(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
2019 年 1 月 10 日 (10.01.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/007252 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *G07C 9/00* (2006.01)
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2018/093269

(22) 国际申请日: 2018 年 6 月 28 日 (28.06.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710538445.9 2017年7月4日 (04.07.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 罗金华 (LUO, Jinhua); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, JO, 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,

(54) **Title:** CONTROL METHOD AND APPARATUS

(54) **发明名称**: 一种控制方法及装置

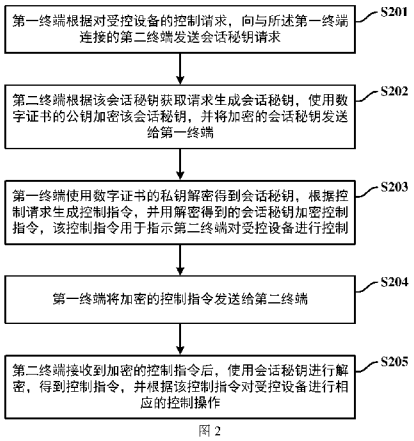

图 2

S201 A first terminal sends a session key acquisition request to a second terminal connected to the first terminal according to a control request of a controlled device

S202 The second terminal generates a session key according to the session key acquisition request, uses a public key of a digital certificate to encrypt the session key, and sends the encrypted session key to the first terminal

S203 The first terminal uses a private key of the digital certificate for decryption so as to obtain the session key, generates a control instruction according to the control request, and encrypts the control instruction with the decrypted session key, the control instruction being used for instructing the second terminal to control the controlled device

S204 The first terminal sends the encrypted control instruction to the second terminal

S205 After receiving the encrypted control instruction, the second terminal uses the session key for decryption so as to obtain a control instruction, and performs corresponding control operations on the controlled device according to the control instruction

(57) Abstract: Disclosed are a control method and apparatus. In the present application, a mobile terminal sends a session key acquisition request to a control terminal connected to the mobile terminal according to a door lock control request; the control terminal generates a session key according to the session key acquisition request, uses a public key of a digital certificate to encrypt the session key, and sends the encrypted session key to the mobile terminal; the mobile terminal uses a private key of the digital certificate for decryption so as to obtain the session key, generates a door lock control instruction according to the door lock control request, encrypts a door lock control instruction by using the session key, and sends the encrypted door lock control instruction to the control terminal; and the control terminal uses the session key to decrypt the door lock control instruction, and performs a door lock control operation according to the decrypted door lock control instruction. By applying the present invention, the security of the control operation can be improved.

(57) 摘要: 本申请公开了一种控制方法及装置。本申请中，移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求；控制终端根据会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述移动终端；移动终端使用数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，使用会话秘钥加密门锁控制指令，并将加密的门锁控制指令发送给所述控制终端；控制终端使用所述会话秘钥解密得到所述门锁控制指令，根据解密得到的门锁控制指令进行门锁控制操作。采用本发明可提高控制操作的安全性。

WO 2019/007252 A1

[见续页]

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, 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))。

一种控制方法及装置

本申请要求2017年07月04日递交的申请号为201710538445.9、发明名称为“一种控制方法及装置”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

本申请涉及通信技术领域，尤其涉及一种控制方法及装置。

背景技术

随着智能移动终端（比如智能手机）的普及，在越来越多的场景下，可使用智能移动终端对一些设备进行控制。

一个具体的例子是，可使用智能手机控制车辆车门的开关。在该例子中，智能手机与车辆中设置的车载终端建立蓝牙链路，并通过蓝牙链路向该车载终端发送开车门的控制指令，车载终端根据该控制指令打开车门。

在上述过程中，如果开车门的指令为明文指令，则会到来很大的安全隐患。比如，若该指令被非法智能手机捕获，则该非法智能手机即可向该车辆的车载终端发送打开车门的指令，并触发该车载终端打开车门。

发明内容

本申请实施例公开了一种控制方法及装置，用以提高控制操作的安全性。

第一方面，提供一种控制方法，包括：

移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求；

所述控制终端根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述移动终端；

所述移动终端使用所述数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，使用所述会话秘钥加密门锁控制指令，并将加密的门锁控制指令发送给所述控制终端；

所述控制终端使用所述会话秘钥解密得到所述门锁控制指令，根据解密得到的门锁控制指令进行门锁控制操作。

第二方面，提供一种控制方法，包括：

移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求；

所述移动终端接收所述控制终端根据所述秘钥会话获取请求发送的会话秘钥，所述会话秘钥使用数字证书的公钥进行加密；

所述移动终端使用所述数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，并用所述会话秘钥加密所述门锁控制指令；

所述移动终端将加密的门锁控制指令发送给所述控制终端，所述门锁控制指令用于指示所述控制终端进行相应门锁控制操作。

可选地，所述会话秘钥获取请求中包括所述数字证书。

可选地，所述移动终端中包括第一应用和第二应用，所述第二应用为可信应用；所述移动终端使用所述数字证书的私钥解密得到所述会话秘钥，并用所述会话秘钥加密门锁控制指令，包括：所述第一应用将接收到的加密的会话秘钥发送给所述第二应用；所述第二应用从所述移动终端的安全存储区获取所述数字证书的私钥，并使用获取到的私钥解密得到会话秘钥；所述移动终端将加密的门锁控制指令发送给所述控制终端，包括：所述第二应用使用解密得到的会话秘钥加密门锁控制指令，并将加密的门锁控制指令发送给第一应用；所述第一应用将加密的门锁控制指令发送给所述控制终端。

可选地，所述第二应用从安全存储区获取所述数字证书的私钥，包括：所述第二应用从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；所述第二应用从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

可选地，所述移动终端中包括第一应用和第二应用，所述第二应用为可信应用；所述方法还包括：所述第二应用生成数字证书的私钥，从所述移动终端的只读存储区读取设备秘钥，使用所述设备秘钥加密所述私钥，并将加密的私钥存储到所述移动终端的安全存储区中；所述第二应用向第一应用发送数字证书请求，所述第一应用将所述数字证书请求发送给认证服务器；所述第二应用接收所述认证服务器根据所述数字证书请求发送的数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息。

可选地，移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求，包括：移动终端接收用户通过门锁控制应用的用户界面提交的门锁控制请求，确定是否与所述门锁控制应用关联的控制终端之间建立连接；若已建立连接，则通过所述连接向所述控制终端发送会话秘钥获取请求。

可选地，所述连接为蓝牙连接。

第三方面，提供一种控制方法，包括：

控制终端接收与所述控制终端连接的移动终端发送的会话秘钥获取请求；

所述控制终端根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述移动终端；

所述控制终端接收所述移动终端发送的加密的门锁控制指令，使用所述会话秘钥解密得到所述门锁控制指令，并根据解密得到的门锁控制指令进行相应门锁控制操作。

可选地，所述会话秘钥获取请求中包括数字证书，所述方法还包括：所述控制终端向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；所述控制终端接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

可选地，所述控制终端和所述移动终端通过蓝牙连接。

第四方面，提供一种控制方法，包括：

第一终端根据对受控设备的控制请求，向与所述第一终端连接的第二终端发送会话秘钥请求；

所述第一终端接收所述第二终端根据所述会话秘钥获取请求返回的会话秘钥，所述会话秘钥使用数字证书的公钥进行加密；

所述第一终端使用所述数字证书的私钥解密得到所述会话秘钥，根据所述控制请求生成控制指令，并用所述会话秘钥加密所述控制指令；

所述第一终端将加密的控制指令发送给所述第二终端，所述控制指令用于指示所述第二终端对所述受控设备进行相应的控制操作。

可选地，所述第一终端中包括第一应用和第二应用，所述第二应用为可信应用；所述第一终端使用所述数字证书的私钥解密得到所述会话秘钥，并用所述会话秘钥加密所述控制指令，包括：所述第一应用将接收到的加密的会话秘钥发送给所述第二应用；所述第二应用从所第一动终端的安全存储区获取所述数字证书的私钥，并使用获取到的私钥解密得到会话秘钥；所述移动终端将加密的控制指令发送给所述第二终端，包括：所述第二应用使用解密得到的会话秘钥加密控制指令，并将加密的控制指令发送给第一应用；所述第一应用将加密的控制指令发送给所述第二终端。

可选地，所述第二应用从安全存储区获取所述数字证书的私钥，包括：所述第二应

用从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；所述第二应用从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

第五方面，提供一种控制方法，包括：

第二终端接收与所述第二终端连接的第一终端发送的会话秘钥获取请求；

所述第二终端根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述第一终端；

所述第二终端接收所述第一终端发送的加密的控制指令，使用所述会话秘钥解密得到所述控制指令，并根据解密得到的控制指令对所述受控设备进行相应的控制操作。

可选地，所述会话秘钥获取请求中包括数字证书，所述方法还包括：所述第二终端向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；所述而终端接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

第六方面，提供一种移动终端，包括：第一应用模块、第二应用模块以及收发器；

第一应用模块，用于根据门锁控制请求，通过所述收发器向与所述移动终端连接的控制终端发送会话秘钥获取请求；以及，通过所述收发器接收所述控制终端根据所述秘钥会话获取请求发送的会话秘钥，并将所述加密的会话秘钥发送给第二应用模块；所述会话秘钥使用数字证书的公钥进行加密；

第二应用模块，用于使用所述数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，用所述会话秘钥加密所述门锁控制指令，并将加密的门锁控制指令发送给所述第一应用模块；

所述第一应用模块还用于，通过所述收发器将加密的门锁控制指令发送给所述控制终端，所述门锁控制指令用于指示所述控制终端进行相应门锁控制操作。

可选地，所述会话秘钥获取请求中包括所述数字证书。

可选地，所述第二应用模块具体用于：从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

可选地，所述第二应用模块还用于：生成数字证书的私钥，从所述移动终端的只读存储区读取设备秘钥，使用所述设备秘钥加密所述私钥，并将加密的私钥存储到所述移

动终端的安全存储区中，向第一应用发送数字证书请求；所述第一应用模块还用于：通过所述收发器将所述数字证书请求发送给认证服务器，通过所述收发器接收所述认证服务器根据所述数字证书请求发送的数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息。

可选地，所述第一应用模块具体用于：接收用户通过门锁控制应用的用户界面提交的门锁控制请求，确定是否与所述门锁控制应用关联的控制终端之间建立连接；所述收发器具体用于：若已建立连接，则通过所述连接向所述控制终端发送会话秘钥获取请求。

可选地，所述连接为蓝牙连接。

第七方面，提供一种控制终端，包括：会话秘钥处理模块、控制指令处理模块和收发器；

会话秘钥处理模块，用于通过所述收发器接收与所述控制终端连接的移动终端发送的会话秘钥获取请求，根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并通过所述收发器将加密的会话秘钥发送给所述移动终端；

