(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115396121 B
(45)授权公告日 2023.03.24

(21)申请号 202211314633.0
(22)申请日 2022.10.26
(65)同一申请的已公布的文献号
申请公布号 CN 115396121 A
(43)申请公布日 2022.11.25
(73)专利权人 广州万协通信息技术有限公司
地址 510400 广东省广州市白云区北太路1633号广州民营科技园科盛路8号配套服务大楼5层A505-63房
(72)发明人 张奇惠 刘家明 王立峰
(74)专利代理机构 北京泽方誉航专利代理事务所(普通合伙) 11884
专利代理师 徐濛
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/00(2022.01)
G06F 21/57(2013.01)
G06F 8/65(2018.01)
(56)对比文件
CN 112328989 A,2021.02.05
审查员 李文聪

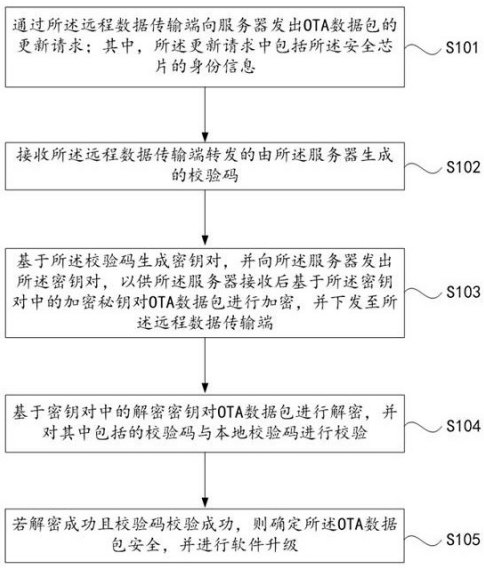
权利要求书2页 说明书11页 附图2页

(54)发明名称

安全芯片OTA数据包的安全认证方法及安全芯片装置

(57)摘要

本申请公开了一种安全芯片OTA数据包的安全认证方法、安全芯片装置、设备及介质，本申请属于通信技术领域。该方法包括：向服务器发出OTA数据包的更新请求；其中，更新请求中包括安全芯片的身份信息；接收服务器生成的校验码；基于校验码生成并向服务器发出密钥对，包括加密密钥及解密密钥，供服务器接收后利用加密秘钥加密OTA数据包，下发至远程数据传输端；利用解密密钥解密OTA数据包，对校验码与本地校验码进行校验；若解密成功且校验码校验成功，确定OTA数据包安全，进行软件升级。本方案设置实时校验码及密钥对，对OTA数据包的下载过程进行双重验证，可以识别用户的真实性，提高用户数据安全性及下载OTA数据包的效率，降低服务器运行和维护的成本。



CN 115396121 B

1.一种安全芯片OTA数据包的安全认证方法,其特征在于,所述方法由安全芯片执行,所述安全芯片连接于远程数据传输端;所述方法包括:

通过所述远程数据传输端向服务器发出OTA数据包的更新请求;其中,所述更新请求中包括所述安全芯片的身份信息;

接收所述远程数据传输端转发的由所述服务器生成的校验码;

基于所述校验码生成密钥对,并向所述服务器发出所述密钥对,其中,包括基于所述校验码生成密钥对,并对所述校验码进行散列值计算,将计算得到的散列值作为密钥对的数字签名,并向所述服务器发出带有所述数字签名的密钥对;以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密,并下发至所述远程数据传输端;

基于密钥对中的解密密钥对OTA数据包进行解密,并对其中包括的校验码与本地校验码进行校验;

若解密成功且校验码校验成功,则确定所述OTA数据包安全,并进行软件升级。

2.根据权利要求1所述的方法,其特征在于,在基于密钥对中的解密密钥对OTA数据包进行解密,并对其中包括的校验码与本地校验码进行校验之后,所述方法还包括:

若基于密钥对中的解密密钥无法对接收到的OTA数据包进行解密,或者解密成功后得到的校验码与本地校验码不一致,则确定所述OTA数据包无效。

3.根据权利要求2所述的方法,其特征在于,在确定所述OTA数据包无效之后,所述方法还包括:

获取所述OTA数据包中包括的会话ID;其中,所述会话ID是所述服务器基于所述更新请求生成的;

识别所述会话ID是否与当前的更新请求相匹配,若不匹配,则向所述服务器发出会话ID错误的反馈信息。

4.根据权利要求1所述的方法,其特征在于,基于所述校验码生成密钥对,包括:

基于所述校验码中的特征位的数字内容生成密钥对;

或者,

基于所述校验码中的目标数字内容所处的特征位生成密钥对;

或者,

基于所述校验码中的预设字段中的数字内容生成密钥对。

5.一种安全芯片OTA数据包的安全认证装置,其特征在于,所述装置配置于安全芯片,所述安全芯片连接于远程数据传输端;所述装置包括:

发送模块,用于通过所述远程数据传输端向服务器发出OTA数据包的更新请求;其中,所述更新请求中包括所述安全芯片的身份信息;

接收模块,用于接收所述远程数据传输端转发的由所述服务器生成的校验码;

密钥对生成模块,用于基于所述校验码生成密钥对,并向所述服务器发出所述密钥对,其中,包括基于所述校验码生成密钥对,并对所述校验码进行散列值计算,将计算得到的散列值作为密钥对的数字签名,并向所述服务器发出带有所述数字签名的密钥对;以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密,并下发至所述远程数据传输端;

