(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111487887 B
(45)授权公告日 2023.11.28

(21)申请号 202010355732.8
(22)申请日 2020.04.29
(65)同一申请的已公布的文献号
申请公布号 CN 111487887 A
(43)申请公布日 2020.08.04
(73)专利权人 青岛海尔科技有限公司
地址 266101 山东省青岛市崂山区海尔路1号海尔工业园
(72)发明人 赵越
(74)专利代理机构 北京康盛知识产权代理有限公司 11331
专利代理师 陶俊洁
(51)Int.Cl.
G05B 15/02(2006.01)
G05B 19/418(2006.01)

(56)对比文件
CN 106603508 A,2017.04.26
CN 106130982 A,2016.11.16
CN 105959189 A,2016.09.21
CN 108173720 A,2018.06.15
WO 2019237502 A1,2019.12.19
CN 110708164 A,2020.01.17
CN 110703622 A,2020.01.17
CN 107566225 A,2018.01.09

审查员 刘佳妮

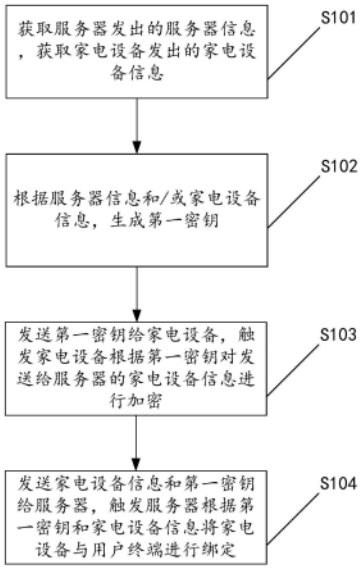
权利要求书3页 说明书12页 附图5页

(54)发明名称

用于绑定家电设备的方法、装置、用户终端、家电设备及服务器

(57)摘要

本申请涉及通信技术领域，公开一种用于绑定家电设备的方法，用于用户终端，包括：获取服务器发出的服务器信息，获取家电设备发出的家电设备信息；根据所述服务器信息和/或家电设备信息，生成第一密钥；发送所述第一密钥给所述家电设备，触发所述家电设备根据所述第一密钥对发送给服务器的家电设备信息进行加密；发送所述家电设备信息和所述第一密钥给所述服务器，触发所述服务器根据所述第一密钥和家电设备信息将所述家电设备与用户终端进行绑定。该方法能够确保服务器和家电设备的安全绑定，能够确保服务器和家电设备首次通信链路建立的安全性。本申请还公开一种用于绑定家电设备的装置、用户终端、家电设备及服务器。



CN 111487887 B

1.一种用于绑定家电设备的方法,用于用户终端,其特征在于,包括:

获取服务器发出的服务器信息,获取家电设备发出的家电设备信息;

根据所述服务器信息和/或家电设备信息,生成第一密钥;

发送所述第一密钥到所述家电设备,触发所述家电设备根据所述第一密钥对发送到服务器的家电设备信息进行加密;

发送所述家电设备信息和所述第一密钥到所述服务器,触发所述服务器根据所述第一密钥和家电设备信息将所述家电设备与用户终端进行绑定;

所述家电设备信息,包括家电设备身份标识,和/或,家电设备联网物理地址;所述服务器信息,包括以下中的一种或多种:服务器版本、服务器地址、用户信息和当前时间信息;

根据所述服务器信息和/或家电设备信息,生成第一密钥,包括:将服务器版本和服务器地址形成第一字段,将家电设备ID和家电设备联网MAC地址形成第二字段,将用户信息和当前时间信息形成第三字段;通过选取第一字段、第二字段和第三字段之中的一种或多种字段进行组合,以预设的对称密钥算法生成第一密钥,或,以预设的非对称密钥算法生成第一密钥。

2.根据权利要求1所述的方法,其特征在于,获取家电设备发出的家电设备信息,包括:

与所述家电设备建立点对点连接后,接收所述家电设备发出的家电设备信息。

3.根据权利要求2所述的方法,其特征在于,与所述家电设备建立点对点连接后,还包括:

获取家电设备发出的操作界面元素信息;

根据所述操作界面元素信息建立用于控制所述家电设备的控制界面。

4.根据权利要求1至3任一项所述的方法,其特征在于,发送所述第一密钥给所述家电设备时,还包括:

发送无线通信连接信息给所述家电设备,触发所述家电设备根据所述无线通信连接信息与所述服务器进行无线数据传输。

5.一种用于绑定家电设备的方法,用于家电设备,其特征在于,包括:

接收用户终端发出的第一密钥;

根据所述第一密钥对家电设备信息进行加密;

发送加密后的家电设备信息给服务器,触发所述服务器根据所述加密后的家电设备信息将所述用户终端与家电设备进行绑定;

接收用户终端发出的第一密钥前,还包括:识别到用户终端并与所述用户终端建立点对点连接;与所述用户终端建立点对点连接后,还包括:发送家电设备信息给所述用户终端,触发所述用户终端根据所述家电设备信息生成第一密钥;

所述家电设备信息,包括家电设备身份标识,和/或,家电设备联网物理地址;服务器信息,包括以下中的一种或多种:服务器版本、服务器地址、用户信息和当前时间信息;

所述用户终端通过以下方式根据所述家电设备信息生成第一密钥:将服务器版本和服务器地址形成第一字段,将家电设备ID和家电设备联网MAC地址形成第二字段,将用户信息和当前时间信息形成第三字段;通过选取第一字段、第二字段和第三字段之中的一种或多种字段进行组合,以预设的对称密钥算法生成第一密钥,或,以预设的非对称密钥算法生成第一密钥。

6.根据权利要求5所述的方法，其特征在于，发送家电设备信息给所述用户终端时，还包括：

发送操作界面元素信息给所述用户终端，触发所述用户终端根据所述家电设备信息建立用于控制所述家电设备的控制界面。

7.根据权利要求5或6所述的方法，其特征在于，接收用户终端发出的第一密钥时，还包括：

接收所述用户终端发出的无线通信连接信息；

根据所述无线通信连接信息与所述服务器进行无线数据传输。

8.根据权利要求5或6所述的方法，其特征在于，触发所述服务器根据所述加密后的家电设备信息将所述用户终端与家电设备进行绑定后，还包括：

接收所述服务器发出的第二密钥；

根据所述第二密钥与所述服务器建立连接。

9.根据权利要求8所述的方法，其特征在于，根据所述第二密钥与所述服务器建立连接后，还包括：

接收所述服务器发出的家电设备控制指令；

执行所述家电设备控制指令并反馈执行信息给所述服务器。

10.一种用于绑定家电设备的方法，用于服务器，其特征在于，包括：

接收用户终端发出的第一密钥和家电设备信息；

接收家电设备发出的加密后的家电设备信息；

根据所述第一密钥对所述加密后的家电设备信息进行解密，得到解密后的家电设备信息；

在根据所述第一密钥对所述加密后的家电设备信息解密成功且所述解密后的家电设备信息与所述用户终端发出的家电设备信息匹配成功的情况下，将所述用户终端与家电设备进行绑定；

接收用户终端发出的第一密钥前，还包括：与用户终端建立连接；发送服务器信息给所述用户终端，触发所述用户终端根据所述服务器信息生成第一密钥；

所述家电设备信息，包括家电设备身份标识，和/或，家电设备联网物理地址；所述服务器信息，包括以下中的一种或多种：服务器版本、服务器地址、用户信息和当前时间信息；

所述服务器通过以下方式根据所述服务器信息生成第一密钥：将服务器版本、服务器地址等要素形成第一字段，将家电设备ID和家电设备联网MAC地址形成第二字段，将用户信息和当前时间信息形成第三字段；通过选取第一字段、第二字段和第三字段之中的一种或多种字段进行组合，以预设的对称密钥算法生成第一密钥，或，以预设的非对称密钥算法生成第一密钥。

