

支付业务实现的方法和装置

技术领域

[01] 本说明书一个或多个实施例涉及信息安全技术领域，尤其涉及用于实现支付业务的方法和装置。

背景技术

[02] 现有支付业务的实现方法可以由付款方和收款方中的任意一方，将支付账户信息提供给另一方，由另一方生成支付账单，并将支付账单提供给服务器端，由服务器进行账单扣款处理。

[03] 在现有支付业务的实现方法中，提供支付账单信息的一方将原始的支付账户信息直接提供给另一方，这样则会造成支付账户信息的泄露，从而降低了支付业务的安全性。因此，需要提供更为安全的方案，以降低支付账户信息泄露的风险。

发明内容

[04] 本说明书一个或多个实施例描述了支付业务的实现方法和装置，能够降低支付账户信息泄露的风险。

[05] 根据第一方面，提供了一种支付业务的实现方法，应用于进行支付业务的终端中，所述方法包括：生成随机数；利用所述随机数对所述终端的原始支付账户信息进行变形处理，得到变形后的支付账户信息；根据预先获取的公钥及第一加密算法，对所述变形后的支付账户信息进行加密，得到第一支付账户信息；根据所述第一支付账户信息，得到匿名支付账户信息；利用所述匿名支付账户信息，进行支付操作。

[06] 在一个实施例中，所述生成随机数包括：根据第二加密算法的密钥长度，生成长度等于该密钥长度的所述随机数；所述利用所述随机数对所述终端的原始支付账户信息进行变形处理，包括：利用所述随机数作为所述第二加密算法的密钥，并利用所述第二加密算法对所述终端的原始支付账户信息进行加密。

[07] 在一个实施例中，在所述利用所述第二加密算法对所述终端的原始支付账户信息进行加密之后，并在所述得到变形后的支付账户信息之前，进一步包括：将所述随机数与第二支付账户信息进行第一组合处理，得到所述变形后的支付账户信息；其中，所述第二支付账户信息为利用所述第二加密算法对所述终端的原始支付账户信息进行加密后得到的支付账户信息。

[08] 在一个实施例中，所述变形后的支付账户信息中未携带所述随机数；所述根据第一支付账户信息，得到匿名支付账户信息，包括：将所述随机数与所述第一支付账户信息进行第二组合处理，得到所述匿名支付账户信息。

[09] 在一个实施例中，所述变形后的支付账户信息中携带所述随机数；所述根据第一支付账户信息，得到匿名支付账户信息，包括：将所述第一支付账户信息直接确定为所述匿名支付账户信息。

[10]在一个实施例中，所述进行支付业务的终端为：提供支付账户信息的终端；所述利用所述匿名支付账户信息进行支付操作，包括：将所述匿名支付账户信息提供给另一个终端。

[11]在一个实施例中，所述进行支付业务的终端为：向服务器提供支付账单的终端；所述利用所述匿名支付账户信息进行支付操作，包括：利用所述匿名支付账户信息，生成匿名支付账单；将所述匿名支付账单发送给服务器。

[12]第二方面，提供了一种支付业务的实现方法，应用于服务器，包括：接收匿名支付账单；从所述匿名支付账单中得到匿名支付账户信息；利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，得到变形后的支付账户信息；其中，所述私钥对应于进行支付业务的终端所获取的公钥；得到随机数；利用所述随机数对所述变形后的支付账户信息进行逆变处理，得到原始支付账户信息；根据所述原始支付账户信息，进行账单扣款处理。

[13]在一个实施例中，所述变形后的支付账户信息中未携带所述随机数；所述得到随机数，包括：对所述匿名支付账户信息进行第二解组合处理，从该第二解组合处理后得到的支付账户信息中提取出所述随机数；所述利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，包括：从所述第二解组合处理后得到的支付账户信息中提取出第一支付账户信息；以及利用所述私钥以及所述第一解密算法，对所述第一支付账户信息进行解密。

[14]在一个实施例中，所述变形后的支付账户信息中携带所述随机数；所述利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，包括：利用所述私钥以及所述第一解密算法，对所述匿名支付账户信息进行解密；所述得到随机数，包括：对该解密后得到的支付账户信息进行第一解组合处理，从该第一解组合处理后得到的支付账户信息中提取出所述随机数。

[15]第三方面，还提供了一种支付业务的实现装置，设置于进行支付业务的终端中，所述装置包括：随机数生成单元，配置为生成随机数；变形处理单元，配置为利用所述随机数对所述终端的原始支付账户信息进行变形处理，得到变形后的支付账户信息；加密处理单元，配置为根据预先获取的公钥及第一加密算法，对所述变形后的支付账户信息进行加密，得到第一支付账户信息；匿名账户确定单元，配置为根据所述第一支付账户信息，得到匿名支付账户信息；支付处理单元，配置为利用所述匿名支付账户信息，进行支付操作。

[16]在一个实施例中，所述随机数生成单元，配置为：根据第二加密算法的密钥长度，生成长度等于该密钥长度的所述随机数；所述变形处理单元，配置为：利用所述随机数作为所述第二加密算法的密钥，并利用该第二加密算法对所述终端的原始支付账户信息进行加密。

[17]在一个实施例中，所述变形处理单元，进一步配置为：将所述随机数与第二支付账户信息进行第一组合处理，得到变形后的支付账户信息；其中，所述第二支付账户信息为利用所述第二加密算法对所述终端的原始支付账户信息进行加密后得到的支付账户信息。

[18]在一个实施例中，所述变形后的支付账户信息中未携带所述随机数；所述匿名账户确定单元，配置为：将所述随机数与所述第一支付账户信息进行第二组合处理，得到所述匿名支付账户信息。

