(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118632249 A
(43)申请公布日 2024.09.10

(21)申请号 202410906180.3

(22)申请日 2024.07.08

(71)申请人 深圳市爱协生科技股份有限公司
地址 518000 广东省深圳市宝安区新安街道留芳路6号庭威工业园3号楼7楼D、E区

(72)发明人 莫虬 孙添平

(74)专利代理机构 深圳市嘉勤知识产权代理有限公司 44651
专利代理师 汤金燕

(51)Int.Cl.
H04W 12/06(2021.01)
H04L 9/40(2022.01)
H04L 9/08(2006.01)

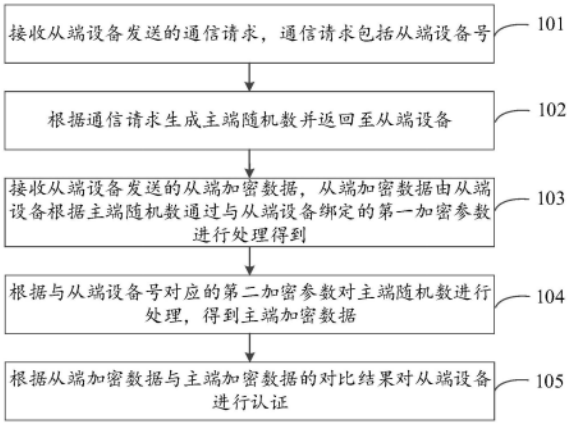
权利要求书2页 说明书10页 附图3页

(54)发明名称

设备通信的认证方法、装置、电子设备及存储介质

(57)摘要

本申请实施例公开了一种设备通信的认证方法、装置、电子设备及存储介质。该方案可以接收从端设备发送的通信请求,通信请求包括从端设备号,根据通信请求生成主端随机数并返回至从端设备,接收从端设备发送的从端加密数据,从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到,根据与从端设备号对应的第二加密参数对主端随机数进行处理,得到主端加密数据,根据从端加密数据与主端加密数据的对比结果对从端设备进行认证。本申请实施例可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。



CN 118632249 A

1.一种设备通信的认证方法,其特征在于,包括:

接收从端设备发送的通信请求,所述通信请求包括从端设备号;

根据所述通信请求生成主端随机数并返回至所述从端设备;

接收所述从端设备发送的从端加密数据,所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理,得到主端加密数据;

根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

2.如权利要求1所述的设备通信的认证方法,其特征在于,在根据所述通信请求生成主端随机数并返回至所述从端设备之后,所述方法还包括:

接收所述从端设备生成并发送的从端随机数以及从端加密数据,所述从端加密数据由从端设备根据所述主端随机数和从端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

根据与所述从端设备号对应的第二加密参数对所述主端随机数和从端随机数进行处理,得到主端加密数据。

3.如权利要求2所述的设备通信的认证方法,其特征在于,所述方法还包括:

所述从端加密数据由从端设备根据所述主端随机数、从端随机数以及从端设备号通过与所述从端设备绑定的第一加密参数进行处理得到;

根据与所述从端设备号对应的第二加密参数对所述主端随机数、从端随机数以及从端设备号进行处理,得到主端加密数据。

4.如权利要求1所述的设备通信的认证方法,其特征在于,在接收从端设备发送的通信请求之后,所述方法还包括:

获取历史认证记录,并判断所述历史认证记录中是否存在所述从端设备号的认证失败信息;

若存在,则拒绝所述通信请求。

5.如权利要求1所述的设备通信的认证方法,其特征在于,根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证,包括:

判断所述从端加密数据与所述主端加密数据是否相同;

若相同,则确定所述从端设备认证成功。

6.如权利要求5所述的设备通信的认证方法,其特征在于,所述方法还包括:

若所述从端加密数据与所述主端加密数据不相同,则确认所述从端设备认证失败;

将所述从端设备号设置对应的预设时长,以使在所述预设时长之内直接拒绝包含所述从端设备号的通信请求。

7.如权利要求6所述的设备通信的认证方法,其特征在于,在所述从端加密数据与所述主端加密数据不相同之后,所述方法给还包括:

根据MD5值或哈希值对所述从端加密数据在收发前后的完整性进行验证;

若验证未通过,则重新接收所述从端设备发送的从端加密数据以进行对比;

若验证通过,则确认所述从端设备认证失败。

8.一种设备通信的认证装置,其特征在于,包括:

第一接收模块,用于接收从端设备发送的通信请求,所述通信请求包括从端设备号;

生成模块,用于根据所述通信请求生成主端随机数并返回至所述从端设备;

第二接收模块,用于接收所述从端设备发送的从端加密数据,所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

处理模块,用于根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理,得到主端加密数据;

认证模块,用于根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

9.一种电子设备,其特征在于,所述电子设备包括存储器和处理器,所述存储器中存储有计算机程序,所述处理器通过调用所述存储器中存储的所述计算机程序,执行如权利要求1-7任一项所述的设备通信的认证方法中的步骤。

10.一种存储介质,其特征在于,所述存储介质存储有计算机程序,所述计算机程序适于处理器进行加载,以执行如权利要求1-7任一项所述的设备通信的认证方法中的步骤。

设备通信的认证方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及通信技术领域,具体涉及一种设备通信的认证方法、装置、电子设备及存储介质。