11.根据权利要求10所述的方法，其特征在于，所述解密后的家电设备信息与所述用户终端发出的家电设备信息匹配成功，包括：

所述用户终端发出的家电设备信息与所述解密后的家电设备信息相同；或，

多个所述用户终端发出的家电设备信息中，任一所述用户终端发出的家电设备信息与所述解密后的家电设备信息相同。

12.根据权利要求10或11所述的方法，其特征在于，在根据所述第一密钥对所述加密后

的家电设备信息解密成功且所述解密后的家电设备信息与所述用户终端发出的家电设备信息匹配成功的情况下，还包括：

生成第二密钥；

发送所述第二密钥给所述家电设备，触发所述家电设备根据所述第二密钥与服务器建立连接。

13.根据权利要求12所述的方法，其特征在于，根据以下中的一种或多种生成所述第二密钥：

用户信息、当前时间信息和解密后的家电设备信息。

14.根据权利要求12所述的方法，其特征在于，家电设备根据所述第二密钥与服务器建立连接后，还包括：

发送家电设备控制指令给所述家电设备，触发所述家电设备执行所述家电设备控制指令。

15.一种用于绑定家电设备的装置，包括第一处理器和存储有程序指令的第一存储器，其特征在于，所述第一处理器被配置为在执行所述程序指令时，执行如权利要求1至4任一项所述的用于绑定家电设备的方法。

16.一种用于绑定家电设备的装置，包括第二处理器和存储有程序指令的第二存储器，其特征在于，所述第二处理器被配置为在执行所述程序指令时，执行如权利要求5至9任一项所述的用于绑定家电设备的方法。

17.一种用于绑定家电设备的装置，包括第三处理器和存储有程序指令的第三存储器，其特征在于，所述第三处理器被配置为在执行所述程序指令时，执行如权利要求10至14任一项所述的用于绑定家电设备的方法。

18.一种用户终端，其特征在于，包括如权利要求15所述的用于绑定家电设备的装置。

19.一种家电设备，其特征在于，包括如权利要求16所述的用于绑定家电设备的装置。

20.一种服务器，其特征在于，包括如权利要求17所述的用于绑定家电设备的装置。

用于绑定家电设备的方法、装置、用户终端、家电设备及服务器

技术领域

[0001] 本申请涉及通信技术领域，例如涉及一种用于绑定家电设备的方法、装置、用户终端、家电设备及服务器。

背景技术

[0002] 现在随着智能家电的普及，越来越多的智能家电支持手机绑定和远程控制，潜移默化的改变了人类的生活，但当前家电绑定的方式对专业基础知识有一定的门槛要求。

[0003] 在实现本公开实施例的过程中，发现相关技术中至少存在如下问题：现有家电设备首次绑定用户终端并与厂家服务器通信时，在家电设备首次和厂家服务器通信后才获得安全密钥以具备后续的安全通信条件，但在厂家服务器接收智能家电第一次连接时，容易受到虚假设备的连接测试攻击。

发明内容

[0004] 为了对披露的实施例的一些方面有基本的理解，下面给出了简单的概括。所述概括不是泛泛评述，也不是要确定关键/重要组成元素或描绘这些实施例的保护范围，而是作为后面的详细说明的序言。

[0005] 本公开实施例提供了一种用于绑定家电设备的方法、装置、用户终端、家电设备及服务器，以提高家电设备与用户终端绑定的安全性。

[0006] 在一些实施例中，所述用于绑定家电设备的方法，用于用户终端，包括：

[0007] 获取服务器发出的服务器信息，获取家电设备发出的家电设备信息；

[0008] 根据所述服务器信息和/或家电设备信息，生成第一密钥；

[0009] 发送所述第一密钥给所述家电设备，触发所述家电设备根据所述第一密钥对发送给服务器的家电设备信息进行加密；

[0010] 发送所述家电设备信息和所述第一密钥给所述服务器，触发所述服务器根据所述第一密钥和家电设备信息将所述家电设备与用户终端进行绑定。

[0011] 在一些实施例中，所述用于绑定家电设备的装置包括：包括第一处理器和存储有程序指令的第一存储器，该第一处理器被配置为在执行所述程序指令时，执行上述的用于绑定家电设备的方法。

[0012] 在一些实施例中，所述用户终端包括上述的用于绑定家电设备的装置。

[0013] 在一些实施例中，所述用于绑定家电设备的方法，用于家电设备，包括：

[0014] 接收用户终端发出的第一密钥；

[0015] 根据所述第一密钥对家电设备信息进行加密；

[0016] 发送加密后的家电设备信息给服务器，触发所述服务器根据所述加密后的家电设备信息将所述用户终端与家电设备进行绑定。

[0017] 在一些实施例中，所述用于绑定家电设备的装置包括：包括第二处理器和存储有

程序指令的第二存储器，该第二处理器被配置为在执行所述程序指令时，执行上述的用于绑定家电设备的方法。

[0018] 在一些实施例中，所述家电设备包括上述的用于绑定家电设备的装置。

[0019] 在一些实施例中，所述用于绑定家电设备的方法，用于服务器，包括：

[0020] 接收用户终端发出的第一密钥和家电设备信息；

[0021] 接收家电设备发出的加密后的家电设备信息；

[0022] 根据所述第一密钥对所述加密后的家电设备信息进行解密，得到解密后的家电设备信息；

[0023] 在根据所述第一密钥对所述加密后的家电设备信息解密成功且所述解密后的家电设备信息与所述用户终端发出的家电设备信息匹配成功的情况下，将所述用户终端与家电设备进行绑定。

[0024] 在一些实施例中，所述用于绑定家电设备的装置包括：包括第三处理器和存储有程序指令的第三存储器，该第三处理器被配置为在执行所述程序指令时，执行上述的用于绑定家电设备的方法。

[0025] 在一些实施例中，所述服务器包括上述的用于绑定家电设备的装置。

[0026] 本公开实施例提供的用于绑定家电设备的方法、装置、用户终端、家电设备及服务器，可以实现以下技术效果：通过发送家电设备信息给服务器，并分别发送密钥给家电设备和服务器，使得家电设备第一次发起与服务器连接时，服务器可以通过家电设备发送的信息和用户终端上传的信息做对照，检验家电设备连接的真实性和合法性，确保了服务器和家电设备首次通信链路的安全建立，从而确保了用户终端和家电设备的安全绑定。

[0027] 以上的总体描述和下文中的描述仅是示例性和解释性的，不用于限制本申请。

附图说明

[0028] 一个或多个实施例通过与之对应的附图进行示例性说明，这些示例性说明和附图并不构成对实施例的限定，附图中具有相同参考数字标号的元件示为类似的元件，附图不构成比例限制，并且其中：

[0029] 图1是本公开实施例提供的一个用于绑定家电设备的方法的示意图；

[0030] 图2是本公开实施例提供的另一个用于绑定家电设备的方法的示意图；

[0031] 图3是本公开实施例提供的另一个用于绑定家电设备的方法的示意图；

[0032] 图4本公开实施例提供的一个用于绑定家电设备的方法的时序图；

[0033] 图5是本公开实施例提供的一个用于绑定家电设备的装置的示意图；

[0034] 图6是本公开实施例提供的另一个用于绑定家电设备的装置的示意图；

[0035] 图7是本公开实施例提供的另一个用于绑定家电设备的装置的示意图。

具体实施方式

[0036] 为了能够更加详尽地了解本公开实施例的特点与技术内容，下面结合附图对本公开实施例的实现进行详细阐述，所附附图仅供参考说明之用，并非用来限定本公开实施例。在以下的技术描述中，为方便解释起见，通过多个细节以提供对所披露实施例的充分理解。然而，在没有这些细节的情况下，一个或多个实施例仍然可以实施。在其它情况下，为简化

附图,熟知的结构和装置可以简化展示。

[0037] 本公开实施例的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本公开实施例的实施例。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含。