[19]在一个实施例中，所述变形后的支付账户信息中携带所述随机数；所述匿名账户确定单元，配置为：将所述第一支付账户信息直接确定为所述匿名支付账户信息。

[20]在一个实施例中，所述进行支付业务的终端为：提供支付账户信息的终端；所述支付处理单元，配置为：将所述匿名支付账户信息提供给另一个终端。

[21]在一个实施例中，所述进行支付业务的终端为：向服务器提供支付账单的终端；所述支付处理单元，配置为：利用所述匿名支付账户信息，生成匿名支付账单；将所述匿名支付账单发送给服务器。

[22]第四方面，还提供了一种服务器，包括：接收单元，配置为接收匿名支付账单；账户获取单元，配置为从所述匿名支付账单中得到匿名支付账户信息；解密处理单元，配置为利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，得到变形后的支付账户信息；其中，所述私钥对应于进行支付业务的终端所获取的公钥；随机数获取单元，配置为得到随机数；逆变处理单元，配置为利用所述随机数对所述变形后的支付账户信息进行逆变处理，得到原始支付账户信息；扣款处理单元，配置为根据所述原始支付账户信息，进行账单扣款处理。

[23]在一个实施例中，所述变形后的支付账户信息中未携带所述随机数；所述随机数获取单元，配置为：对所述匿名支付账户信息进行第二解组合处理，从该第二解组合处理后得到的支付账户信息中提取出所述随机数；所述解密处理单元，配置为：从所述第二解组合处理后得到的支付账户信息中提取出第一支付账户信息；以及利用所述私钥以及所述第一解密算法，对所述第一支付账户信息进行解密。

[24]在一个实施例中，所述变形后的支付账户信息中携带所述随机数；所述解密处理单元，配置为：利用所述私钥以及所述第一解密算法，对所述匿名支付账户信息进行解密；所述随机数获取单元，配置为：对该解密后得到的支付账户信息进行第一解组合处理，从该第一解组合处理后得到的支付账户信息中提取出所述随机数。

[25]第五方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述本说明书任一实施例提供的方法。

[26]在本说明书实施例提供的支付业务的实现方法和装置中，用于得到匿名支付账户信息的第一支付账户信息是利用公钥加密得到的，在利用匿名支付账户信息进行支付操作时，即使其他终端获取到该匿名支付账户信息，由于没有与该公钥对应的私钥，因此无法从匿名支付账户信息中解密出原始支付账户信息，因此降低了支付账户信息被泄露的风险；同时，由于每次加密使用的公钥相同，且被加密的原始支付账户信息也相同，那么，为了防止每次使用公钥加密后得到的匿名支付账户信息相同，可以利用随机数来实现干扰处理，在每次干扰处理时，通过使用随机数对同一个原始支付信息进行变形处理，每次得到的该变形后的支付账户信息不同，使得公钥每次加密的信息不同，进而使得每次得到的匿名支付账户信息不同。也就是说，既能通过加密的方式来提供终端的原始支

付账户信息，又能使得每次提供的加密后的原始支付账户信息的内容不同，如此能够进一步防止其他终端利用相同的匿名支付账户信息进行身份锁定，因此，本说明书实施例提供的方法能够降低支付账户信息泄露的风险。

附图说明

[27]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，下面描述中的附图是本说明书的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[28]图1是本说明书一个实施例提供的支付业务的实现方法的流程图；

[29]图2是本说明书另一个实施例提供的支付业务的实现方法的流程图；

[30]图3是本说明书一个实施例中终端A与终端B分别向服务器进行匿名功能申请的流程图；

[31]图4是本说明书一个实施例中终端A、终端B与服务器在实现支付业务时的流程图；

[32]图5是本说明书一个实施例中支付业务的实现装置的结构示意图；

[33]图6是本说明书一个实施例中服务器的结构示意图。

具体实施方式

[34]下面结合附图，对本说明书提供的方案进行描述。

[35]在现有支付业务的实现方法中，提供支付账单信息的一方是将原始的支付账户信息直接提供给另一方，而该另一方也是利用原始的支付账户信息生成支付账单，因此会造成支付账户信息的泄露。如果要降低支付账户信息泄露的风险，则支付账户信息提供方不能直接将原始的支付账户信息提供给另一方，该另一方也不能直接利用原始的支付账户信息生成支付账单。因此，需要对该原始的支付账户信息进行匿名处理。

[36]在本说明书的一个实施例中，对原始的支付账户信息进行匿名处理的方式可以是采用公钥加密私钥解密的方式来实现，由终端利用公钥对原始支付账户信息加密得到匿名支付账户信息，而其他获取到匿名支付账户信息的终端由于没有私钥，因此无法从匿名支付账户信息中得到原始的支付账户信息。

[37]另外，考虑到针对同一个原始的支付账户信息，每次加密使用的公钥及被加密的原始支付账户信息相同，即得到的加密后的支付账户信息的内容相同，直接利用该加密后的支付账户信息作为匿名支付账户信息，则可能导致其他终端可以通过相同的匿名支付账户信息进行身份锁定。因此，可以进行干扰处理，使得针对同一个原始的支付账户信息，每次得到的匿名支付账户信息的内容不同。具体地，可以考虑利用随机数来实现该干扰处理。

[38]下面描述以上构思的具体实施方式。

[39]图1示出根据一个实施例的支付业务的实现方法的流程图。可以理解，该方法可以通过任何具有计算、处理能力的装置、设备、平台、设备集群来执行。参见图1，该方法应用于进行支付业务的终端，具体的实现包括：