解密模块,用于基于密钥对中的解密密钥对OTA数据包进行解密,并对其中包括的校验

码与本地校验码进行校验；

升级模块，用于若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。

6.根据权利要求5所述的装置，其特征在于，所述装置还包括解密无效确定模块，所述解密无效确定模块用于：

若基于密钥对中的解密密钥无法对接收到的OTA数据包进行解密，或者解密成功后得到的校验码与本地校验码不一致，则确定所述OTA数据包无效。

7.一种电子设备，其特征在于，包括处理器，存储器及存储在所述存储器上并可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如权利要求1-4中任一项所述的安全芯片OTA数据包的安全认证方法的步骤。

8.一种可读存储介质，其特征在于，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如权利要求1-4中任一项所述的安全芯片OTA数据包的安全认证方法的步骤。

安全芯片OTA数据包的安全认证方法及安全芯片装置

技术领域

[0001] 本申请属于通信技术领域,具体涉及一种安全芯片OTA数据包的安全认证方法、安全芯片装置、设备及介质。

背景技术

[0002] 随着科学技术的不断发展,一块又一块的智能大屏幕进入到汽车中,通过车载软件,人们可以完成导航、点外卖、看书听歌以及玩游戏等一系列任务。但同时,软件对汽车的影响也在不断面临挑战,如今的软件系统和应用程序更新迭代的越来越快,用户的需求也在不断提高,所以系统必须要定期进行升级,增加对不同的设备和软件的兼容或兼容度,以及解决某些设备客观存在的问题。而OTA技术(Over-the-Air Technology,空中下载技术)可以使汽车即使不去车厂也能进行在线升级,以享受汽车厂商推动的升级包,提升驾驶体验。OTA技术是通过移动通信的空中接口实现对移动终端设备及SIM卡数据进行远程管理的技术。但OTA也成了黑客的重点攻击对象,如进行窃听攻击、恶意升级、回滚攻击、DDOS攻击(Distributed Denial of Service,分布式拒绝服务)等,使整车OTA升级面临多维安全挑战。DDOS攻击是利用大量合法的分布式服务器对目标发送请求,从而导致正常合法用户无法获得服务的攻击。在此背景下,就有了提高OTA升级的安全性的研究。

[0003] 如今的OTA认证方式是由服务器下发经过数字签名的数据包,车辆端通过预先设置的密钥进行解密,和签名验证,就可以完成认证,实现升级。

[0004] 但是目前固定数字签名和固定密钥的方式会存在较多的安全隐患。如果攻击者通过窃听网络数据等方式对密钥及数字签名进行破解后,就可以一直对车辆进行攻击,驾驶员以及乘客的安全也难以得到保证。因此,如何在车辆使用OTA技术进行系统升级或软件更新时,采用实时密钥及实时数字签名是本领域亟待解决的问题。

发明内容

[0005] 本申请的目的是提供一种安全芯片OTA数据包的安全认证方法、安全芯片装置、设备及介质,解决了现有技术中使用固定签名和固定密钥的方式传输OTA数据包带来安全隐患的问题。通过设置实时校验码以及密钥对的方式,对OTA数据包的下载过程进行了双重验证,可以很好识别用户的真实性,避免攻击者进行OTA数据包的恶意请求而导致服务器瘫痪的情况发生。同时提高了用户数据安全性以及下载OTA数据包的效率,降低了服务器运行和维护的成本。

[0006] 第一方面,本申请提供了一种安全芯片OTA数据包的安全认证方法,所述方法由安全芯片执行,所述安全芯片连接于远程数据传输端;所述方法包括:

[0007] 通过所述远程数据传输端向服务器发出OTA数据包的更新请求;其中,所述更新请求中包括所述安全芯片的身份信息;

[0008] 接收所述远程数据传输端转发的由所述服务器生成的校验码;