[0038] 除非另有说明,术语“多个”表示两个或两个以上。

[0039] 本公开实施例中,字符“/”表示前后对象是一种“或”的关系。例如,A/B表示:A或B。

[0040] 术语“和/或”是一种描述对象的关联关系,表示可以存在三种关系。例如,A和/或B,表示:A或B,或,A和B这三种关系。

[0041] 结合图1所示,本公开实施例提供一种用于绑定家电设备的方法,用于用户终端,包括:

[0042] 步骤S101,获取服务器发出的服务器信息,获取家电设备发出的家电设备信息;

[0043] 步骤S102,根据服务器信息和/或家电设备信息,生成第一密钥;

[0044] 步骤S103,发送第一密钥给家电设备,触发家电设备根据第一密钥对发送给服务器的家电设备信息进行加密;

[0045] 步骤S104,发送家电设备信息和第一密钥给服务器,触发服务器根据第一密钥和家电设备信息将家电设备与用户终端进行绑定。

[0046] 采用本公开实施例提供的用于绑定家电设备的方法,根据服务器信息和家电设备信息生成第一密钥,将第一密钥发送给家电设备和服务器,触发家电设备根据第一密钥对发送给服务器的家电设备信息进行加密,确保了服务器和家电设备首次通信链路建立的安全性。并触发服务器根据用户终端发送的第一密钥和家电设备信息对家电设备和用户终端进行绑定,提高了家电设备绑定的安全性。

[0047] 可选地,触发服务器根据第一密钥对家电设备发送的加密后的家电设备信息进行解密;并触发服务器将用户终端发送的家电设备信息作为对照信息与解密后的家电设备信息进行匹配,验证解密后的家电设备信息的真实性和合法性,当用户终端发送的家电设备信息与解密后的家电设备信息匹配成功,则将用户终端与家电设备进行绑定。可选地,用户终端发送的家电设备信息与解密后的家电设备信息相同即为匹配成功。

[0048] 可选地,通过WIFI连接服务器,获取服务器发送的服务器信息。

[0049] 可选地,获取家电设备发出的家电设备信息,包括:与家电设备建立点对点连接后,接收家电设备发出的家电设备信息。可选地,与家电设备通过NFC(Near Field Communication,近场通信)建立点对点通信。

[0050] 可选地,服务器信息,包括以下中的一种或多种:服务器版本、服务器地址、用户信息和当前时间信息。可选地,用户信息为通过用户终端当前登录的用户的信息;当前时间信息为用户终端触发绑定操作时服务器的当前时间。可选地,用户终端触发绑定操作为用户终端与服务器建立连接。

[0051] 可选地,家电设备信息,包括家电设备身份标识,和/或,家电设备联网物理地址。

[0052] 可选地,将服务器版本、服务器地址等要素形成第一字段,将家电设备ID(Identity Document,身份标识)、家电设备联网MAC地址(Media Access Control Address,物理地址)等要素形成第二字段,将当前通过用户终端登录的用户信息及服务器

的当前时间形成第三字段。通过选取第一字段、第二字段和第三字段之中的一种或多种字段进行组合，以TDEA(Triple Data Encryption Algorithm，三重数据加密算法)、Blowfish(区块加密算法)、3DES(Triple DES)等对称密钥算法生成第一密钥，或，以RSA加密算法(RSA algorithm)等非对称密钥算法生成第一密钥。

[0053] 将第一密钥通过NFC发送到家电设备，通过WIFI发送给服务器，用作家电设备和服务器第一次建立安全连接使用的临时密钥，确保了家电设备与服务器首次建立连接的安全性，从而提高了家电设备绑定的效率和安全性。

[0054] 可选地，与家电设备建立点对点连接后，还包括：获取家电设备发出的操作界面元素信息；根据操作界面元素信息建立用于控制家电设备的控制界面。这样，在用户终端内建立家电设备控制界面，使得用户终端可作为家电设备尤其是无屏家电设备的操作界面，便于用户直观操作家电设备。

[0055] 可选地，发送第一密钥给家电设备时，还包括：发送无线通信连接信息给家电设备，触发家电设备根据无线通信连接信息与服务器进行无线数据传输。

[0056] 结合图2所示，本公开实施例提供另一种用于绑定家电设备的方法，用于家电设备，包括：

[0057] 步骤S201、接收用户终端发出的第一密钥；

[0058] 步骤S202、根据第一密钥对家电设备信息进行加密；

[0059] 步骤S203、发送加密后的家电设备信息给服务器，触发服务器根据加密后的家电设备信息将用户终端与家电设备进行绑定。

[0060] 采用本公开实施例提供的用于绑定家电设备的方法，根据用户终端发送的第一密钥对家电设备信息进行加密，并发送加密后的家电设备信息给服务器，确保了服务器和家电设备建立首次通信链路的安全性。并触发服务器根据加密后的家电设备信息将用户终端与家电设备进行绑定，提高了家电设备绑定的安全性。

[0061] 可选地，触发服务器根据第一密钥对加密后的家电设备信息进行解密；并触发服务器根据用户终端发送的家电设备信息作为对照信息与解密后的家电设备信息进行匹配，验证解密后的家电设备信息的真实性和合法性，当用户终端发送的家电设备信息与解密后的家电设备信息匹配成功，则将用户终端与家电设备进行绑定。可选地，用户终端发送的家电设备信息与解密后的家电设备信息相同即为匹配成功。

[0062] 可选地，家电设备信息，包括家电设备身份标识，和/或，家电设备联网物理地址。

[0063] 可选地，接收用户终端发出的第一密钥前，还包括：识别到用户终端并与用户终端建立点对点连接。可选地，与用户终端通过NFC(Near Field Communication，近场通信)建立点对点通信。

[0064] 可选地，与用户终端建立点对点连接后，还包括：发送家电设备信息给用户终端，触发用户终端根据家电设备信息生成第一密钥。

[0065] 可选地，触发用户终端将服务器版本、服务器地址等要素形成第一字段，将家电设备ID(Identity Document，身份标识)、家电设备联网MAC地址(Media Access Control Address，物理地址)等要素形成第二字段，将当前通过用户终端登录的用户信息及服务器的当前时间形成第三字段；通过选取第一字段、第二字段和第三字段之中的一种或多种字段进行组合，以TDEA(Triple Data Encryption Algorithm，三重数据加密算法)、Blowfish

(区块加密算法)、3DES(Triple DES)等对称密钥算法生成第一密钥,或,以RSA加密算法(RSA algorithm)等非对称密钥算法生成第一密钥。

[0066] 通过NFC接收用户终端发出的第一密钥,根据第一密钥对发送到服务器的家电设备信息进行加密,将第一密钥用作家电设备和服务器第一次安全连接建立使用的临时密钥,确保了家电设备与服务器首次建立连接的安全性,从而提高了家电设备绑定的效率和安全性。

[0067] 可选地,发送家电设备信息给用户终端时,还包括:发送操作界面元素信息给用户终端,触发用户终端根据家电设备信息建立用于控制家电设备的控制界面。这样,在用户终端内建立家电设备控制界面,使得用户终端可作为家电设备尤其是无屏家电设备的操作界面,便于用户直观操作家电设备。

[0068] 可选地,接收用户终端发出的第一密钥时,还包括:接收用户终端发出的无线通信连接信息;根据无线通信连接信息与服务器进行无线数据传输。

[0069] 可选地,触发服务器根据加密后的家电设备信息将用户终端与家电设备进行绑定后,还包括:接收服务器发出的第二密钥;根据第二密钥与服务器建立连接。

[0070] 可选地,根据第二密钥与服务器建立连接后,还包括:接收服务器发出的家电设备控制指令;执行家电设备控制指令并反馈执行信息给服务器。

[0071] 结合图3所示,本公开实施例提供另一种用于绑定家电设备的方法,用于服务器,包括:

[0072] 步骤S301、接收用户终端发出的第一密钥和家电设备信息;

[0073] 步骤S302、接收家电设备发出的加密后的家电设备信息;