[40]步骤100：生成随机数。

[41]步骤102：利用所述随机数对所述终端的原始支付账户信息进行变形处理，得到变形后的支付账户信息。

[42]步骤104：根据从服务器端获取的公钥及第一加密算法，对所述变形后的支付账户信息进行加密，得到第一支付账户信息。

[43]步骤106：根据所述第一支付账户信息，得到匿名支付账户信息。

[44]步骤108：利用所述匿名支付账户信息，进行支付操作。

[45]在图1所示的支付业务的实现方法中，用于得到匿名支付账户信息的第一支付账户信息是利用公钥加密得到的，在利用匿名支付账户信息进行支付操作时，即使其他终端获取到该匿名支付账户信息，由于没有与该公钥对应的私钥，因此无法从匿名支付账户信息中解密出原始支付账户信息，因此降低了支付账户信息被泄露的风险；同时，由于每次加密使用的公钥相同，且被加密的原始支付账户信息也相同，那么，为了防止每次使用公钥加密后得到的匿名支付账户信息相同，可以利用随机数来实现干扰处理，在每次干扰处理时，通过使用随机数对同一个原始支付信息进行变形处理，每次得到的该变形后的支付账户信息不同，使得公钥每次加密的信息不同，进而使得每次得到的匿名支付账户信息不同。也就是说，既能通过加密的方式来提供终端的原始支付账户信息，又能使得每次提供的加密后的原始支付账户信息的内容不同，如此能够进一步防止其他终端利用相同的匿名支付账户信息进行身份锁定，因此，本说明书实施例提供的方法能够降低支付账户信息泄露的风险。

[46]下面描述图1所示的各个步骤的执行方式。

[47]在步骤100，生成随机数。

[48]随机数是一个随机数序列，生成随机数的方法可以是用户随机输入的数，然后利用一个随机函数根据用户输入的数产生该随机数序列，将产生的该随机数序列作为实际使用的随机数。该生成随机数的方法也可以是利用一个随机数生成器产生随机数列作为基础，然后使用另一个生成器对随机数列进行重新排列，将排列后得到的新数列作为实际使用的随机数。

[49]在步骤102，根据生成的随机数对终端的原始支付账户信息进行变形处理，得到变形后的支付账户信息。

[50]终端的原始支付账户信息用于表征终端的真实身份，该原始支付账户信息可以包括但不限于：用户名、账号、银行卡号、身份证号和昵称中的至少一种。

[51]在本步骤102中对原始支付账户信息进行变形处理时，可以采用多种变形处理方式，比如：方式一、利用随机数进行加密处理的方式；方式二、利用随机数进行内容重排的方式。

[52]在利用上述方式一对原始支付账户信息进行变形处理时，终端中存储有与服务器端协商的第二加密算法，可以采用该第二加密算法对原始支付账户信息加密，那么在步骤100生成随机数时，需要根据第二加密算法的秘钥长度，生成长度等于该秘钥长度的所述随机数。

[53]具体地，步骤102中利用所述随机数对所述终端的原始支付账户信息进行变形处理，包括：利用所述随机数作为所述第二加密算法的密钥，并利用该第二加密算法对所述终端的原始支付账户信息进行加密。

[54]本说明书的实施例中，该第二加密算法可以为高级加密标准（Advanced Encryption Standard, AES）加密算法，或者SM4加密算法。

[55]在利用上述方式二对原始支付账户信息进行变形处理时，可以将随机数穿插在原始支付账户信息对应的字节中，或者将随机数与原始支付账户信息的字节进行拼接等方式实现对原始支付账户信息的变形处理。

[56]由于对原始支付账户信息进行变形处理的随机数，是在终端侧随机生成的，为了保证服务器能够对变形后的支付账户信息进行逆变处理得到终端的原始支付账户信息，需要让服务器能够获取到该随机数，也就是说，在提供给外部的匿名支付账户信息中需要携带该随机数。

[57]在本说明书一个实施例中，在步骤102中对原始支付账户信息进行变形处理时，无论采用上述方式一或方式二完成了初步变形处理后，都可以进一步执行如下步骤（记为步骤S）的处理，包括：将随机数与该初步变形处理后的支付账户信息进行第一组合处理，使得在变形后的支付账户信息中携带该随机数。比如，当采用上述方式一时，在利用第二加密算法对所述终端的原始支付账户信息进行加密之后，并在得到变形后的支付账户信息之前，进一步包括：将所述随机数与第二支付账户信息进行第一组合处理，得到所述变形后的支付账户信息；其中，所述第二支付账户信息为利用所述第二加密算法对所述终端的原始支付账户信息进行加密后得到的支付账户信息。

[58]在步骤104，终端预先获取公钥及第一加密算法，根据获取的该公钥和第一加密算法，对步骤102中得到的变形后的支付账户信息进行加密，得到第一支付账户信息。

[59]由于进行支付操作时生成的匿名支付账单需要发送给服务器，由服务器对匿名支付账单中的匿名支付账户信息进行解密，因此，该公钥和第一加密算法可以从服务器端预先获取。

[60]具体地，终端在支付业务进行前，可以先向服务器进行匿名功能申请或注册请求，接收服务器针对该申请或注册请求所发送的公钥和第一加密算法，该第一加密算法是非对称加密算法。需要说明的是，由于进行支付业务的不同终端在进行支付操作时，均需要将匿名支付账单发送给服务器进行处理，因此，进行支付业务的不同终端从服务器端获取的公钥及第一加密算法都相同。

[61]另外，终端从服务器端获取公钥的方式，也可以是获取到包含有该公钥的证书，基于证书机制，在使用该公钥加密前，可以向第三方机构对该证书进行认证，以确保接收到的证书为服务器发送的有效证书。

[62]在步骤 106, 根据步骤 104 中得到的第一支付账户信息, 得到匿名支付账户信息。

[63]如步骤 102 所述, 需要让服务器能够获取到该随机数, 即需要在匿名支付账户信息中携带该随机数。在本说明书的一个实施例中, 在步骤 102 中包括两种方式, 方式 A 是变形后的支付账户信息中未携带随机数, 方式 B 是变形后的支付账户信息中携带了随机数。针对这两种方式, 步骤 106 的处理方式不同。下面描述具体实现。