控制指令处理模块，用于通过所述收发器接收所述移动终端发送的加密的门锁控制指令，使用所述会话秘钥解密得到所述门锁控制指令，并根据解密得到的门锁控制指令进行相应门锁控制操作。

可选地，所述会话秘钥获取请求中包括数字证书，所述控制终端中还包括：证书验证模块，用于通过所述收发器向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；以及，通过所述收发器接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

可选地，所述连接为蓝牙连接。

第八方面，提供一种终端，包括：第一应用模块、第二应用模块以及收发器；

第一应用模块，用于根据对受控设备的控制请求，通过所述收发器向与所述第一终端连接的第二终端发送会话秘钥获取请求；以及，通过所述收发器接收所述第二终端根据所述秘钥会话获取请求发送的会话秘钥，并将所述加密的会话秘钥发送给第二应用模块；所述会话秘钥使用数字证书的公钥进行加密；

第二应用模块，用于使用所述数字证书的私钥解密得到所述会话秘钥，根据所述控制请求生成控制指令，用所述会话秘钥加密所述控制指令，并将加密的控制指令发送给所述第一应用模块；

所述第一应用模块还用于，通过所述收发器将加密的控制指令发送给所述控制终端，所述控制指令用于指示所述第二终端对所述受控设备进行相应控制操作。

可选地，所述第二应用模块具体用于：从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

第九方面，提供一种终端，包括：会话秘钥处理模块、控制指令处理模块和收发器；

会话秘钥处理模块，用于通过所述收发器接收与所述第二终端连接的第一终端发送的会话秘钥获取请求，根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并通过所述收发器将加密的会话秘钥发送给所述第一终端；

控制指令处理模块，用于通过所述收发器接收所述第一终端发送的加密的控制指令，使用所述会话秘钥解密得到所述控制指令，并根据解密得到的控制指令对受控设备进行相应控制操作。

可选地，所述会话秘钥获取请求中包括数字证书，所述第二终端中还包括：证书验证模块，用于通过所述收发器向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；以及，通过所述收发器接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

第十方面，提供一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行上述第二方面中任一项所述的方法。

第十一方面，提供一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行上述第三方面中任一项所述的方法。

第十二方面，提供一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行上述第四方面中任一项所述的方法。

第十三方面，提供一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行上述第五方面中任一项所述的方法。

第十四方面，提供一种装置，包括：一个或多个处理器；以及一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被所述一个或多个处理器执行时，使得所述装置执行上述第二方面或第四方面中任一项所述的方法。

第十五方面，提供一种装置，包括：一个或多个处理器；以及一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被所述一个或多个处理器执行时，使得

所述装置执行上述第三方面或第五方面中任一项所述的方法。

本申请的上述实施例中，第一终端（比如移动终端）在需要对受控设备（比如门锁）进行控制时，向与该第一终端连接的第二终端（比如控制终端）发送会话秘钥获取请求，第二终端生成会话秘钥并使用数字证书的私钥进行加密后发送给第一终端，第一终端使用数字证书的私钥解密得到会话秘钥，用该会话秘钥加密控制指令，并将加密的控制指令发送给该第二终端，以使该第二终端根据该控制指令对受控设备进行相应的控制操作。由于一方面第二终端用数字证书的公钥对会话秘钥进行加密，另一方面，第一终端用会话秘钥对控制指令进行加密，保证了控制指令传输的安全性。

附图说明

图 1 示例性地示出了本申请实施例所使用的系统架构示意图；

图 2 示例性地示出了本申请实施例提供的一种对受控设备进行控制的流程示意图；

图 3 示例性地示出了本申请实施例提供的数字证书的申请流程示意图；

图 4 示例性地示出了本申请实施例提供的 TEE 架构示意图；

图 5 示例性地示出了基于 TEE 技术实现的对受控设备进行控制的流程示意图；

图 6 示例性地示出了基于 TEE 技术实现的数字证书申请的流程示意图；

图 7 示例性地示出了本申请实施例提供的第一终端的结构示意图；

图 8 示例性地示出了本申请实施例提供的第二终端的结构示意图；

图 9 示例性地示出了本申请实施例提供的装置的结构示意图；

图 10 示例性地示出了本申请另一实施例提供的装置的结构示意图。

具体实施方式

虽然本申请的概念易于进行各种修改和替代形式，但是其具体实施例已经通过附图中的示例示出并且将在本文中详细描述。然而，应当理解，没有意图将本申请的概念限制为所公开的特定形式，而是相反，意图是覆盖与本申请以及所附权利要求一致的所有修改、等同物和替代物。

说明书中对“一个实施例”、“实施例”、“说明性实施例”等的引用，指示所描述的实施例可包括特定特征、结构或特性，但是每个实施例可以或可以不必包括特定特征、结构或特性。此外，这样的短语不一定指的是相同的实施例。进一步地，认为在本领域技术人员的知识范围内，当结合实施例描述特定特征、结构或特性时，结合无论是

否明确描述的其它实施例影响这样的特征，结构或特性。另外，应当理解，以“A，B和C中的至少一个”的形式包括在列表中的项目可以表示（A）;（B）;（C）;（A和B）;（A和C）;（B和C）;或（A，B和C）。类似地，以“A，B或C中的至少一个”的形式列出的项目可以表示（A）;（B）;（C）;（A和B）;（A和C）;（B和C）或（A，B和C）。

在一些情况下，所公开的实施例可以在硬件、固件、软件或其任何组合中实现。所公开的实施例还可以被实现为由一个或多个暂时性或非暂时性机器可读（例如，计算机可读）存储介质携带或存储的指令，其可以由一个或多个处理器读取和执行。机器可读存储介质可以体现为用于以机器可读形式（例如，易失性或非易失性存储器、介质盘或其他介质）存储或传输信息的任何存储设备，机制或其他物理结构的设备）。

在附图中，一些结构或方法特征可以以特定布置和/或顺序示出。然而，应当理解，可能不需要这样的具体布置和/或排序。相反，在一些实施例中，这些特征可以以与说明性附图中所示不同的方式和/或顺序来布置。另外，在特定图中包括结构或方法特征并不意味着暗示这种特征在所有实施例中都是需要的，并且在一些实施例中可以不包括或可以与其他特征组合。

下面结合附图对本申请实施例进行详细描述。

图1示例性地示出了本申请实施例所使用的系统架构。如图所示，该架构中可包括：第一终端101、第二终端102、受控设备103，以及认证服务器104。其中，第一终端101和第二终端102具有无线通信功能。

认证服务器104主要用于数字证书的发放和管理，第二终端102可使用数字证书的公钥加密其所生成的会话秘钥并发送给第一终端101，第一终端101可使用该数字证书的私钥解密得到会话秘钥，用会话秘钥加密控制指令发送给第二终端102，第二终端102可使用会话秘钥解密得到控制指令，并根据该控制指令对受控设备104进行控制操作。

第一终端101和第二终端102之间可建立通信链路，第一终端101可通过该通信链路向第二终端102发送数字证书，第二终端102可通过该通信链路向第一终端101发送会话秘钥，以使第一终端101使用该会话秘钥加密控制指令，并将加密的控制指令通过该通信链路发送给第二终端 102。所述通信链路可以是基于蓝牙（Bluetooth）通信协议的无线链路，也可以基于其他通信协议的链路，所述其他无线通信协议包括但不限于：Wi-Fi、以太网（ethernet）、专用短程通信技术（Dedicated Short Range Communications，简称DSRC）。

第二终端 102 与受控设备 103 之间电性连接，第二终端 102 可根据第一终端 101 发送的控制指令对受控设备 103 进行相应控制操作。

第一终端 101 和第二终端 102 分别与认证服务器 104 通过网络 105 进行信息交互。第一终端 101 可从认证服务器 104 获取数字证书，第二终端 102 可请求认证服务器 104 对数字证书进行有效性验证。可选地，所述网络 105 可以是无线蜂窝网络，比如长期演进（Long Term Evolution，简称 LTE）系统或其演进系统。

可选地，第一终端 101 可以是移动终端，具体地，可以是智能手机、平板电脑、笔记本电脑、个人数字助理（Personal Digital Assistant，简称 PDA）、智能穿戴设备或类似设备。第二终端 102 可以是控制终端，比如车载终端等设备，在家居环境下，控制终端还可以是路由器、智能音响等各类智能设备。在一个例子中，第一终端 101 为智能终端，比如智能手机；第二终端 102 为车载终端，该车载终端是汽车中用于通信的一个设备，一般支持蓝牙、3G/4G、Wi-Fi、DSRC 等通信技术，也作为待机唤醒设备；受控设备 103 为门锁装置，比如车辆的门锁控制装置，用于控制车门的开启和关闭。

可选地，为了提高安全性，第一终端 101 可以采用可信执行环境（Trusted Execution Enviroment，简称 TEE）硬件技术实现，认证服务器 104 可以是可信服务器。

基于上述架构，本申请实施例利用数字证书的秘钥对机制，对会话秘钥进行加解密，而会话秘钥用于对第一终端发送给第二终端的控制指令进行加解密，从而提高了控制指令传输的安全性，进而提高了对受控设备进行控制操作的安全性。其中，数字证书是经数字签名的电子文件，其中可包含公开密钥（即公钥）、拥有者信息以及公钥。数字证书可只在特定的时间段内有效。

基于图 1 所示的系统架构，图 2 示例性地示出了本申请实施例提供的一种对受控设备进行控制的流程示意图。如图所示，该流程可包括：

S201：第一终端根据对受控设备的控制请求，向与所述第一终端连接的第二终端发送会话秘钥请求。

该步骤中，第一终端可根据用户发起的对受控设备进行控制操作的请求，生成所述会话秘钥获取请求，并将该会话秘钥获取请求发送给第二终端。用户可通过多种方式发起对受控设备进行控制操作的请求，比如，第一终端中存在用于对门锁进行控制的应用程序，该应用程序提供有用户操作界面，供用户通过屏幕操作提交控制请求。基于该第一终端，在该用户界面上通过用户手势方式发起该请求，第一终端根据对用户手势的识别，确定接收到用户发起的对受控设备进行控制操作的请求，再比如，用户可通过语音

发送控制指令，第一终端根据对语音的识别，确定接收到用户发起的对受控设备进行控制操作的请求。

在具体实施时，当用户发起对受控设备的控制请求后，若第一终端与第二终端已经建立通信链路，则可通过该通信链路将该会话秘钥获取请求发送给该第二终端，否则，可先与第二终端建立通信链路，再通过该通信链路将该会话秘钥获取发送给该第二终端。

可选地，第一终端发送的会话秘钥获取请求中可包含数字证书。第一终端中保存的数字证书可能有多个，不同的数字证书用于不同的应用，可预先设置数字证书与相应的应用之间的对应关系。第一终端在接收到对受控设备的控制请求后，可根据该控制请求所对应的应用，获取该应用所对应的数字证书。

S202：第二终端接收到第一终端发送的会话秘钥获取请求后，可根据该会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密该会话秘钥，并将加密的会话秘钥发送给第一终端。