[0074] 步骤S303、根据第一密钥对加密后的家电设备信息进行解密,得到解密后的家电设备信息;

[0075] 步骤S304、在根据第一密钥对加密后的家电设备信息解密成功且解密后的家电设备信息与用户终端发出的家电设备信息匹配成功的情况下,将用户终端与家电设备进行绑定。

[0076] 可选地,用户终端发送的家电设备信息与解密后的家电设备信息相同即为匹配成功。

[0077] 采用本公开实施例提供的用于绑定家电设备的方法,通过获取用户终端发出的第一密钥和家电设备信息,根据第一密钥对加密后的家电设备信息进行解密,将用户终端发送的家电设备信息与解密后的家电设备信息进行匹配,匹配成功的情况下,用户终端与家电设备才能绑定,确保了服务器和家电设备首次通信链路建立的安全性的同时,提高了家电设备绑定的安全性。

[0078] 可选地,家电设备信息,包括家电设备身份标识,和/或,家电设备联网物理地址。

[0079] 可选地,解密后的家电设备信息与用户终端发出的家电设备信息匹配成功,包括:用户终端发出的家电设备信息与解密后的家电设备信息相同;或,多个用户终端发出的家电设备信息中,任一用户终端发出的家电设备信息与解密后的家电设备信息相同。

[0080] 可选地,接收用户终端发出的第一密钥前,还包括:与用户终端建立连接;发送服务器信息给用户终端,触发用户终端根据服务器信息生成第一密钥。可选地,通过WIFI与用户终端建立连接。

[0081] 可选地，服务器信息，包括以下中的一种或多种：服务器版本、服务器地址、用户信息和当前时间信息。可选地，用户信息为通过用户终端当前登录的用户的信息；当前时间信息为用户终端触发绑定操作时服务器的当前时间。可选地，用户终端触发绑定操作为用户终端与服务器建立连接。

[0082] 可选地，触发用户终端将服务器版本、服务器地址等要素形成第一字段，将家电设备ID(Identity Document，身份标识)、家电设备联网MAC地址(Media Access Control Address，物理地址)等要素形成第二字段，将当前通过用户终端登录的用户信息及服务器的当前时间形成第三字段；通过选取第一字段、第二字段和第三字段之中的一种或多种字段进行组合，以TDEA(Triple Data Encryption Algorithm，三重数据加密算法)、Blowfish(区块加密算法)、3DES(Triple DES)等对称密钥算法生成第一密钥，或，以RSA加密算法(RSA algorithm)等非对称密钥算法生成第一密钥。

[0083] 通过WIFI接收用户终端发出的第一密钥，根据第一密钥对加密后的家电设备信息进行解密，将第一密钥用作家电设备和服务器第一次安全连接建立使用的临时密钥，确保了家电设备与服务器首次建立连接的安全性，从而提高了家电设备绑定的效率和安全性。

[0084] 可选地，在根据第一密钥对加密后的家电设备信息解密成功且解密后的家电设备信息与用户终端发出的家电设备信息匹配成功的情况下，还包括：生成第二密钥；发送第二密钥给家电设备，触发家电设备根据第二密钥与服务器建立连接。可选地，记录第二密钥的生成时间和过期时间，当第二密钥过期，则生成新的第二密钥，并更新第二密钥的生成时间和过期时间。第二密钥为家电设备与服务器建立安全连接的正式密钥。

[0085] 可选地，根据以下中的一种或多种生成第二密钥：

[0086] 用户信息、当前时间信息和解密后的家电设备信息。可选地，用户信息为与服务器建立连接的用户终端的用户信息；当前时间信息为服务器的当前时间信息。

[0087] 可选地，通过选取用户信息、当前时间信息和解密后的家电设备信息中的一种或多种进行组合，以非对称密钥算法生成第二密钥。

[0088] 可选地，家电设备根据第二密钥与服务器建立连接后，还包括：

[0089] 发送家电设备控制指令给家电设备，触发家电设备执行家电设备控制指令。

[0090] 如图4所示，在实际应用中，绑定家电设备的方法具体包括如下步骤：

[0091] 步骤S401、用户终端开启家电设备管控APP，登录账号和密码，并开启NFC使用权限；

[0092] 步骤S402、用户终端通过WIFI与服务器建立连接；

[0093] 步骤S403、服务器发送用户信息和服务器当前的时间信息到用户终端；

[0094] 步骤S404、用户终端根据用户信息及服务器的当前时间形成第一密钥所需的第三字段；

[0095] 步骤S405、用户终端向服务器发送请求服务器版本和服务器地址的请求信息；

[0096] 步骤S406、服务器发送服务器版本和服务器地址给用户终端；

[0097] 步骤S407、用户终端根据服务器版本和服务器地址形成第一密钥所需的第一字段；

[0098] 步骤S408、用户终端与家电设备通过NFC建立点对点通信；

[0099] 步骤S409、家电设备识别到用户终端并与用户终端通过NFC建立点对点通信；

[0100] 步骤S410、家电设备发送家电设备信息，即家电设备ID和家电设备MAC地址到用户终端；

[0101] 步骤S411、用户终端根据家电设备ID和家电设备MAC地址形成第一密钥所需的第二字段；

[0102] 步骤S412、家电设备发送操作界面元素信息给用户终端；

[0103] 步骤S413、用户终端根据家电设备信息建立用于控制家电设备的控制界面；

[0104] 步骤S414、用户终端根据第一字段、第二字段和第三字段通过加密算法生成第一密钥；

[0105] 步骤S415、用户终端发送家电设备信息和第一密钥到服务器；

[0106] 步骤S416、用户终端发送第一密钥和WIFI连接信息给家电设备；

[0107] 步骤S417、家电设备通过WIFI连接信息连接网络，与服务器进行无线数据传输；

[0108] 步骤S418、家电设备通过第一密钥向服务器发起首次安全通信连接请求，即家电设备发送根据第一密钥加密后的家电设备信息给服务器；

[0109] 步骤S419、服务器根据第一密钥对家电设备发送的加密后的家电设备信息进行解密，并将用户终端发送的家电设备信息与解密后的家电设备信息进行匹配；

[0110] 步骤S420、在用户终端发送的家电设备信息与解密后的家电设备信息匹配成功的情况下，服务器与家电设备建立首次安全连接，同时，绑定家电设备与用户终端；服务器生成第二密钥，并记录第二密钥生成时间和过期时间；

[0111] 步骤S421、服务器发送第二密钥给家电设备；

[0112] 步骤S422、服务器发送家电设备与用户终端绑定成功消息给用户终端；

[0113] 步骤S423、用户终端激活控制家电设备的控制界面；

[0114] 步骤S424、家电设备通过第二密钥向服务器发起建立连接请求；

[0115] 步骤S425、服务器接收家电设备通过第二密钥向服务器发起建立连接请求；

[0116] 步骤S426、在第二密钥正确且在有效期内，服务器发送家电设备与服务器连接成功消息给用户终端；

[0117] 步骤S427、用户终端通过控制界面显示家电设备在线信息；

[0118] 步骤S428、用户终端发送家电设备控制指令给服务器；

[0119] 步骤S429、服务器发送家电设备控制指令给家电设备；

[0120] 步骤S430、家电设备获得控制指令并执行该控制指令；

[0121] 步骤S431、家电设备向服务器返回执行成功信息；

[0122] 步骤S432、服务器向用户终端返回家电设备控制指令执行成功信息；

[0123] 步骤S433、用户终端通过控制界面显示执行成功效果。

[0124] 通过上述公开实施例提供的绑定家电设备的方法，能够通过基于NFC建立用户终端与家电设备的通信链路，以家电设备预制的操作界面元素信息在用户终端中建立用于控制家电设备的控制界面，为家电设备的配置及操作提供了便利性。并且由用户终端生成安全通信的第一密钥，通过NFC传输第一密钥给家电设备，通过无线通信网络传输第一密钥给服务器，使家电设备和服务器首次建立连接更加安全；同时，由家电设备通过NFC传输给用户终端的家电设备信息，通过用户终端再次传输给服务器，在家电设备还未向服务器发起连时，即获得家电设备的重要信息作为对比依据，使得家电设备在真实发起第一次向服务