[64]方式 A、在变形后的支付账户信息中不携带该随机数, 而是在进行加密处理之后, 将加密后的支付账户信息与该随机数进行组合。

[65]在该方式 A 中, 处理的顺序是: 对原始支付账户信息进行变形处理; 之后, 对未携带随机数的变形后的支付账户信息进行加密; 之后, 将加密后的支付账户信息与随机数进行组合, 得到匿名支付账户信息。

[66]相应地, 对应于该方式 A, 步骤 106 中根据第一支付账户信息, 得到匿名支付账户信息, 包括: 将随机数与上述第一支付账户信息进行第二组合处理, 得到所述匿名支付账户信息。

[67]其中, 将随机数与第一支付账户信息进行第二组合处理的方式, 可以包括但不限于: 随机数与第一支付账户信息进行先后顺序的拼接、随机数穿插在第一支付账户信息中、随机数与第一支付账户信息进行异或运算。

[68]进一步地, 还可以利用一个完整性计算规则对进行第二组合处理后的支付账户信息进行计算, 例如, 哈希计算, 计算完成后得到匿名支付账户信息。

[69]方式 B、在未进行加密处理之前, 在变形后的支付账户信息中携带该随机数;

[70]在该方式 B 中, 处理的顺序是: 对原始支付账户信息进行变形处理; 之后, 在该变形处理后的支付账户信息中携带随机数(比如通过上述步骤 S 的处理完成在该变形处理后的支付账户信息中携带随机数); 之后, 对携带该随机数的变形后的支付账户信息进行加密, 得到匿名支付账户信息。

[71]相应地, 对应于该方式 B, 步骤 106 中根据第一支付账户信息, 得到匿名支付账户信息, 包括: 将所述第一支付账户信息直接确定为所述匿名支付账户信息。

[72]在步骤 108, 利用所述匿名支付账户信息, 进行支付操作。

[73]在实际应用中, 进行支付业务的两个终端中一个终端用于提供支付账户信息, 另一个终端用于向服务器提供支付账单, 两个终端在利用匿名支付账户信息进行支付操作的处理过程不同。上述图 1 所示的方法既适用于提供支付账户信息的终端(也就是说, 进行支付业务的终端为提供支付账户信息的终端), 也适用于接收该支付账户信息并生成支付账单的终端(也就是说, 进行支付业务的终端为向服务器提供支付账单的终端)。

[74]在本说明书的一个实施例中, 在进行支付业务的终端为: 提供支付账户信息的终端时, 步骤 108 中利用匿名支付账户信息进行支付操作, 包括: 将匿名支付账户信息提供给另一个终端。

[75]其中, 将匿名支付账户信息提供给另一个终端的方式, 可以包括近场通信(Near Field Communication, NFC)、WIFI、3G/4G/5G、POS 机刷卡技术、二维码扫码技术、条形

码扫码技术、蓝牙、红外、短消息 (Short Message Service, SMS)、多媒体消息 (Multimedia Message Service, MMS) 等。

[76] 需要说明的是, 该提供支付账户信息的终端可以是收款方, 也可以是付款方。以二维码扫码技术为例, 在该提供支付账户信息的终端是收款方时, 提供支付账户信息的终端可以根据得到的该匿名支付账户信息生成一个收款码, 向服务器提供支付账单的终端对该收款码进行扫码得到该匿名支付账户信息; 在该提供支付账户信息的终端是付款方时, 提供支付账户信息的终端可以根据得到的该匿名支付账户信息生成一个付款码, 向服务器提供支付账单的终端对该付款码进行扫码得到该匿名支付账户信息。

[77] 在本说明书的一个实施例中, 在进行支付业务的终端为: 向服务器提供支付账单的终端时, 步骤 108 中利用匿名支付账户信息进行支付操作, 包括: 利用所述匿名支付账户信息, 生成匿名支付账单; 将所述匿名支付账单发送给服务器。

[78] 由于向服务器提供支付账单的终端, 在生成匿名支付账单后, 是将匿名支付账单发送给服务器, 因此, 该向服务器提供支付账单的终端可以利用上述步骤 100 至步骤 106 对自身的原始支付账户信息进行匿名, 生成的匿名支付账单中包括两个匿名支付账户信息 (一个对应提供支付账户信息的终端, 另一个对应向服务器提供支付账单的终端), 也可以不对自身的原始支付账户信息进行匿名, 生成的匿名支付账单中包括一个原始支付账户信息 (对应向服务器提供支付账单的终端) 和一个匿名支付账户信息 (对应提供支付账户信息的终端)。

[79] 为了保证服务器能够根据该匿名支付账单实现账单扣款处理, 该匿名支付账单中还需要至少包括付款方、收款方和支付金额, 以使服务器在从匿名支付账户信息中得到原始支付账户信息后, 从付款方向收款方进行拨款。

[80] 图 2 示出根据一个实施例的支付业务的实现方法的流程图。可以理解, 该方法可以通过任何具有计算、处理能力的装置、设备、平台、设备集群来执行。参见图 2, 该方法应用于服务器端, 具体的实现包括:

[81] 步骤 200, 接收匿名支付账单。

[82] 步骤 202, 从所述匿名支付账单中得到匿名支付账户信息。

[83] 步骤 204, 利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理, 得到变形后的支付账户信息; 其中, 所述私钥对应于进行支付业务的终端所获取的公钥。

[84] 步骤 206, 得到随机数。

[85] 步骤 208, 利用所述随机数对所述变形后的支付账户信息进行逆变处理, 得到原始支付账户信息。

[86] 步骤 210, 根据所述原始支付账户信息, 进行账单扣款处理。

[87] 在图 2 所示的支付业务的实现方法中, 由于服务器中预先设置有私钥和第一解密算法, 该私钥对应于进行支付业务的终端加密时使用的公钥, 因此可以利用私钥和第一解密算法对匿名支付账户信息进行解密, 由于进行支付业务的终端在加密时利用随机数对

