

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 6 月 7 日 (07.06.2018)



(10) 国际公布号
WO 2018/098886 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01) **B60R 25/20** (2013.01)

中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(21) 国际申请号: PCT/CN2016/113399

(22) 国际申请日: 2016 年 12 月 30 日 (30.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611076026.X 2016年11月29日 (29.11.2016) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(72) 发明人: 董德 (DONG, De); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 潘露杰 (PAN, Lujie); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 孙素珍 (SUN, Suzhen);

(74) 代理人: 深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市龙华新区龙观东路83号荣群大厦9楼, Guangdong 518109 (CN)。

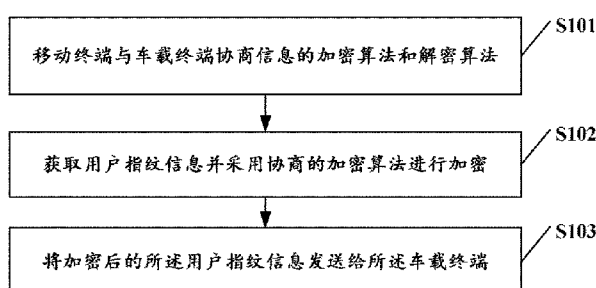
(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,

(54) Title: METHOD FOR OPENING VEHICLE DOOR, MOBILE TERMINAL, VEHICLE-MOUNTED TERMINAL, AND SYSTEM

(54) 发明名称: 一种开启车门的方法、移动终端、车载终端及系统

[Fig. 1]



S101 A mobile terminal negotiates, with a vehicle-mounted terminal, an encryption algorithm and a decryption algorithm for information
S102 Acquire user fingerprint information and encrypt same using the negotiated encryption algorithm
S103 Send the encrypted user fingerprint information to the vehicle-mounted terminal

(57) Abstract: A method for opening a vehicle door, a mobile terminal, a vehicle-mounted terminal and a system, the method comprising: a mobile terminal negotiating, with a vehicle-mounted terminal, an encryption algorithm and a decryption algorithm for information (S101); acquiring user fingerprint information and encrypting same using the negotiated encryption algorithm (S102); and sending the encrypted user fingerprint information to the vehicle-mounted terminal (S103), the vehicle-mounted terminal decrypting the encrypted user fingerprint information using the negotiated decryption algorithm, comparing same with pre-stored user fingerprint information, and if both match, opening the vehicle door. The described method can help conveniently and securely open the vehicle door.

(57) 摘要: 一种开启车门的方法、移动终端、车载终端及系统, 方法包括: 移动终端与车载终端协商信息的加密算法和解密算法 (S101); 获取用户指纹信息并采用协商的加密算法进行加密 (S102); 将加密后的用户指纹信息发送给所述车载终端 (S103), 所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的用户指纹信息匹配并在匹配成功后开启汽车车门。采用上述方法, 可提升车门开启的便利性和安全性。

NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

一种开启车门的方法、移动终端、车载终端及系统

- [1] 本申请要求于2016年11月29日提交中国专利局，申请号为201611076026.X、发明名称为“一种开启车门的方法、移动终端、车载终端及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

- [2] 本发明涉及通信技术领域，尤其涉及一种开启车门的方法、移动终端、车载终端及系统。

背景技术

- [3] 随着人们生活水平的不断提高，越来越多的用户家庭拥有自己的汽车。不管是上班代步、商务接待或者外出旅游等，都可以为用户带来非常大的便利，同时也利于扩大用户的活动半径。

- [4] 用户需要使用汽车时，必须先开启车门。目前现有的开启车门的方式有传统的插入钥匙开门，这种方式比较繁琐；另外对于配置了无钥匙进入系统的车型，还可以通过钥匙与车门的无线连接，当钥匙与汽车距离较近时直接开启车门，但是这种方式安全性较差。且有时候用户可能会将钥匙忘在车中，目前若出现这种情况，上述两种方式均无法打开车门。因此，需要一种便利而安全的开启车门的方式。

对发明的公开

发明内容

- [5] 本发明实施例所要解决的技术问题在于，提供一种开启车门的方法、移动终端、车载终端及系统。可提升车门开启的便利性和安全性。
- [6] 为了解决上述技术问题，本发明实施例第一方面提供了一种开启车门的方法，包括：
- [7] 移动终端与车载终端协商信息的加密算法和解密算法；
- [8] 获取用户指纹信息并采用协商的加密算法进行加密；
- [9] 将加密后的用户指纹信息发送给所述车载终端，所述加密后的用户指纹信息用

于在所述车载终端采用协商的解密算法对其解密后与预存的用户指纹信息匹配并在匹配成功后开启汽车车门。

[10] 本发明实施例第二方面提供了一种移动终端，包括：

[11] 协商单元，设置为与车载终端协商信息的加密算法和解密算法；

[12] 加密单元，设置为获取用户指纹信息并采用协商的加密算法进行加密；

[13] 发送单元，设置为将加密后的用户指纹信息发送给所述车载终端，所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的用户指纹信息匹配并在匹配成功后开启汽车车门。

[14] 本发明实施例第三方面提供了一种移动终端，包括：

[15] 处理器、存储器、接口电路和总线，所述处理器、存储器、接口电路通过总线连接，其中，所述存储器用于存储一组程序代码，所述处理器用于调用所述存储器中存储的程序代码，执行以下操作：

[16] 与车载终端协商信息的加密算法和解密算法；

[17] 获取用户指纹信息并采用协商的加密算法进行加密；

[18] 将加密后的用户指纹信息发送给所述车载终端，所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的用户指纹信息匹配并在匹配成功后开启汽车车门。

