

密钥保护方法和系统

技术领域

5 本发明涉及信息安全技术领域，特别涉及一种密钥保护方法和一种密钥保护系统。

背景技术

近年来，伴随互联网以及金融信息化的快速发展，网上银行因其便利、高效等优点迅速得到用户和银行业界的普遍推崇，其中数字证书是通过网上银行进行交易时用户和银行服务器的身份标识，可以保证网上交易的安全。

目前，用户公钥证书的生成均由银行服务器完成，经过第三方电子商务认证服务器认证之后再下发给用户所使用的终端。存在的问题是，银行服务器在下发用户公钥证书给终端的过程中，银行服务器可能不知道所发送的具体终端，从而有可能遭到拦截，用户公钥证书在下发的过程中存在被盗取的安全隐患，同时在交易的过程中不能保证用户私钥的安全，存在安全隐患。

发明内容

本发明的目的旨在至少解决上述技术缺陷之一。

为达到上述目的，本发明第一个目的在于提出一种密钥保护方法，该方法包括以下步骤：

20 步骤：a、移动终端接收注册指令，并根据所述注册指令生成用户公钥和私钥，以及在所述移动终端通过移动银行服务器和银行综合前置服务器的身份认证时，所述移动银行服务器将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成所述用户公钥证书并保存；b、所述移动银行服务器根据所述用户公钥证书对所述移动终端发送的加密的用户交易信息进行验证，在验证通过之后，所述银行综合前置服务器执行交易；以及 c、所述移动终端在所述交易执行之后生成更新私钥保护参数，并将所述更新私钥保护参数发送至所述移动银行服务器，所述移动终端接收所述移动银行服务器更新成功结果，根据更新私钥保护参数对所述用户私钥进行加密存储。

根据本发明实施例的密钥保护方法，在移动终端生成用户公钥和私钥，并通过移动银行服务器和银行综合前置服务器多方对移动终端进行验证，并在验证之后移动银行服务器

将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书，同时在交易时，移动银行服务器可以通过用户公钥证书进行验证，并在交易完成更新用户私钥的私钥保护参数，由此，在用户公钥证书的生成中移动银行服务器经过对移动终端进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全，增加攻击的难度，同时在交易的过程中通过用户公钥证书进行验签，可以保证交易安全性，且在交易执行之后更新私钥保护参数以对用户私钥进行加密存储，进一步保证安全性。

为达到上述目的，本发明第二个目的在于提出一种密钥保护系统，该系统包括：移动终端、移动银行服务器和银行综合前置服务器，其中，所述移动终端，用于接收注册指令，并根据所述注册指令生成用户公钥和私钥；所述移动银行服务器在移动终端进行注册时，将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成所述用户公钥证书并保存；所述移动银行服务器根据所述用户数字证书对所述移动终端发送的加密的用户交易信息进行验证，并在验证通过之后，所述银行综合前置服务器执行交易；所述移动终端在所述交易执行之后生成更新私钥保护参数，并将所述更新私钥保护参数发送至所述移动银行服务器，所述移动终端接收所述移动银行服务器更新成功结果，根据更新私钥保护参数对所述用户私钥进行加密存储。

根据本发明实施例的密钥保护系统，在移动终端生成用户公钥和私钥，并通过移动银行服务器和银行综合前置服务器多方对移动终端进行验证，并在验证之后移动银行服务器将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书，同时在交易时，移动银行服务器可以通过用户公钥证书进行验证，并在交易完成更新用户私钥的私钥保护参数，由此，在用户公钥证书的生成中移动银行服务器经过对移动终端进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全，增加攻击的难度，同时在交易的过程中通过用户公钥证书进行验签，可以保证交易安全性，且在交易执行之后更新私钥保护参数以对用户私钥进行加密存储，进一步保证安全性。

本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 为本发明实施例的密钥保护方法的流程图；

图 2 为本发明一个实施例的用户公钥证书生成方法的流程图；

5 图 3 为本发明另一个实施例的用户公钥证书生成方法的流程图；

图 4 为本发明一个实施例的交易方法的流程图；

图 5 为本发明另一个实施例的交易方法的流程图；

图 6 为本发明一个实施例的用户私钥的存储方法的流程图；以及

图 7 为根据本发明实施例的密钥保护系统的结构框图。

10

具体实施方式

下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发
15 明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

在本发明的描述中，需要理解的是，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通
20 过中间媒介间接相连。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，
25 并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，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，这应被本发明的实施例所属技术领域的技术人员所理解。

下面参考附图描述根据本发明实施例的密钥保护方法和密钥保护系统。

图 1 为本发明实施例的密钥保护方法的流程图。

如图 1 所示，根据本发明实施例的密钥保护方法包括下述步骤：

步骤 S101，移动终端接收注册指令，并根据注册指令生成用户公钥和私钥，以及在移动终端通过移动银行服务器和银行综合前置服务器的身份认证时，移动银行服务器将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书并保存。

具体地，移动终端下载银行客户端软件，移动终端通过银行客户端软件进行注册，当移动终端接收到用户的注册指令之后，在移动终端中生成用户公钥和私钥，并在注册的过程中移动银行服务器和银行综合前置服务器对移动终端的身份进行认证，如果移动终端的身份认证通过之后，移动银行服务器将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书并保存，其中用户公钥证书存储在移动银行服务器和银行综合前置服务器中。

步骤 S102，移动银行服务器根据用户公钥证书对移动终端发送的加密的用户交易信息进行验证，在验证通过之后，银行综合前置服务器执行交易。

具体地，用户公钥证书生成之后，用户可以通过移动终端与移动银行服务器和银行综合前置服务器进行交易，移动银行服务器根据存储的用户公钥证书对移动终端发送的加密的用户交易信息进行验证，验证通过后，银行综合前置服务器根据用户交易信息执行交易。