原始支付账户信息进行了变形处理，且随机数携带在匿名支付账户信息中，因此，服务器可以从匿名支付账户信息中得到随机数，从而可以利用随机数对解密后得到的支付账户信息进行逆变处理，从而得到原始支付账户信息。如此，存储有私钥的服务器可以从匿名支付账户信息中得到原始支付账户信息，从而进行账单扣款处理，其他终端由于没有私钥，因此无法从匿名支付账户信息中得到原始支付账户信息，从而降低了支付账户信息泄露的风险。

[88]下面描述图 2 所示的各个步骤的执行方式。

[89]在步骤 200 之前，服务器接收进行支付业务的终端发送的匿名功能申请或注册请求，服务器生成第一加密算法的公私密钥对，该第一加密算法是非对称加密算法，服务器将密钥对中的公钥发送给向其发送匿名功能申请或注册请求的终端，与公钥对应的私钥及与第一加密算法对应的第一解密算法进行本地存储。

[90]在步骤 200 和步骤 202 中，该匿名支付账单是由向服务器提供支付账单的终端发送过来的，若向服务器提供支付账单的终端在生成匿名支付账单之前对自身的原始支付账户信息进行了匿名处理，那么该匿名支付账单中包括两个匿名支付账户信息（一个对应提供支付账户信息的终端，另一个对应向服务器提供支付账单的终端）；若向服务器提供支付账单的终端在生成匿名支付账单之前未对自身的原始支付账户信息进行匿名处理，那么该匿名支付账单包括一个原始支付账户信息（对应向服务器提供支付账单的终端）和一个匿名支付账户信息（对应提供支付账户信息的终端）。

[91]为了保证服务器能够根据匿名支付账单完成账单扣款处理，该匿名支付账单中至少还需要包括付款方、收款方和支付金额。

[92]在步骤 204 和步骤 206 中，为了实现对匿名支付账户信息进行解密处理，需要先确定随机数的携带方式，随机数的携带包括两种，方式 A 是变形后的支付账户信息中未携带随机数，方式 B 是变形后的支付账户信息中携带了随机数。

[93]进行支付业务的终端在匿名处理过程中，是利用方式 A 还是方式 B 对随机数进行携带，会影响步骤 204 和步骤 206 的处理方式，具体描述该处理方式。

[94]如果进行支付业务的终端是用方式 A 对随机数进行携带的：那么步骤 206 中，就需要从匿名支付账户信息中得到随机数，步骤 204 中，就需要先从匿名支付账户信息中提取出随机数，并对提取出随机数后得到的支付账户信息进行解密处理。对应于方式 A，步骤 206 中所述得到随机数，包括：对所述匿名支付账户信息进行第二解组合处理，从该第二解组合处理后得到的支付账户信息中提取出所述随机数。步骤 204 中，所述利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，包括：从所述第二解组合处理后得到的支付账户信息中提取出第一支付账户信息；以及利用所述私钥以及所述第一加密算法，对所述第一支付账户信息进行解密。

[95]其中，该第二解组合处理方式与终端进行第二组合处理时的方式相对应，两个处理方式是一个可逆过程。

[96]如果进行支付业务的终端是用方式 B 对随机数进行携带的：那么步骤 204 中，就可以利用私钥直接对匿名支付账户信息进行解密，步骤 206 中，就需要从解密后得到的支

付账户信息中获取随机数。对应于方式 B，步骤 204 中，所述利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，包括：利用所述私钥以及所述第一解密算法，对所述匿名支付账户信息进行解密。步骤 206 中，所述得到随机数，包括：对该解密后得到的支付账户信息进行第一解组合处理，从该第一解组合处理后得到的支付账户信息中提取出所述随机数。

[97] 其中，该解密后得到的支付账户信息为变形后的支付账户信息，在终端侧该变形后的支付账户信息是由随机数和第二支付账户信息通过第一组合处理后得到的，那么第一解组合处理方式与终端进行第一组合处理时的方式相对应，两个处理方式是一个可逆过程。

[98] 在步骤 208，在得到随机数之后，可以利用该随机数对所述变形后的支付账户信息进行逆变处理，得到原始支付账户信息。

[99] 在本说明书的一个实施例中，由于终端在对原始支付账户信息进行变形处理时，可以采用多种变形处理方式，比如方式一利用随机数进行加密处理的方式，方式二利用随机数进行内容重排的方式，终端在采用不同变形处理方式进行变形处理时，服务器需进行的逆变处理方式不同。

[100] 在终端采用方式一进行变形处理，且终端采用方式 A 对随机数进行携带：

[101] 服务器中存储有与终端在加密时使用的第二加密算法所对应的第二解密算法，服务器利用得到的随机数和该第二解密算法，对变形后的支付账户信息进行解密，得到原始支付账户信息。

[102] 在终端采用方式一进行变形处理，且终端采用方式 B 对随机数进行携带：相同的，服务器中存储有与终端在加密时使用的第二加密算法所对应的第二解密算法，服务器利用得到的随机数和该第二解密算法，对第一解组合处理后得到的支付账户信息中提取出随机数之后得到的支付账户信息进行解密，从而得到原始支付账户信息。

[103] 在终端采用方式二进行变形处理，且终端采用方式 A 对随机数进行携带：服务器对变形后的支付账户信息进行逆变处理，得到原始支付账户信息。

[104] 在终端采用方式二进行变形处理，且终端采用方式 B 对随机数进行携带：服务器对第一解组合处理后得到的支付账户信息中提取出随机数之后得到的支付账户信息进行逆变处理，从而得到原始支付账户信息。

[105] 在步骤 210，服务器可以根据匿名支付账单中的付款方、收款方、支付金额以及解密得到的原始支付账户信息，从付款方向收款方进行拨款处理，从而完成账单扣款处理。