背景技术

[0002] 在电子设备中,一般可以通过具有Wifi(IEEE 802.11a/b/g/n),UWB,蓝牙(Bluetooth)和红外(Irda)等多种无线网络通讯方式进行通信以及数据交换,当然也可以通过有线连接的方式进行通信。这些无线或有线通讯连接方式可以进行移动设备间的信息交换和功能共享,例如用户可以通过对应接口实现电子设备间的流媒体文件传输、通讯录备份等功能。

[0003] 申请人在具体使用过程中发现:在多个通信设备之间若不进行防伪认证,便可以轻易通过一复制或伪造的从设备与主设备进行连接,从而对主设备上存储的资料进行复制和窃取,并且主设备在和伪造的从设备通信时和原样品完全一样,无法对从设备进行区分,严重破坏了信息的安全性。

发明内容

[0004] 本申请实施例提供一种设备通信的认证方法、装置、电子设备及存储介质,可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。

[0005] 本申请实施例提供一种设备通信的认证方法,包括:

[0006] 接收从端设备发送的通信请求,所述通信请求包括从端设备号;

[0007] 根据所述通信请求生成主端随机数并返回至所述从端设备;

[0008] 接收所述从端设备发送的从端加密数据,所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

[0009] 根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理,得到主端加密数据;

[0010] 根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

[0011] 在一实施例中,在根据所述通信请求生成主端随机数并返回至所述从端设备之后,所述方法还包括:

[0012] 接收所述从端设备生成并发送的从端随机数以及从端加密数据,所述从端加密数据由从端设备根据所述主端随机数和从端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

[0013] 根据与所述从端设备号对应的第二加密参数对所述主端随机数和从端随机数进行处理,得到主端加密数据。

[0014] 在一实施例中,所述方法还包括:

[0015] 所述从端加密数据由从端设备根据所述主端随机数、从端随机数以及从端设备号通过与所述从端设备绑定的第一加密参数进行处理得到；

[0016] 根据与所述从端设备号对应的第二加密参数对所述主端随机数、从端随机数以及从端设备号进行处理，得到主端加密数据。

[0017] 在一实施例中，在接收从端设备发送的通信请求之后，所述方法还包括：

[0018] 获取历史认证记录，并判断所述历史认证记录中是否存在所述从端设备号的认证失败信息；

[0019] 若存在，则拒绝所述通信请求。

[0020] 在一实施例中，根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证，包括：

[0021] 判断所述从端加密数据与所述主端加密数据是否相同；

[0022] 若相同，则确定所述从端设备认证成功。

[0023] 在一实施例中，所述方法还包括：

[0024] 若所述从端加密数据与所述主端加密数据不相同，则确认所述从端设备认证失败；

[0025] 将所述从端设备号设置对应的预设时长，以使在所述预设时长之内直接拒绝包含所述从端设备号的通信请求。

[0026] 在一实施例中，在所述从端加密数据与所述主端加密数据不相同之后，所述方法给还包括：

[0027] 根据MD5值或哈希值对所述从端加密数据在收发前后的完整性进行验证；

[0028] 若验证未通过，则重新接收所述从端设备发送的从端加密数据以进行对比；

[0029] 若验证通过，则确认所述从端设备认证失败。

[0030] 本申请实施例还提供一种设备通信的认证装置，包括：

[0031] 第一接收模块，用于接收从端设备发送的通信请求，所述通信请求包括从端设备号；

[0032] 生成模块，用于根据所述通信请求生成主端随机数并返回至所述从端设备；

[0033] 第二接收模块，用于接收所述从端设备发送的从端加密数据，所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到；

[0034] 处理模块，用于根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理，得到主端加密数据；

[0035] 认证模块，用于根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

[0036] 本申请实施例还提供一种电子设备，其特征在于，所述电子设备包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器通过调用所述存储器中存储的所述计算机程序，执行本申请实施例提供的任一项所述设备通信的认证方法中的步骤。

[0037] 本申请实施例还提供一种存储介质，其特征在于，所述存储介质存储有计算机程序，所述计算机程序适于处理器进行加载，以执行本申请实施例提供的任一项所述设备通信的认证方法中的步骤。

[0038] 本申请实施例提供的设备通信的认证方法，可以接收从端设备发送的通信请求，

通信请求包括从端设备号,根据通信请求生成主端随机数并返回至从端设备,接收从端设备发送的从端加密数据,从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到,根据与从端设备号对应的第二加密参数对主端随机数进行处理,得到主端加密数据,根据从端加密数据与主端加密数据的对比结果对从端设备进行认证。本申请实施例可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。

附图说明

[0039] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例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申请的一些实施例,对于本领域技术人员来讲,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。

[0040] 图1是本申请实施例提供的设备通信的认证方法的第一种流程示意图;

[0041] 图2是本申请实施例提供的设备通信的认证方法的第二种流程示意图;

[0042] 图3是本申请实施例提供的数据加密流程示意图;

[0043] 图4是本申请实施例提供的设备通信的认证装置的一种结构示意图;

[0044] 图5是本申请实施例提供的终端的结构示意图。

具体实施方式

[0045] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0046] 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,本申请不同实施例中具有同样命名的部件、特征、要素可能具有相同含义,也可能具有不同含义,其具体含义需以其在该具体实施例中的解释或者进一步结合该具体实施例中上下文进行确定。