其中，会话秘钥可采用对称加密算法的密钥。该会话密钥可在每次会话时产生，会话结束后终止。其中，这里的一次“会话”是指一次从接收到第一终端发送的数字证书后生成会话秘钥，并将其发送给第一终端，到接收到第一终端发送的用该会话秘钥加密的控制指令，用该会话秘钥进行解密，执行解密得到的控制指令的过程。

进一步地，若会话秘钥获取请求中包含有数字证书，则第二终端还要对该数字证书进行验证，并在验证通过后生成会话秘钥。第二终端可通过与认证服务器之间的交互，实现对数字证书的有效性验证过程。具体地，第二终端向认证服务器发送用于确认数字证书是否有效的验证请求，该验证请求中可包含所请求验证的数字证书或者包含所请求验证的数字证书的索引信息；认证服务器接收到该验证请求后，可判断所请求验证的数字证书是否已被回收，若未被回收，则判断该数字证书是否在有效期内，若在有效期内，则向第二终端返回验证为有效的验证结果，否则，向第二终端返回验证为无效的验证结果。

进一步地，数字证书验证通过后，第二终端可将该数字证书进行保存，以便以后使用。

S203：第一终端接收到加密的会话秘钥后，使用数字证书的私钥解密得到会话秘钥，根据所述控制请求生成控制指令，并用解密得到的会话秘钥加密控制指令，该控制指令用于指示第二终端对受控设备进行相应控制。

S204：第一终端将加密的控制指令发送给第二终端。

S205：第二终端接收到加密的控制指令后，使用会话秘钥进行解密，得到控制指令，并根据该控制指令对受控设备进行相应的控制操作。

可选地，第一终端中的数字证书，可通过以下过程申请得到。图 3 示例性地示出了本申请实施例提供的数字证书的申请流程示意图。该流程可包括：

S301：第一终端生成数字证书的公钥和私钥。该数字证书与用于对受控设备进行控制的应用相对应。

S302：第一终端向认证服务器发送数字证书请求，所述数字证书请求中包括所述数字证书的公钥。

S303：第一终端与认证服务器之间进行必要的身份认证，并在身份认证通过后，认证服务器向第一终端发送数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息。

该步骤中，第一终端和认证服务器之间可采用多种方式进行身份认证。比如，以第一终端为智能手机为例，认证服务器可通过短消息方式向该智能手机发送验证码，并指示第一终端发送接收到的验证码，如果智能终端发送的验证码与认证服务器通过短消息方式发送的验证码相同，则认证服务器对该智能手机验证通过。

S304：第一终端接收到认证服务器发送的数字证书后进行保存。

可选地，认证服务器可在数字证书失效后，将失效的数字证书进行回收，比如，将失效的数字证书放入失效队列。可选地，认证服务器可在收到第二终端发送的数字证书验证请求后，判断所请求验证的数字证书是否失效，若已失效，则将失效的数字证书放入失效队列；认证服务器也可以按照设定时间或设定周期判断所分发的数字证书是否已失效，若发现失效的数字证书，则将失效的数字证书放入失效队列。

通过以上描述可以看出，第一终端在需要对受控设备进行控制时，将数字证书发送给与该第一终端连接的第二终端，接收第二终端发送的加密的会话秘钥，使用该数字证书的私钥解密得到会话秘钥，用该会话秘钥加密控制指令，并将加密的控制指令发送给该第二终端，以使该第二终端根据该车门控制指令对受控设备进行相应的控制操作。由于一方面第二终端用数字证书的公钥对会话秘钥进行加密，另一方面，第一终端用会话秘钥对控制指令进行加密，保证了控制指令传输的安全性。

上述对受控设备进行控制的流程以及数字证书申请流程，可应用于通过移动终端（比如智能手机）控制门锁（比如车门门锁）的场景。在该场景中，上述流程中的“第一终端”为移动终端（比如智能手机），“第二终端”为控制终端（比如车载终端），“受

控设备”为门锁控制装置（比如车辆的门锁控制装置），控制指令为对门锁进行相应的控制操作的控制指令。

通过以上描述可以看出，移动终端在需要进行门锁控制时，将数字证书发送给与该移动终端连接的控制终端，接收控制终端发送的加密的会话秘钥，使用该数字证书的私钥解密得到会话秘钥，用该会话秘钥加密门锁控制指令，并将加密的门锁控制指令发送给该控制终端，以使该控制终端根据该门锁控制指令对门锁进行相应的控制操作。由于一方面控制终端用数字证书的公钥对会话秘钥进行加密，另一方面，移动终端用会话秘钥对控制指令进行加密，保证了门锁控制指令传输的安全性。

为了进一步提高安全性，本申请实施例还提供了一种基于 TEE 硬件技术来保证秘钥安全性的方案。

TEE 技术提供了安全执行环境，使得工作在此模式下的代码不会受到恶意软件的攻击。其基本原理是：只有可信的代码经过签名校验才可以工作在 TEE 中，并且这些代码所操作的敏感数据严格保护在安全内存区域中，不会被非 TEE 代码访问。

本申请实施例中，一方面，数字证书的私钥的生成、存储和使用，以及会话秘钥的使用均基于第一终端的 TEE 实现，保证了对密钥的相关操作是安全可靠的。另一方面，第二终端需要对第一终端发送的数字证书进行认证，在保证数字证书有效的情况下完成后续相关的指令操作，从而保证了对受控设备进行控制操作的安全性。

如图 4 所示，在前述实施例提供的控制流程的基础上，结合 TEE 技术，则第一终端中包括两个应用：第一应用 401 和第二应用 402。进一步地，第一终端中还包括收发器（未在图中示出），该收发器可以是无线收发器，用于接收和/或发送无线信号。这两个应用相互配合来实现上述第一终端侧的流程。其中，第二应用为可信应用，即，第二应用是基于可信操作系统（Trust OS）的应用程序。第二应用主要用于在控制流程中进行加密、解密操作，在数字证书申请流程中，生成数字证书的秘钥对（包括公钥和私钥）。第一应用主要用于与第二应用交互、与第二终端交互以及与认证服务器交互。

如图 4 所示，在第一终端中包括第一存储区 410、第二存储区 420 和第三存储区 430。其中，第一存储区 410 用于存储数字证书，第二存储区 420 为安全存储区，用于存储数字证书的私钥和会话秘钥；第三存储区 430 为只读存储器的存储区，用于存储设备秘钥。设备秘钥具有唯一性，即一个终端的设备秘钥与其他终端的设备秘钥不同。设备秘钥通常在终端出厂前烧录到第三存储区。第一应用 401 可访问第一存储区 410，第二应用 402 可访问第二存储区 420 以及第三存储区 430。

基于图 4 所示的 TEE 架构，图 5 示例性地示出了基于 TEE 技术实现的对受控设备进行控制的流程示意图。如图所示，该流程可包括：

S501：第一终端中的第一应用根据对受控设备的控制请求，通过收发器向第二终端发送会话秘钥获取请求。

可选地，该会话秘钥获取请求中可包含数字证书。第一应用可从第一存储区读取与该控制请求对应的数字证书，将该数字证书携带于会话秘钥获取请求发送给与该第一终端连接的第二终端。该步骤的实现可参照图 2 中的步骤 S201。

S502：第二终端接收到第一终端发送的会话秘钥获取请求后，可向认证服务器发送用于确认数字证书是否有效的验证请求，该验证请求中可包含所请求验证的数字证书或者包含所请求验证的数字证书的索引信息。

S503：认证服务器接收到该验证请求后，可判断所请求验证的数字证书是否已被回收，若未被回收，则判断该数字证书是否在有效期内，若在有效期内，则向第二终端返回验证为有效的验证结果，否则，向第二终端返回验证为无效的验证结果。本例子中，认证服务器返回验证为有效的验证结果。上述 S502~S503 为可选步骤（图中用虚线表示）。

S504：第二终端接生成用于本次控制流程的会话秘钥，使用该数字证书的公钥加密该会话秘钥，并将加密的会话秘钥发送给第一终端中的第一应用。该步骤的实现可如图 2 中的步骤 S202。

S505：第一终端中的第一应用通过收发器接收到加密的会话秘钥后，将其发送给第一终端中的第二应用。

S506：第一终端中的第二应用使用数字证书的私钥解密得到会话秘钥，根据所述控制请求生成控制指令，并用解密得到的会话秘钥加密控制指令，并将加密的控制指令发送给第一终端中的第一应用。

该过程中，可选地，第一终端中的第二应用可首先从第三存储区读取设备秘钥，从第二存储区读取加密的数字证书私钥，然后用该设备秘钥对该加密的数字证书私钥进行解密，再用该数字证书私钥对接收到的加密的会话秘钥进行解密。

S507：第一终端中的第一应用将加密的控制指令通过收发器发送给第二终端。第二终端接收到加密的控制指令后，使用会话秘钥进行解密，得到控制指令，并根据该控制指令对受控设备进行相应的控制操作。

进一步地，在 S506 中，第一终端中的第二应用可在解密得到该会话秘钥后将其存储在第二存储区。在 S507 中，第二终端在执行该控制指令后可向第一终端中的第一应用返

回响应，第一终端中的第一应用可将该响应发送给第一终端中的第二应用，第二应用可根据该响应，将第二存储区中存储的该会话秘钥删除。

基于图 4 所示的 TEE 架构，图 6 示例性地示出了基于 TEE 技术实现的数字证书申请的流程示意图。如图所示，该流程可包括：

S601：第一终端中的第二应用生成数字证书的公钥和私钥，并将该数字证书的私钥存储在第二存储区。该数字证书与用于对受控设备进行控制的应用相对应。

可选地，第一终端中的第二应用在生成数字证书的私钥后，可从第三存储区读取设备秘钥，用户该设备秘钥加密数字证书的私钥，并将加密的数字证书私钥存储到第二存储区。

S602：第一终端中的第二应用向第二终端中的第一应用发送数字证书请求，该数字证书请求中包括所述数字证书的公钥。

S603：第一终端中的第一应用通过收发器向认证服务器发送数字证书请求。

S604：第一终端中的第一应用与认证服务器之间进行必要的身份认证，并在身份认证通过后，认证服务器向第一终端发送数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期等信息。

S604：第一终端中的第一应用通过收发器接收到认证服务器发送的数字证书后，将该数字证书存储在第一存储区。

上述对受控设备进行控制的流程以及数字证书申请流程，可应用于通过移动终端（比如智能手机）控制门锁的场景。在该场景中，上述流程中的“第一终端”为移动终端（比如智能手机），“第二终端”为控制终端，“受控设备”为门锁控制装置，控制指令为对门锁进行相应的控制操作的控制指令。