[106] 需要说明的是，为了保证服务器生成的非对称加密算法的私钥，在长期使用中的安全性，可以实行一种公私密钥对的定期更新机制，例如，每隔一个时间段，服务器重新生成一次非对称加密算法的公私密钥对，当进行支付业务的终端与服务器之间进行交互时，将该重新生成的公私密钥对中的公钥发送给该终端，以使该终端在下次匿名时使用该重新生成的公钥进行加密。

[107] 在步骤 210 之后，服务器还可以将账单扣款处理结果发送给两个终端，但需要保

证发送给向服务器提供支付账单的终端的账单扣款处理结果中,对提供支付账户信息的终端的原始支付账户信息进行匿名,发送给提供支付账户信息的终端的账单扣款处理结果中,对向服务器提供支付账单的终端的原始支付账户信息进行匿名。

[108] 下面以终端 A 和终端 B 进行支付业务,终端 A 用于提供支付账户信息,终端 B 用于向服务器发送支付账单为例,对终端 A、终端 B 和服务器三端的交互过程进行说明。

[109] 请参考图 3,为本说明书实施例中终端 A 与终端 B 分别向服务器进行匿名功能申请的交互流程图,该方法包括:步骤 300,终端 A、终端 B 分别向服务器发送匿名功能申请。

[110] 步骤 302,服务器生成非对称加密算法的公私密钥对,存储公私密钥对中的私钥。

[111] 在后续过程中还可能需要服务器对终端的原始支付账户信息进行匿名处理,因此,服务器还可以将该公钥进行存储。

[112] 步骤 304,服务器将公私密钥对中的公钥分别发送给终端 A、终端 B。

[113] 步骤 306,终端 A、终端 B 存储接收到的公钥。

[114] 可以理解,步骤 300 和步骤 302 不存在先后顺序,可以是服务器先执行了步骤 302,然后有终端向服务器发送匿名功能申请,服务器将已经生成的公钥发送给该终端;也可以是服务器在首次接收到终端向其发送匿名功能申请后,又执行的步骤 302,在该情况下,后续终端在向服务器发送匿名功能申请时,服务器可以直接将生成的公钥发送给后续终端。

[115] 请参考图 4,为本说明书实施例中终端 A、终端 B 与服务器在实现支付业务时的交互流程图,该方法包括:

[116] 步骤 A1,终端 A 生成随机数 A,随机数 A 的长度与加密算法 M 的密钥长度相等。

[117] 步骤 A2,终端 A 将随机数 A 作为加密算法 M 的加密密钥,利用加密算法 M 对终端 A 的原始支付账户信息 UAID 进行加密,得到 TA1, $TA1=M(A,UAID)$ 。

[118] 步骤 A3,终端 A 使用非对称加密算法 SM2 和公钥 public_key,对 TA1 进行加密,得到 TA2, $TA2=SM2(public_key,TA1)$ 。

[119] 步骤 A4,终端 A 将随机数 A 和 TA2 进行组合处理,得到匿名支付账户信息 NAID, $NAID=\{A,TA2\}$ 数组。

[120] 步骤 A5,终端 A 将 NAID 提供给终端 B。

[121] 步骤 B1,终端 B 生成随机数 B,随机数 B 的长度与加密算法 M 的密钥长度相等。

[122] 步骤 B2,终端 B 将随机数 B 作为加密算法 M 的加密密钥,利用加密算法 M 对终端 B 的原始支付账户信息 UBID 进行加密,得到 TB1, $TB1=M(B,UBID)$ 。

[123] 步骤 B3,终端 B 使用非对称加密算法 SM2 和公钥 public_key,对 TB1 进行加密,得到 TB2, $TB2=SM2(public_key,TB1)$ 。

[124] 步骤 B4,终端 B 将随机数 B 和 TB2 进行组合处理,得到匿名支付账户信息 NBID,

NBID={B,TB2}数组。

[125] 步骤 B5, 终端 B 利用 NAID 和 NBID, 生成匿名支付账单。

[126] 步骤 B6, 终端 B 将匿名支付账单发送给服务器。

[127] 步骤 C1, 服务器从匿名支付账单中得到 NAID 和 NBID。

[128] 步骤 C2, 服务器对 NAID、NBID 分别进行解组合处理, 以从 NAID 中提取出随机数 A 和 TA2, 从 NBID 中提取出随机数 B 和 TB2。

[129] 步骤 C3, 服务器根据私钥和非对称加密算法 SM2 对 TA2、TB2 进行解密处理, 得到 TA1、TB1。

[130] 步骤 C4, 服务器利用随机数 A 和加密算法 M 对 TA1 解密, 得到 UAID, 利用随机数 B 和加密算法 M 对 TB1 解密, 得到 UBID。

[131] 步骤 C5, 服务器根据 UAID、UBID, 完成账单扣款处理。

[132] 以上为终端 A、终端 B 和服务器之间实现支付业务的过程。

[133] 另一方面的实施例, 还提供了一种支付业务的实现装置, 该装置设置于进行支付业务的终端中。如图 5 示出一个实施例的支付业务的实现装置。可以理解, 该装置可以通过任何具有计算、处理能力的装置、设备、平台和设备集群来实现。如图 5 所示, 该装置 50 包括: 随机数生成单元 51, 配置为生成随机数; 变形处理单元 52, 配置为利用所述随机数对所述终端的原始支付账户信息进行变形处理, 得到变形后的支付账户信息; 加密处理单元 53, 配置为根据预先获取的公钥及第一加密算法, 对所述变形后的支付账户信息进行加密, 得到第一支付账户信息; 匿名账户确定单元 54, 配置为根据所述第一支付账户信息, 得到匿名支付账户信息; 支付处理单元 55, 配置为利用所述匿名支付账户信息, 进行支付操作。