[19] 其中，所述加密算法和解密算法为非对称密钥。

[20] 其中，所述加密算法和解密算法对应且同时动态变化。

[21] 其中，所述处理器还用于：

[22] 获取所述移动终端的标识信息并采用协商的加密算法进行加密；

[23] 在将加密后的所述用户指纹信息发送给所述车载终端时，还包括：

[24] 将加密后的标识信息发送给所述车载终端，所述加密后的标识信息用于在所述车载终端采用协商的解密算法对其解密后与预存的标识信息匹配并在用户指纹信息与标识信息均匹配成功后开启汽车车门。

[25] 其中，所述处理器还用于：

[26] 在解密后的信息均匹配成功后，所述移动终端发送控制指令至所述车载终端，控制所述车载终端开启汽车车门。

- [27] 本发明实施例第四方面提供一种开启车门的方法，包括：
- [28] 车载终端与移动终端协商信息的加密算法和解密算法；
- [29] 接收所述移动终端发送的加密后的信息；
- [30] 采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；
- [31] 若所述信息匹配成功，则开启汽车车门或者接收所述移动终端发送的控制指令，开启汽车车门；
- [32] 其中，所述信息包括用户指纹信息。
- [33] 本发明实施例第五方面提供一种车载终端，包括：
- [34] 协商单元，设置为与移动终端协商信息的加密算法和解密算法；
- [35] 接收单元，设置为接收所述移动终端发送的加密后的信息；
- [36] 解密单元，设置为采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；
- [37] 开启单元，若所述信息匹配成功，则开启汽车车门；
- [38] 或者所述接收单元还设置为接收所述移动终端发送的控制指令，指示所述开启单元开启汽车车门；
- [39] 其中，所述信息包括用户指纹信息。
- [40] 本发明实施例第六方面提供一种车载终端，包括：
- [41] 处理器、存储器、接口电路和总线，所述处理器、存储器、接口电路通过总线连接，其中，所述存储器用于存储一组程序代码，所述处理器用于调用所述存储器中存储的程序代码，执行以下操作：
- [42] 与移动终端协商信息的加密算法和解密算法；
- [43] 接收所述移动终端发送的加密后的信息；
- [44] 采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；
- [45] 若所述信息匹配成功，则开启汽车车门或者接收所述移动终端发送的控制指令，开启汽车车门；
- [46] 其中，所述信息包括用户指纹信息。
- [47] 其中，所述加密算法和解密算法为非对称密钥。
- [48] 其中，所述加密算法和解密算法对应且同时动态变化。

- [49] 其中，所述信息还包括所述移动终端的标识信息。
- [50] 其中，所述处理器还用于：
- [51] 若所述信息连续预设次数匹配失败，则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接。
- [52] 本发明实施例第七方面提供一种系统，包括：
- [53] 如本发明第二方面任一实现方式所述的移动终端；以及
- [54] 如本发明第五方面任一实现方式所述的车载终端。
- [55] 实施本发明实施例，具有如下有益效果：
- [56] 通过发送加密后的指纹信息而并不发送车门开启指令到车载终端，从而可以为系统提供双层防护，第一层由加密算法构成的解密防护，第二层是由指纹信息的唯一性和复杂性构成的复杂计算防护，使得偷窃者无法破解或模拟移动终端发送给车载终端的信号，在实现利用用户移动终端解锁车门，方便用户使用的同时，保证了用户汽车的安全。

附图说明

- [57] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。
- [58] 图1是本发明开启车门的方法的第一实施例的流程示意图；
- [59] 图2是本发明开启车门的方法的第二实施例的流程示意图；
- [60] 图3是本发明开启车门的方法的第三实施例的流程示意图；
- [61] 图4是本发明移动终端的第一实施例的组成示意图；
- [62] 图5是本发明移动终端的第二实施例的组成示意图；
- [63] 图6是本发明车载终端的第一实施例的组成示意图；
- [64] 图7是本发明车载终端的第二实施例的组成示意图；
- [65] 图8是本发明系统的组成及交互流程示意图。

具体实施方式

- [66] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、

完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[67] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“第三”等是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或装置没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或装置固有的其它步骤或单元。

[68] 本发明实施例中的移动终端，是一种为用户提供语音和/或数据连通性的设备，其可以和车载终端建立无线数据连接，且具备指纹获取模组，可以采集用户指纹。该移动终端可以包括但不限于智能手机（如Android手机、iOS手机、Windows Phone手机等）、平板电脑、掌上电脑、笔记本电脑、移动互联网设备（Mobile Internet Devices, MID）或穿戴式设备等，上述移动终端仅是举例，而非穷举，包含但不限于上述移动终端。

[69] 本发明实施例中的车载终端，可以与移动终端建立无线数据连接，其可以与汽车上的中控集成设置，也可以独立设置，本发明实施例不作任何限定，在其存储器中可以预先存储用户的指纹信息和用户使用的移动终端的标识信息。其可以对汽车上的各个部位进行控制，如车门、大灯、雨刮器、空调、车窗和天窗等。