器连接时，通过其发送到服务器的信息和用户终端发送到服务器的信息进行匹配检验，有助于服务器检测到虚假的家电设备连接请求，大大提高了服务器的安全和效率，且在匹配成功的情况下，用户终端与家电设备才能绑定，这也大大提高了用户终端与家电设备绑定的安全性。

[0125] 结合图5所示，本公开实施例提供一种用于绑定家电设备的装置，包括第一处理器(processor)100和存储有程序指令的第一存储器(memory)101，还可以包括第一通信接口(Communication Interface)102和第一总线103。其中，第一处理器100、第一通信接口102、第一存储器101可以通过第一总线103完成相互间的通信。第一通信接口102可以用于信息传输。第一处理器100可以调用第一存储器101中的程序指令，以执行上述实施例的用于绑定家电设备的方法。

[0126] 此外，上述的第一存储器101中的程序指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。

[0127] 第一存储器101作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序，如本公开实施例中的方法对应的程序指令/模块。第一处理器100通过运行存储在第一存储器101中的程序指令/模块，从而执行功能应用以及数据处理，即实现上述实施例中用于绑定家电设备的方法。

[0128] 第一存储器101可包括第一存储程序区和第一存储数据区，其中，第一存储程序区可存储操作系统、至少一个功能所需的应用程序；第一存储数据区可存储根据终端设备的使用所创建的数据等。此外，第一存储器101可以包括高速随机存取存储器，还可以包括非易失性存储器。

[0129] 采用本公开实施例提供的用于绑定家电设备的装置，根据服务器信息和家电设备信息生成第一密钥，将第一密钥发送给家电设备和服务器，触发家电设备根据第一密钥对发送给服务器的家电设备信息进行加密，确保了服务器和家电设备首次通信链路建立的安全性。并触发服务器根据用户终端发送的第一密钥和家电设备信息对家电设备和用户终端进行绑定，提高了家电设备绑定的安全性。

[0130] 结合图6所示，本公开实施例提供另一种用于通信的装置，包括第二处理器(processor)200和存储有程序指令的第二存储器(memory)201，还可以包括第二通信接口(Communication Interface)202和第二总线203。其中，第二处理器200、第二通信接口202、第二存储器201可以通过第二总线203完成相互间的通信。第二通信接口202可以用于信息传输。第二处理器200可以调用第二存储器201中的程序指令，以执行上述实施例的用于绑定家电设备的方法

[0131] 此外，上述的第二存储器201中的程序指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。

[0132] 第二存储器201作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序，如本公开实施例中的方法对应的程序指令/模块。第二处理器200通过运行存储在第二存储器201中的程序指令/模块，从而执行功能应用以及数据处理，即实现上述实施例中用于绑定家电设备的方法。

[0133] 第二存储器201可包括第二存储程序区和第二存储数据区，其中，第二存储程序区可存储操作系统、至少一个功能所需的应用程序；第二存储数据区可存储根据终端设备的

使用所创建的数据等。此外，第二存储器201可以包括高速随机存取存储器，还可以包括非易失性存储器。

[0134] 采用本公开实施例提供的用于绑定家电设备的装置，根据用户终端发送的第一密钥对家电设备信息进行加密，并发送加密后的家电设备信息给服务器，确保了服务器和家电设备首次通信链路建立的安全性。并触发服务器根据加密后的家电设备信息将用户终端与家电设备进行绑定，提高了家电设备绑定的安全性。

[0135] 结合图7所示，本公开实施例提供另一种用于通信的装置，包括第三处理器(processor)300和存储有程序指令的第三存储器(memory)301，还可以包括第三通信接口(Communication Interface)302和第三总线303。其中，第三处理器300、第三通信接口302、第三存储器301可以通过第三总线303完成相互间的通信。第三通信接口302可以用于信息传输。第三处理器300可以调用第三存储器301中的程序指令，以执行上述实施例的用于绑定家电设备的方法

[0136] 此外，上述的第三存储器301中的程序指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。

[0137] 第三存储器301作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序，如本公开实施例中的方法对应的程序指令/模块。第三处理器300通过运行存储在第三存储器301中的程序指令/模块，从而执行功能应用以及数据处理，即实现上述实施例中用于绑定家电设备的方法。

[0138] 第三存储器301可包括第三存储程序区和第三存储数据区，其中，第三存储程序区可存储操作系统、至少一个功能所需的应用程序；第三存储数据区可存储根据终端设备的使用所创建的数据等。此外，第三存储器301可以包括高速随机存取存储器，还可以包括非易失性存储器。

[0139] 采用本公开实施例提供的用于绑定家电设备的装置，通过获取用户终端发出的第一密钥和家电设备信息，根据第一密钥对加密后的家电设备信息进行解密，得到解密后的家电设备信息，将用户终端发送的家电设备信息与解密后的家电设备信息进行匹配，匹配成功的情况下，用户终端与家电设备才能绑定，确保了服务器和家电设备首次通信链路建立的安全性的同时，提高了家电设备绑定的安全性。

[0140] 在一些实施例中，用户终端为智能手机、平板电脑等。可选地，用户终端包括：第一NFC通信模块、控制界面生成模块、第一密钥生成模块和第一传输控制模块；

[0141] 第一NFC通信模块，用于于家电设备建立NFC点对点通信，接收家电设备发送到用户终端的家电设备操作界面元素信息和家电设备信息，发送第一密钥给家电设备；

[0142] 控制界面生成模块，用于根据家电设备发送的操作界面元素信息建立用于控制家电设备的控制界面，并通过NFC通信与家电设备互动；

[0143] 第一密钥生成模块，用于生成第一密钥；

[0144] 第一传输控制模块，用于管理用户终端与服务器，和，用户终端与家电设备之间的数据传输，用于发送第一密钥和家电设备信息给服务器，接收服务器发送的服务器信息。

[0145] 可选地，家电设备包括：第二NFC通信模块、第一安全通信模块和第二传输控制模块；

[0146] 第二NFC通信模块，用于监听靠近家电设备的用户终端，并建立于识别到的用户终

端建立NFC点对点通信，发送家电设备信息和家电设备操作界面元素信息到用户终端，接收用户终端发送的第一密钥；

[0147] 第一安全通信模块，用于与服务器通过第二密钥建立安全通信链路；

[0148] 第二传输控制模块，用于管理家电设备与用户终端，和家电设备与服务器之间的数据传输；接收服务器发送的第二密钥。

[0149] 可选地，服务器包括：第二安全通信模块、设备检验模块、第二密钥生成模块和第三传输控制模块；

[0150] 第二安全通信模块，用于接收家电设备的安全通信连接请求；

[0151] 设备检验模块，用于通过用户终端发送的家电设备信息与解密后的家电设备发送的家电设备信息进行匹配，来检验家电设备发送的家电设备信息的真实性和合法性；

[0152] 第二密钥生成模块，用于生成第二密钥，以便更新家电设备与服务器之间的安全通信密钥；

[0153] 第三传输控制模块，用于管理服务器与用户终端，和，服务器与家电设备之间的数据传输，接收用户终端发送的第一密钥和家电设备信息，发送第二密钥给家电设备。

[0154] 通过用户终端与家电设备建立NFC点对点通信，接收来自家电设备发送的家电设备信息，在用户终端需要绑定家电设备的同时，将通过服务器信息和家电设备信息生成的第一密钥通过NFC发送给家电设备，使家电设备对发送给服务器的家电设备信息进行加密；同时，将家电设备信息和第一密钥发送给服务器，使服务器首次获得即将第一次与其连接的家电设备信息，使家电设备第一次发起与服务器连接时，服务器可以通过家电设备发送的信息进行解密后与用户终端上传的信息进行匹配，检验家电设备连接的真实性和合法性，从而确保了服务器和家电设备首次通信链路建立的安全性；并在匹配成功的情况下，用户终端与家电设备才能绑定，也提高了家电设备绑定的安全性；并且在此安全链路下服务器生成第二密钥，将第二密钥发送到家电设备，完成第一密钥的更新，后续通信将通过第二密钥进行建立。