[134] 一种可能的实施方式中, 所述随机数生成单元 51, 配置为: 根据第二加密算法的密钥长度, 生成长度等于该密钥长度的所述随机数; 所述变形处理单元 52, 配置为: 利用所述随机数作为所述第二加密算法的密钥, 并利用该第二加密算法对所述终端的原始支付账户信息进行加密。

[135] 一种可能的实施方式中, 所述变形处理单元 52, 进一步配置为: 将所述随机数与第二支付账户信息进行第一组合处理, 得到变形后的支付账户信息; 其中, 所述第二支付账户信息为利用所述第二加密算法对所述终端的原始支付账户信息进行加密后得到的支付账户信息。

[136] 一种可能的实施方式中, 所述变形后的支付账户信息中未携带所述随机数; 所述匿名账户确定单元 54, 配置为: 将所述随机数与所述第一支付账户信息进行第二组合处理, 得到所述匿名支付账户信息。

[137] 一种可能的实施方式中, 所述变形后的支付账户信息中携带所述随机数; 所述匿名账户确定单元 54, 配置为: 将所述第一支付账户信息直接确定为所述匿名支付账户信息。

[138] 一种可能的实施方式中, 所述进行支付业务的终端为: 提供支付账户信息的终端; 所述支付处理单元 55, 配置为: 将所述匿名支付账户信息提供给另一个终端。

[139] 一种可能的实施方式中, 所述进行支付业务的终端为: 向服务器提供支付账单的终端; 所述支付处理单元 55, 配置为: 利用所述匿名支付账户信息, 生成匿名支付账单; 将所述匿名支付账单发送给服务器。

[140] 以上为进行支付业务的终端中的支付业务的实现装置, 可以降低支付账户信息泄露的风险。

[141] 另一方面的实施例, 还提供了一种服务器。如图 6 示出一个实施例的服务器。可以理解, 该装置可以通过任何具有计算、处理能力的装置、设备、平台和设备集群来实现。如图 6 所示, 该服务器 60 包括: 接收单元 61, 配置为接收匿名支付账单; 账户获取单元 62, 配置为从所述匿名支付账单中得到匿名支付账户信息; 解密处理单元 63, 配置为利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理, 得到变形后的支付账户信息; 其中, 所述私钥对应于进行支付业务的终端所获取的公钥; 随机数获取单元 64, 配置为得到随机数; 逆变处理单元 65, 配置为利用所述随机数对所述变形后的支付账户信息进行逆变处理, 得到原始支付账户信息; 扣款处理单元 66, 配置为根据所述原始支付账户信息, 进行账单扣款处理。

[142] 一种可能的实施方式中, 所述变形后的支付账户信息中未携带所述随机数; 所述随机数获取单元 64, 配置为: 对所述匿名支付账户信息进行第二解组合处理, 从该第二解组合处理后得到的支付账户信息中提取出所述随机数; 所述解密处理单元 63, 配置为: 从所述第二解组合处理后得到的支付账户信息中提取出第一支付账户信息; 以及利用所述私钥以及所述第一解密算法, 对所述第一支付账户信息进行解密。

[143] 一种可能的实施方式中, 所述变形后的支付账户信息中携带所述随机数; 所述解密处理单元 63, 配置为: 利用所述私钥以及所述第一解密算法, 对所述匿名支付账户信息进行解密; 所述随机数获取单元 64, 配置为: 对该解密后得到的支付账户信息进行第一解组合处理, 从该第一解组合处理后得到的支付账户信息中提取出所述随机数。

[144] 以上为用于实现支付业务的服务器, 可以降低支付账户信息泄露的风险。

[145] 需要说明的是, 本说明书实施例示意的结构并不构成对支付业务的实现装置和/或服务器的具体限定。在说明书的另一些实施例中, 支付业务的实现装置和/或服务器可以包括比图示更多或者更少的部件, 或者组合某些部件, 或者拆分某些部件, 或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[146] 上述装置内的各单元之间的信息交互、执行过程等内容, 由于与本说明书方法实施例基于同一构思, 具体内容可参见本说明书方法实施例中的叙述, 此处不再赘述。

[147] 再一方面的实施例, 还提供了一种计算设备, 包括存储器和处理器, 所述存储器中存储有可执行代码, 所述处理器执行所述可执行代码时, 实现上述各实施例所述的支付业务的实现方法。

[148] 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。

[149] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、挂件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[150] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1.支付业务的实现方法，应用于进行支付业务的终端中，所述方法包括：

生成随机数；

利用所述随机数对所述终端的原始支付账户信息进行变形处理，得到变形后的支付账户信息；

根据预先获取的公钥及第一加密算法，对所述变形后的支付账户信息进行加密，得到第一支付账户信息；

根据所述第一支付账户信息，得到匿名支付账户信息；

利用所述匿名支付账户信息，进行支付操作。

2.根据权利要求1所述的方法，其中，

所述生成随机数包括：根据第二加密算法的密钥长度，生成长度等于该密钥长度的所述随机数；

所述利用所述随机数对所述终端的原始支付账户信息进行变形处理，包括：

利用所述随机数作为所述第二加密算法的密钥，并利用所述第二加密算法对所述终端的原始支付账户信息进行加密。

3.根据权利要求2所述的方法，其中，在所述利用所述第二加密算法对所述终端的原始支付账户信息进行加密之后，并在所述得到变形后的支付账户信息之前，进一步包括：

将所述随机数与第二支付账户信息进行第一组合处理，得到所述变形后的支付账户信息；其中，所述第二支付账户信息为利用所述第二加密算法对所述终端的原始支付账户信息进行加密后得到的支付账户信息。