[70] 下面结合附图，对本发明实施例的内容进行描述。

[71] 请参照图1，为本发明开启车门的方法的第一实施例的流程示意图，在本实施例中，所述方法包括以下步骤：

[72] S101，移动终端与车载终端协商信息的加密算法和解密算法。

[73] 可选地，所述加密算法和解密算法为非对称密钥。

[74] 当然，如果安全性要求较低或者移动终端或车载终端的处理器能力较弱，也可以采用对称密钥，本发明实施例不作任何限定。

- [75] 其中，对称密钥加密也叫秘密/专用密钥加密（Secret Key Encryption, SKE），即发送和接收数据的双方必须使用相同的/对称的密钥对明文进行加密和解密运算。非对称密钥加密也叫公开密钥加密（Public Key Encryption, PKE），是指每个人都有一对唯一对应的密钥：公开密钥和私有密钥，公钥对外公开，私钥由个人秘密保存；用其中一把密钥来加密，就只能用另一把密钥来解密。发送数据的一方用另一方的公钥对发送的信息进行加密，然后由接受者用自己的私钥进行解密。公开密钥加密技术解决了密钥的发布和管理问题，是目前商业密码的核心。使用公开密钥技术，进行数据通信的双方可以安全地确认对方身份和公开密钥，提供通信的可鉴别性。
- [76] 可选地，所述加密算法和解密算法对应且同时动态变化。例如，可以协商多套对应的加解密算法，然后是每次使用时约定使用其中一套，移动终端可以通过发生算法标识信息来告知车载终端。这样动态变化的加解密算法可以进一步提升系统的安全性。
- [77] S102，获取用户指纹信息并采用协商的加密算法进行加密。
- [78] 可选地，在对用户指纹信息进行加密时，需要检测到与车载终端建立了无线数据连接且已获取到用户指纹信息。避免移动终端每次获取到指纹信息后都用该加密算法进行加密。或者也可以在终端打开特定应用的特定界面如汽车控制应用的控制界面后，才对获取到的指纹信息进行加密。
- [79] S103，将加密后的用户指纹信息发送给所述车载终端。
- [80] 其中，所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的指纹信息匹配并在匹配成功后开启汽车车门。。
- [81] 可选地，在发送信息之前，移动终端可以通过短距离无线通信方式与汽车控制终端建立无线数据连接。
- [82] 该短距离无线通信方式因为会用来传输加密后的指纹信息，因此要求保密性好，不扩散。例如，可以为蓝牙，近场通信(Near Field Communication, NFC)，无线保真（Wireless-Fidelity, Wi-Fi）等。本发明实施例不作限定。
- [83] 需要说明的是，由于一个家庭可能存在多个成员，因此可以在汽车的车载终端上预存多个用户的指纹信息，这样家庭成员中的所有用户都可以使用本实施例

中的方法来开启车门。

[84] 可选地，当车载终端对指纹信息的匹配成功之后，可以直接控制汽车车门开启，或者，也可以暂时不开启，等待接收移动终端发送的控制指令再控制车门开启。

[85] 需要说明的是，在本实施例中，具体描述了开启车门的控制，这是进入汽车使用汽车的基本步骤，但是本发明实施例所述的方法除了可以应用在控制车门开启之外，同样还可以应用在汽车其他部件的控制上，例如，移动终端上可以安装一个控制汽车的应用，其中可以模拟汽车的各个部件或者使用多个按键对应汽车的各个部件，用户可以在指纹匹配成功之后，通过移动终端控制汽车的各个部件如大灯、空调、车窗、音响等，本发明实施例不做任何限定。

[86] 可选地，如果匹配失败，则不会开启车门，车载终端也不会执行移动终端发送的控制指令。

[87] 若连续预设次数匹配失败，则所述移动终端发送给所述车载终端的信息在预设时长内被拒收，或者所述移动终端与所述车载终端的连接在预设时长内被断开。

[88] 例如，车载终端可以在连续4次指纹匹配失败后，在一个小时内断开与该移动终端的无线数据连接，或者也可以不断开无线数据连接，但是在一个小时内拒绝接收该移动终端发送的信息。或者还可以在连续匹配失败后引入报警机制以提醒车主。从而提防不法份子持续套取指纹、试图非法开启车门的不良企图，提升系统的安全性。

[89] 下面举例说明本实施例中所述的方法可以运用的场景：

[90] 场景一、用户走到汽车旁边，移动终端自动与车载终端进行蓝牙连接，用户打开移动终端上车门控制应用进入车门开启界面，将手指放在指纹识别模块上，移动终端获取用户指纹，加密该指纹并通过该蓝牙连接发送给车载终端，车载终端对该指纹解密，并与预存的用户指纹匹配，匹配通过，汽车车门解锁。

[91] 场景二、偷窃者在汽车旁破解车载终端的无线连接，例如蓝牙连接，发送窃取的指纹信息到车载终端，车载终端对接收到的指纹信息解密，由于没有匹配的加密算法，因此解密后得到乱码，匹配失败，多次尝试失败后，汽车断开无线

连接，并向车主发送通知。

[92] 在本实施例中，通过发送加密后的指纹信息而并不发送车门开启指令到车载终端，从而可以为系统提供双层防护，第一层由加密算法构成的解密防护，第二层是由指纹信息的唯一性和复杂性构成的复杂计算防护，使得偷窃者无法破解或模拟移动终端发送给车载终端的信号，在实现利用用户移动终端解锁车门，方便用户使用的同时，保证了用户汽车的安全。

[93] 需要说明的是，本发明实施例仅针对较常见的车门开启场景进行了详细描述，但是本实施例所述的方法除了应用于汽车车门开启之外，同样可以应用于其他车门开启的领域如智能门禁等，或者还可以应用于其他可以采用指纹加解密进行验证后进行控制的场景中。

[94] 请参照图2，为本发明开启车门的方法的第二实施例的流程示意图，在本实施例中，所述方法包括：

[95] S201，移动终端与车载终端协商信息的加密算法和解密算法。

[96] S202，获取用户指纹信息和所述移动终端的标识信息并采用协商的加密算法进行加密。

[97] S203，将加密后的所述用户指纹信息和所述标识信息发送给所述车载终端。

[98] 所述加密后的标识信息用于在所述车载终端采用协商的解密算法对其解密后与预存的标识信息匹配并在用户指纹信息与标识信息均匹配成功后开启汽车车门。

[99] 在本发明实施例中，增加了移动终端的标识信息匹配的过程，通过对移动终端标识信息的加密和解密，可以进一步提升系统的安全性。且预存的标识信息中可以包含用户家庭或朋友的多个移动终端的标识信息，结合预存的多个指纹信息，可以实现多个可靠用户的移动终端对车门的开启。