[0155] 本公开实施例提供了一种用户终端，包含上述的用于绑定家电设备的装置。

[0156] 可选地，用户终端为智能手机、平板电脑等。

[0157] 该用户终端能够根据服务器信息和家电设备信息生成第一密钥，将第一密钥发送给家电设备和服务器，触发家电设备根据第一密钥对发送给服务器的家电设备信息进行加密，确保了服务器和家电设备首次通信链路建立的安全性。并触发服务器根据用户终端发送的第一密钥和家电设备信息对家电设备和用户终端进行绑定，提高了家电设备绑定的安全性

[0158] 本公开实施例提供了一种家电设备，包含上述的用于绑定家电设备的装置。该家电设备能够根据用户终端发送的第一密钥对家电设备信息进行加密，并发送加密后的家电设备信息给服务器，确保了服务器和家电设备首次通信链路建立的安全性。并触发服务器根据加密后的家电设备信息将用户终端与家电设备进行绑定，提高了家电设备绑定的安全性。

[0159] 本公开实施例提供了一种服务器，包含上述的用于绑定家电设备的装置。该服务器能够通过获取用户终端发出的第一密钥和家电设备信息，根据第一密钥对加密后的家电设备信息进行解密，得到解密后的家电设备信息，将用户终端发送的家电设备信息与解密

后的家电设备信息进行匹配，匹配成功的情况下，用户终端与家电设备才能绑定，确保了服务器和家电设备首次通信链路建立的安全性的同时，提高了家电设备绑定的安全性。

[0160] 本公开实施例提供了一种计算机可读存储介质，存储有计算机可执行指令，计算机可执行指令设置为执行上述用于…的方法。

[0161] 本公开实施例提供了一种计算机程序产品，计算机程序产品包括存储在计算机可读存储介质上的计算机程序，计算机程序包括程序指令，当程序指令被计算机执行时，使计算机执行上述用于…的方法。

[0162] 上述的计算机可读存储介质可以是暂态计算机可读存储介质，也可以是非暂态计算机可读存储介质。

[0163] 本公开实施例的技术方案可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括一个或多个指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本公开实施例所述方法的全部或部分步骤。而前述的存储介质可以是非暂态存储介质，包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等多种可以存储程序代码的介质，也可以是暂态存储介质。

[0164] 以上描述和附图充分地示出了本公开的实施例，以使本领域的技术人员能够实践它们。其他实施例可以包括结构的、逻辑的、电气的、过程的以及其他的改变。实施例仅代表可能的变化。除非明确要求，否则单独的部件和功能是可选的，并且操作的顺序可以变化。一些实施例的部分和特征可以被包括在或替换其他实施例的部分和特征。而且，本申请中使用的用词仅用于描述实施例并且不用于限制权利要求。如在实施例以及权利要求的描述中使用的，除非上下文清楚地表明，否则单数形式的“一个”(a)、“一个”(an)和“所述”(the)旨在同样包括复数形式。类似地，如在本申请中所使用的术语“和/或”是指包含一个或一个以上相关联的列出的任何以及所有可能的组合。另外，当用于本申请中时，术语“包括”(comprise)及其变型“包括”(comprises)和/或包括(comprising)等指陈述的特征、整体、步骤、操作、元素，和/或组件的存在，但不排除一个或一个以上其它特征、整体、步骤、操作、元素、组件和/或这些的分组的存在或添加。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、方法或者设备中还存在另外的相同要素。本文中，每个实施例重点说明的可以是与其他实施例的不同之处，各个实施例之间相同相似部分可以互相参见。对于实施例公开的方法、产品等而言，如果其与实施例公开的方法部分相对应，那么相关之处可以参见方法部分的描述。

[0165] 本领域技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，可以取决于技术方案的特定应用和设计约束条件。所述技术人员可以对每个特定的应用来使用不同方法以实现所描述的功能，但是这种实现不应认为超出本公开实施例的范围。所述技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0166] 本文所披露的实施例中，所揭露的方法、产品(包括但不限于装置、设备等)，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的

划分，可以仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例。另外，在本公开实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0167] 附图中的流程图和框图显示了根据本公开实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这可以依所涉及的功能而定。在附图中的流程图和框图所对应的描述中，不同的方框所对应的操作或步骤也可以以不同于描述中所披露的顺序发生，有时不同的操作或步骤之间不存在特定的顺序。例如，两个连续的操作或步骤实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这可以依所涉及的功能而定。框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

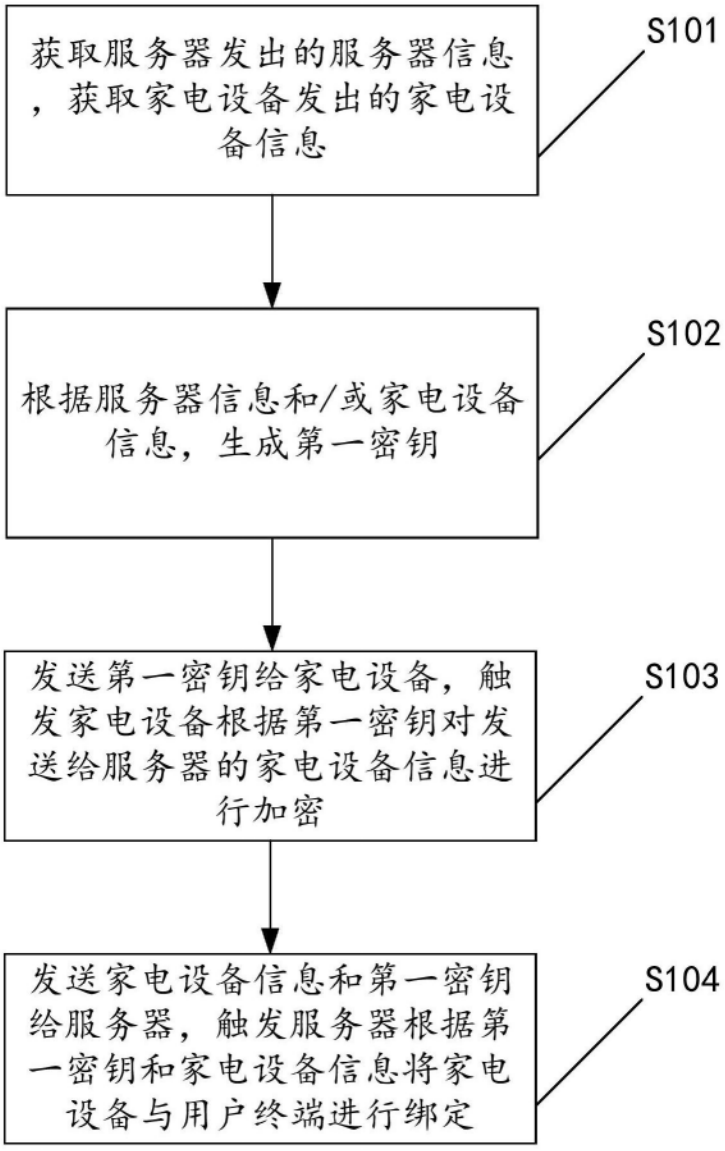

获取服务器发出的服务器信息，获取家电设备发出的家电设备信息
S101
根据服务器信息和/或家电设备信息，生成第一密钥
S102
发送第一密钥给家电设备，触发家电设备根据第一密钥对发送给服务器的家电设备信息进行加密
S103
发送家电设备信息和第一密钥给服务器，触发服务器根据第一密钥和家电设备信息将家电设备与用户终端进行绑定
S104