[0047] 应该理解的是,虽然本申请实施例中的流程图中的各个步骤按照箭头的指示依次显示,但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明,这些步骤的执行并没有严格的顺序限制,其可以以其他的顺序执行。而且,图中的至少一部分步骤可以包括多个子步骤或者多个阶段,这些子步骤或者阶段并不必然是在同一时刻执行完成,而是可以在不同的时刻执行,其执行顺序也不必然是依次进行,而是可以与其他步骤或者其他步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0048] 需要说明的是,在本文中,采用了诸如101、102等步骤代号,其目的是为了更清楚简要地表述相应内容,不构成顺序上的实质性限制,本领域技术人员在具体实施时,可能会先执行102后执行101等,但这些均应在本申请的保护范围之内。

[0049] 在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0050] 本申请实施例提供一种设备通信的认证方法,该设备通信的认证方法的执行主体可以是本申请实施例提供的设备通信的认证装置,或者集成了该设备通信的认证装置的服务器,其中该设备通信的认证装置可以采用硬件或者软件的方式实现。

[0051] 如图1所示,图1是本申请实施例提供的设备通信的认证方法的第一流程示意图,该设备通信的认证方法的具体流程可以如下:

[0052] 101、接收从端设备发送的通信请求,通信请求包括从端设备号。

[0053] 在本实施例中,上述设备通信的认证方法的执行主体为主端设备,在其他从端设备想要与当前主端设备进行通信认证时,需要先发送携带从端设备对应的设备号的请求信息,主端设备在接收到后便可以从中提取出从端设备号。其中,上述从端设备号与从端设备对应且具有唯一性,具体可以为从端设备的IMEl(Intemnational Mobile Equipment ldentity,国际移动设备识别码)号,该IMEl是设备的唯一标识符。在其他实施例中,上述从端设备号也可以为设备序列号、设备ID或者UUID(Universally Unique Identifier,通用唯一识别码)等。

[0054] 在一实施例中,上述从端设备号便可以用于在主端设备的历史认证记录中进行查找,从而确定在历史认证记录中是否存在与从端设备号相同且认证失败的记录,若存在,也即该从端设备号已经认证失败过,因此便无需执行后续步骤,直接将该从端设备号对应的通信请求进行拒绝或忽略即可。也即在接收从端设备发送的通信请求之后,该方法还可以包括:获取历史认证记录,并判断所述历史认证记录中是否存在所述从端设备号的认证失败信息,若存在,则拒绝所述通信请求。

[0055] 102、根据通信请求生成主端随机数并返回至从端设备。

[0056] 在一实施例中,主端设备在接收到通信请求后便可以计算生成一个主端随机数,比如为一个32bit的随机数,以便后续从端设备以及主端设备来分别进行加密处理。其中,该主端随机数是指主端设备中的随机数产生单元在第一时刻所产生的随机数,随机数产生单元在不同的时刻所产生的随机数将不同。

[0057] 在一实施例中,上述主端随机数可以通过调用操作系统提供的随机数生成API、使用编程语言内置的随机数生成函数或库、或者采用专门的随机数生成算法等方式来实现。其中,许多操作系统提供了生成随机数的API,这些API可以生成高质量的随机数,满足大多数应用的需求。相应的,大多数编程语言也都提供了生成随机数的库或函数,如Python的random模块、Java的Random类、C++的<random>库等。而为了进一步提升安全性,还可以使用加密安全的随机数生成算法,如Merkle-Damgård结构的哈希函数(如SHA-256)与计数器模式相结合来生成随机数。

[0058] 在一实施例中,主端随机数可以通过主端设备与从端设备之间的所建立的数据通信连接发送至从端设备,可选地,可以通过主端设备与从端设备之间的信令路由进行发送。可选地,还可以将主端随机数写入文件,然后通过文件共享或传输协议(如FTP、SFTP等)将文件发送给从端。

[0059] 103、接收从端设备发送的从端加密数据,从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到。

[0060] 在一实施例中,从端设备在接收到主端设备发送的主端随机数之后,便可以基于该主端随机数通过与从端设备绑定的第一加密参数进行加密处理,以得到从端加密数据。需要说明的是,上述与从端设备绑定的第一加密参数具有唯一性,也即不同的从端设备所绑定的加密参数也均不相同。从而可以保证即便是伪造的从端设备,也只能使用本设备对应的第一加密参数进行加密。

[0061] 在对主端随机数进行加密时,使用的加密算法例如可以是:高级加密标准(Advanced Encryption Standard,AES)算法、数据加密标准(DataEncryption Standard,DES)、三重数据加密算法(Triple Data Encryption Standard,3DES)、非对称加密算法例如RSA等加密算法。在根据上述算法加密时,需按照对应的第一加密参数进行加密,加密完成得到的从端加密数据便可以由从端设备发送至主端设备。

[0062] 104、根据与从端设备号对应的第二加密参数对主端随机数进行处理,得到主端加密数据。

[0063] 在一实施例中,在接收到从端设备发送的从端加密数据后,主端设备就可以以同样的方式对主端随机数进行加密,在主端设备进行加密时则需要依据从端设备号确定与该设备号绑定且具有唯一性的第二加密参数进行处理,从而得到主端加密数据。