[100] 请参照图3，为本发明开启车门的方法的第三实施例的流程示意图，在本实施例中，所述方法包括以下步骤：

[101] S301，车载终端与移动终端协商信息的加密算法和解密算法。

[102] 可选地，所述加密算法和解密算法为非对称密钥。

[103] 当然，如果安全性要求较低或者移动终端或车载终端的处理器能力较弱，也可

以采用对称密钥，本发明实施例不作任何限定。

- [104] 其中，对称密钥加密也叫秘密/专用密钥加密（Secret Key Encryption, SKE），即发送和接收数据的双方必须使用相同的/对称的密钥对明文进行加密和解密运算。非对称密钥加密也叫公开密钥加密（Public Key Encryption, PKE），是指每个人都有一对唯一对应的密钥：公开密钥和私有密钥，公钥对外公开，私钥由个人秘密保存；用其中一把密钥来加密，就只能用另一把密钥来解密。发送数据的一方用另一方的公钥对发送的信息进行加密，然后由接受者用自己的私钥进行解密。公开密钥加密技术解决了密钥的发布和管理问题，是目前商业密码的核心。使用公开密钥技术，进行数据通信的双方可以安全地确认对方身份和公开密钥，提供通信的可鉴别性。
- [105] 可选地，所述加密算法和解密算法对应且同时动态变化。例如，可以协商多套对应的加解密算法，然后是每次使用时约定使用其中一套，移动终端可以通过发生算法标识信息来告知车载终端。这样动态变化的加解密算法可以进一步提升系统的安全性。
- [106] S302，接收所述移动终端发送的加密后的信息。
- [107] S303，采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配。
- [108] S304，若所述信息匹配成功，则开启汽车车门或者接收所述移动终端发送的控制指令，开启汽车车门。
- [109] 可选地，所述信息包括用户指纹信息。
- [110] 可选地，所述信息还包括所述移动终端的标识信息。
- [111] 可选地，若所述信息连续预设次数匹配失败，则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接。
- [112] 请参照图4，为本发明移动终端的第一实施例的组成示意图；在本实施例中，所述车载终端包括：
- [113] 协商单元100，设置为与车载终端协商信息的加密算法和解密算法；
- [114] 加密单元200，设置为获取用户指纹信息并采用协商的加密算法进行加密；
- [115] 发送单元300，设置为将加密后的用户指纹信息发送给所述车载终端，所述加

密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的指纹信息匹配并在匹配成功后开启汽车车门。

[116] 可选地，所述加密算法和解密算法为非对称密钥。

[117] 可选地，所述加密算法和解密算法对应且同时动态变化。

[118] 可选地，所述加密单元200还设置为：

[119] 获取所述移动终端的标识信息并采用协商的加密算法进行加密；

[120] 所述发送单元300还设置为：

[121] 将加密后的标识信息发送给所述车载终端，所述加密后的标识信息用于在所述车载终端采用协商的解密算法对其解密后与预存的标识信息匹配并在用户指纹信息与标识信息均匹配成功后开启汽车车门。

[122] 可选地，所述发送单元300还设置为：

[123] 在解密后的信息均匹配成功后，所述移动终端发送控制指令至所述车载终端，控制所述车载终端开启汽车车门。

[124] 以上协商单元100、加密单元200和发送单元300可以独立存在，也可以集成设置，协商单元100、加密单元200或发送单元300可以以硬件的形式独立于移动终端的处理器单独设置，且设置形式可以是微处理器的形式；也可以以硬件形式内嵌于该移动终端的处理器中，还可以以软件形式存储于该移动终端的存储器中，以便于该移动终端的处理器调用执行以上协商单元100、加密单元200和发送单元300对应的操作。

[125] 例如，在本发明移动终端的第一实施例（图4所示的实施例）中，加密单元200可以为该移动终端的处理器，而协商单元100和发送单元300的功能可以内嵌于该处理器中，也可以独立于处理器单独设置，也可以以软件的形式存储于存储器中，由处理器调用实现其功能。本发明实施例不做任何限制。以上处理器可以为中央处理单元（CPU）、微处理器、单片机等。

[126] 请参照图5，为本发明移动终端的第二实施例的组成示意图，在本实施例中，所述移动终端包括：

[127] 处理器110、存储器120、接口电路130和总线140，所述处理器110、存储器120、接口电路130通过总线140连接，其中，所述存储器120用于存储一组程序代码

，所述处理器110用于调用所述存储器120中存储的程序代码，执行以下操作：

- [128] 与车载终端协商信息的加密算法和解密算法；
- [129] 获取用户指纹信息并采用协商的加密算法进行加密；
- [130] 将加密后的用户指纹信息发送给所述车载终端，所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的用户指纹信息匹配并在匹配成功后开启汽车车门。
- [131] 可选地，所述加密算法和解密算法为非对称密钥。
- [132] 可选地，所述加密算法和解密算法对应且同时动态变化。
- [133] 可选地，所述处理器110还用于：
- [134] 获取所述移动终端的标识信息并采用协商的加密算法进行加密；
- [135] 在将加密后的所述用户指纹信息发送给所述车载终端时，还包括：
- [136] 将加密后的标识信息发送给所述车载终端，所述加密后的标识信息用于在所述车载终端采用协商的解密算法对其解密后与预存的标识信息匹配并在用户指纹信息与标识信息均匹配成功后开启汽车车门。
- [137] 可选地，所述处理器110还用于：
- [138] 在解密后的信息均匹配成功后，所述移动终端发送控制指令至所述车载终端，控制所述车载终端开启汽车车门。
- [139] 请参照图6，为本发明车载终端的第一实施例的组成示意图；在本实施例中，所述车载终端包括：
- [140] 协商单元400，设置为与移动终端协商信息的加密算法和解密算法；
- [141] 接收单元500，设置为接收所述移动终端发送的加密后的信息；
- [142] 解密单元600，设置为采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；
- [143] 开启单元700，若所述信息匹配成功，则开启汽车车门；
- [144] 或者所述接收单元500还设置为接收所述移动终端发送的控制指令，指示所述开启单元700开启汽车车门；
- [145] 其中，所述信息包括用户指纹信息。
- [146] 可选地，所述信息还包括所述移动终端的标识信息。