[0009] 基于所述校验码生成密钥对,并向所述服务器发出所述密钥对,以供所述服务器

接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端；

[0010] 基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验；

[0011] 若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。

[0012] 进一步的，基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，包括：

[0013] 基于所述校验码生成密钥对，并对所述校验码进行散列值计算，将计算得到的散列值作为密钥对的数字签名，并向所述服务器发出带有所述数字签名的密钥对。

[0014] 进一步的，在基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验之后，所述方法还包括：

[0015] 若基于密钥对中的解密密钥无法对接收到的OTA数据包进行解密，或者解密成功后得到的校验码与本地校验码不一致，则确定所述OTA数据包无效。

[0016] 进一步的，在确定所述OTA数据包无效之后，所述方法还包括：

[0017] 获取所述OTA数据包中包括的会话ID；其中，所述会话ID是所述服务器基于所述更新请求生成的；

[0018] 识别所述会话ID是否与当前的更新请求相匹配，若不匹配，则向所述服务器发出会话ID错误的反馈信息。

[0019] 进一步的，基于所述校验码生成密钥对，包括：

[0020] 基于所述校验码中的特征位的数字内容生成密钥对；

[0021] 或者，

[0022] 基于所述校验码中的目标数字内容所处的特征位生成密钥对；

[0023] 或者，

[0024] 基于所述校验码中的预设字段中的数字内容生成密钥对。

[0025] 第二方面，本申请提供了一种安全芯片OTA数据包的安全认证安全芯片装置，所述装置配置于安全芯片，所述安全芯片连接于远程数据传输端；所述装置包括：

[0026] 发送模块，用于通过所述远程数据传输端向服务器发出OTA数据包的更新请求；其中，所述更新请求中包括所述安全芯片的身份信息；

[0027] 接收模块，用于接收所述远程数据传输端转发的由所述服务器生成的校验码；

[0028] 密钥对生成模块，用于基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端；

[0029] 解密模块，用于基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验；

[0030] 升级模块，用于若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。

[0031] 进一步的，所述密钥对生成模块用于：

[0032] 基于所述校验码生成密钥对，并对所述校验码进行散列值计算，将计算得到的散列值作为密钥对的数字签名，并向所述服务器发出带有所述数字签名的密钥对。

[0033] 进一步的，所述装置还包括解密无效确定模块，所述解密无效确定模块用于：

[0034] 若基于密钥对中的解密密钥无法对接收到的OTA数据包进行解密，或者解密成功后得到的校验码与本地校验码不一致，则确定所述OTA数据包无效。

[0035] 第三方面，本申请提供了一种电子设备，该电子设备包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第一方面所述的安全芯片OTA数据包的安全认证方法的步骤。

[0036] 第四方面，本申请提供了一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如第一方面所述的安全芯片OTA数据包的安全认证方法的步骤。

[0037] 在本申请中，接收所述远程数据传输端转发的由所述服务器生成的校验码；基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端；基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验；若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。本方案通过设置实时校验码以及密钥对的方式，对OTA数据包的下载过程进行了双重验证，可以很好识别用户的真实性，避免攻击者进行OTA数据包的恶意请求而导致服务器瘫痪的情况发生。同时提高了用户数据安全性以及下载OTA数据包的效率，降低了服务器运行和维护的成本。

附图说明

[0038] 图1是本申请实施例一提供的安全芯片OTA数据包的安全认证方法的流程示意图；

[0039] 图2是本申请实施例二提供的安全芯片OTA数据包的安全认证安全芯片装置的结构示意图；

[0040] 图3是本申请实施例提供的电子设备的结构示意图。

具体实施方式

[0041] 为了使本申请的目的、技术方案和优点更加清楚，下面结合附图对本申请具体实施例作进一步的详细描述。可以理解的是，此处所描述的具体实施例仅仅用于解释本申请，而非对本申请的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本申请相关的部分而非全部内容。在更加详细地讨论示例性实施例之前应当提到的是，一些示例性实施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作(或步骤)描述成顺序的处理，但是其中的许多操作可以被并行地、并发地或者同时实施。此外，各项操作的顺序可以被重新安排。当其操作完成时所述处理可以被终止，但是还可以具有未包括在附图中的附加步骤。所述处理可以对应于方法、函数、规程、子例程、子程序等等。

[0042] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员获得的所有其他实施例，都属于本申请保护的范围。

[0043] 本申请的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象，而不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，以便本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施，且“第一”、“第二”等所区分的对象通常为一类，并不限定对象的个数，例如第一对象可以是一个，也可

以是多个。此外，说明书以及权利要求中“和/或”表示所连接对象的至少其中之一，字符“/”，一般表示前后关联对象是一种“或”的关系。

[0044] 下面结合附图，通过具体的实施例及其应用场景对本申请实施例提供的安全芯片OTA数据包的安全认证方法、安全芯片装置、设备及介质进行详细地说明。

[0045] 实施例一

[0046] 图1是本申请实施例一提供的安全芯片OTA数据包的安全认证方法的流程示意图。如图1所示，具体包括如下步骤：

[0047] S101，通过所述远程数据传输端向服务器发出OTA数据包的更新请求；其中，所述更新请求中包括所述安全芯片的身份信息。

[0048] 首先，本方案的使用场景可以是用户在通过车辆上位机使用OTA数据包对车辆进行在线升级的场景。目前在线升级，分成SOTA和FOTA两种大的方向，SOTA就是软件升级，FOTA就是固件升级。软件升级可以进行车载大屏、UI、交互、软件的优化以及语音唤醒等等这一方面的升级。固件升级可以改变车辆的充放电、动能回收、加速性能以及辅助驾驶系统逻辑等等与深度驾控有关的体验。

[0049] 基于上述使用场景，可以理解的，本申请的执行主体可以是安全芯片，此处不做过多的限定。

[0050] 本方案中，该方法由安全芯片执行，所述安全芯片连接于远程数据传输端。

[0051] 安全芯片可以是可独立进行密钥生成、加解密的装置，内部拥有独立的处理器和存储单元，可存储密钥和特征数据，为上位机提供加密和安全认证服务。用安全芯片进行加密，密钥被存储在硬件中，被窃的数据无法解密，从而保护数据安全。

[0052] 远程数据传输端可以是智能网关，智能网关是局域网络智能化的关键，一般支持虚拟网络接入、wifi接入、有线宽带接入等，通过它可实现对局域网内各传感器、网络设备、摄像头以及主机等设备的信息采集、信息输入、信息输出、集中控制、远程控制以及联动控制等功能。本方案中，智能网关通过连接服务器与安全芯片进行OTA数据包的更新请求、校验码以及密钥对的传输。

[0053] 本方案中，服务器可以是在网络中为其它客户机(如PC机、智能手机、ATM等终端甚至是火车系统等大型设备)提供计算或者应用服务的计算机。服务器具有高速的CPU运算能力、长时间的可靠运行、强大的I/O外部数据吞吐能力以及更好的扩展性。具体的，本方案中，服务器负责生成校验码以及加密OTA数据包，然后传输给安全芯片。

[0054] OTA数据包可以是通过服务器OTA技术给车辆推送的升级包。OTA即空间下载技术，是通过移动通信(GSM或CDMA)的空中接口对SIM卡数据及应用进行远程管理的技术。空中接口可以采用WAP、GPRS、CDMA1X及短消息技术。OTA技术的应用，使得移动通信不仅可以提供语音和数据服务，而且还能提供新业务下载。升级包可以是SOTA升级包或者FOTA升级包。