基于相同的技术构思，本申请实施例还提供了一种第一终端，该终端可实现前述实施例中第一终端所执行的流程。

参见图 7，为本申请实施例提供的第一终端的结构示意图。该终端可包括：第一应用模块 701、第二应用模块 702，还可包括收发器（未在图中示出）。

第一应用模块 701，用于根据对受控设备的控制请求，通过所述收发器向与所述第一终端连接的第二终端发送会话秘钥获取请求；以及，通过所述收发器接收所述第二终端根据所述秘钥会话获取请求发送的会话秘钥，并将所述加密的会话秘钥发送给第二应用模块；所述会话秘钥使用数字证书的公钥进行加密；

第二应用模块 702，用于使用所述数字证书的私钥解密得到所述会话秘钥，根据所

述控制请求生成控制指令，用所述会话秘钥加密所述控制指令，并将加密的控制指令发送给所述第一应用模块；

所述第一应用模块 701 还用于，通过所述收发器将加密的控制指令发送给第二终端，所述控制指令用于指示所述第二终端对所述受控设备进行相应控制操作。

可选地，所述第二应用模块 702 具体用于：从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

可选地，所述会话秘钥获取请求中包括所述数字证书。

可选地，第二应用模块 702 还用于：生成数字证书的私钥，从所述第一终端的只读存储区读取设备秘钥，使用所述设备秘钥加密所述私钥，并将加密的私钥存储到所述移动终端的安全存储区中，向第一应用发送数字证书请求；所述第一应用模块 701 还用于：通过所述收发器将所述数字证书请求发送给认证服务器，通过所述收发器接收所述认证服务器根据所述数字证书请求发送的数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息。

可选地，所述第一应用模块 701 具体用于：接收用户通过门锁控制应用的用户界面提交的门锁控制请求，确定是否与所述门锁控制应用关联的第二终端之间建立连接；所述收发器具体用于：若已建立连接，则通过所述连接向所述第二终端发送会话秘钥获取请求。可选地，所述连接为蓝牙连接。

可选地，所述第一终端可以是移动终端，所述第二终端可以是控制终端（比如车载终端）。相应地，所述控制请求为门锁控制请求（比如车门控制请求），所述控制指令为门锁控制指令（比如车门控制指令）。

基于相同的技术构思，本申请实施例还提供了一种第二终端，该终端可实现前述实施例中第二终端所执行的流程。

参见图 8，为本申请实施例提供的第二终端的结构示意图。该终端可包括：会话秘钥处理模块 801、控制指令处理模块 802，还可包括收发器（未在图中示出）。

会话秘钥处理模块 801，用于通过所述收发器接收与所述第二终端连接的第一终端发送的会话秘钥获取请求，根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并通过所述收发器将加密的会话秘钥发送给所述第一终端；

控制指令处理模块 802，用于通过所述收发器接收所述第一终端发送的加密的控制指令，使用所述会话秘钥解密得到所述控制指令，并根据解密得到的控制指令对受控设

备进行相应控制操作。

可选地，所述会话秘钥获取请求中包括数字证书，所述第二终端中还包括证书验证模块 703。证书验证模块 703 用于通过所述收发器向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；以及，通过所述收发器接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

可选地，所述第一终端和所述第二终端之间的连接为蓝牙连接。

可选地，所述第一终端可以是移动终端，所述第二终端可以是控制终端（比如车载终端）。相应地，所述控制请求为门锁控制请求（比如车门控制请求），所述控制指令为门锁控制指令（比如车门控制指令）。

基于相同的技术构思，本申请实施例还提供了一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行前述实施例描述的第一终端执行的控制方法。

基于相同的技术构思，本申请实施例还提供了一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行前述实施例描述的第二终端执行的控制方法。

基于相同的技术构思，本申请实施例还提供了一种装置 1100，该装置 1100 可实现前述实施例描述的第一终端执行的流程。

图 9 示例性地示出了根据各种实施例的示例装置 1100，装置 1100 可包括一个或多个处理器 1102，系统控制逻辑 1101 耦合于至少一个处理器 1102，非易失性存储器（non-volatile memory，NMV）/存储器 1104 耦合于系统控制逻辑 1101，网络接口 1106 耦合于系统控制逻辑 1101。

处理器 1102 可包括一个或多个单核处理器或多核处理器。处理器 1102 可包括任何一般用途处理器或专用处理器（如图像处理器、应用处理器基带处理器等）的组合。

一个实施例中的系统控制逻辑 1101，可包括任何适当的接口控制器，以提供到处理器 1102 中的至少一个的任何合适的接口，和/或提供到与系统控制逻辑 1101 通信的任何合适的设备或组件的任何合适的接口。

一个实施例中的系统控制逻辑 1101，可包括一个或多个内存控制器，以提供到系统内存 1103 的接口。系统内存 1103 用来加载以及存储数据和/或指令。例如，对应装置 1100，

在一个实施例中，系统内存 1103 可包括任何合适的易失性存储器。

NVM/存储器 1104 可包括一个或多个有形的非暂时的计算机可读介质，用于存储数据和/或指令。例如，NVM/存储器 1104 可包括任何合适的非易失性存储装置，如一个或多个硬盘（hard disk device，HDD），一个或多个光盘（compact disk，CD），和/或一个或多个数字通用盘（digital versatile disk，DVD）。

NVM/存储器 1104 可包括存储资源，该存储资源物理上是该系统所安装的或者可以被访问的设备的一部分，但不一定是设备的一部分。例如，NVM/存储器 1104 可经由网络接口 1106 被网络访问。

系统内存 1103 以及 NVM/存储器 1104 可分别包括临时的或持久的指令 1110 的副本。指令 1110 可包括当由处理器 1102 中的至少一个执行时导致装置 1100 实现图 2 至图 6 描述的方法之一或组合的指令。各实施例中，指令 1110 或硬件、固件，和/或软件组件可另外地/可替换地被置于系统控制逻辑 1101，网络接口 1106 和/或处理器 1102。

网络接口 1106 可包括一个接收器来为装置 1100 提供无线接口来与一个或多个网络和/或任何合适的设备进行通信。网络接口 1106 可包括任何合适的硬件和/或固件。网络接口 1106 可包括多个天线来提供多输入多输出无线接口。在一个实施例中，网络接口 1106 可包括一个网络适配器、一个无线网络适配器、一个电话调制解调器，和/或无线调制解调器。

在一个实施例中，处理器 1102 中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑一起封装。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑一起封装以形成系统级封装。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑集成在相同的管芯上。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑集成在相同的管芯上以形成系统芯片。

装置 1100 可进一步包括输入/输出装置 1105。输入/输出装置 1105 可包括用户接口旨在使用户与装置 1100 进行交互，可包括外围组件接口，其被设计为使得外围组件能够与系统交互，和/或，可包括传感器，旨在确定环境条件和/或有关装置 1100 的位置信息。

基于相同的技术构思，本申请实施例还提供了一种装置，该装置可实现前述实施例描述的第二终端执行的流程。

图 10 示例性地示出了根据各种实施例的示例装置 1200，装置 1200 可包括一个或多个处理器 1202，系统控制逻辑 1201 耦合于至少一个处理器 1202，非易失性存储器

（non-volatile memory，NMV）/存储器 1204 耦合于系统控制逻辑 1201，网络接口 1206 耦合于系统控制逻辑 1201。

处理器 1202 可包括一个或多个单核处理器或多核处理器。处理器 1202 可包括任何一般用途处理器或专用处理器（如图像处理器、应用处理器基带处理器等）的组合。

一个实施例中的系统控制逻辑 1201，可包括任何适当的接口控制器，以提供到处理器 1202 中的至少一个的任何合适的接口，和/或提供到与系统控制逻辑 1201 通信的任何合适的设备或组件的任何合适的接口。

一个实施例中的系统控制逻辑 1201，可包括一个或多个内存控制器，以提供到系统内存 1203 的接口。系统内存 1203 用来加载以及存储数据和/或指令。例如，对应装置 1200，在一个实施例中，系统内存 1203 可包括任何合适的易失性存储器。

NVM/存储器 1204 可包括一个或多个有形的非暂时的计算机可读介质，用于存储数据和/或指令。例如，NVM/存储器 1204 可包括任何合适的非易失性存储装置，如一个或多个硬盘（hard disk device，HDD），一个或多个光盘（compact disk，CD），和/或一个或多个数字通用盘（digital versatile disk，DVD）。

NVM/存储器 1204 可包括存储资源，该存储资源物理上是该系统所安装的或者可以被访问的设备的一部分，但不一定是设备的一部分。例如，NVM/存储器 1204 可经由网络接口 1206 被网络访问。

系统内存 1203 以及 NVM/存储器 1204 可分别包括临时的或持久的指令 1210 的副本。指令 1210 可包括当由处理器 1202 中的至少一个执行时导致装置 1200 实现图 2 至图 6 描述的方法之一或组合的指令。各实施例中，指令 1210 或硬件、固件，和/或软件组件可另外地/可替换地被置于系统控制逻辑 1201，网络接口 1206 和/或处理器 1202。

网络接口 1206 可包括一个接收器来为装置 1200 提供无线接口来与一个或多个网络和/或任何合适的设备进行通信。网络接口 1206 可包括任何合适的硬件和/或固件。网络接口 1206 可包括多个天线来提供多输入多输出无线接口。在一个实施例中，网络接口 1206 可包括一个网络适配器、一个无线网络适配器、一个电话调制解调器，和/或无线调制解调器。

在一个实施例中，处理器 1202 中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑一起封装。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑一起封装以形成系统级封装。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑集成在相同的管芯上。

在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑集成在相同的管芯上以形成系统芯片。

装置 1200 可进一步包括输入/输出装置 1205。输入/输出装置 1205 可包括用户接口旨在使用户与装置 1200 进行交互，可包括外围组件接口，其被设计为使得外围组件能够与系统交互，和/或，可包括传感器，旨在确定环境条件和/或有关装置 1200 的位置信息。

权 利 要 求 书

1.一种控制方法，其特征在于，包括：

移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求；

所述控制终端根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述移动终端；

所述移动终端使用所述数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，使用所述会话秘钥加密门锁控制指令，并将加密的门锁控制指令发送给所述控制终端；

所述控制终端使用所述会话秘钥解密得到所述门锁控制指令，根据解密得到的门锁控制指令进行门锁控制操作。

2.一种控制方法，其特征在于，包括：

移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求；

所述移动终端接收所述控制终端根据所述秘钥会话获取请求发送的会话秘钥，所述会话秘钥使用数字证书的公钥进行加密；

所述移动终端使用所述数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，并用所述会话秘钥加密所述门锁控制指令；