图1

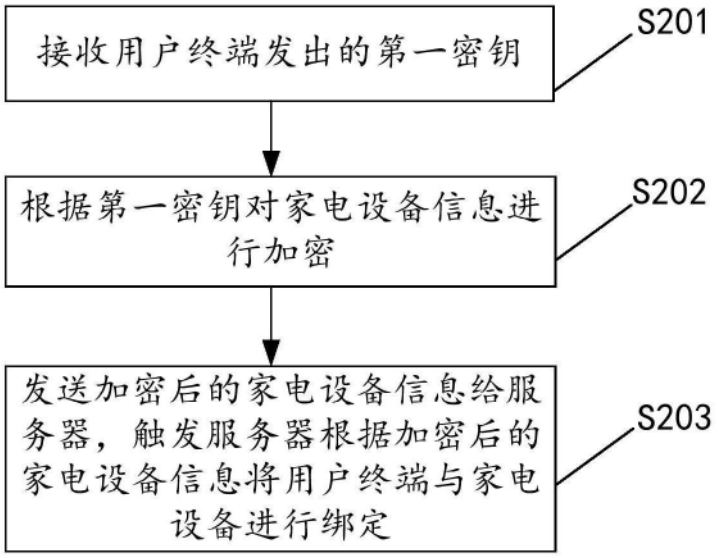

接收用户终端发出的第一密钥
S201
根据第一密钥对家电设备信息进行加密
S202
发送加密后的家电设备信息给服务器，触发服务器根据加密后的家电设备信息将用户终端与家电设备进行绑定
S203

图2

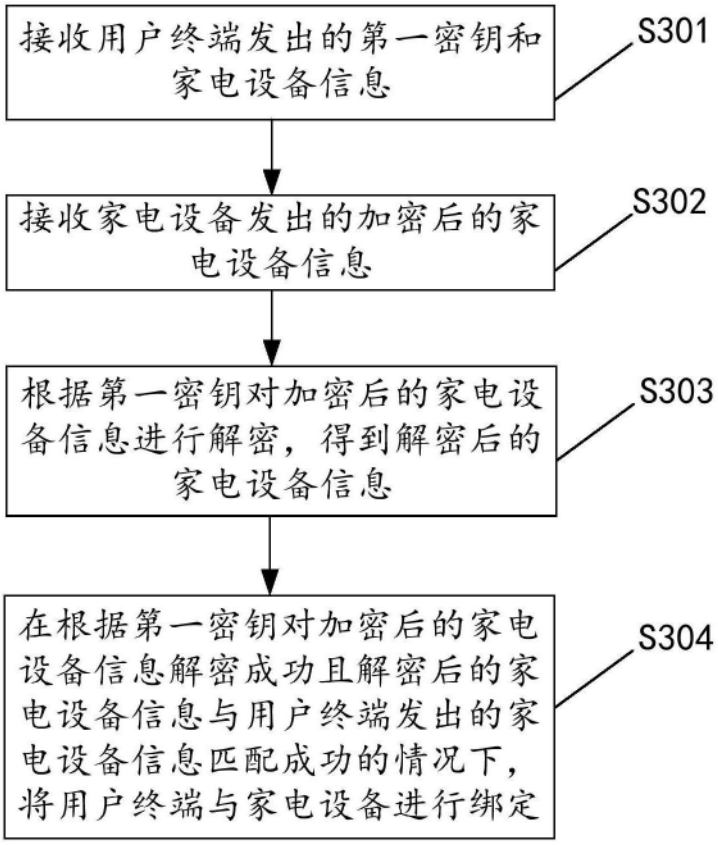

接收用户终端发出的第一密钥和家电设备信息
S301
接收家电设备发出的加密后的家电设备信息
S302
根据第一密钥对加密后的家电设备信息进行解密，得到解密后的家电设备信息
S303
在根据第一密钥对加密后的家电设备信息解密成功且解密后的家电设备信息与用户终端发出的家电设备信息匹配成功的情况下，将用户终端与家电设备进行绑定
S304