[0055] 更新请求可以是用户通过点击车辆上位机相应按钮后，安全芯片向服务器发出的下载车厂推送的升级包的请求。只有车厂的服务器接收到车机发送的OTA数据包的更新请求，并在对车辆验证成功后才会对该车发送相应的OTA数据包。

[0056] 身份信息可以是安全芯片的编号以及安全芯片对应的车辆信息。由于每个安全芯片的编号是独一无二的，当服务器接收到安全芯片发送的更新请求时，首先验证安全芯片的编号是否在服务器的服务范围内。若在服务范围内，可以查询对应的车辆信息是否正确，

即是否在此车厂的服务范围内，只有两者均验证正确时，车厂才会对该车辆发送OTA数据包。这样验证的意义是为了确保此OTA数据包不会发送到该车厂服务范围以外的车辆，由于不同车厂生产的车辆配置不一样，所以在升级时用到的OTA数据包也不一样，若有误发情况，可能造成车辆软件以及硬件的故障，从而对车辆安全构成一定的威胁。

[0057] 发出OTA数据包的更新请求可以是用户想接收该车车厂推送的升级包，并点击车辆上位机的相应按钮后，安全芯片通过远程数据传输端将该更新请求传输到车厂服务器的过程。

[0058] S102，接收所述远程数据传输端转发的由所述服务器生成的校验码。

[0059] 校验码可以是车厂为了验证车辆身份，为车辆发送OTA数据包所设置的验证码，可以包括数字以及字母的形式。本方案中，可以采用数字作为校验码，例如，服务器收到车机发出的OTA数据包的更新请求后，实时生成的验证码为123456，然后将验证码通过远程数据传输端传输给安全芯片，作为之后校验环节的依据。

[0060] 接收可以是安全芯片收到远程数据传输端传送的校验码的过程。当安全芯片接收到服务器传送的校验码后，可以将校验码暂时存储在内部的存储单元中，以便接下来与解密环节生成的本地校验码进行校验。

[0061] 转发可以是远程数据传输端接收到服务器传送的校验码后，将此校验码发送到安全芯片的过程。

[0062] 生成可以是服务器接收到安全芯片传送的OTA数据包的更新请求后，调用生成校验码的方法生成校验码的过程。在校验码生成成功后，服务器会调用发送校验码的方法将校验码发送给远程数据传输端。传送成功后，可以使用redisLock来对发送校验码的进行相应的限制，第一个校验码发送之后的50秒内不允许再次发送验证码，目的是为了防止攻击者恶意调取接口。

[0063] S103，基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端。

[0064] 密钥对可以是在非对称加密技术中的两种密钥，分为私钥和公钥，私钥是密钥对所有者持有，不可公布，公钥是密钥对持有者公布给他人的。

[0065] 加密密钥可以是密钥对中的公钥，公钥用来给数据加密，用公钥加密的数据只能使用私钥解密。使用公钥加密需要使用不同的密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。

[0066] 生成密钥对可以是安全芯片根据校验码按照一定算法提取密码的过程，具体的，可以使用gpg生成密钥对。使用gpg生成密钥对的代码如下：

[0067] [root@CentOS-8-LinuxIV ~]# gpg --gen-key

[0068] 生成密钥对后，会将公钥、私钥以及配置存储在.gnupg/的目录中，由于gpg生成的公钥是二进制的不能直接查看，因此需要使用ascii导出来，代码如下：

[0069] gpg --export -a -o pub.key

[0070] 这样生成的文件就可以直接查看了。

[0071] 发出密钥对可以是当通过握手协商阶段后，安全芯片使用HTTPS协议将密钥对传

输给服务器的过程。握手协商阶段需要经历两个小的阶段，第一阶段为协商TLS版本以及相关信息阶段，主要功能是协商双方都支持的版本与算法。第二阶段为非对称加密秘钥协商阶段，主要功能是通过非对称加密随机协商后续需要使用的对称秘钥。里面涉及到了数字CA证书(需要专门的机构颁发)，证书可以理解为公钥的载体。

[0072] 加密可以是以某种特殊的算法改变原有的信息数据的过程，加密可以使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。本方案中，服务器会使用安全芯片传送的密钥对的加密密钥对OTA数据包进行加密。

[0073] 下发可以是当服务器对OTA数据包加密成功后，将加密后的OTA数据包传输至远程数据传输端的过程。

[0074] 在上述各技术方案的基础上，可选的，基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，包括：

[0075] 基于所述校验码生成密钥对，并对所述校验码进行散列值计算，将计算得到的散列值作为密钥对的数字签名，并向所述服务器发出带有所述数字签名的密钥对。

[0076] 散列值可以是一种从任何一种数据中创建小的数字“指纹”的方法。散列函数把消息或数据压缩成摘要，使得数据量变小，将数据的格式固定下来。该函数将数据打乱混合，重新创建一个叫做散列值的指纹。散列值通常用一个短的随机字母和数字组成的字符串来代表。本方案中，散列值可以是以校验码为基础，利用散列算法计算后得到的字符串。