- [147] 可选地，所述加密算法和解密算法为非对称密钥。
- [148] 可选地，所述加密算法和解密算法对应且同时动态变化。
- [149] 可选地，所述接收单元500还设置为：
- [150] 若所述信息连续预设次数匹配失败，则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接。
- [151] 以上协商单元400、接收单元500、解密单元600和开启单元700可以独立存在，也可以集成设置，协商单元400、接收单元500、解密单元600或开启单元700可以以硬件的形式独立于车载终端的处理器单独设置，且设置形式可以是微处理器的形式；也可以以硬件形式内嵌于该车载终端的处理器中，还可以以软件形式存储于该车载终端的存储器中，以便于该车载终端的处理器调用执行以上协商单元400、接收单元500、解密单元600和开启单元700对应的操作。
- [152] 例如，在本发明车载终端的第一实施例（图6所示的实施例）中，解密单元600可以为该车载终端的处理器，而协商单元400、接收单元500和开启单元700的功能可以内嵌于该处理器中，也可以独立于处理器单独设置，也可以以软件的形式存储于存储器中，由处理器调用实现其功能。本发明实施例不做任何限制。以上处理器可以为中央处理单元（CPU）、微处理器、单片机等。
- [153] 请参照图7，为本发明车载终端的第二实施例的组成示意图，在本实施例中，所述车载终端包括：
- [154] 处理器210、存储器220、接口电路230和总线240，所述处理器210、存储器220、接口电路230通过总线240连接，其中，所述存储器220用于存储一组程序代码，所述处理器210用于调用所述存储器220中存储的程序代码，执行以下操作：
- [155] 与移动终端协商信息的加密算法和解密算法；
- [156] 接收所述移动终端发送的加密后的信息；
- [157] 采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；
- [158] 若所述信息匹配成功，则开启汽车车门或者接收所述移动终端发送的控制指令，开启汽车车门；
- [159] 其中，所述信息包括用户指纹信息。
- [160] 可选地，所述加密算法和解密算法为非对称密钥。

- [161] 可选地,所述加密算法和解密算法对应且同时动态变化。
- [162] 可选地,所述信息还包括所述移动终端的标识信息。
- [163] 可选地,所述处理器110还用于:
- [164] 若所述信息连续预设次数匹配失败,则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接。
- [165] 请参照图8,为本发明实施例系统的组成及交互流程示意图;在本实施例中,所述系统包括:
- [166] 移动终端10和车载终端20;
- [167] 其中,移动终端10用于与车载终端协商信息的加密算法和解密算法,获取用户的信息并采用协商的加密算法进行加密,将加密后的信息发送给所述车载终端。
- [168] 车载终端,用于与所述移动终端协商信息的加密算法和解密算法;接收所述移动终端发送的加密后的信息;采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配;若信息匹配成功,则开启汽车车门或者接收所述移动终端发送的控制指令,控制汽车车门开启;若信息连续预设次数匹配失败,则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接;
- [169] 其中,所述信息包括用户指纹信息,或者包括用户指纹信息和所述移动终端的标识信息
- [170] 具体交互流程如下:
- [171] S801,移动终端与汽车控制终端协商信息的加密算法和解密算法。
- [172] S802,移动终端通过短距离无线通信方式与汽车控制终端建立数据连接。
- [173] S803,移动终端获取用户指纹信息。
- [174] S804,移动终端采用协商的加密算法加密该指纹信息。
- [175] S805,移动终端通过建立好的数据连接发送该加密后的指纹信息。
- [176] S806,利用协商的解密算法对该加密后的指纹信息进行解密。
- [177] S807,得到解密后的指纹信息后,与预存的用户指纹信息进行匹配。
- [178] S808,当匹配成功时,接收移动终端对汽车的控制指令开启车门,或直接开启

车门。

[179] 可选地，在进行加解密和匹配时还可以增加移动终端的标识信息以进一步提升系统安全性，且在连续匹配失败后，车载终端20可以拒收移动终端10发送的信息或断开与移动终端10的连接，或者还可以在连续匹配失败后引入报警机制以提醒车主。

[180] 需要说明的是，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它实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置实施例而言，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。

[181] 通过上述实施例的描述，本发明具有以下优点：

[182] 通过发送加密后的指纹信息而并不发送车门开启指令到车载终端，从而可以为系统提供双层防护，第一层由加密算法构成的解密防护，第二层是由指纹信息的唯一性和复杂性构成的复杂计算防护，使得偷窃者无法破解或模拟移动终端发送给车载终端的信号，在实现利用用户移动终端解锁车门，方便用户使用的同时，保证了用户汽车的安全。

[183] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，简称ROM）或随机存储记忆体（Random Access Memory，简称RAM）等。