图3

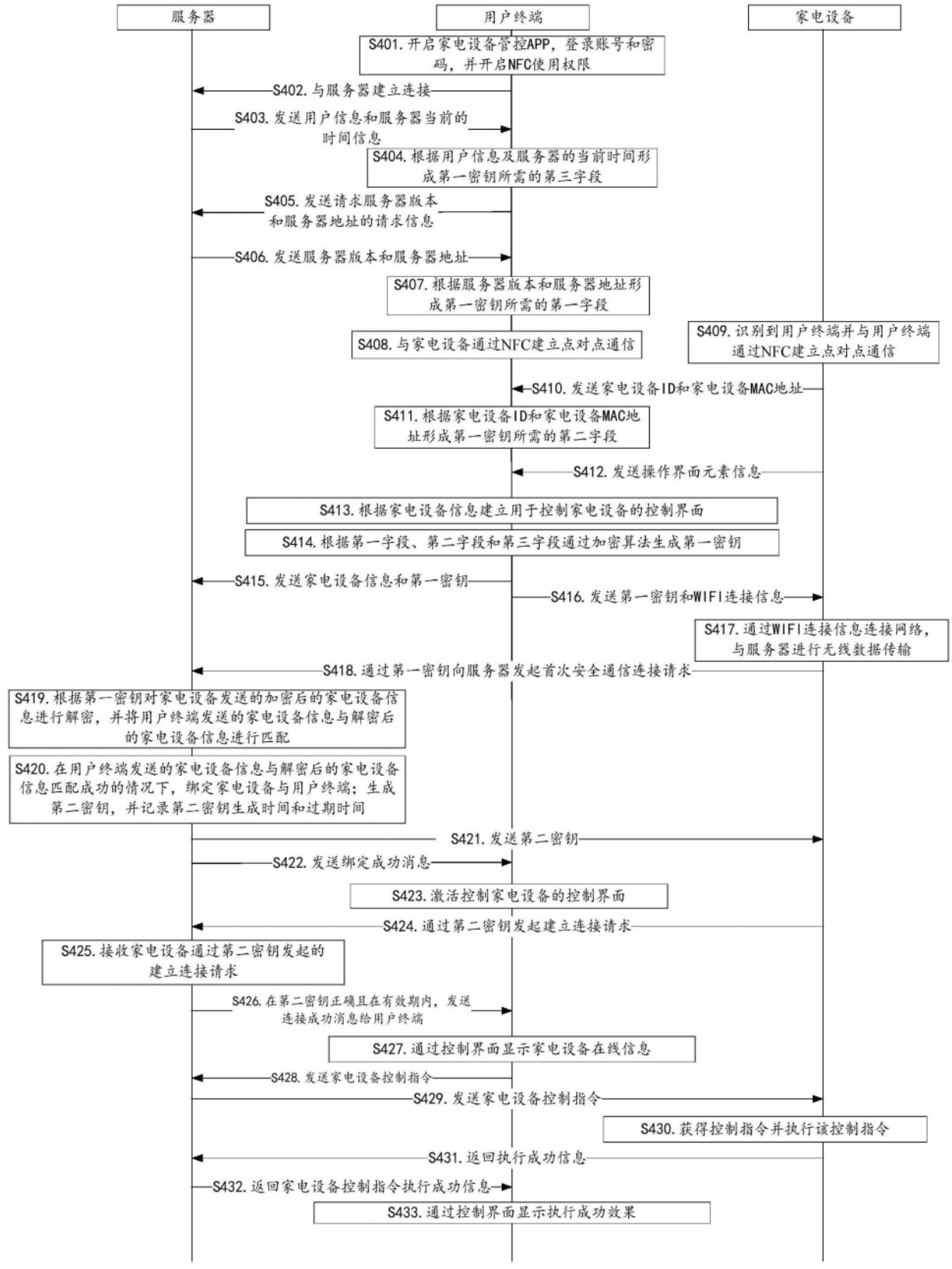

服务器
用户终端
家电设备
S401. 开启家电设备管控APP，登录账号和密码，并开启NFC使用权限
S402. 与服务器建立连接
S403. 发送用户信息和服务器当前的时间信息
S404. 根据用户信息及服务器的当前时间形成第一密钥所需的第三字段
S405. 发送请求服务器版本和服务器地址的请求信息
S406. 发送服务器版本和服务器地址
S407. 根据服务器版本和服务器地址形成第一密钥所需的第一字段
S408. 与家电设备通过NFC建立点对点通信
S409. 识别到用户终端并与用户终端通过NFC建立点对点通信
S410. 发送家电设备ID和家电设备MAC地址
S411. 根据家电设备ID和家电设备MAC地址形成第一密钥所需的第二字段
S412. 发送操作界面元素信息
S413. 根据家电设备信息建立用于控制家电设备的控制界面
S414. 根据第一字段、第二字段和第三字段通过加密算法生成第一密钥
S415. 发送家电设备信息和第一密钥
S416. 发送第一密钥和WIFI连接信息
S417. 通过WIFI连接信息连接网络，与服务器进行无线数据传输
S418. 通过第一密钥向服务器发起首次安全通信连接请求
S419. 根据第一密钥对家电设备发送的加密后的家电设备信息进行解密，并将用户终端发送的家电设备信息与解密后的家电设备信息进行匹配
S420. 在用户终端发送的家电设备信息与解密后的家电设备信息匹配成功的情况下，绑定家电设备与用户终端；生成第二密钥，并记录第二密钥生成时间和过期时间
S421. 发送第二密钥
S422. 发送绑定成功消息
S423. 激活控制家电设备的控制界面
S424. 通过第二密钥发起建立连接请求
S425. 接收家电设备通过第二密钥发起的建立连接请求
S426. 在第二密钥正确且在有效期内，发送连接成功消息给用户终端
S427. 通过控制界面显示家电设备在线信息
S428. 发送家电设备控制指令
S429. 发送家电设备控制指令
S430. 获得控制指令并执行该控制指令
S431. 返回执行成功信息
S432. 返回家电设备控制指令执行成功信息
S433. 通过控制界面显示执行成功效果

图4

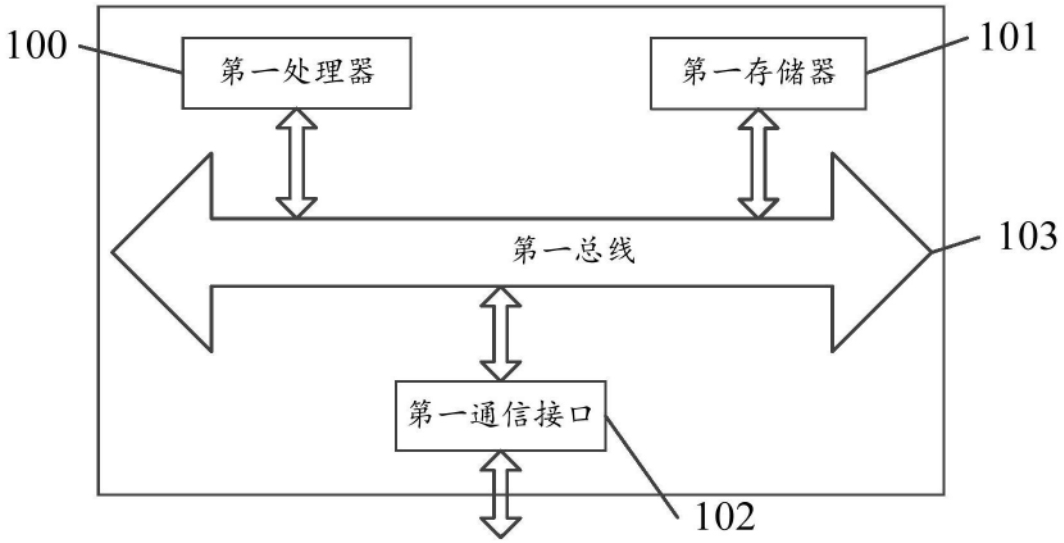

100
第一处理器
101
第一存储器
103
第一总线
第一通信接口
102

图5

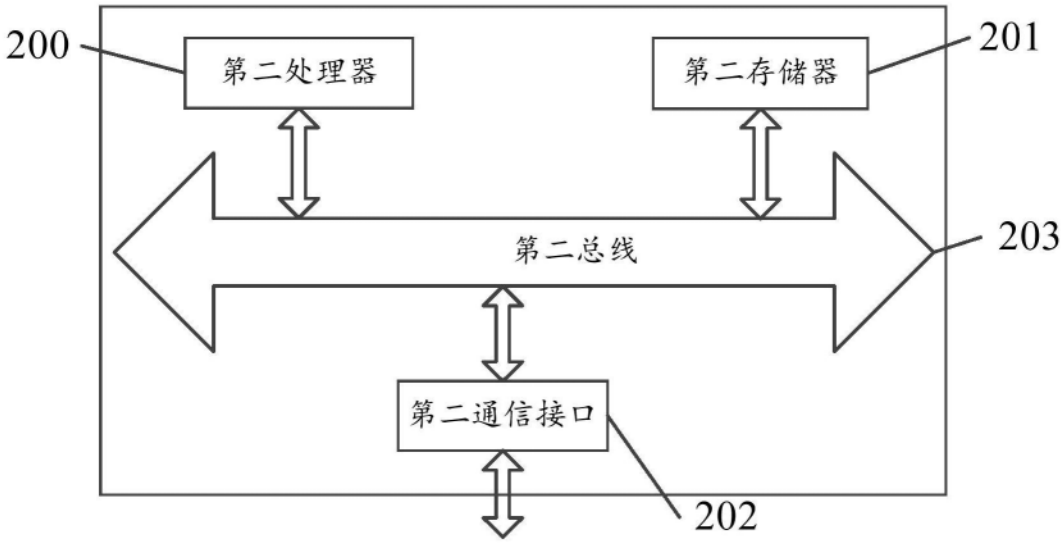

200
第二处理器
201
第二存储器
203
第二总线
第二通信接口
202

图6

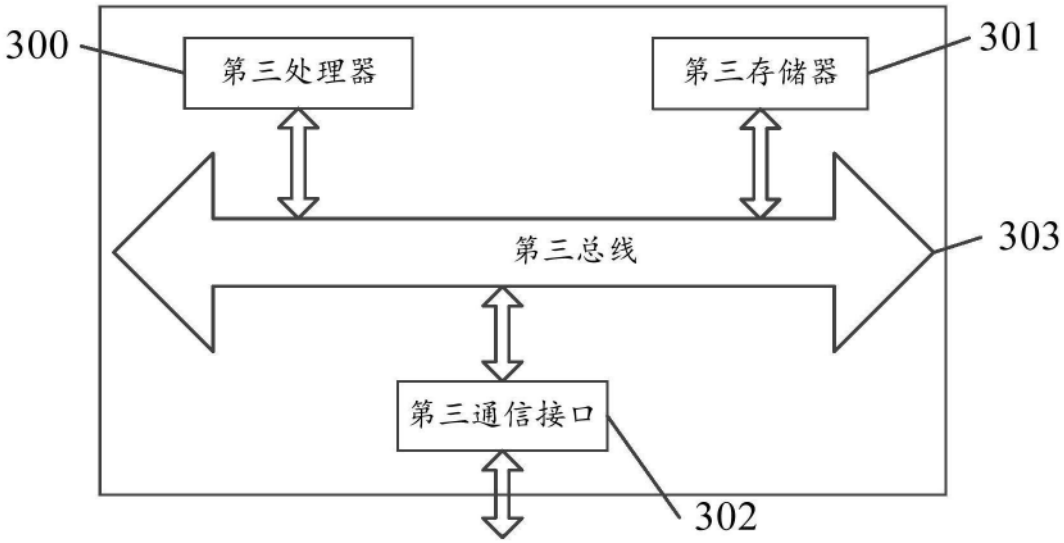


图7