[0077] 数字签名可以是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。它是一种类似写在纸上的普通的物理签名，但是在使用了公钥加密领域的技术来实现的，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。数字签名是非对称密钥加密技术与数字摘要技术的应用。本方案中，在服务器对OTA数据包进行加密前，要使用服务器自己的私钥对OTA数据包(一般是OTA数据包的摘要)进行签名。当安全芯片对OTA数据包的内容进行解密，得到解密后的明文后，要用服务器的公钥解签服务器用自己的私钥的数字签名。服务器的签名只有服务器的公钥才能解密，这样安全芯片就能确定这个OTA数据包是服务器发来的。

[0078] 计算可以是使用散列算法将校验码转换为散列值的过程。典型的散列算法包括MD2、MD4、MD5以及SHA-1，本方案中，可以采用SHA-1作为散列算法。SHA-1即安全散列算法1，可以生成一个被称为消息摘要的160位(20字节)散列值，散列值通常的呈现形式为40个十六进制数。

[0079] 本方案通过在安全芯片向服务器发送密钥对时增加数字签名的方式，可以使安全芯片确保接收到的OTA数据包为服务器发送的。若仅有服务器对OTA数据包加密的过程，则只能保证服务器确认OTA数据包被安全芯片读取，而安全芯片则无法确定此OTA数据包的来源。若增加数字签名，则可以使安全芯片确定OTA数据包是服务器发送的，在一定程度上增加了OTA数据包传输的安全性。

[0080] 在上述各技术方案的基础上，可选的，基于所述校验码生成密钥对，包括：

[0081] 基于所述校验码中的特征位的数字内容生成密钥对；

[0082] 或者，

[0083] 基于所述校验码中的目标数字内容所处的特征位生成密钥对；

[0084] 或者，

[0085] 基于所述校验码中的预设字段中的数字内容生成密钥对。

[0086] 本方案中，特征位可以是此校验码区别于其他校验码的检验码。由于校验码数量过多，但若随意扩展长度可能导致违反校验码标准，系统无法识别。所以可以将校验码某一位设置为检验码，以保证此校验码可以区别于其他校验码。例如，校验码为六位数字，将最后一位数字作为特征位，此特征位可以是根据一定算法计算而得的。

[0087] 数字内容可以是特征位对应的数字，例如，校验码为123456，预先设置了将校验码的最后一位数字作为特征位，则此校验码的数字内容为6。

[0088] 目标数字内容所处的特征位可以是将校验码的某一固定位置的数字作为生成密钥对的数字。例如，校验码为123456，预先设置了第三位为特征位，则此校验码生成密钥对的数字为3。

[0089] 预设字段可以是将校验码某一段数字作为生成密钥对的数字。例如，校验码为123456，预先设置了将第二到第四位的数字作为生成密钥对的数字，则此校验码生成密钥对的数字为234。

[0090] 生成可以是根据校验码中的特征位的数字内容、校验码中的目标数字内容所处的特征位以及校验码中的预设字段中的数字内容通过一定算法得到密钥对的过程。

[0091] 本方案中，通过设置不同的生成密钥对的方式，使安全芯片在生成密钥对的选择更加广泛，提高了生成密钥对的灵活性。若仅有一种方式，在校验码过多时，生成密钥对的速度会降低。若设置不同方式，在一种方式生成密钥对时排队的校验码过多，可以自动跳转另一种方式，提高生成密钥对的速度，也在一定程度上缓解了服务器的压力。

[0092] S104，基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验。

[0093] 解密密钥可以是密钥对中的私钥，当安全芯片收到服务器传输的加密后的OTA数据包后，会使用密钥对中的私钥解密服务器利用安全芯片的公钥进行加密的内容。

[0094] 本地校验码可以是安全芯片在使用解密密钥对OTA数据包进行解密过程中，产生的实时的验证码。由于安全芯片生成的密钥对是根据服务器生成的校验码通过一定算法得到的，所以在解密过程中也会将加密后的验证码转换为简明文本。

[0095] 解密可以是安全芯片利用解密密钥将加密后的OTA数据包转换为简明文本的过程。整个加密以及解密的过程就保证了端到端的唯一确认，服务器的加密只有安全芯片的私钥才能解密，这样服务器就能确定这份信息只能被安全芯片读取。

[0096] 校验可以是安全芯片将存储在存储单元的校验码与解密得到的校验码进行比对的过程，若比对一致则校验成功；若比对不一致则校验失败。例如之前存储在安全芯片的存储单元的校验码为123456，解密得到的校验码也必须为123456才为校验成功。

[0097] 在上述各技术方案的基础上，可选的，在基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验之后，所述方法还包括：

[0098] 若基于密钥对中的解密密钥无法对接收到的OTA数据包进行解密，或者解密成功后得到的校验码与本地校验码不一致，则确定所述OTA数据包无效。

[0099] 确定OTA数据包无效可以是安全芯片在将解密时生成的本地校验码与存储在存储单元的校验码比对不一致后，判断已经遭受到了外界攻击，自动取消软件升级的过程。也可

以是安全芯片在解密过程中无法解密时，即无法利用解密密钥将加密后的OTA数据包转换为简明文本时，则安全芯片判断已经遭受到外界攻击，自动取消软件升级。具体的，外界攻击可以是静态攻击或者动态攻击。静态攻击是指在芯片没有工作，但电源可能接通的情况下，采用腐蚀剂、高倍显微镜、照相机、操作台和探针等设备和材料对安全芯片进行分析，这种攻击手段没有时间限制，可以按照攻击者的进程展开攻击。动态攻击则指在芯片工作的状况下展开的攻击行为。

[0100] 本方案通过设置安全芯片受到外界攻击时的应对方案，将用户进行软件升级时会发生的情况考虑的更加全面，在一定程度上保证了用户在进行软件升级时的私密性及安全性。