[184] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

权利要求书

- [权利要求 1] 一种开启车门的方法，其特征在于，包括：
移动终端与车载终端协商信息的加密算法和解密算法；
获取用户指纹信息并采用协商的加密算法进行加密；
将加密后的用户指纹信息发送给所述车载终端，所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的指纹信息匹配并在匹配成功后开启汽车车门。
- [权利要求 2] 如权利要求1所述的方法，其特征在于，所述加密算法和解密算法为非对称密钥。
- [权利要求 3] 如权利要求1所述的方法，其特征在于，所述加密算法和解密算法对应且同时动态变化。
- [权利要求 4] 如权利要求1所述的方法，其特征在于，在获取用户指纹信息并采用协商的加密算法进行加密时，还包括：
获取所述移动终端的标识信息并采用协商的加密算法进行加密；
在将加密后的所述用户指纹信息发送给所述车载终端时，还包括：
将加密后的标识信息发送给所述车载终端，所述加密后的标识信息用于在所述车载终端采用协商的解密算法对其解密后与预存的标识信息匹配并在用户指纹信息与标识信息均匹配成功后开启汽车车门。
- [权利要求 5] 如权利要求1-4任一项所述的方法，其特征在于，还包括：
在解密后的信息均匹配成功后，所述移动终端发送控制指令至所述车载终端，控制所述车载终端开启汽车车门。
- [权利要求 6] 一种移动终端，其特征在于，包括：
协商单元，设置为与车载终端协商信息的加密算法和解密算法；
加密单元，设置为获取用户指纹信息并采用协商的加密算法进行加密；
发送单元，设置为将加密后的用户指纹信息发送给所述车载终端

，所述加密后的用户指纹信息用于在所述车载终端采用协商的解密算法对其解密后与预存的指纹信息匹配并在匹配成功后开启汽车车门。

[权利要求 7] 如权利要求6所述的移动终端，其特征在于，所述加密算法和解密算法为非对称密钥。

[权利要求 8] 如权利要求6所述的移动终端，其特征在于，所述加密算法和解密算法对应且同时动态变化。

[权利要求 9] 如权利要求6所述的移动终端，其特征在于，所述加密单元还设置为：

获取所述移动终端的标识信息并采用协商的加密算法进行加密；

所述发送单元还设置为：

将加密后的标识信息发送给所述车载终端，所述加密后的标识信息用于在所述车载终端采用协商的解密算法对其解密后与预存的标识信息匹配并在用户指纹信息与标识信息均匹配成功后开启汽车车门。

[权利要求 10] 如权利要求6-9任一项所述的移动终端，其特征在于，所述发送单元还设置为：

在解密后的信息均匹配成功后，所述移动终端发送控制指令至所述车载终端，控制所述车载终端开启汽车车门。

[权利要求 11] 一种开启车门的方法，其特征在于，包括：

车载终端与移动终端协商信息的加密算法和解密算法；

接收所述移动终端发送的加密后的信息；

采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；

若所述信息匹配成功，则开启汽车车门或者接收所述移动终端发送的控制指令，开启汽车车门；

其中，所述信息包括用户指纹信息。

[权利要求 12] 如权利要求11所述的方法，其特征在于，所述加密算法和解密算

法为非对称密钥。

- [权利要求 13] 如权利要求11所述的方法，其特征在于，所述加密算法和解密算法对应且同时动态变化。
- [权利要求 14] 如权利要求11所述的方法，其特征在于，所述信息还包括所述移动终端的标识信息。
- [权利要求 15] 如权利要求11-14任一项所述的方法，其特征在于，若所述信息连续预设次数匹配失败，则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接。
- [权利要求 16] 一种车载终端，其特征在于，包括：
协商单元，设置为与移动终端协商信息的加密算法和解密算法；
接收单元，设置为接收所述移动终端发送的加密后的信息；
解密单元，设置为采用协商的解密算法对接收到的信息进行解密并与预存的信息进行匹配；
开启单元，若所述信息匹配成功，则开启汽车车门；
或者所述接收单元还设置为接收所述移动终端发送的控制指令，指示所述开启单元开启汽车车门；
其中，所述信息包括用户指纹信息。
- [权利要求 17] 如权利要求16所述的车载终端，其特征在于，所述加密算法和解密算法为非对称密钥。
- [权利要求 18] 如权利要求16所述的车载终端，其特征在于，所述加密算法和解密算法对应且同时动态变化。
- [权利要求 19] 如权利要求16所述的车载终端，其特征在于，所述信息还包括所述移动终端的标识信息。
- [权利要求 20] 如权利要求16-19任一项所述的车载终端，其特征在于，所述接收单元还设置为：
若所述信息连续预设次数匹配失败，则在预设时长内拒收所述移动终端发送的信息或者在预设时长内断开与所述移动终端的连接。

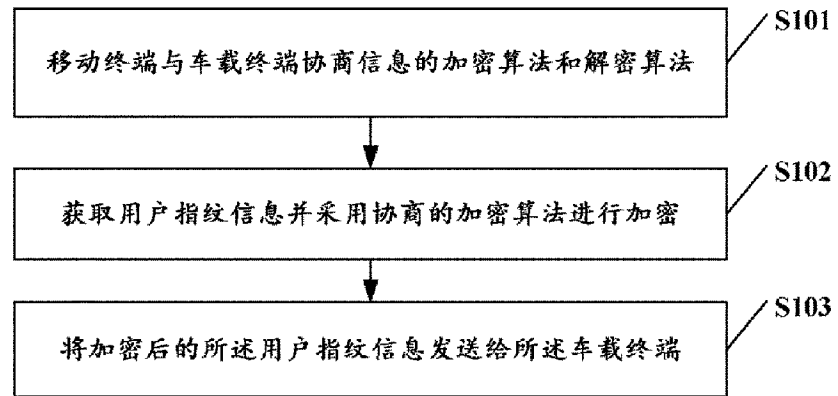
[权利要求 21]

