NFC便携设备的写入、支付方法、装置以及设备

技术领域

本说明书涉及计算机软件技术领域，尤其涉及针对近场通信（NFC）便携设备的写入、基于NFC设备的支付处理方法、装置以及设备。

背景技术

智能手机的使用普及给人们的生活带来了便利。通过使用智能手机上的各种应用，能够相应地进行各种业务，很多业务都涉及到支付。

在现有技术中，一般通过手机银行或者二维码扫描进行支付，这些支付方式强依赖于手机，操作步骤较为繁琐。

基于现有技术，需要更为便利的支付方案。

发明内容

本说明书实施例提供针对NFC便携设备的写入、基于NFC设备的支付处理方法、装置以及设备，用以解决如下技术问题：需要更为便利的支付方案。

为解决上述技术问题，本说明书实施例是这样实现的：

本说明书实施例提供的一种基于NFC便携设备的支付方法，包括：

所述NFC便携设备获取NFC写入信息，所述NFC写入信息包括密钥对标识和对应的公钥；

当进入消费机具的NFC通信范围时，接收所述消费机具发送的消费金额信息；

利用所述公钥，对所述消费金额信息加密得到加密信息；

将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的一种针对 NFC 便携设备的写入方法，包括:

NFC 写入端获取用户账户关联的密钥对标识和对应的密钥对中的公钥;

将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

本说明书实施例提供的另一种基于 NFC 便携设备的支付方法，包括:

消费机具当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息;

接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中;

将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的再一种基于 NFC 便携设备的支付方法，包括:

服务端接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具;

根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息;

根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的一种基于 NFC 便携设备的支付装置，所述装置位于所述 NFC 便携设备，包括:

获取模块，获取 NFC 写入信息，所述 NFC 写入信息包括密钥对标识和对应的公钥;

接收模块，当进入消费机具的 NFC 通信范围时，接收所述消费机具发送的消费金额信息;

加密模块，利用所述公钥，对所述消费金额信息加密得到加密信息；

发送模块，将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的一种针对 NFC 便携设备的写入装置，所述装置位于 NFC 写入端，包括：

获取模块，获取用户账户关联的密钥对标识和对应的密钥对中的公钥；

写入模块，将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

本说明书实施例提供的另一种基于 NFC 便携设备的支付装置，所述装置位于消费机具，包括：

第一发送模块，当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息；

接收模块，接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中；

第二发送模块，将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的再一种基于 NFC 便携设备的支付装置，所述装置位于服务端，包括：

接收模块，接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具；

确定模块，根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息；

扣款模块，根据所述消费金额信息，从所述密钥对标识预先关联的用

户账户中扣款。

本说明书实施例提供的一种基于 NFC 便携设备的支付设备，所述设备为所述 NFC 便携设备，包括:

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够:

获取NFC写入信息，所述NFC写入信息包括密钥对标识和对应的公钥;

当进入消费机具的 NFC 通信范围时，接收所述消费机具发送的消费金额信息;

利用所述公钥，对所述消费金额信息加密得到加密信息;

将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的一种针对 NFC 便携设备的写入设备，所述设备为 NFC 写入端，包括:

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够:

获取用户账户关联的密钥对标识和对应的密钥对中的公钥;

将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

本说明书实施例提供的另一种基于 NFC 便携设备的支付设备，所述设备为消费机具，包括:

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息；

接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中；

将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例提供的再一种基于 NFC 便携设备的支付设备，所述设备为消费机具，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具；

根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息；

根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：使得支付操作更为便捷，而且未必要依赖于手机，NFC 便携设备比如是支持 NFC 的可穿戴设备或者卡片等；不仅如此，即使 NFC 便携设备丢失，可以便利地解除对应的密钥对标识与用户账户之间的关联关系，使得 NFC 便

携设备不能够通过用户账户支付，以保障用户资金安全。

附图说明

为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本说明书的方案在一种实际应用场景下涉及的一种整体架构示意图；