所述移动终端将加密的门锁控制指令发送给所述控制终端，所述门锁控制指令用于指示所述控制终端进行相应门锁控制操作。

3.如权利要求 2 所述的方法，其特征在于，所述会话秘钥获取请求中包括所述数字证书。

4.如权利要求 2 所述的方法，其特征在于，所述移动终端中包括第一应用和第二应用，所述第二应用为可信应用；

所述移动终端使用所述数字证书的私钥解密得到所述会话秘钥，并用所述会话秘钥加密门锁控制指令，包括：

所述第一应用将接收到的加密的会话秘钥发送给所述第二应用；

所述第二应用从所述移动终端的安全存储区获取所述数字证书的私钥，并使用获取到的私钥解密得到会话秘钥；

所述移动终端将加密的门锁控制指令发送给所述控制终端，包括：

所述第二应用使用解密得到的会话秘钥加密门锁控制指令，并将加密的门锁控制指令发送给第一应用；

所述第一应用将加密的门锁控制指令发送给所述控制终端。

5.如权利要求 4 所述的方法，其特征在于，所述第二应用从安全存储区获取所述数字证书的私钥，包括：

所述第二应用从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；

所述第二应用从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

6.如权利要求 2 所述的方法，其特征在于，所述移动终端中包括第一应用和第二应用，所述第二应用为可信应用；

所述方法还包括：

所述第二应用生成数字证书的私钥，从所述移动终端的只读存储区读取设备秘钥，使用所述设备秘钥加密所述私钥，并将加密的私钥存储到所述移动终端的安全存储区中；

所述第二应用向第一应用发送数字证书请求，所述第一应用将所述数字证书请求发送给认证服务器；

所述第二应用接收所述认证服务器根据所述数字证书请求发送的数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息。

7.如权利要求 2 至 5 中任一项所述的方法，其特征在于，移动终端根据门锁控制请求，向与所述移动终端连接的控制终端发送会话秘钥获取请求，包括：

移动终端接收用户通过门锁控制应用的用户界面提交的门锁控制请求，确定是否与所述门锁控制应用关联的控制终端之间建立连接；若已建立连接，则通过所述连接向所述控制终端发送会话秘钥获取请求。

8.如权利要求 7 所述的方法，其特征在于，所述连接为蓝牙连接。

9.一种控制方法，其特征在于，包括：

控制终端接收与所述控制终端连接的移动终端发送的会话秘钥获取请求；

所述控制终端根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述移动终端；

所述控制终端接收所述移动终端发送的加密的门锁控制指令，使用所述会话秘钥解

密得到所述门锁控制指令，并根据解密得到的门锁控制指令进行相应门锁控制操作。

10.如权利要求 9 所述的方法，其特征在于，所述会话秘钥获取请求中包括数字证书，所述方法还包括：

所述控制终端向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；

所述控制终端接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

11.如权利要求 9 或 10 所述的方法，其特征在于，所述控制终端和所述移动终端通过蓝牙连接。

12.一种控制方法，其特征在于，包括：

第一终端根据对受控设备的控制请求，向与所述第一终端连接的第二终端发送会话秘钥请求；

所述第一终端接收所述第二终端根据所述会话秘钥获取请求返回的会话秘钥，所述会话秘钥使用数字证书的公钥进行加密；

所述第一终端使用所述数字证书的私钥解密得到所述会话秘钥，根据所述控制请求生成控制指令，并用所述会话秘钥加密所述控制指令；

所述第一终端将加密的控制指令发送给所述第二终端，所述控制指令用于指示所述第二终端对所述受控设备进行相应的控制操作。

13.如权利要求 12 所述的方法，其特征在于，所述第一终端中包括第一应用和第二应用，所述第二应用为可信应用；

所述第一终端使用所述数字证书的私钥解密得到所述会话秘钥，并用所述会话秘钥加密所述控制指令，包括：

所述第一应用将接收到的加密的会话秘钥发送给所述第二应用；

所述第二应用从所第一动终端的安全存储区获取所述数字证书的私钥，并使用获取到的私钥解密得到会话秘钥；

所述第一终端将加密的控制指令发送给所述第二终端，包括：

所述第二应用使用解密得到的会话秘钥加密控制指令，并将加密的控制指令发送给第一应用；

所述第一应用将加密的控制指令发送给所述第二终端。

14.如权利要求 13 所述的方法，其特征在于，所述第二应用从安全存储区获取所述数字证书的私钥，包括：

所述第二应用从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；

所述第二应用从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

15.一种控制方法，其特征在于，包括：

第二终端接收与所述第二终端连接的第一终端发送的会话秘钥获取请求；

所述第二终端根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并将加密的会话秘钥发送给所述第一终端；

所述第二终端接收所述第一终端发送的加密的控制指令，使用所述会话秘钥解密得到所述控制指令，并根据解密得到的控制指令对受控设备进行相应的控制操作。

16.如权利要求 15 所述的方法，其特征在于，所述会话秘钥获取请求中包括数字证书，所述方法还包括：

所述第二终端向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；

所述第二终端接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

17.一种移动终端，其特征在于，包括：第一应用模块、第二应用模块以及收发器；

第一应用模块，用于根据门锁控制请求，通过所述收发器向与所述移动终端连接的控制终端发送会话秘钥获取请求；以及，通过所述收发器接收所述控制终端根据所述秘钥会话获取请求发送的会话秘钥，并将加密的所述会话秘钥发送给第二应用模块；所述会话秘钥使用数字证书的公钥进行加密；

第二应用模块，用于使用所述数字证书的私钥解密得到所述会话秘钥，根据所述门锁控制请求生成门锁控制指令，用所述会话秘钥加密所述门锁控制指令，并将加密的门锁控制指令发送给所述第一应用模块；

所述第一应用模块还用于，通过所述收发器将加密的门锁控制指令发送给所述控制终端，所述门锁控制指令用于指示所述控制终端进行相应门锁控制操作。

18.如权利要求 17 所述的移动终端，其特征在于，所述会话秘钥获取请求中包括所

述数字证书。

19.如权利要求 17 所述的移动终端，其特征在于，所述第二应用模块具体用于：

从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；

从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

20.如权利要求 17 所述的移动终端，其特征在于，所述第二应用模块还用于：生成数字证书的私钥，从所述移动终端的只读存储区读取设备秘钥，使用所述设备秘钥加密所述私钥，并将加密的私钥存储到所述移动终端的安全存储区中，向第一应用发送数字证书请求；

所述第一应用模块还用于：通过所述收发器将所述数字证书请求发送给认证服务器，通过所述收发器接收所述认证服务器根据所述数字证书请求发送的数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息。

21.如权利要求 17 至 20 中任一项所述的移动终端，其特征在于，所述第一应用模块具体用于：接收用户通过门锁控制应用的用户界面提交的门锁控制请求，确定是否与所述门锁控制应用关联的控制终端之间建立连接；

所述收发器具体用于：若已建立连接，则通过所述连接向所述控制终端发送会话秘钥获取请求。

22.如权利要求 21 所述的移动终端，其特征在于，所述连接为蓝牙连接。

23.一种控制终端，其特征在于，包括：会话秘钥处理模块、控制指令处理模块和收发器；

会话秘钥处理模块，用于通过所述收发器接收与所述控制终端连接的移动终端发送的会话秘钥获取请求，根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并通过所述收发器将加密的会话秘钥发送给所述移动终端；

控制指令处理模块，用于通过所述收发器接收所述移动终端发送的加密的门锁控制指令，使用所述会话秘钥解密得到所述门锁控制指令，并根据解密得到的门锁控制指令进行相应门锁控制操作。

24.如权利要求 23 所述的控制终端，其特征在于，所述会话秘钥获取请求中包括数字证书，所述控制终端中还包括：

证书验证模块，用于通过所述收发器向认证服务器发送用于确认所述数字证书是否

有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；以及，通过所述收发器接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

25.如权利要求 23 或 24 所述的控制终端，其特征在于，所述连接为蓝牙连接。

26.一种终端，其特征在于，包括：第一应用模块、第二应用模块以及收发器；

第一应用模块，用于根据对受控设备的控制请求，通过所述收发器向与第一终端连接的第二终端发送会话秘钥获取请求；以及，通过所述收发器接收所述第二终端根据所述秘钥会话获取请求发送的会话秘钥，并将加密的所述会话秘钥发送给第二应用模块；所述会话秘钥使用数字证书的公钥进行加密；

第二应用模块，用于使用所述数字证书的私钥解密得到所述会话秘钥，根据所述控制请求生成控制指令，用所述会话秘钥加密所述控制指令，并将加密的控制指令发送给所述第一应用模块；

所述第一应用模块还用于，通过所述收发器将加密的控制指令发送给第二终端，所述控制指令用于指示所述第二终端对所述受控设备进行相应控制操作。

27.如权利要求 26 所述的终端，其特征在于，所述第二应用模块具体用于：从安全存储区获取所述数字证书的私钥，所述数字证书的私钥被设备秘钥进行了加密；从只读存储区获取所述设备秘钥，并使用所述设备秘钥对加密的数字证书的私钥进行解密。

28.一种终端，其特征在于，包括：会话秘钥处理模块、控制指令处理模块和收发器；

会话秘钥处理模块，用于通过所述收发器接收与第二终端连接的第一终端发送的会话秘钥获取请求，根据所述会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密所述会话秘钥，并通过所述收发器将加密的会话秘钥发送给所述第一终端；

控制指令处理模块，用于通过所述收发器接收所述第一终端发送的加密的控制指令，使用所述会话秘钥解密得到所述控制指令，并根据解密得到的控制指令对受控设备进行相应控制操作。

29.如权利要求 28 所述的终端，其特征在于，所述会话秘钥获取请求中包括数字证书，所述第二终端中还包括：

证书验证模块，用于通过所述收发器向认证服务器发送用于确认所述数字证书是否有效的验证请求，所述验证请求用于触发所述认证服务器在所述数字证书未被回收且在有效期内的情况下返回用于指示所述数字证书有效的验证结果；以及，通过所述收发器

接收所述认证服务器返回的验证结果，并根据所述验证结果确认所述数字证书是否有效。

30.一个或多个计算机可读介质，其特征在于，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行如权利要求 2-8 中任一项所述的方法。

31.一个或多个计算机可读介质，其特征在于，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行如权利要求 9-11 中任一项所述的方法。

32.一个或多个计算机可读介质，其特征在于，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行如权利要求 12-14 中任一项所述的方法。

33.一个或多个计算机可读介质，其特征在于，所述可读介质上存储有指令，所述指令被一个或多个处理器执行时，使得通信设备执行如权利要求 15-16 中任一项所述的方法。

34.一种装置，其特征在于，包括：一个或多个处理器；以及一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被所述一个或多个处理器执行时，使得所述装置执行如权利要求 2-8、12-14 中任一项所述的方法。

35.一种装置，其特征在于，包括：一个或多个处理器；以及一个或多个计算机可读介质，所述可读介质上存储有指令，所述指令被所述一个或多个处理器执行时，使得所述装置执行如权利要求 9-11、15-16 中任一项所述的方法。