一种系统，其特征在于，包括：

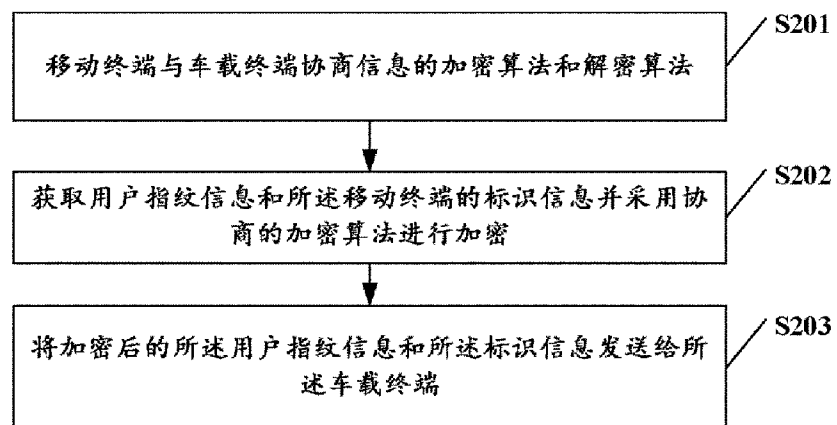
如权利要求6-10任一项所述的移动终端；以及

如权利要求16-20任一项所述的车载终端。

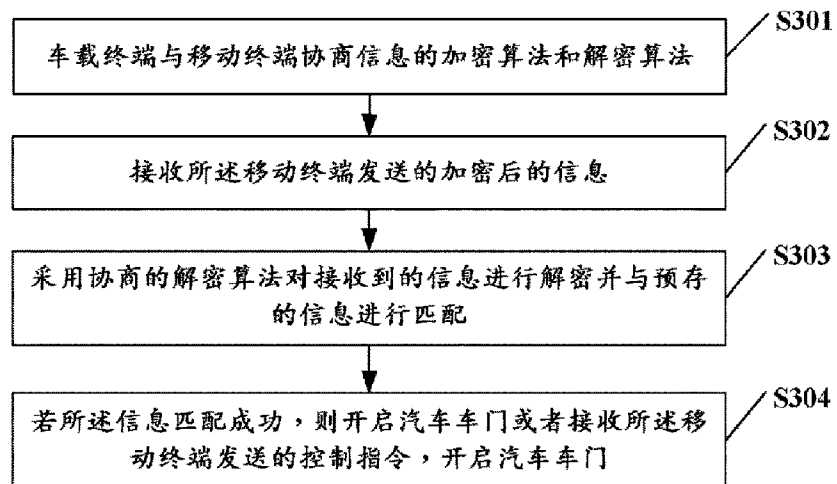
[Fig. 1]



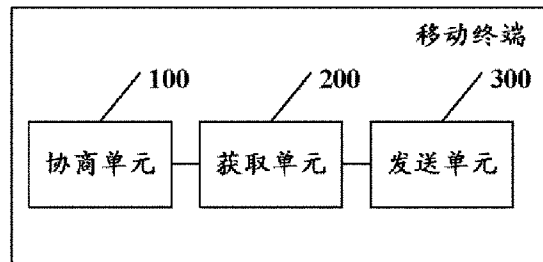
[Fig. 2]



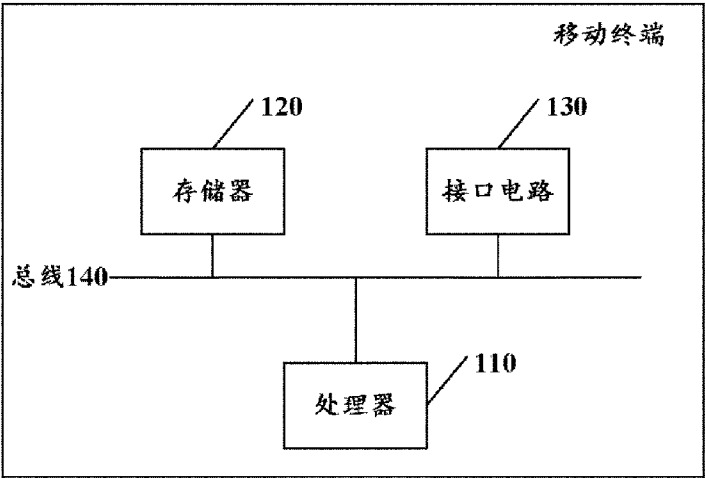
[Fig. 3]



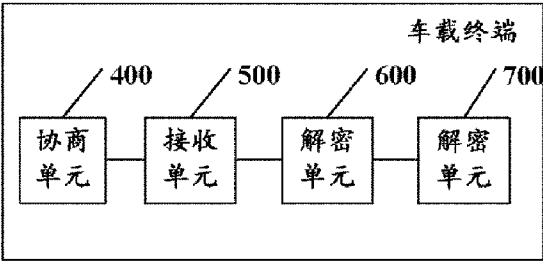
[Fig. 4]



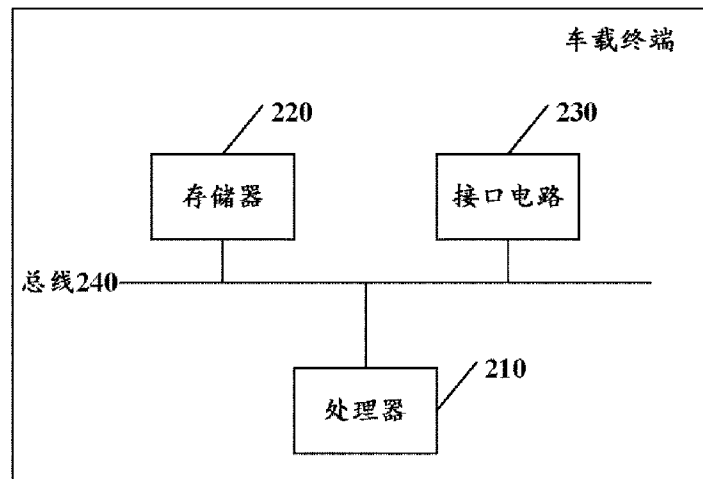
[Fig. 5]