图 2 为本说明书实施例提供的一种基于 NFC 便携设备的支付方法的流程示意图；

图 3 为本说明书实施例提供的一种针对 NFC 便携设备的写入方法的流程示意图；

图 4 为本说明书实施例提供的另一种基于 NFC 便携设备的支付方法的流程示意图；

图 5 为本说明书实施例提供的再一种基于 NFC 便携设备的支付方法的流程示意图；

图 6 为本说明书实施例提供的对应于图 2 的一种基于 NFC 便携设备的支付装置的结构示意图；

图 7 为本说明书实施例提供的对应于图 3 的一种针对 NFC 便携设备的写入装置的结构示意图；

图 8 为本说明书实施例提供的对应于图 4 的一种基于 NFC 便携设备的支付装置的结构示意图；

图 9 为本说明书实施例提供的对应于图 5 的一种基于 NFC 便携设备的支付装置的结构示意图。

具体实施方式

本说明书实施例提供针对 NFC 便携设备的写入、基于 NFC 设备的支付处理方法、装置以及设备。

为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本说明书实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

图 1 为本说明书的方案在一种实际应用场景下涉及的一种整体架构示意图。该整体架构中，主要涉及四端：NFC 便携设备（比如智能手环等）、NFC 写入端（比如智能手机等）、消费机具（比如收银机等）、服务端（比如支付服务器）等。

工作流程主要包括两个阶段：写入阶段、支付阶段。写入阶段即为启用 NFC 便携设备时的初始化阶段，在写入阶段，基于用户账户授权，NFC 写入端能够将支付所需要用到的信息写入 NFC 便携设备中，所写入的信息可以获取自服务端。写入后，NFC 便携设备即可以用于支付，比如，NFC 便携设备通过碰触消费机具进行 NFC 通信，以为支付而进行信息交互，消费机具基于交互结果与服务端进行通信，请求服务端扣款，从而完成支付。

下面分别从 NFC 便携设备、NFC 写入端、消费机具和服务端的角度对本说明书的方案详细说明。

图 2 为本说明书实施例提供的一种基于 NFC 便携设备的支付方法的流程示意图，执行主体为 NFC 便携设备。

图 2 中的流程可以包括以下步骤：

S202：NFC 便携设备获取 NFC 写入信息，所述 NFC 写入信息包括密钥对标识和对应的公钥。

在本说明书实施例中，NFC 便携设备可以是手机以外的设备，其优选地是支持 NFC 的可穿戴设备或者卡片，比如，智能手表、智能手环、智能

戒指、智能纽扣、智能工卡等。

需要说明的是，NFC 便携设备本身可以是不带电的，如此无须担心设备电力耗尽而无法使用（手机支付存在这个问题），适用性更好。当然，在这种情况下，NFC 便携设备仍应当支持计算功能，比如，其可以是包含线圈的卡片，该线圈可以被另一带电设备（比如消费机具等）激活，该卡片则能够利用线圈激活所产生的能量进行计算。

在本说明书实施例中，密钥对标识和对应的密钥对与指定的用户账户具有关联关系，基于用户账户的权限，密钥对标识和对应的公钥被写入 NFC 便携设备中，写入后，用户能够利用 NFC 便携设备便利地进行 NFC 支付，而无需执行诸如登录账户或者扫码等相对繁琐的动作，所支付的资金将从用户账户中扣除。

所述关联关系能够根据用户的请求或者服务端的自动策略而解除，从而有利于防止 NFC 便携设备被他人冒用。一个用户账户可以同时关联多个密钥对标识，从而能够同时支持多个 NFC 便携设备。

在本说明书实施例中，公钥用于支付过程中 NFC 便携设备加密诸如消费金额等所需信息，密钥对中的私钥可以保存于服务端用于解密，密钥对标识用于服务端查找解密所需的私钥。一般地，服务端为支付服务器。

根据密钥对标识，能够在一定范围内唯一确定密钥对。比如，一个用户账户可以关联多个密钥对标识，其中的每个密钥对标识在这多个密钥对标识中通常是唯一的，而未必是全局唯一；再比如，每个密钥对标识也可以在所有用户账户关联的全部密钥对标识中是唯一的；等等。唯一性的范围可以根据业务实际需求决定。

密钥对标识的生成方式这里不做限定，比如，可以通过对对应的公钥和/或私钥进行哈希计算，生成密钥对标识。

S204：当进入消费机具的 NFC 通信范围时，接收所述消费机具发送的消费金额信息。

在本说明书实施例中，消费机具比如是支持 NFC 的收银机、销售终端

（POS）机等。当需要支付时，用户可以使NFC便携设备靠近消费机具（比如，用智能手环触碰消费机具等），使得NFC便携设备与消费机具之间进行相应的NFC通信，收发支付所需要使用的信息。