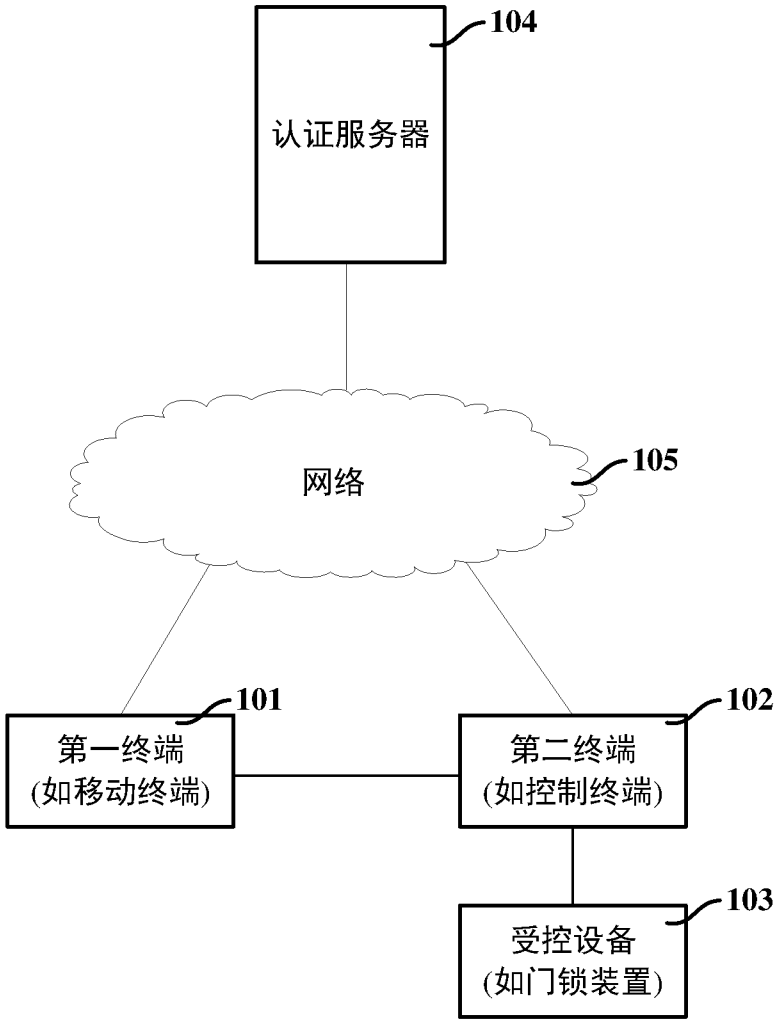

图 1

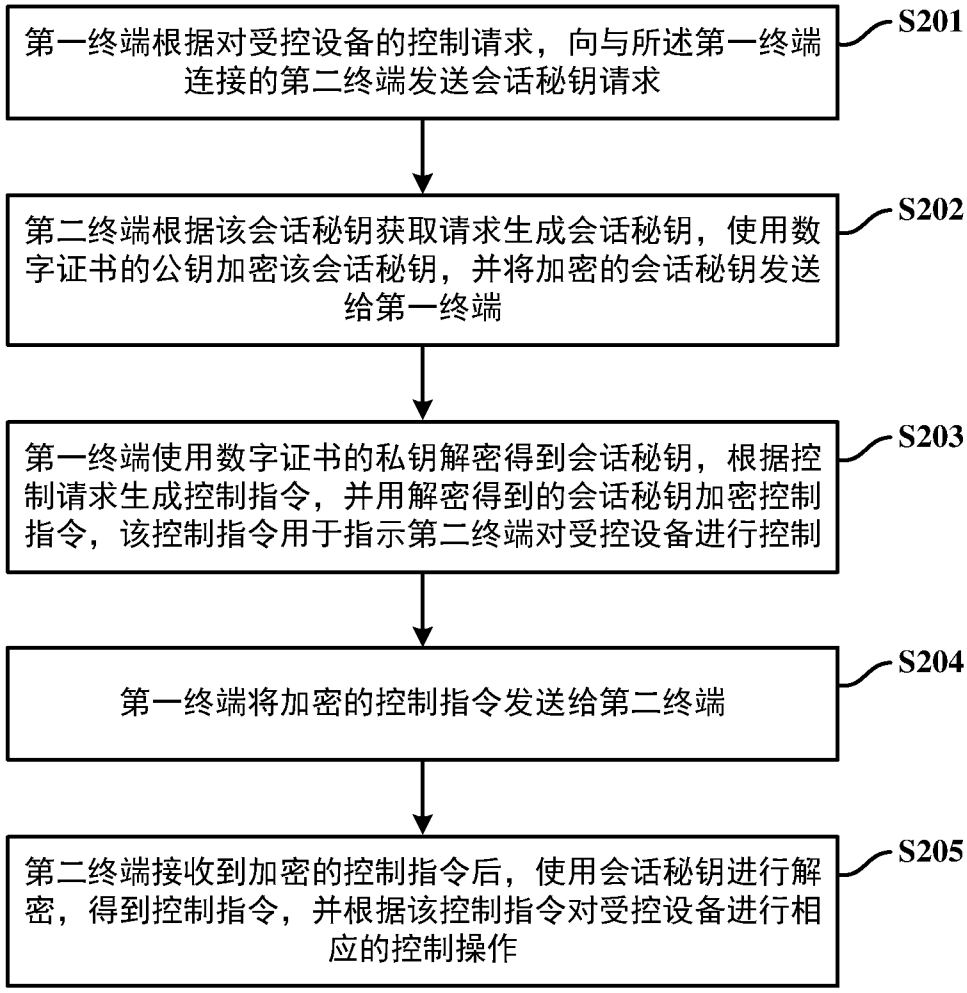
第一终端根据对受控设备的控制请求，向与所述第一终端连接的第二终端发送会话秘钥请求
S201
第二终端根据该会话秘钥获取请求生成会话秘钥，使用数字证书的公钥加密该会话秘钥，并将加密的会话秘钥发送给第一终端
S202
第一终端使用数字证书的私钥解密得到会话秘钥，根据控制请求生成控制指令，并用解密得到的会话秘钥加密控制指令，该控制指令用于指示第二终端对受控设备进行控制
S203
第一终端将加密的控制指令发送给第二终端
S204
第二终端接收到加密的控制指令后，使用会话秘钥进行解密，得到控制指令，并根据该控制指令对受控设备进行相应的控制操作
S205

图 2

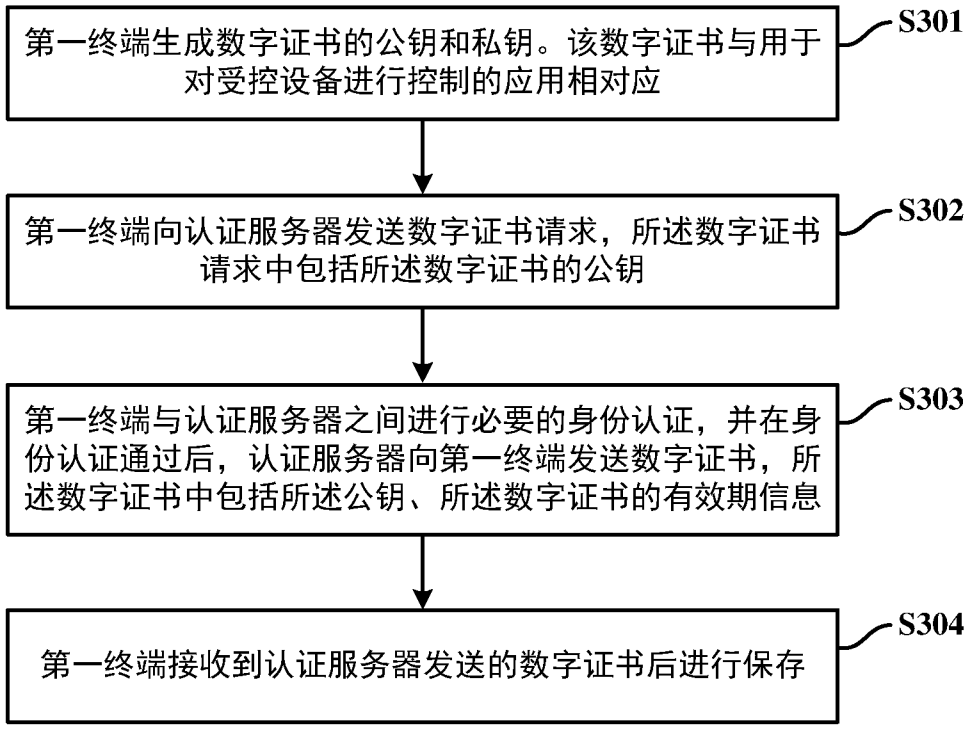
第一终端生成数字证书的公钥和私钥。该数字证书与用于对受控设备进行控制的应用相对应
S301
第一终端向认证服务器发送数字证书请求，所述数字证书请求中包括所述数字证书的公钥
S302
第一终端与认证服务器之间进行必要的身份认证，并在身份认证通过后，认证服务器向第一终端发送数字证书，所述数字证书中包括所述公钥、所述数字证书的有效期信息
S303
第一终端接收到认证服务器发送的数字证书后进行保存
S304

图 3

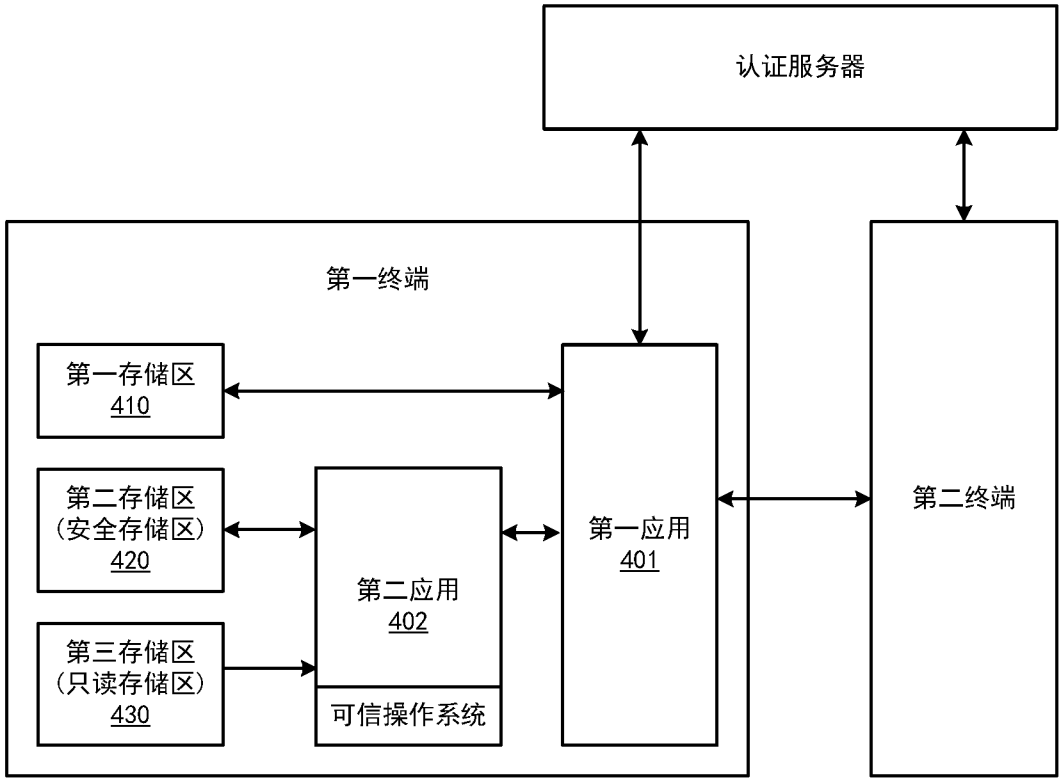
认证服务器
第一终端
第一存储区
410
第二存储区
（安全存储区）
420
第三存储区
（只读存储区）
430
第二应用
402
可信操作系统
第一应用
401
第二终端