[0064] 其中,主端设备中可以存储其他全部从端设备的设备号以及相应的加密参数之间的对应关系,需要说明的是,上述从端设备号与加密参数一一对应,且不同的加密参数均不相同。

[0065] 105、根据从端加密数据与主端加密数据的对比结果对从端设备进行认证。

[0066] 通过对上述步骤104中得到的主端加密数据以及步骤103中接收到的从端加密数据进行对比,如果两个数据一致则确认通过从端设备的验证,也即确认该从端设备认证成功。在本申请实施例中,由于上述从端设备对应的加密参数具有唯一性,因此即便伪造了从端设备在与主端设备认证的过程中,其伪造设备使用的加密参数也必然与从端设备码对应的加密参数不同,最终生成的从端加密数据与主端加密数据也不相同,因此通过本实施例提供的方法可以轻易判断出从端设备是否为伪造设备,从而进行防伪认证。

[0067] 由上所述,本申请实施例提出的设备通信的认证方法可以接收从端设备发送的通信请求,通信请求包括从端设备号,根据通信请求生成主端随机数并返回至从端设备,接收从端设备发送的从端加密数据,从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到,根据与从端设备号对应的第二加密参数对主端随机数进行处理,得到主端加密数据,根据从端加密数据与主端加密数据的对比结果对从端设备进行认证。本申请实施例可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。

[0068] 请参阅图2,图2是本申请实施例提供的设备通信的认证方法的第二种流程示意图。所述方法包括:

[0069] 201、接收从端设备发送的通信请求,通信请求包括从端设备号。

[0070] 202、根据通信请求生成主端随机数并返回至从端设备。

[0071] 主端设备在接收到从端设备的通信请求后可以计算生成一个主端随机数,比如为一个32bit的随机数,然后返回至从端设备,以便后续从端设备以及主端设备来分别进行加密处理。

[0072] 203、接收从端设备生成并发送的从端随机数以及从端加密数据。

[0073] 在一实施例中,从端设备在接收到主端设备发送的主端随机数之后,也可以生成从端随机数,比如也生成32bit的随机数,然后结合主端随机数以及从端设备号进行加密。因此上述从端加密数据由从端设备根据主端随机数、从端随机数以及从端设备号通过与从端设备绑定的第一加密参数进行处理得到。其中,在进行加密处理之前,可以先由主端随机数、从端随机数以及从端设备号组成基础数据,然后针对该基础数据利用与从端设备绑定的第一加密参数进行加密处理,如图3所示。上述与从端设备绑定的第一加密参数具有唯一性,也即不同的从端设备所绑定的加密参数也均不相同。

[0074] 204、根据与从端设备号对应的第二加密参数对主端随机数、从端随机数以及从端设备号进行处理,得到主端加密数据。

[0075] 主端设备在接收到从端设备的加密数据后就获取到以下数据:从端加密数据、主端随机数、从端随机数、以及从端设备号。在一实施例中,主端设备在接收到从端设备发送的从端加密数据后,主端设备就可以以同样的方式对主端随机数、从端随机数、以及从端设备号进行加密,在主端设备进行加密时则需要依据从端设备号确定与该设备号绑定且具有唯一性的第二加密参数进行处理,从而得到主端加密数据。

[0076] 205、判断从端加密数据与主端加密数据是否相同,若是则执行步骤206,若否,则执行步骤207。

[0077] 206、确定从端设备认证成功。

[0078] 通过对上述步骤204中得到的主端加密数据以及步骤203中接收到的从端加密数据进行对比,如果两个数据一致则确认通过从端设备的验证,也即确认该从端设备认证成功。

[0079] 207,确认从端设备认证失败,并将从端设备号设置对应的预设时长,以使在预设时长之内直接拒绝包含从端设备号的通信请求。

[0080] 在一实施例中,若上述从端加密数据与主端加密数据不一致,则说明从端加密数据与主端加密数据是分别采用两种加密参数进行加密得到的数据,因此确定该从端设备为伪造设备,认证失败。进一步的,在确定认证失败后还可以记录此次认证使用的从端设备号,并在一定时间内拒绝此设备号的通信请示。通过上述延时机制,增加不断重试的暴力破解的难度,进而提升数据安全性。

[0081] 在一实施例中,考虑到上述从端加密数据与主端加密数据不一致还有可能是由于传输过程中的信息丢失造成的,因此还可以在从端加密数据收发前后对其完整性进行验证,也即在从端加密数据与主端加密数据不相同之后,该方法给还可以包括:根据MD5值或哈希值对从端加密数据在收发前后的完整性进行验证,若验证未通过,则重新接收从端设备发送的从端加密数据以进行对比,若验证通过,则确认从端设备认证失败。

[0082] 通过上述设备通信的认证方法可以使得直接复制的伪装样品不再有通过认证的机会,另外主端随机数及从端随机数双重随机数下增加了破解难度,在本申请当中,由于每个从端设备有唯一的设备号,也对应唯一的加密算法参数,进一步增加破解难度,相较于现