S206：利用所述公钥，对所述消费金额信息加密得到加密信息。

在本说明书实施例中，加密信息内还可以包含除消费金额信息以外的更多信息，比如，账户识别信息、当前时间等，账户识别信息比如是账户识别码、账户别称等。

S208：将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

在本说明书实施例中，消费机具在接收到加密信息和密钥对标识后，可以直接发送给服务端，或者进行一定处理后再发送给服务端。所述处理比如是附加业务场景数据、对加密信息和/或密钥对标识进行格式化、二次加密等。

服务端根据密钥对标识，能够查找到对应的私钥，进而对加密信息解密。服务端可以根据密钥对标识确定用户账户；或者，若从消费机具获取的信息中携带有账户识别信息，则也可以根据账户识别信息确定用户账户。

在本说明书实施例中，为了进一步地提高支付安全性，上述步骤中还可以加入用户校验动作。比如，在NFC便携设备加密前或者向消费机具发送信息前，可以校验用户的指纹或者密码，校验通过再继续执行流程。

通过图2的方法，使得支付操作更为便捷，而且未必要依赖于手机，NFC便携设备比如是支持NFC的可穿戴设备或者卡片等；不仅如此，即使NFC便携设备丢失，可以便利地解除对应的密钥对标识与用户账户之间的关联关系，使得NFC便携设备不能够通过用户账户支付，以保障用户资金安全。

基于图2的方法，本说明书实施例还提供了该方法的一些具体实施方案，以及扩展方案，下面进行说明。

在本说明书实施例中，常见的NFC写入端比如是用户的手机，当用户准备启用一个NFC便携设备时，可以用自己的用户账户登录手机上的支付应用，然后，向服务端请求待写入的信息，服务端响应于该请求，可以新生成密钥对（比如RSA密钥对等）及其标识，并与用户账户进行关联，这里的关联可以是指与用户账户直接关联，也可以指与用户账户的账户识别信息关联。进一步地，服务端将密钥对标识和对应的公钥下发至手机，同时还可以将账户识别信息也下发至手机，手机基于用户账户的权限，将密钥对标识和对应的公钥、账户识别信息写入NFC便携设备中。

需要说明的是，用户登录的设备和 NFC 写入端也可以不是同一设备，在这种情况下，可以由登录的设备请求服务端，再授权NFC写入端执行写入动作。

在本说明书实施例中，根据上面的分析，对于步骤S202，所述密钥对标识及其对应的密钥对可以由所述服务端预先生成，并下发所述密钥对标识和所述密钥对中的所述公钥，再由NFC写入端将所述下发的信息写入所述NFC便携设备中。

进一步地，所述NFC写入信息还可以包括关联于所述密钥对标识的用户账户的账户识别信息。在这种情况下，对于步骤S208，所述将所述加密信息和所述密钥对标识发送给所述消费机具，还可以包括：将所述账户识别信息发送给所述消费机具，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

若密钥对标识是全局唯一，则服务端可以利用密钥对标识直接查找到对应的私钥，这种查找方式可能会耗费较多的资源。针对这个问题，服务端可以先利用账户识别信息查找到关联的各密钥对标识，则有效地缩小了查找范围，再在各密钥对标识查找当前的密钥对标识，进而查找到对应的私钥，如此，效率较高，耗费的资源较少。

在本说明书实施例中，为了提高安全性，还可以在支付过程中加入时效性校验动作。比如，对于步骤S206，所述利用所述公钥，对所述消费金

额信息加密得到加密信息，具体可以包括：获取当前时间；利用所述公钥，对所述消费金额信息和所述当前时间加密得到加密信息；其中，所述当前时间用于所述服务端在所述扣款前进行时效性校验。

服务端将成功解密后得到的当前时间与服务端时间进行比较；若时间差距在设定的阈值以内，则认为该当前时间尚具有时效性，可以扣款；否则，可以拒绝本次支付。

基于同样的思路，本说明书实施例还提供了一种针对 NFC 便携设备的写入方法的流程示意图，执行主体为 NFC 写入端。如图 3 所示。

图 3 中的流程可以包括以下步骤：

S302：NFC 写入端获取用户账户关联的密钥对标识和对应的密钥对中的公钥。

S304：将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

在本说明书实施例中，若 NFC 写入端即为用户登录用户账户的设备，则对于步骤 S302，所述获取用户账户关联的密钥对标识和对应的密钥对中的公钥，具体可以包括：请求服务端生成关联于用户账户的密钥对标识和对应的密钥对；接收所述服务端返回的所述密钥对标识和所述密钥对中的公钥；其中，当所述 NFC 便携设备通过所述用户账户支付时，由所述服务端扣款。