图 4

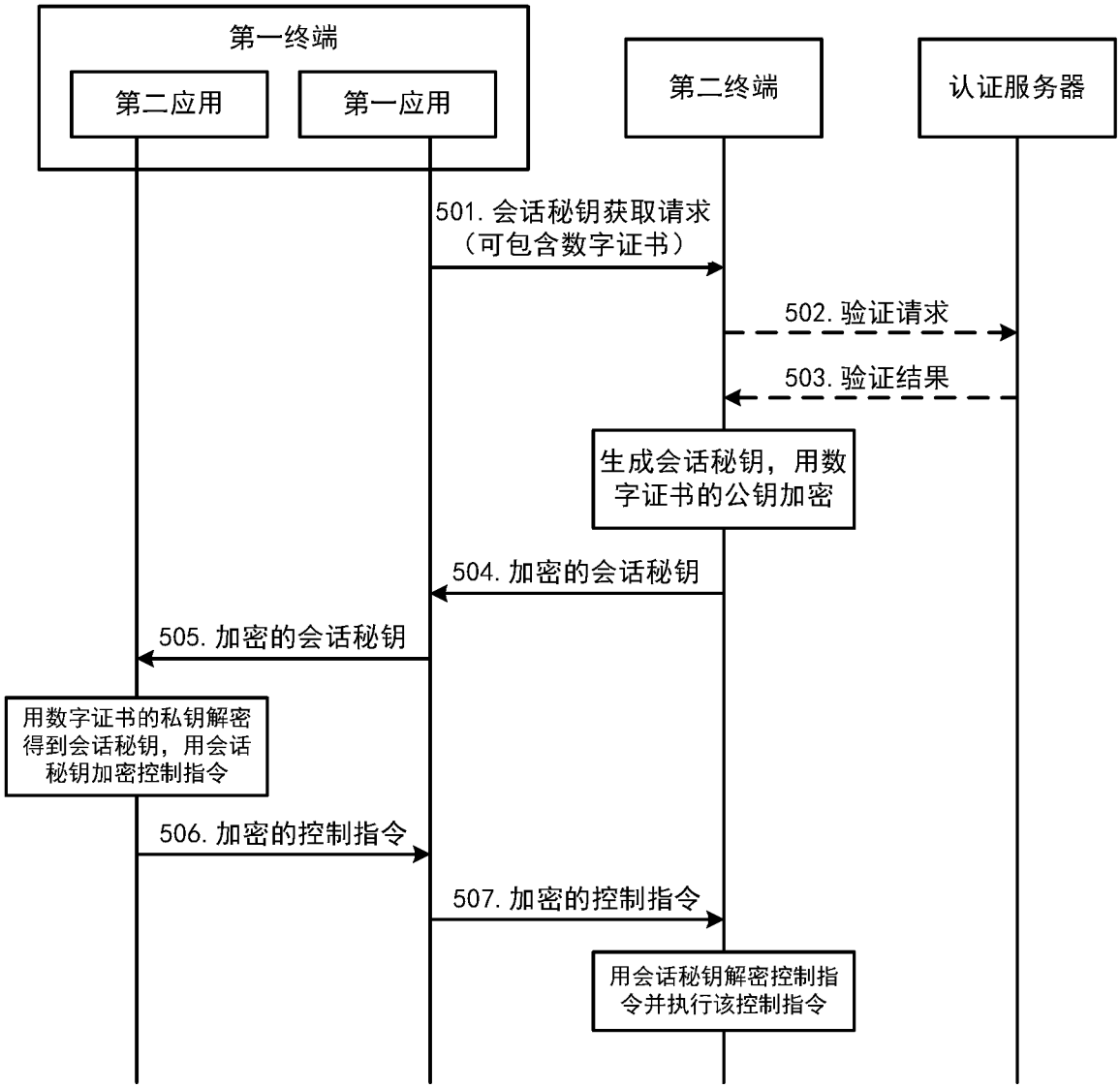
第一终端
第二应用
第一应用
第二终端
认证服务器
501. 会话秘钥获取请求
（可包含数字证书）
502. 验证请求
503. 验证结果
生成会话秘钥，用数字证书的公钥加密
504. 加密的会话秘钥
505. 加密的会话秘钥
用数字证书的私钥解密得到会话秘钥，用会话秘钥加密控制指令
506. 加密的控制指令
507. 加密的控制指令
用会话秘钥解密控制指令并执行该控制指令

图 5

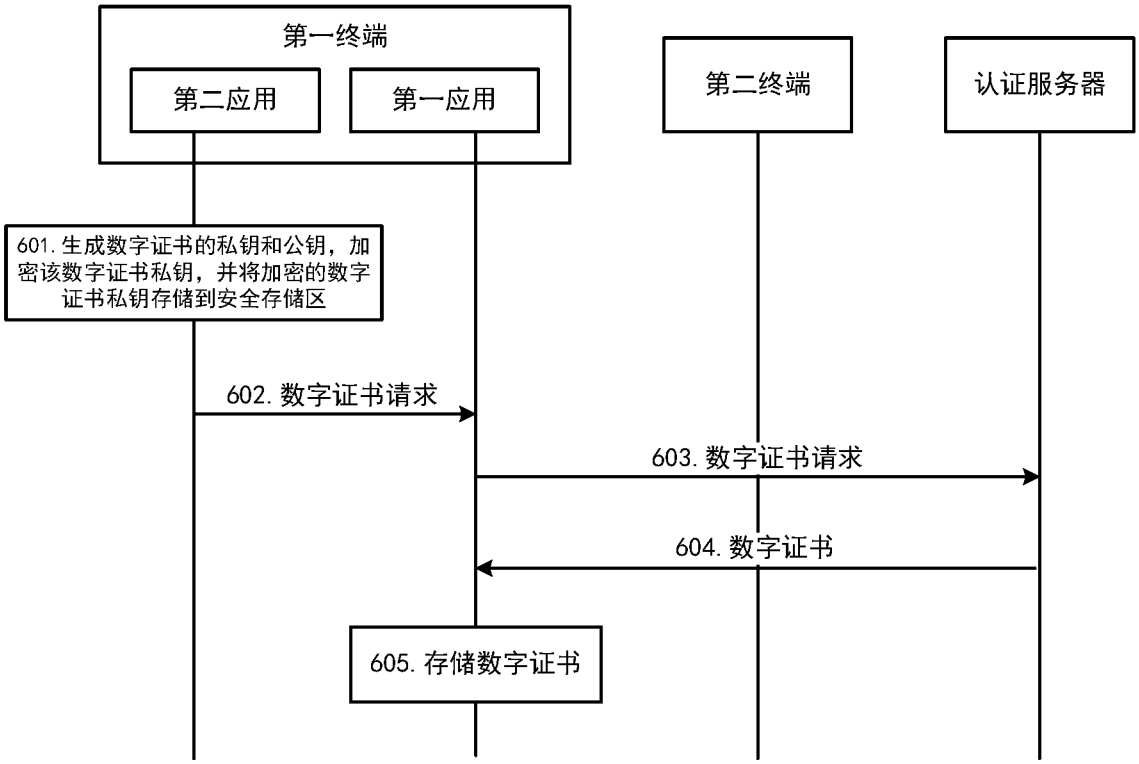
第一终端
第二应用
第一应用
第二终端
认证服务器
601. 生成数字证书的私钥和公钥，加密该数字证书私钥，并将加密的数字证书私钥存储到安全存储区
602. 数字证书请求
603. 数字证书请求
604. 数字证书
605. 存储数字证书

图 6

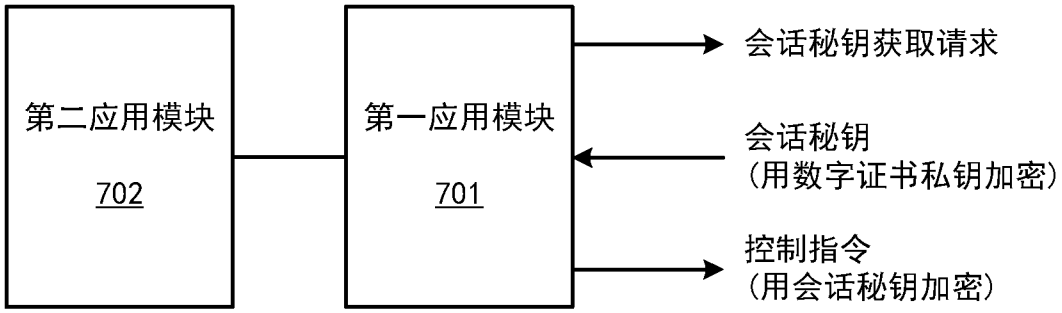
第二应用模块
702
第一应用模块
701
会话秘钥获取请求
会话秘钥
（用数字证书私钥加密）
控制指令
（用会话秘钥加密）

图 7

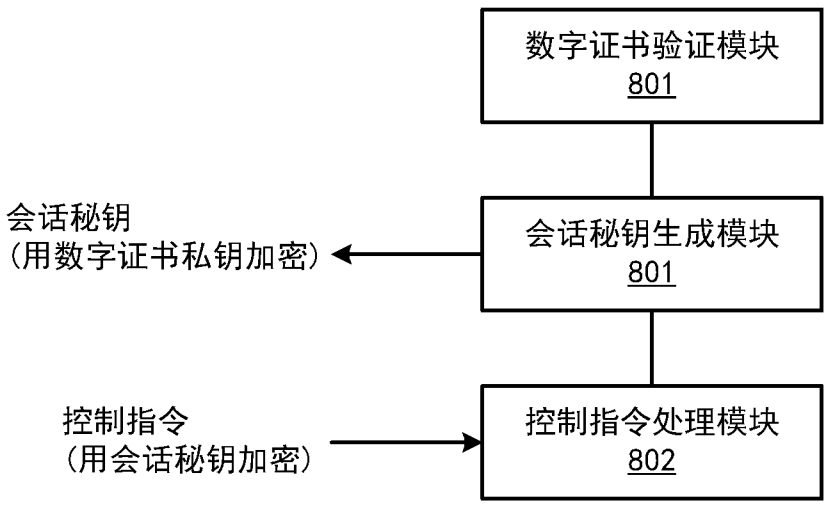
数字证书验证模块
801
会话秘钥
（用数字证书私钥加密）
会话秘钥生成模块
801
控制指令
（用会话秘钥加密）
控制指令处理模块
802