有技术大幅提升了数据安全性。

[0083] 由上所述,本申请实施例提出的设备通信的认证方法可以接收从端设备发送的通信请求,通信请求包括从端设备号,根据通信请求生成主端随机数并返回至从端设备,接收从端设备生成并发送的从端随机数以及从端加密数据,根据与从端设备号对应的第二加密参数对主端随机数、从端随机数以及从端设备号进行处理,得到主端加密数据,判断从端加密数据与主端加密数据是否相同,若是,则确定从端设备认证成功,若否,则确认从端设备认证失败,并将从端设备号设置对应的预设时长,以使在预设时长之内直接拒绝包含从端设备号的通信请求。本申请实施例可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。

[0084] 为了实施以上方法,本申请实施例还提供一种设备通信的认证装置,该设备通信的认证装置具体可以集成在终端设备如手机、平板电脑等设备中。

[0085] 例如,如图4所示,是本申请实施例提供的设备通信的认证装置的第一种结构示意图。该设备通信的认证装置可以包括:

[0086] 第一接收模块301,用于接收从端设备发送的通信请求,所述通信请求包括从端设备号;

[0087] 生成模块302,用于根据所述通信请求生成主端随机数并返回至所述从端设备;

[0088] 第二接收模块303,用于接收所述从端设备发送的从端加密数据,所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

[0089] 处理模块304,用于根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理,得到主端加密数据;

[0090] 认证模块305,用于根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

[0091] 由上可知,本申请实施例提出的设备通信的认证装置,可以接收从端设备发送的通信请求,通信请求包括从端设备号,根据通信请求生成主端随机数并返回至从端设备,接收从端设备发送的从端加密数据,从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到,根据与从端设备号对应的第二加密参数对主端随机数进行处理,得到主端加密数据,根据从端加密数据与主端加密数据的对比结果对从端设备进行认证。本申请实施例可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。

[0092] 上述所有的技术方案,可以采用任意结合形成本申请的可选实施例,在此不再一一赘述。

[0093] 相应的,本申请实施例还提供一种电子设备,该电子设备可以为终端或者服务器,该终端可以为智能手机、平板电脑、笔记本电脑、触控屏幕、游戏机、个人计算机(PC,Personal Computer)、个人数字助理(Personal Digital Assistant,PDA)等终端设备。如图5所示,图5为本申请实施例提供的电子设备的结构示意图。该电子设备400包括有一个或者一个以上处理核心的处理器401、有一个或一个以上计算机可读存储介质的存储器402及

存储在存储器402上并可在处理器上运行的计算机程序。其中,处理器401与存储器402电性连接。本领域技术人员可以理解,图中示出的电子设备结构并不构成对电子设备的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0094] 处理器401是电子设备400的控制中心,利用各种接口和线路连接整个电子设备400的各个部分,通过运行或加载存储在存储器402内的软件程序和/或模块,以及调用存储在存储器402内的数据,执行电子设备400的各种功能和处理数据,从而对电子设备400进行整体监控。

[0095] 在本申请实施例中,电子设备400中的处理器401会按照如下的步骤,将一个或一个以上的应用程序的进程对应的指令加载到存储器402中,并由处理器401来运行存储在存储器402中的应用程序,从而实现各种功能:

[0096] 接收从端设备发送的通信请求,所述通信请求包括从端设备号;

[0097] 根据所述通信请求生成主端随机数并返回至所述从端设备;

[0098] 接收所述从端设备发送的从端加密数据,所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

[0099] 根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理,得到主端加密数据;

[0100] 根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

[0101] 以上各个操作的具体实施可参见前面的实施例,在此不再赘述。

[0102] 可选的,如图5所示,电子设备400还包括:触控显示屏403、射频电路404、音频电路405、输入单元406以及电源407。其中,处理器401分别与触控显示屏403、射频电路404、音频电路405、输入单元406以及电源407电性连接。本领域技术人员可以理解,图5中示出的电子设备结构并不构成对电子设备的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0103] 触控显示屏403可用于显示图形用户界面以及接收用户作用于图形用户界面产生的操作指令。触控显示屏403可以包括显示面板和触控面板。其中,显示面板可用于显示由用户输入的信息或提供给用户的信息以及电子设备的各种图形用户接口,这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。可选的,可以采用液晶显示器(LCD,Liquid Crystal Display)、有机发光二极管(OLED,Organic Light-Emitting Diode)等形式来配置显示面板。触控面板可用于收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触控面板上或在触控面板附近的操作),并生成相应的操作指令,且操作指令执行对应程序。可选的,触控面板可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器401,并能接收处理器401发来的命令并加以执行。触控面板可覆盖显示面板,当触控面板检测到在其上或附近的触摸操作后,传送给处理器401以确定触摸事件的类型,随后处理器401根据触摸事件的类型在显示面板上提供相应的视觉输出。在本申请实施例中,可以将触控面板与显示面板集成到触控显示屏403而实现输入和输出功能。但是在某些实施例中,触控面板与触控面板可以作为两个独立的部件来实现输入和输出功能。即触控

显示屏403也可以作为输入单元406的一部分实现输入功能。

[0104] 在本申请实施例中,通过处理器401执行应用程序在触控显示屏403上生成图形用户界面。该触控显示屏403用于呈现图形用户界面以及接收用户作用于图形用户界面产生的操作指令。

[0105] 射频电路404可以用于收发射频信号,以通过无线通信与网络设备或其他电子设备建立无线通讯,与网络设备或其他电子设备之间收发信号。通常,射频电路404包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM,Subscriber Identity Module)卡、收发信机、耦合器、低噪声放大器(LNA,Low Noise Amplifier)、双工器等。