在本说明书实施例中，对于步骤 S302，所述获取用户账户关联的密钥对标识和对应的密钥对中的公钥，还可以包括：获取所述用户账户的账户识别信息。相应地，对于步骤 S304，所述将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，还可以包括：将所述账户识别信息写入所述 NFC 便携设备中，以用于所述服务端查找所述密钥对中的私钥用于所述扣款。

在本说明书实施例中，当用户丢失了 NFC 便携设备，可以通过登录了用户账户的设备或者上述 NFC 写入端，请求服务端解除用户账户与密钥对标识之间的关联关系，若关联关系解除，则对应的 NFC 便携设备不能够基

于该密钥对标识成功支付，从而能够防止 NFC 便携设备被人冒用。

基于同样的思路，本说明书实施例还提供了另一种基于 NFC 便携设备的支付方法的流程示意图，执行主体为消费机具。如图 4 所示。

图 4 中的流程可以包括以下步骤：

S402：消费机具当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息。

S404：接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中。

S406：将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

在本说明书实施例中，对于步骤 S404，所述接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，还可以包括：接收所述 NFC 便携设备发送的所述用户账户的账户识别信息，所述账户识别信息被预先写入所述 NFC 便携设备中。相应地，对于步骤 S406，所述将所述加密信息和所述密钥对标识发送给服务端，还可以包括：将所述账户识别信息发送给所述服务端，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

在本说明书实施例中，对于步骤 S406，所述将所述加密信息和所述密钥对标识发送给服务端，还可以包括：将相应的业务场景信息发送给所述服务端，以用于生成相应的业务单据。

基于同样的思路，本说明书实施例还提供了再一种基于 NFC 便携设备的支付方法的流程示意图，执行主体为服务端。如图 5 所示。

图 5 中的流程可以包括以下步骤：

S502：服务端接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的

公钥加密生成，并通过 NFC 通信方式发送给所述消费机具。

S504：根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息。

S506：根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

在本说明书实施例中，对于步骤 S502，所述接收消费机具发送的密钥对标识和包含消费金额信息的加密信息前，还可以执行：预先生成所述密钥对标识及其对应的密钥对，并与所述用户账户进行关联；下发所述密钥对标识和所述密钥对中的所述公钥，以用于 NFC 写入端将所述下发的信息写入所述 NFC 便携设备中。

在本说明书实施例中，对于步骤 S502，所述接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，还可以包括：接收所述消费机具发送的所述用户账户的账户识别信息，所述账户识别信息由 NFC 便携设备通过 NFC 通信方式发送给所述消费机具。相应地，对于步骤 S504，所述根据所述密钥对标识，确定所述密钥对标识对应的私钥，具体可以包括：根据所述账户识别信息，确定所述用户账户对应的各密钥对标识；根据所述各密钥对标识和所述消费机具发送的密钥对标识，确定所述消费机具发送的密钥对标识对应的私钥。

在本说明书实施例中，所述加密信息中还包括所述 NFC 便携设备获取的当前时间。在这种情况下，对于步骤 S506，所述加密信息中还包括所述 NFC 便携设备获取的当前时间；所述根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款前，还可以执行：根据服务端时间确定所述当前时间是否尚具有时效性，若是，则可以扣款，否则，可以拒绝本次支付。

基于同样的思路，本说明书实施例还提供了上述各方法对应的装置，如图 6~图 9 所示，其中，虚线方框表示可选的模块。

图 6 为本说明书实施例提供的对应于图 2 的一种基于 NFC 便携设备的

支付装置的结构示意图，所述装置位于所述 NFC 便携设备，包括:

获取模块 601，获取 NFC 写入信息，所述 NFC 写入信息包括密钥对标识和对应的公钥;

接收模块 602，当进入消费机具的 NFC 通信范围时，接收所述消费机具发送的消费金额信息;

加密模块 603，利用所述公钥，对所述消费金额信息加密得到加密信息;