4.根据权利要求1所述的方法，其中，所述变形后的支付账户信息中未携带所述随机数；

所述根据第一支付账户信息，得到匿名支付账户信息，包括：

将所述随机数与所述第一支付账户信息进行第二组合处理，得到所述匿名支付账户信息。

5.根据权利要求1所述的方法，其中，所述变形后的支付账户信息中携带所述随机数；

所述根据第一支付账户信息，得到匿名支付账户信息，包括：

将所述第一支付账户信息直接确定为所述匿名支付账户信息。

6.根据权利要求1至5中任一所述的方法，所述进行支付业务的终端为：提供支付账户信息的终端；

所述利用所述匿名支付账户信息进行支付操作，包括：

将所述匿名支付账户信息提供给另一个终端。

7.根据权利要求1至5中任一所述的方法，所述进行支付业务的终端为：向服务器提供支付账单的终端；

所述利用所述匿名支付账户信息进行支付操作，包括：

利用所述匿名支付账户信息，生成匿名支付账单；

将所述匿名支付账单发送给服务器。

8.支付业务的实现方法，应用于服务器，包括：

接收匿名支付账单；

从所述匿名支付账单中得到匿名支付账户信息；

利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，得到变形后的支付账户信息；其中，所述私钥对应于进行支付业务的终端所获取的公钥；得到随机数；

利用所述随机数对所述变形后的支付账户信息进行逆变处理，得到原始支付账户信息；

根据所述原始支付账户信息，进行账单扣款处理。

9.根据权利要求8所述的方法，其中，所述变形后的支付账户信息中未携带所述随机数；

所述得到随机数，包括：对所述匿名支付账户信息进行第二解组合处理，从该第二解组合处理后得到的支付账户信息中提取出所述随机数；

所述利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，包括：

从所述第二解组合处理后得到的支付账户信息中提取出第一支付账户信息；以及利用所述私钥以及所述第一解密算法，对所述第一支付账户信息进行解密。

10.根据权利要求8所述的方法，其中，所述变形后的支付账户信息中携带所述随机数；

所述利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理，包括：利用所述私钥以及所述第一解密算法，对所述匿名支付账户信息进行解密；

所述得到随机数，包括：对该解密后得到的支付账户信息进行第一解组合处理，从该第一解组合处理后得到的支付账户信息中提取出所述随机数。

11.支付业务的实现装置，设置于进行支付业务的终端中，所述装置包括：

随机数生成单元，配置为生成随机数；

变形处理单元，配置为利用所述随机数对所述终端的原始支付账户信息进行变形处理，得到变形后的支付账户信息；

加密处理单元，配置为根据预先获取的公钥及第一加密算法，对所述变形后的支付账户信息进行加密，得到第一支付账户信息；

匿名账户确定单元，配置为根据所述第一支付账户信息，得到匿名支付账户信息；

支付处理单元，配置为利用所述匿名支付账户信息，进行支付操作。

12.根据权利要求11所述的装置，其中，

所述随机数生成单元，配置为：根据第二加密算法的密钥长度，生成长度等于该密钥长度的所述随机数；

所述变形处理单元，配置为：

利用所述随机数作为所述第二加密算法的密钥，并利用该第二加密算法对所述终端的原始支付账户信息进行加密。

13.根据权利要求12所述的装置，其中，所述变形处理单元，进一步配置为：

将所述随机数与第二支付账户信息进行第一组合处理，得到变形后的支付账户信息；其中，所述第二支付账户信息为利用所述第二加密算法对所述终端的原始支付账户信息进行加密后得到的支付账户信息。

14.根据权利要求 11 所述的装置,其中,所述变形后的支付账户信息中未携带所述随机数;

所述匿名账户确定单元,配置为:

将所述随机数与所述第一支付账户信息进行第二组合处理,得到所述匿名支付账户信息。

15.根据权利要求 11 所述的装置,其中,所述变形后的支付账户信息中携带所述随机数;

所述匿名账户确定单元,配置为:

将所述第一支付账户信息直接确定为所述匿名支付账户信息。

16.根据权利要求 11 至 15 中任一所述的装置,所述进行支付业务的终端为:提供支付账户信息的终端;

所述支付处理单元,配置为:

将所述匿名支付账户信息提供给另一个终端。

17.根据权利要求 11 至 15 中任一所述的装置,所述进行支付业务的终端为:向服务器提供支付账单的终端;

所述支付处理单元,配置为:

利用所述匿名支付账户信息,生成匿名支付账单;

将所述匿名支付账单发送给服务器。

18.服务器,包括:

接收单元,配置为接收匿名支付账单;

账户获取单元,配置为从所述匿名支付账单中得到匿名支付账户信息;

解密处理单元,配置为利用预先设置的私钥、第一解密算法以及所述匿名支付账户信息进行解密处理,得到变形后的支付账户信息;其中,所述私钥对应于进行支付业务的终端所获取的公钥;

随机数获取单元,配置为得到随机数;

逆变处理单元,配置为利用所述随机数对所述变形后的支付账户信息进行逆变处理,得到原始支付账户信息;

扣款处理单元,配置为根据所述原始支付账户信息,进行账单扣款处理。

19.根据权利要求 18 所述的服务器,其中,所述变形后的支付账户信息中未携带所述随机数;

所述随机数获取单元,配置为:对所述匿名支付账户信息进行第二解组合处理,从该第二解组合处理后得到的支付账户信息中提取出所述随机数;

所述解密处理单元,配置为:

从所述第二解组合处理后得到的支付账户信息中提取出第一支付账户信息;以及利用所述私钥以及所述第一解密算法,对所述第一支付账户信息进行解密。

20.根据权利要求 18 所述的服务器,其中,所述变形后的支付账户信息中携带所述随机数;

所述解密处理单元,配置为:利用所述私钥以及所述第一解密算法,对所述匿名支付账户信息进行解密;

所述随机数获取单元,配置为:对该解密后得到的支付账户信息进行第一解组合处

理，从该第一解组合处理后得到的支付账户信息中提取出所述随机数。

21.一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-10 中任一项所述的方法。