[0101] 在上述各技术方案的基础上，可选的，在确定所述OTA数据包无效之后，所述方法还包括：

[0102] 获取所述OTA数据包中包括的会话ID；其中，所述会话ID是所述服务器基于所述更新请求生成的；

[0103] 识别所述会话ID是否与当前的更新请求相匹配，若不匹配，则向所述服务器发出会话ID错误的反馈信息。

[0104] 本方案中，会话ID可以是服务器收到安全芯片的更新请求后，根据更新请求赋予的特定的编号，可以包括字母、数字以及文字的形式。本方案中，会话ID可以是按照更新请求发送到服务器的先后顺序采用数字形式编写的编号，例如，第一个更新请求编号为1001，则此请求的会话ID为1001。第二个更新请求编号为1002，则此请求的会话ID为1002。

[0105] 反馈信息可以是安全芯片确定会话ID与更新请求不匹配后向服务器发送的状态回执错误码。状态回执错误码可以是字母以及数字，本方案中，可以利用数字表示状态回执错误码。在数据库服务器中可以有存储状态回执错误码、错误原因以及解决方法的数据库表，数据库服务器与本方案所述服务器相连接。当安全芯片向服务器发送状态回执错误码时，服务器会将此状态回执错误码转发给数据库服务器，数据库服务器会自动调用数据库表，并利用状态回执错误码查询对应的错误原因以及解决方法。查询成功后，数据库服务器可以将错误原因以及解决方法反馈给服务器，然后由服务器转发给安全芯片，此时用户可以通过上位机查看这些信息并根据解决方法进行对应操作。例如，当安全芯片向服务器发送的状态回执错误码为105，服务器将此状态回执错误码转发给数据库服务器，数据库服务器在对应的数据库表查询后发现错误原因为会话ID与更新请求不匹配，解决方案为重新发送更新请求。在服务器将这些信息发送给安全芯片后，用户可以在车辆上位机查看信息并进行重新发送更新请求的操作。

[0106] 生成可以是服务器根据更新请求发送到服务器的先后顺序对更新请求进行编号的过程，即产生会话ID的过程。

[0107] 识别可以是安全芯片将会话ID与更新请求进行比对的过程，若此会话ID和对应的更新请求与服务器发送的会话ID和对应的更新请求不一致，则确定会话ID与当前的更新请求不匹配。例如，当服务器接收到安全芯片发送的更新请求时，产生的会话ID为1001，更新请求为车机1更新。但安全芯片获取到的OTA数据包中的会话ID为1002，更新请求为车机1更新。则识别后确定会话ID和对应的更新请求不匹配，无法进行接下来的软件升级操作。造成不匹配的原因可能是在OTA数据包的传输过程中，遭受到了外界攻击，篡改了其中的会话

ID。

[0108] 本方案中，通过当安全芯片识别到会话ID与当前的更新请求不匹配，向服务器发送会话ID错误的反馈信息的方式，可以使车厂维护人员利用此反馈信息进行相应的维护，以不断提高OTA数据包传输的安全性。

[0109] S105，若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。

[0110] 确定可以是在解密以及验证码校验环节均成功后，安全芯片生成token并发送给车辆上位机的过程。token相当于OTA数据包的明文，是可以解码的，上位机拿到token后进行解码，解码成功就可拿到OTA数据包，以进行接下来升级的操作。

[0111] 升级可以是用户在通过车辆上位机屏幕获得可以升级的提示后，点击屏幕相应按钮后，安装服务器传送的OTA数据包的过程。

[0112] 本实施例所提供的技术方案，接收所述远程数据传输端转发的由所述服务器生成的校验码；基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端；基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验；若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。本方案通过设置实时校验码以及密钥对的方式，对OTA数据包的下载过程进行了双重验证，可以很好识别用户的真实性，避免攻击者进行OTA数据包的恶意请求而导致服务器瘫痪的情况发生。同时提高了用户数据安全性以及下载OTA数据包的效率，降低了服务器运行和维护的成本。

[0113] 实施例二

[0114] 图2是本申请实施例二提供的安全芯片OTA数据包的安全认证安全芯片装置的结构示意图。所述装置配置于安全芯片，所述安全芯片连接于远程数据传输端；如图2所示，所述安全芯片装置包括：

[0115] 发送模块201，用于通过所述远程数据传输端向服务器发出OTA数据包的更新请求；其中，所述更新请求中包括所述安全芯片的身份信息；

[0116] 接收模块202，用于接收所述远程数据传输端转发的由所述服务器生成的校验码；

[0117] 密钥对生成模块203，用于基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端；

[0118] 解密模块204，用于基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验；

[0119] 升级模块205，用于若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。

[0120] 进一步的，所述密钥对生成模块用于：

[0121] 基于所述校验码生成密钥对，并对所述校验码进行散列值计算，将计算得到的散列值作为密钥对的数字签名，并向所述服务器发出带有所述数字签名的密钥对。

[0122] 进一步的，所述装置还包括解密无效确定模块，所述解密无效确定模块用于：

[0123] 若基于密钥对中的解密密钥无法对接收到的OTA数据包进行解密，或者解密成功

后得到的校验码与本地校验码不一致，则确定所述OTA数据包无效。

[0124] 在本申请实施例中，发送模块，用于通过所述远程数据传输端向服务器发出OTA数据包的更新请求；其中，所述更新请求中包括所述安全芯片的身份信息；接收模块，用于接收所述远程数据传输端转发的由所述服务器生成的校验码；密钥对生成模块，用于基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端；解密模块，用于基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验；升级模块，用于若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级。本方案通过设置检验实时校验码以及密钥对的装置，对OTA数据包的下载过程进行了双重验证，可以很好识别用户的真实性，避免攻击者进行OTA数据包的恶意请求而导致服务器瘫痪的情况发生。同时提高了用户数据安全性以及下载OTA数据包的效率，降低了服务器运行和维护的成本。