发送模块 604，将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

可选地，所述密钥对标识及其对应的密钥对由所述服务端预先生成，并下发所述密钥对标识和所述密钥对中的所述公钥，再由 NFC 写入端将所述下发的信息写入所述 NFC 便携设备中。

可选地，所述 NFC 写入信息还包括关联于所述密钥对标识的用户账户的账户识别信息;

所述发送模块 604 将所述加密信息和所述密钥对标识发送给所述消费机具，还包括:

所述发送模块 604 将所述账户识别信息发送给所述消费机具，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

可选地，所述加密模块 603 利用所述公钥，对所述消费金额信息加密得到加密信息，具体包括:

所述加密模块 603 获取当前时间;

利用所述公钥，对所述消费金额信息和所述当前时间加密得到加密信息;

其中，所述当前时间用于所述服务端在所述扣款前进行时效性校验。

可选地，所述 NFC 便携设备为支持 NFC 功能的可穿戴设备或者卡片。

图 7 为本说明书实施例提供的对应于图 3 的一种针对 NFC 便携设备的写入装置的结构示意图，所述装置位于 NFC 写入端，包括:

获取模块 701，获取用户账户关联的密钥对标识和对应的密钥对中的公钥；

写入模块 702，将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

可选地，所述获取模块 701 获取用户账户关联的密钥对标识和对应的密钥对中的公钥，具体包括：

所述获取模块 701 请求服务端生成关联于用户账户的密钥对标识和对应的密钥对；

接收所述服务端返回的所述密钥对标识和所述密钥对中的公钥；

其中，当所述 NFC 便携设备通过所述用户账户支付时，由所述服务端扣款。

可选地，所述获取模块 701 获取用户账户关联的密钥对标识和对应的密钥对中的公钥，还包括：

所述获取模块 701 获取所述用户账户的账户识别信息；

所述写入模块 702 将所述密钥对标识和所述公钥写入所述 NFC 便携设备中，还包括：

所述写入模块 702 将所述账户识别信息写入所述 NFC 便携设备中，以用于所述服务端查找所述密钥对中的私钥用于所述扣款。

可选地，所述装置还包括：

解除模块 703，请求所述服务端解除所述用户账户与所述密钥对标识之间的关联关系，若所述关联关系解除，则所述 NFC 便携设备不能够基于所述密钥对标识成功支付。

图 8 为本说明书实施例提供的对应于图 4 的一种基于 NFC 便携设备的支付装置的结构示意图，所述装置位于消费机具，包括：

第一发送模块 801，当所述 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息；

接收模块 802，接收所述 NFC 便携设备发送的密钥对标识和利用对应

的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中；

第二发送模块 803，将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

可选地，所述接收模块 802 接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，还包括：

所述接收模块 802 接收所述 NFC 便携设备发送的所述用户账户的账户识别信息，所述账户识别信息被预先写入所述 NFC 便携设备中；

所述第二发送模块 803 将所述加密信息和所述密钥对标识发送给服务端，还包括：

所述第二发送模块 803 将所述账户识别信息发送给所述服务端，以用于所述服务端查找所述解密需要使用的所述密钥对中的私钥。

可选地，所述第二发送模块 803 将所述加密信息和所述密钥对标识发送给服务端，还包括：

所述第二发送模块 803 将相应的业务场景信息发送给所述服务端，以用于生成相应的业务单据。

图 9 为本说明书实施例提供的对应于图 5 的一种基于 NFC 便携设备的支付装置的结构示意图，所述装置位于服务端，包括：

接收模块 901，接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具；

确定模块 902，根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息；

扣款模块 903，根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

可选地，所述装置还包括：

关联下发模块 904，在所述接收模块 901 接收消费机具发送的密钥对标识和包含消费金额信息的加密信息前，预先生成所述密钥对标识及其对应的密钥对，并与所述用户账户进行关联；