[0106] 音频电路405可以用于通过扬声器、传声器提供用户与电子设备之间的音频接口。音频电路405可将接收到的音频数据转换后的电信号,传输到扬声器,由扬声器转换为声音信号输出;另一方面,传声器将收集的声音信号转换为电信号,由音频电路405接收后转换为音频数据,再将音频数据输出处理器401处理后,经射频电路404以发送给比如另一电子设备,或者将音频数据输出至存储器402以便进一步处理。音频电路405还可能包括耳塞插孔,以提供外设耳机与电子设备的通信。

[0107] 输入单元406可用于接收输入的数字、字符信息或用户特征信息(例如指纹、虹膜、面部信息等),以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。

[0108] 电源407用于给电子设备400的各个部件供电。可选的,电源407可以通过电源管理系统与处理器401逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源407还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0109] 尽管图5中未示出,电子设备400还可以包括摄像头、传感器、无线保真模块、蓝牙模块等,在此不再赘述。

[0110] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0111] 由上可知,本实施例提供的电子设备,通过接收从端设备发送的通信请求,通信请求包括从端设备号,根据通信请求生成主端随机数并返回至从端设备,接收从端设备发送的从端加密数据,从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到,根据与从端设备号对应的第二加密参数对主端随机数进行处理,得到主端加密数据,根据从端加密数据与主端加密数据的对比结果对从端设备进行认证。本申请实施例可以由主设备和从设备分别进行数据加密,并基于从设备绑定的加密参数的唯一性进行对比,再根据对比结果进行设备认证,从而有效提升了数据的安全性。

[0112] 本领域普通技术人员可以理解,上述实施例的各种方法中的全部或部分步骤可以通过指令来完成,或通过指令控制相关的硬件来完成,该指令可以存储于一计算机可读存储介质中,并由处理器进行加载和执行。

[0113] 为此,本申请实施例提供一种计算机可读存储介质,其中存储有多条计算机程序,该计算机程序能够被处理器进行加载,以执行本申请实施例所提供的任一种设备通信的认证方法中的步骤。例如,该计算机程序可以执行如下步骤:

[0114] 接收从端设备发送的通信请求,所述通信请求包括从端设备号;

[0115] 根据所述通信请求生成主端随机数并返回至所述从端设备;

[0116] 接收所述从端设备发送的从端加密数据,所述从端加密数据由从端设备根据所述主端随机数通过与所述从端设备绑定的第一加密参数进行处理得到;

[0117] 根据与所述从端设备号对应的第二加密参数对所述主端随机数进行处理,得到主端加密数据;

[0118] 根据所述从端加密数据与所述主端加密数据的对比结果对所述从端设备进行认证。

[0119] 以上各个操作的具体实施可参见前面的实施例,在此不再赘述。

[0120] 其中,该存储介质可以包括:只读存储器(ROM,Read Only Memory)、随机存取记忆体(RAM,Random Access Memory)、磁盘或光盘等。

[0121] 由于该存储介质中所存储的计算机程序,可以执行本申请实施例所提供的任一种设备通信的认证方法中的步骤,因此,可以实现本申请实施例所提供的任一种设备通信的认证方法所能实现的有益效果,详见前面的实施例,在此不再赘述。

[0122] 以上对本申请实施例所提供的一种设备通信的认证方法、装置、电子设备及存储介质进行了详细介绍,本文中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

