是, 生成第一对称密钥与第二对称密钥的数据 (数据、随机数值) 与方式是相同的, 即第一对称密钥与第二对称密钥的内容是相同的, 是一对对应的对称密钥。

[0100] 步骤 105, 第二终端基于所述第二对称密钥向第一终端发送通信信息;

[0101] 在具体实现中, 第二终端可以基于第二对称密钥与第一终端进行通信。

[0102] 在本发明的一种优选实施例中, 步骤 105 可以包括如下子步骤:

[0103] 子步骤 S31, 第二终端采用所述第二对称密钥对网络配置参数进行加密, 以获得参数密文;

[0104] 在实际应用中, 第二终端可以采用 AES、DES、3DES、BLOWFISH、IDEA、FEAL 等对称密钥加密算法对网络配置参数进行加密。

[0105] 网络配置参数可以用于接入网络的参数信息。

[0106] 例如, 若通过 Wi-Fi 接入 WLAN, 则该网络配置参数一般可以包括 SSID (Service Set Identifier, 服务集标识)、密码, 在某些情况下, 还可以包括加密方式等。

[0107] 子步骤 S32, 第二终端将所述参数密文广播至第一终端。

[0108] 在具体实现中, 第一终端与第二终端可以位于同一网络环境中, 如位于 Wi-Fi 的环境中, 通过 IP (Internet Protocol, 网络之间互连的协议) 网络的物理层发送携带参数密文的广播, 如 UDP (User Datagram Protocol, 用户数据包协议) 的数据包。

[0109] 第一终端在进入初始化状态后, 开始监听同一网络 (如 Wi-Fi) 中的广播, 如接收 UDP 的数据包。

[0110] 步骤 106, 第一终端基于所述第一对称密钥对通信信息进行响应。

[0111] 在具体实现中, 第一终端可以基于第一对称密钥与第二终端进行通信。

[0112] 在本发明的一种优选实施例中, 步骤 106 可以包括如下子步骤:

[0113] 子步骤 S41, 第一终端采用所述第一对称密钥对所述参数密文进行解密, 以获得网

络配置参数；

[0114] 子步骤 S42, 第一终端采用所述网络配置参数进行设置, 以接入网络。

[0115] 在本发明实施例中, 第一终端通过广播, 如 UDP 的数据包 (长度), 获取参数密文, 采用 AES、DES、3DES、BLOWFISH、IDEA、FEAL 等对称密钥加密算法对参数密文进行解密, 获得网络配置参数。

[0116] 第一终端切换网络模式, 通过连接网络, 如 Wi-Fi, 完成配置。

[0117] 在完成配置接入网络之后, 对称密钥 (如第一对称密钥、第二对称密钥) 失效, 即第一终端与第二终端之间可以不基于对称密钥 (如第一对称密钥、第二对称密钥) 进行通信。

[0118] 需要说明的是, 对于方法实施例, 为了简单描述, 故将其都表述为一系列的动作组合, 但是本领域技术人员应该知悉, 本发明实施例并不受所描述的动作顺序的限制, 因为依据本发明实施例, 某些步骤可以采用其他顺序或者同时进行。其次, 本领域技术人员也应该知悉, 说明书中所描述的实施例均属于优选实施例, 所涉及的动作并不一定是本发明实施例所必须的。

[0119] 参照图 2, 示出了本发明的一种基于对称密钥进行通信的系统实施例的结构框图, 所述系统可以包括第一终端 210 与第二终端 220；

[0120] 其中, 所述第一终端 210 具体可以包括如下模块：

[0121] 随机数值生成模块 211, 用于生成随机数值；

[0122] 第一对称密钥生成模块 212, 用于依据所述随机数值与在第一终端中预置的数据生成第一对称密钥；

[0123] 提示信息生成模块 213, 用于针对所述随机数值生成提示信息；

[0124] 响应模块 214, 用于基于所述第一对称密钥对通信信息进行响应；

[0125] 所述第二终端 220 具体可以包括如下模块：

[0126] 第二对称密钥生成模块 221, 用于在接收到针对所述提示信息获得的随机数值时, 依据所述随机数值与在第二终端中预置的数据生成第二对称密钥；

[0127] 通信模块 222, 用于基于所述第二对称密钥向第一终端发送通信信息。

[0128] 在本发明的一种优选实施例中, 所述通信模块 222 可以包括如下子模块：

[0129] 加密子模块, 用于采用所述第二对称密钥对网络配置参数进行加密, 以获得参数密文；

[0130] 广播子模块, 用于将所述参数密文广播至第一终端。

[0131] 在本发明的一种优选实施例中, 所述响应模块 214 可以包括如下子模块：

[0132] 解密子模块, 用于采用所述第一对称密钥对所述参数密文进行解密, 以获得网络配置参数；

[0133] 配置子模块, 用于采用所述网络配置参数进行设置, 以接入网络。

[0134] 在本发明实施例的一种优选示例中, 所述随机数值生成模块 211 可以包括如下子模块：

[0135] 初始生成子模块, 用于在第一次使用时或恢复出厂设置时, 生成随机数值。

[0136] 在本发明实施例的一种优选示例中, 所述提示信息生成模块 213 可以包括如下子模块：

[0137] 第一驱动子模块,用于驱动指示灯闪烁与所述随机数值相等的次数;

[0138] 和/或,

[0139] 第二驱动子模块,用于驱动数码管显示所述随机数值。

[0140] 在具体实现中,所述第一终端可以为无用户界面的终端。

[0141] 对于系统实施例而言,由于其与方法实施例基本相似,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0142] 本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。