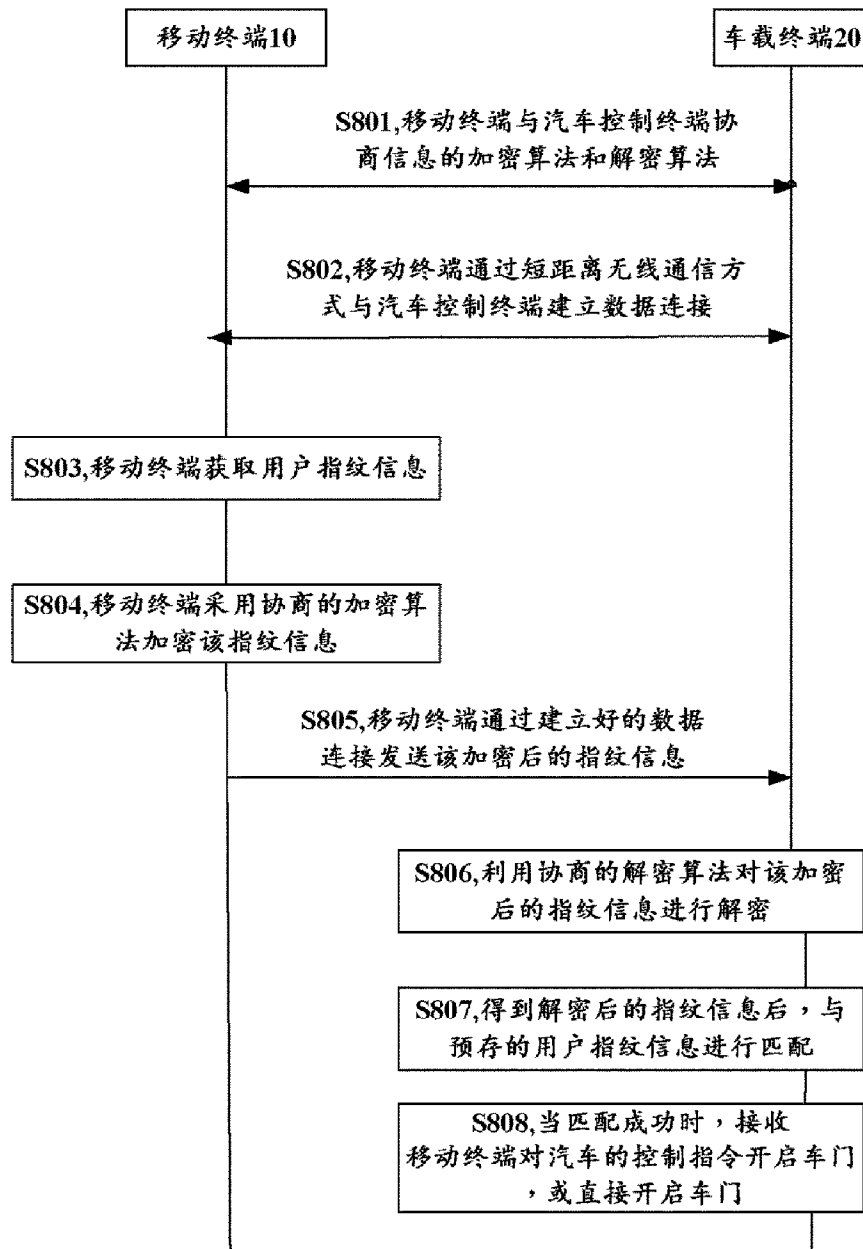
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/113399

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i; B60R 25/20 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 车, 锁, 加密, 解密, 加解密, 指纹, car, lock, encrypt, decrypt, encipher, decipher, fingerprint

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102682506 A (BEIJING HUADA INFOSEC TECHNOLOGY CO., LTD.), 19 September 2012 (19.09.2012), description, paragraphs [0022]-[0051]	1-21
X	CN 102936980 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.), 20 February 2013 (20.02.2013), description, paragraphs [0044]-[0099]	1-21
A	CN 105227516 A (ZTE CORP.), 06 January 2016 (06.01.2016), entire document	1-21
A	CN 105701896 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 22 June 2016 (22.06.2016), entire document	1-21

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	
“A” document defining the general state of the art which is not considered to be of particular relevance	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E” earlier application or patent but published on or after the international filing date	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O” document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
19 July 2017

Date of mailing of the international search report
07 September 2017

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
GONG, Yu
Telephone No. (86-10) 62413917

International application No.
PCT/CN2016/113399

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2016/113399

A. 主题的分类

H04W 12/04(2009.01)i; B60R 25/20(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; B60R

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPODOC: 车, 锁, 加密, 解密, 加解密, 指纹, car, lock, encrypt, decrypt, encipher, decipher, fingerprint

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 102682506 A (北京华大信安科技有限公司) 2012年 9月 19日 (2012 - 09 - 19) 说明书第[0022]-[0051]段	1-21
X	CN 102936980 A (北京小米科技有限责任公司) 2013年 2月 20日 (2013 - 02 - 20) 说明书第[0044]-[0099]段	1-21
A	CN 105227516 A (中兴通讯股份有限公司) 2016年 1月 6日 (2016 - 01 - 06) 全文	1-21
A	CN 105701896 A (宇龙计算机通信科技深圳有限公司) 2016年 6月 22日 (2016 - 06 - 22) 全文	1-21

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2017年 7月 19日

国际检索报告邮寄日期

2017年 9月 7日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

巩瑜

电话号码 (86-10)62413917

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/113399

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	102682506	A	2012年 9月 19日	无	
CN	102936980	A	2013年 2月 20日	无	
CN	105227516	A	2016年 1月 6日	WO 2015180261 A1	2015年 12月 3日
CN	105701896	A	2016年 6月 22日	无	