[0125] 本申请实施例提供的安全芯片OTA数据包的安全认证装置能够实现上述方法实施例实现的各个过程，为避免重复，这里不再赘述。

[0126] 实施例三

[0127] 图3是本申请实施例提供的电子设备的结构示意图。如图3所示，本申请实施例还提供一种电子设备300，包括处理器301，存储器302，存储在存储器302上并可在所述处理器301上运行的程序或指令，该程序或指令被处理器301执行时实现上述安全芯片OTA数据包的安全认证方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

[0128] 需要说明的是，本申请实施例中的电子设备包括上述所述的移动电子设备和非移动电子设备。

[0129] 实施例四

[0130] 本申请实施例还提供一种可读存储介质，所述可读存储介质上存储有程序或指令，该程序或指令被处理器执行时实现上述安全芯片OTA数据包的安全认证方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

[0131] 其中，所述处理器为上述实施例中所述的电子设备中的处理器。所述可读存储介质，包括计算机可读存储介质，如计算机只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等。

[0132] 实施例五

[0133] 本申请实施例另提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现上述鞋体设计数据的存储方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

[0134] 应理解，本申请实施例提到的芯片还可以称为系统级芯片、系统芯片、芯片系统或片上系统芯片等。

[0135] 需要说明的是，在本文中，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、物品或者装置不仅包括那些要素，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、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该

要素的过程、方法、物品或者装置中还存在另外的相同要素。此外，需要指出的是，本申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能，还可包括根据所涉及的功能按基本同时的方式或按相反的顺序来执行功能，例如，可以按不同于所描述的次序来执行所描述的方法，并且还可以添加、省去、或组合各种步骤。另外，参照某些示例所描述的特征可在其他示例中被组合。

[0136] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以计算机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(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端(可以是手机，计算机，服务器，或者网络设备等)执行本申请各个实施例所述的方法。

[0137] 上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本申请的保护之内。

[0138] 上述仅为本申请的较佳实施例及所运用的技术原理。本申请不限于这里所述的特定实施例，对本领域技术人员来说能够进行的各种明显变化、重新调整及替代均不会脱离本申请的保护范围。因此，虽然通过以上实施例对本申请进行了较为详细的说明，但是本申请不仅仅限于以上实施例，在不脱离本申请构思的情况下，还可以包括更多其他等效实施例，而本申请的范围由权利要求的范围决定。