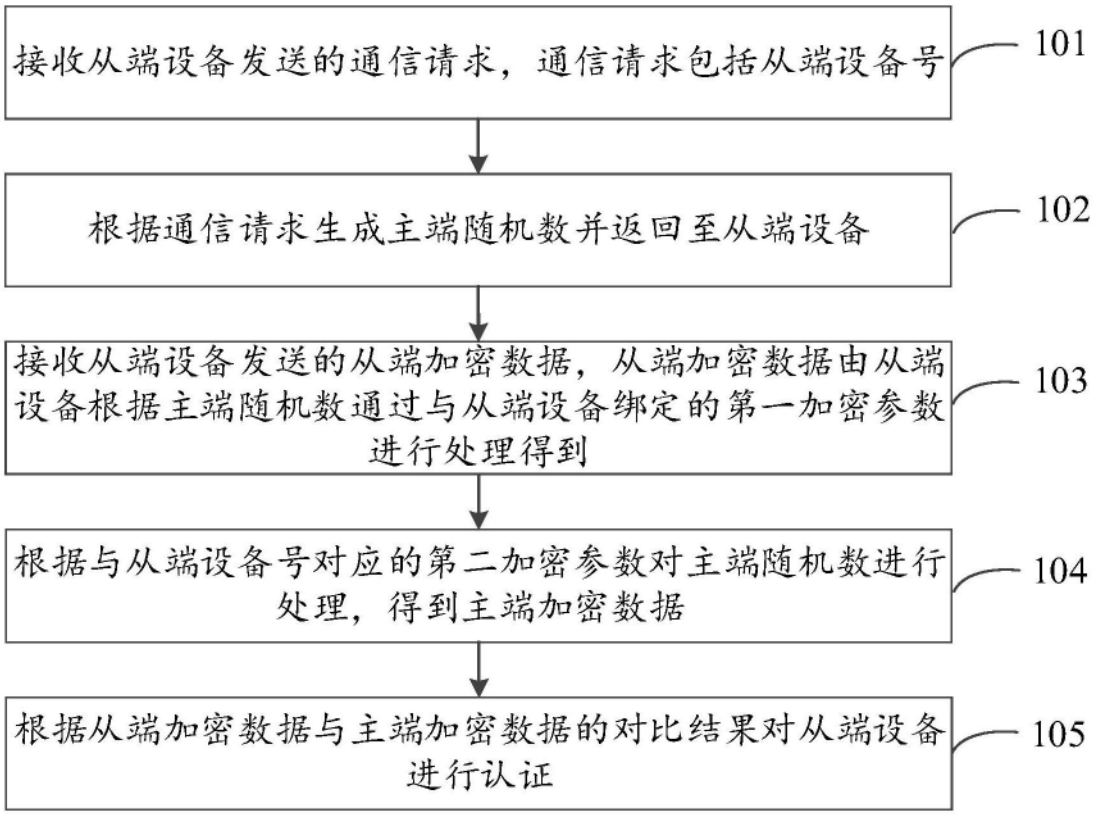

接收从端设备发送的通信请求，通信请求包括从端设备号
101
根据通信请求生成主端随机数并返回至从端设备
102
接收从端设备发送的从端加密数据，从端加密数据由从端设备根据主端随机数通过与从端设备绑定的第一加密参数进行处理得到
103
根据与从端设备号对应的第二加密参数对主端随机数进行处理，得到主端加密数据
104
根据从端加密数据与主端加密数据的对比结果对从端设备进行认证
105