下发所述密钥对标识和所述密钥对中的所述公钥，以用于 NFC 写入端将所述下发的信息写入所述 NFC 便携设备中。

可选地，所述接收模块 901 接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，还包括：

所述接收模块 901 接收所述消费机具发送的所述用户账户的账户识别信息，所述账户识别信息由所述 NFC 便携设备通过 NFC 通信方式发送给所述消费机具；

所述确定模块 902 根据所述密钥对标识，确定所述密钥对标识对应的私钥，具体包括：

所述确定模块 902 根据所述账户识别信息，确定所述用户账户对应的各密钥对标识；

根据所述各密钥对标识和所述消费机具发送的密钥对标识，确定所述消费机具发送的密钥对标识对应的私钥。

可选地，所述加密信息中还包括所述 NFC 便携设备获取的当前时间；

所述扣款模块 903 根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款前，还执行：

所述扣款模块 903 根据服务端时间确定所述当前时间尚具有时效性。

基于同样的思路，本说明书实施例还提供了对应于图 2 的一种基于 NFC 便携设备的支付设备，所述设备为所述 NFC 便携设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

获取 NFC 写入信息，所述 NFC 写入信息包括密钥对标识和对应的公钥；

当进入消费机具的NFC通信范围时，接收所述消费机具发送的消费金额信息；

利用所述公钥，对所述消费金额信息加密得到加密信息；

将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

基于同样的思路，本说明书实施例还提供对应于图3的一种针对NFC便携设备的写入设备，所述设备为NFC写入端，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

获取用户账户关联的密钥对标识和对应的密钥对中的公钥；

将所述密钥对标识和所述公钥写入所述NFC便携设备中，以用于所述NFC便携设备通过所述用户账户支付。

基于同样的思路，本说明书实施例还提供了对应于图4的一种基于NFC便携设备的支付设备，所述设备为消费机具，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

当所述NFC便携设备进入其NFC通信范围时，向所述NFC便携设备发送消费金额信息；

接收所述NFC便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述NFC便携设备中；

将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

基于同样的思路，本说明书实施例还提供了对应于图5的一种基于NFC便携设备的支付设备，所述设备为消费机具，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由所述NFC便携设备利用所述密钥对标识对应的公钥加密生成，并通过NFC通信方式发送给所述消费机具；

根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息；

根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

基于同样的思路，本说明书实施例还提供了对应于图2的一种非易失性计算机存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为：

获取NFC写入信息，所述NFC写入信息包括密钥对标识和对应的公钥；

当进入消费机具的NFC通信范围时，接收所述消费机具发送的消费金额信息；

利用所述公钥，对所述消费金额信息加密得到加密信息；

将所述加密信息和所述密钥对标识发送给所述消费机具，以用于服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

基于同样的思路，本说明书实施例还提供了对应于图3的一种非易失

性计算机存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为：

获取用户账户关联的密钥对标识和对应的密钥对中的公钥；

将所述密钥对标识和所述公钥写入 NFC 便携设备中，以用于所述 NFC 便携设备通过所述用户账户支付。

基于同样的思路，本说明书实施例还提供了对应于图 4 的一种非易失性计算机存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为：

当 NFC 便携设备进入其 NFC 通信范围时，向所述 NFC 便携设备发送消费金额信息；

接收所述 NFC 便携设备发送的密钥对标识和利用对应的公钥对所述消费金额信息加密得到的加密信息，所述密钥对标识和所述公钥被预先写入所述 NFC 便携设备中；

将所述加密信息和所述密钥对标识发送给服务端，以用于所述服务端解密后根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

基于同样的思路，本说明书实施例还提供了对应于图 5 的一种非易失性计算机存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为：

接收消费机具发送的密钥对标识和包含消费金额信息的加密信息，所述加密信息由 NFC 便携设备利用所述密钥对标识对应的公钥加密生成，并通过 NFC 通信方式发送给所述消费机具；

根据所述密钥对标识，确定所述密钥对标识对应的私钥，并用所述私钥对所述加密信息解密得到所述消费金额信息；

根据所述消费金额信息，从所述密钥对标识预先关联的用户账户中扣款。

上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求

书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置、设备、非易失性计算机存储介质实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本说明书实施例提供的装置、设备、非易失性计算机存储介质与方法是对应的，因此，装置、设备、非易失性计算机存储介质也具有与对应方法类似的有益技术效果，由于上面已经对方法的有益技术效果进行了详细说明，因此，这里不再赘述对应装置、设备、非易失性计算机存储介质的有益技术效果。

在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译

器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电

话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

本领域内的技术人员应明白，本说明书实施例可提供为方法、系统、或计算机程序产品。因此，本说明书实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本说明书是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流

程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

还需要说明的是，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、商品或者设备不仅包括那些要素，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、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本领域技术人员应明白，本说明书实施例可提供为方法、系统或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于

磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

以上所述仅为本说明书实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。