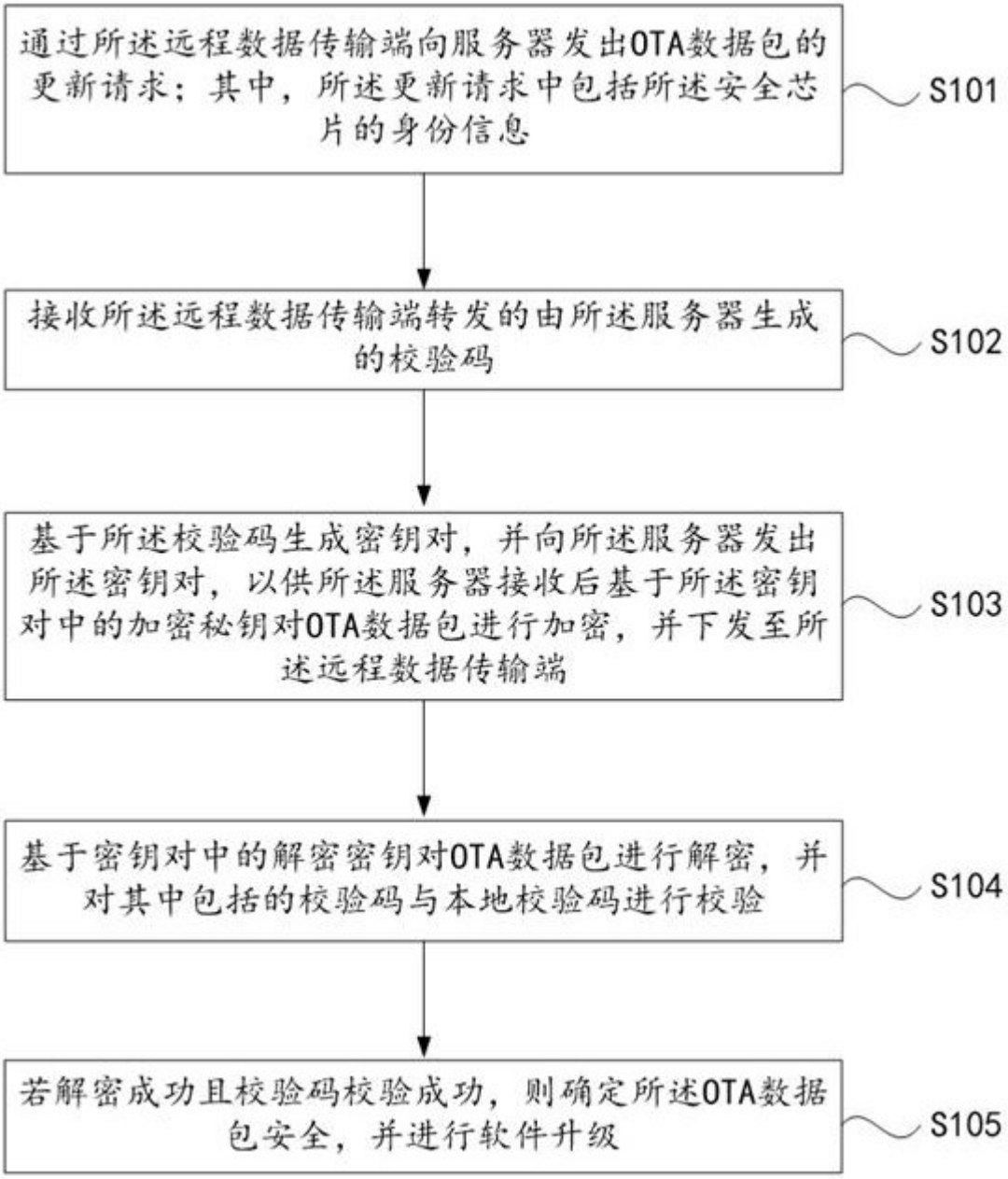

通过所述远程数据传输端向服务器发出OTA数据包的更新请求；其中，所述更新请求中包括所述安全芯片的身份信息
S101
接收所述远程数据传输端转发的由所述服务器生成的校验码
S102
基于所述校验码生成密钥对，并向所述服务器发出所述密钥对，以供所述服务器接收后基于所述密钥对中的加密秘钥对OTA数据包进行加密，并下发至所述远程数据传输端
S103
基于密钥对中的解密密钥对OTA数据包进行解密，并对其中包括的校验码与本地校验码进行校验
S104
若解密成功且校验码校验成功，则确定所述OTA数据包安全，并进行软件升级
S105

图1

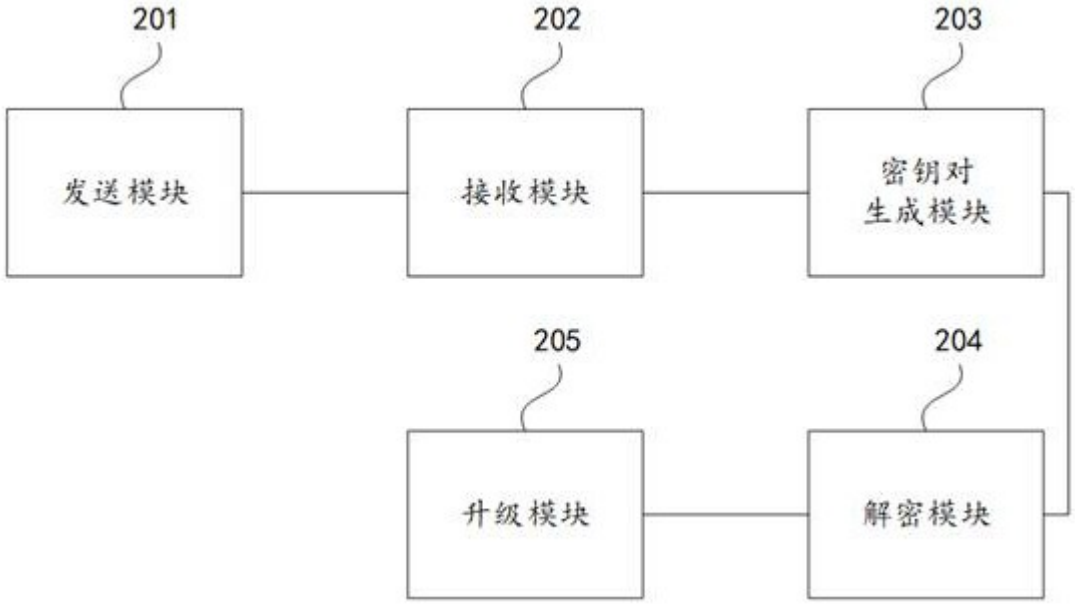

201
202
203
发送模块
接收模块
密钥对
生成模块
205
204
升级模块
解密模块

图2

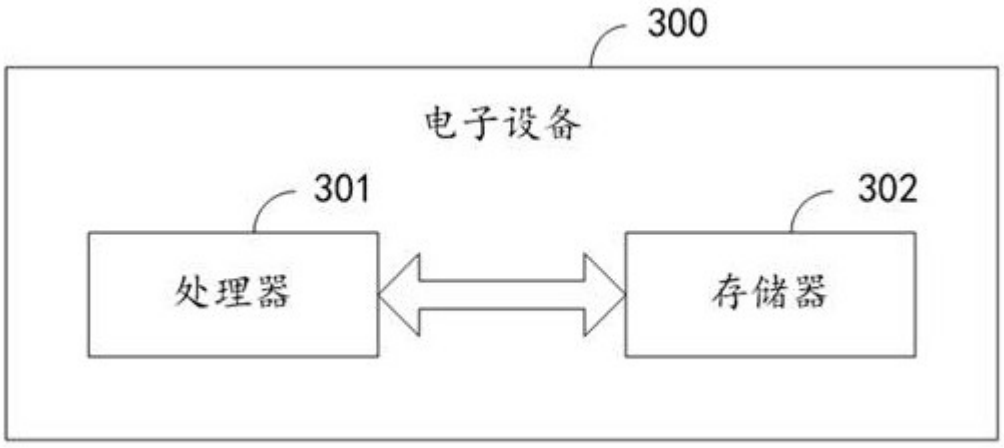

300
电子设备
301
302
处理器
存储器

图3