图1

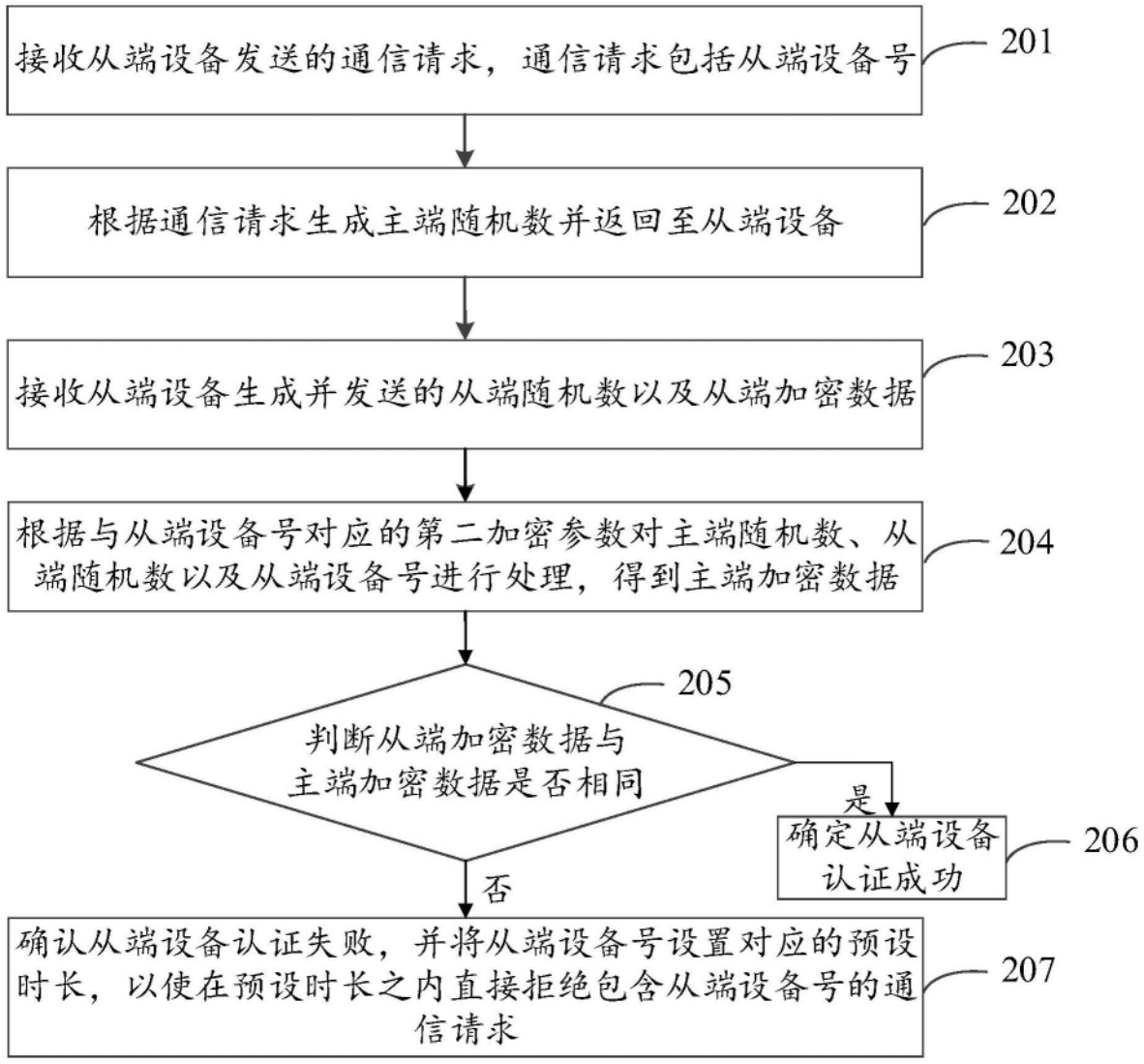

接收从端设备发送的通信请求，通信请求包括从端设备号
201
根据通信请求生成主端随机数并返回至从端设备
202
接收从端设备生成并发送的从端随机数以及从端加密数据
203
根据与从端设备号对应的第二加密参数对主端随机数、从端随机数以及从端设备号进行处理，得到主端加密数据
204
判断从端加密数据与主端加密数据是否相同
205
是
确定从端设备认证成功
206
否
确认从端设备认证失败，并将从端设备号设置对应的预设时长，以使在预设时长之内直接拒绝包含从端设备号的通信请求
207

图2

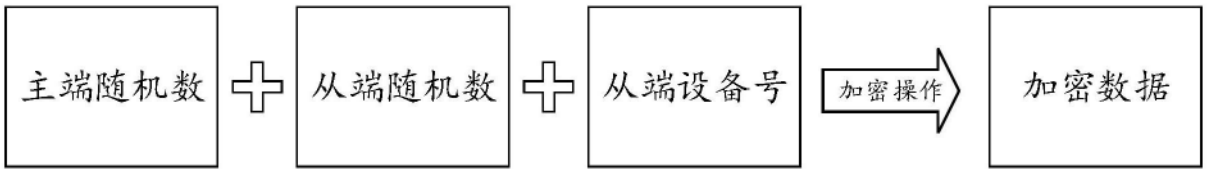

主端随机数
从端随机数
从端设备号
加密操作
加密数据

图3

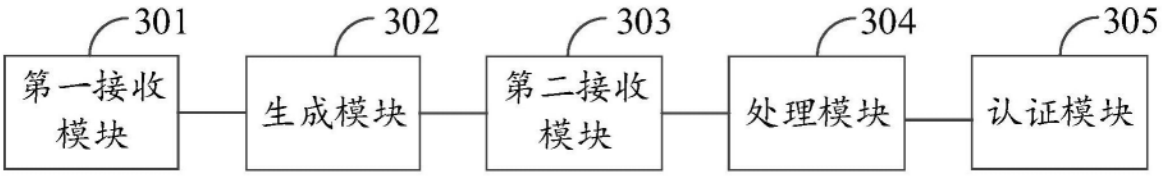

301
第一接收模块
302
生成模块
303
第二接收模块
304
处理模块
305
认证模块

图4

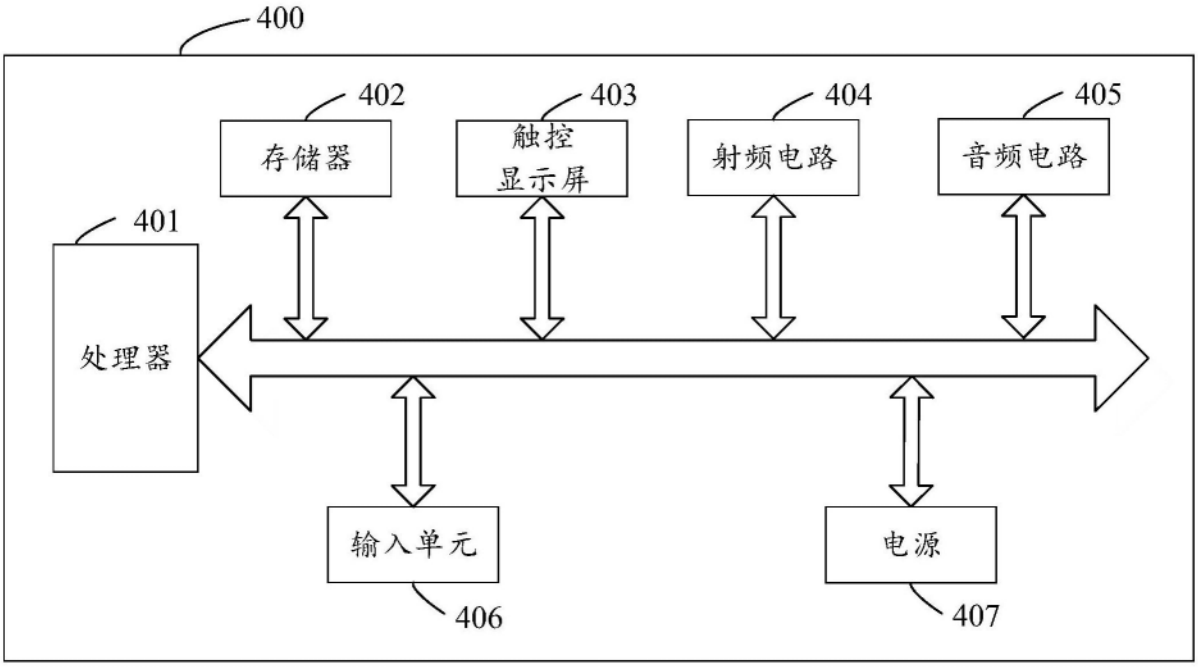

400
401
处理器
402
存储器
403
触控显示屏
404
射频电路
405
音频电路
406
输入单元
407
电源

图5