图 8

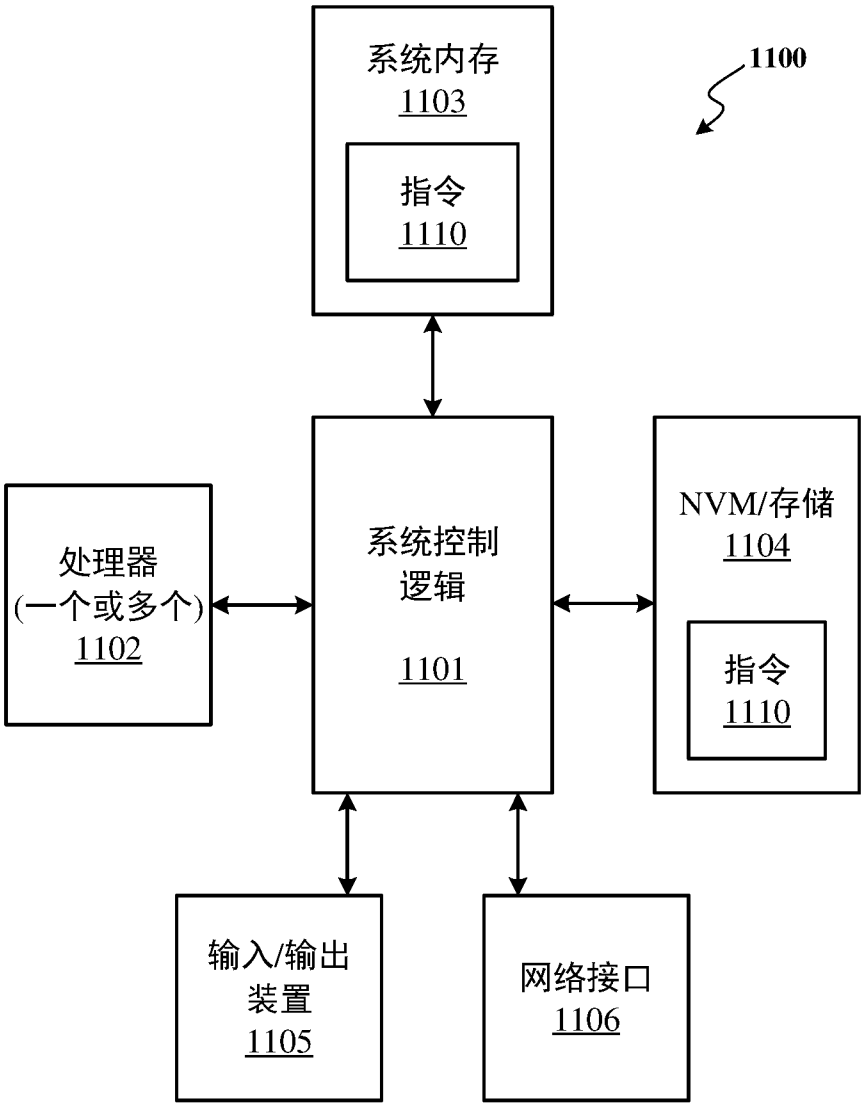
系统内存
1103
指令
1110
1100
处理器
(一个或多个)
1102
系统控制
逻辑
1101
NVM/存储
1104
指令
1110
输入/输出
装置
1105
网络接口
1106

图 9

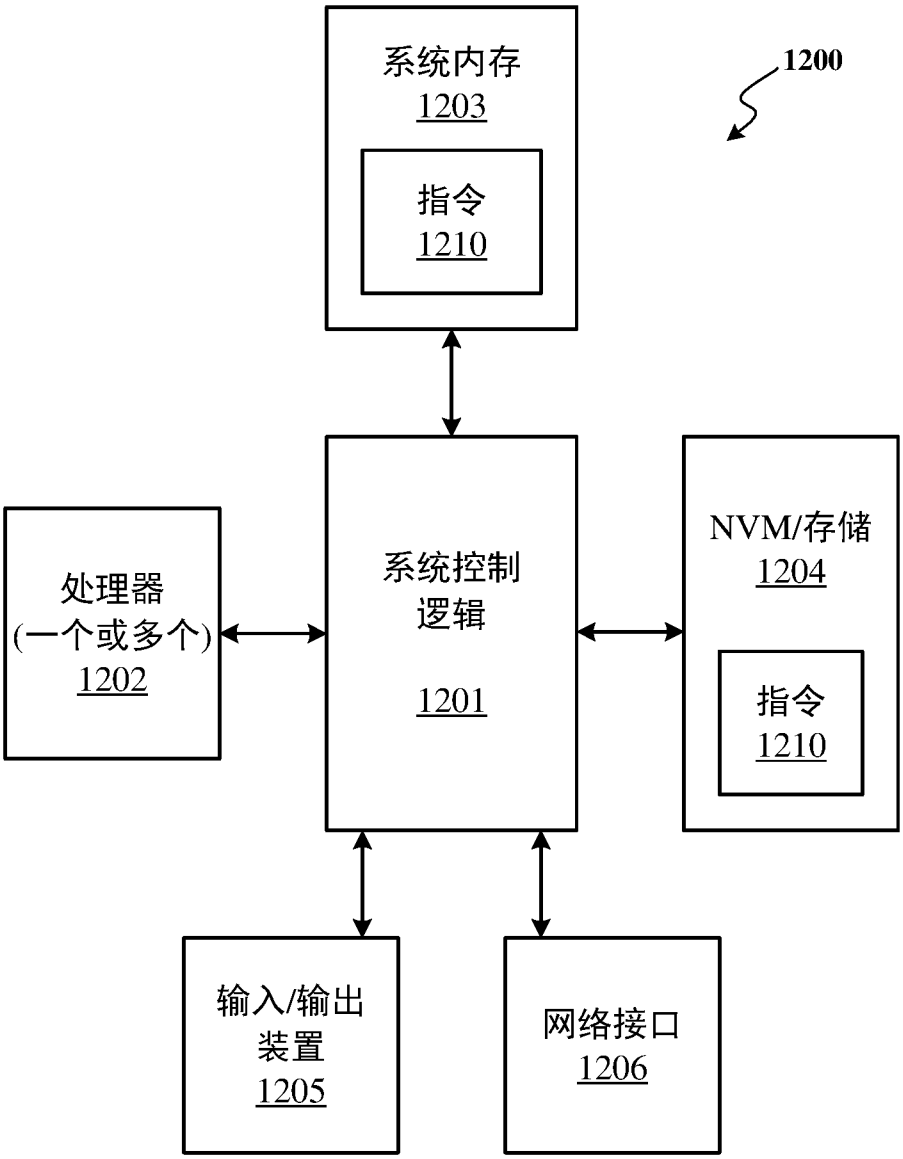
系统内存
1203
指令
1210
1200
处理器
(一个或多个)
1202
系统控制
逻辑
1201
NVM/存储
1204
指令
1210
输入/输出
装置
1205
网络接口
1206

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/093269

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/08(2006.01)i; G07C 9/00(2006.01)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)

H04L G07C

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)

CNTXT; CNABS; VEN; USTXT; EPTXT; WOTXT; CNKI: 门, 车, 锁, 加密, 密钥, 秘钥, 密码, 公钥, 私钥, 数字证书, 遥控, 控制, 指令, 蓝牙, 近场通信, 近距离通信, 对称算法, vehicle?, door?, lock+, unlock+, private 1d key, public 1d key, cipherkey, encryption, control, remote, instruction, command, Bluetooth, NFC, near 1w field, ZigBee, wifi

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104658090 A (HANGZHOU SYNOCHIP TECHNOLOGIES CO. LTD.) 27 May 2015 (2015-05-27) description, paragraphs [0010]-[0022], and figure 1	1-3, 7-9 , 11, 12, 15, 17, 18, 21-23, 25, 26, 28, 30-35
Y	CN 105307165 A (CHINA MINSHENG BANKING CORP., LTD.) 03 February 2016 (2016-02-03) description, paragraphs [0039]-[0058]	1-3, 7-9 , 11, 12, 15, 17, 18, 21-23, 25, 26, 28, 30-35
A	CN 105281909 A (ZHEJIANG JULIAN TECHNOLOGY CO., LTD.) 27 January 2016 (2016-01-27) entire document	1-35
A	US 9189900 B1 (PENILLA, A.A. ET AL.) 17 November 2015 (2015-11-17) entire document	1-35

☐ 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

"E" earlier application or patent but published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 August 2018	**03 September 2018**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/093269

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 104658090 A	27 May 2015	CN 104658090 B	21 July 2017
CN 105307165 A	03 February 2016	None	
CN 105281909 A	27 January 2016	None	
US 9189900 B1	17 November 2015	None	

国际检索报告

国际申请号 PCT/CN2018/093269

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/08(2006.01)i; G07C 9/00(2006.01)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)

H04L G07C

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））

CNTXT;CNABS;VEN;USTXT;EPTXT;WOTXT;CNKI：门，车，锁，加密，密钥，秘钥，密码，公钥，私钥，数字证书，遥控，控制，指令，蓝牙，近场通信，近距离通信，对称算法，vehicle?，door?，lock+，unlock+，private 1d key，public 1d key，cipherkey，encryption，control，remote，instruction，command，Bluetooth，NFC，near 1w field，ZigBee，wifi

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
Y	CN 104658090 A (杭州晟元芯片技术有限公司) 2015年 5月 27日 (2015-05-27) 说明书第[0010]-[0022]段，附图1	1-3、7-9、11、12、15、17、18、21-23、25、26、28、30-35
Y	CN 105307165 A (中国民生银行股份有限公司) 2016年 2月 3日 (2016-02-03) 说明书第[0039]-[0058]段	1-3、7-9、11、12、15、17、18、21-23、25、26、28、30-35
A	CN 105281909 A (浙江巨联科技股份有限公司) 2016年 1月 27日 (2016-01-27) 全文	1-35
A	US 9189900 B1 (PENILLA ANGEL A等) 2015年 11月 17日 (2015-11-17) 全文	1-35

☐ 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	国际检索报告邮寄日期
2018年 8月 23日	2018年 9月 3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 张筱蓉 电话号码 (86-512)88996084

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/093269

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 104658090 A	2015年 5月 27日	CN 104658090 B	2017年 7月 21日
CN 105307165 A	2016年 2月 3日	无	
CN 105281909 A	2016年 1月 27日	无	
US 9189900 B1	2015年 11月 17日	无	