[0143] 本领域内的技术人员应明白,本发明实施例的实施例可提供为方法、装置、或计算机程序产品。因此,本发明实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明实施例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、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0144] 本发明实施例是参照根据本发明实施例的方法、终端设备(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终端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终端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。

[0145] 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终端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。

[0146] 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终端设备上,使得在计算机或其他可编程终端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终端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。

[0147] 尽管已描述了本发明实施例的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例做出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明实施例范围的所有变更和修改。

[0148] 最后,还需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0149] 以上对本发明所提供的一种基于对称密钥进行通信的方法和一种基于对称密钥

进行通信的系统,进行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

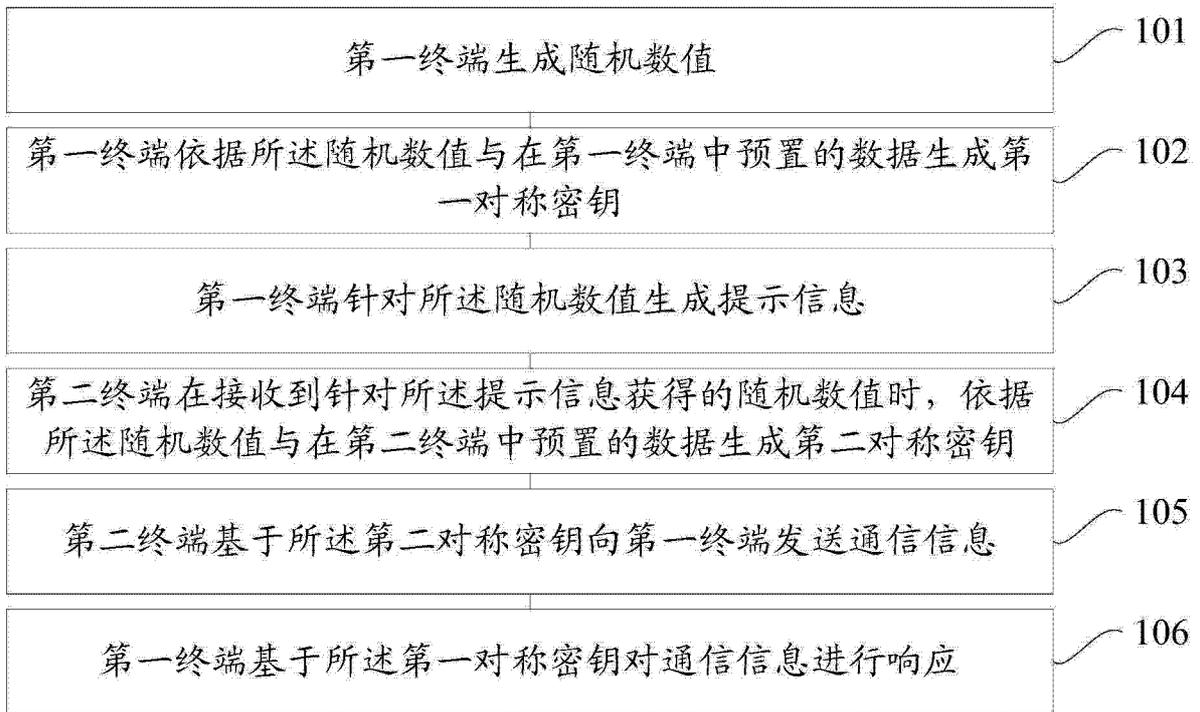


图 1

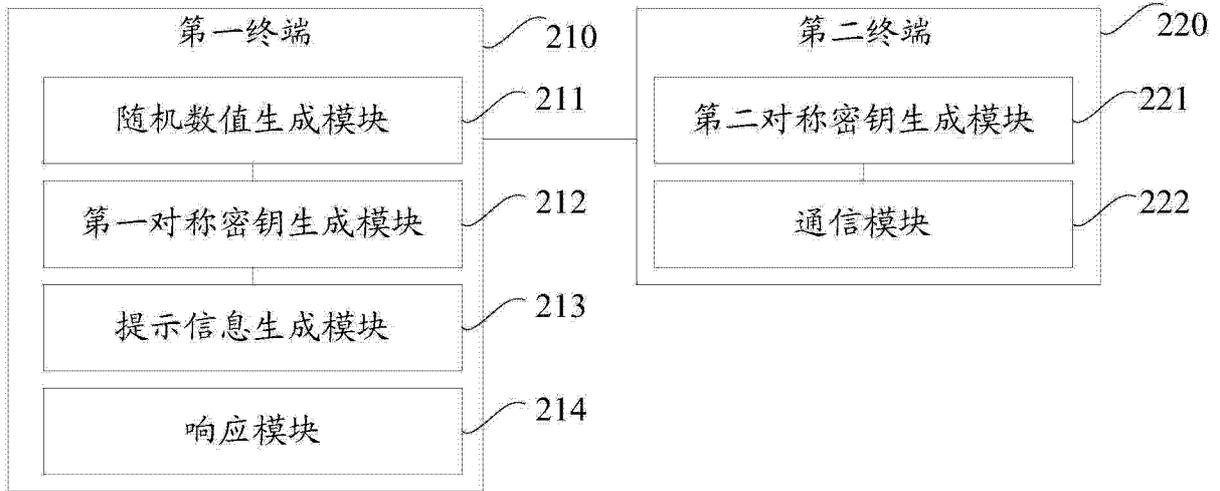


图 2