步骤 S103，移动终端在交易执行之后生成更新私钥保护参数，并将更新私钥保护参数发送至移动银行服务器，移动终端接收移动银行服务器更新成功结果，根据更新私钥保护参数对用户私钥进行加密存储。

根据本发明实施例的密钥保护方法，在移动终端生成用户公钥和私钥，并通过移动银行服务器和银行综合前置服务器多方对移动终端进行验证，并在验证之后移动银行服务器将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书，同时在交易时，移动银行服务器可以通过用户公钥证书进行验证，并在交易完成更新用户私钥的私钥保护参数，由此，在用户公钥证书的生成中移动银行服务器经过对移动终端进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全，增加攻击的难度，同时在交易的过程中通过用户公钥证书进行验证，可以保证交易安全性，且在交易执行之后更新私钥保护参数以对用户私钥进行加密存储，进一步保证安全性。

下面参考附图分别描述图 1 所示的本发明实施例的密钥保护方法中的步骤 S101、S102 及 S103 的实施过程。

图 2 为本发明一个实施例的用户公钥证书生成方法的流程图。

5 如图 2 所示，用户公钥证书生成方法（即步骤 S101）包括下述步骤：

步骤 S201，移动终端获取移动银行服务器的公钥和银行综合前置服务器的公钥，对移动银行服务器的公钥和银行综合前置服务器的公钥进行验证，以及在验证通过之后根据注册指令与移动银行服务器建立连接，并生成用户公钥和私钥。

10 具体的，移动终端下载银行客户端软件，在安装客户端软件时，从所加载的软件中获取移动银行服务器的公钥和银行综合前置服务器的公钥，移动银行服务器的公钥和银行综合前置服务器的公钥的根证书提前预置在移动终端中，在发送注册请求时，可以根据预置的根证书验证移动银行服务器的公钥和银行综合前置服务器的公钥是否正确，其中在移动银行服务器的公钥和银行综合前置服务器的公钥正确时才可以继续执行下述步骤，在移动银行服务器的公钥和银行综合前置服务器的公钥错误时提示错误信息。

15 其中，移动银行服务端的私钥存储在移动银行服务器中，移动银行服务器的公钥和私钥用于对移动终端与移动银行服务端之间的通讯数据进行加密；银行服务端的私钥存储在银行综合前置服务器中，银行综合前置服务器的公钥和私钥用于对交易过程中的银行卡等敏感信息进行加密。

20 当然，本实施例中，可以在用户点击注册后，触发移动终端根据预设的非对称加密算法的密钥生成规则生成用户的公私钥对，移动终端生成用户的公私钥对以便后续执行交易时通过该公私钥对与移动银行服务器进行交互。

步骤 S202，移动终端根据移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器。

25 具体的，第一验证信息由移动银行服务器生成，并下发至移动终端并显示出来，以供用户查看并输入，该第一验证信息可以为图形验证码，从而可以防止攻击。移动终端接收用户输入的第一验证信息（例如图形验证码中的字符）。

另外，本实施例中，第一随机加密参数由移动终端随机生成。

账号信息包括：手机号码、银行卡号、注册完毕后的登录密码；或者账号信息包括：手机号码、银行卡号、注册完毕后的登录密码的哈希值。

步骤 S203, 移动银行服务器根据移动银行服务器的私钥对来自移动终端的信息进行解密, 以获得账号信息、第一验证信息以及第一随机加密参数, 并对第一验证信息进行验证, 验证通过后将账号信息发送至银行综合前置服务器。

具体的, 移动银行服务器验证移动终端发送的第一验证信息与自身生成的第一验证信息是否一致, 一致则通过验证。

另外, 移动银行服务器获取解密信息后, 保存账号信息中的手机号码以及第一随机加密参数。

步骤 S204, 银行综合前置服务器对来自移动银行服务器的账号信息进行验证, 发送验证结果至移动银行服务器。

10 具体的, 银行综合前置服务器验证账号信息中的手机号码和银行卡号是否正确, 发送验证结果至移动银行服务器。

步骤 S205, 在验证结果为正确时, 移动银行服务器生成第二随机加密参数和第二验证信息, 并将第二随机加密参数和第二验证信息发送至移动终端。

15 具体的, 在验证结果为正确时, 移动银行服务器根据第一随机加密参数对第二随机加密参数进行加密, 并将加密后的第二随机加密参数发送至移动终端; 并且利用存储的手机号码将第二验证信息以短信的形式发送至移动终端。

步骤 S206, 移动终端利用第一随机加密参数和第二随机加密参数加密第二验证信息和用户公钥生成第三验证信息, 并将第三验证信息发送至移动银行服务器。

20 具体的, 移动终端根据第一随机加密参数对加密后的第二随机加密参数进行解密, 获得第二随机加密参数; 并接收用户输入的第二验证信息; 移动终端再根据第一随机加密参数和第二随机加密参数对用户输入的第二验证信息和用户公钥进行加密以生成第三验证信息, 将第三验证信息和用户公钥发送至移动银行服务器。

在本实施例中, 可以利用第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行分段做加密以生成第三验证信息, 例如使用 MAC 加密算法。

25 步骤 S207, 移动银行服务器对来自移动终端的第三验证信息进行验证, 并在验证通过后将用户公钥发送至第三方电子商务认证服务器进行认证签名, 以生成用户公钥证书。

具体地, 第三方电子商务认证服务器对用户的公钥进行认证签名, 可以防止用户公钥被冒充, 并将签名之后的用户公钥储存在移动银行服务器中, 移动银行服务器存储签名的用户公钥之后提示用户公钥证书生成成功。

根据本发明实施例的数字证书生成方法，在移动终端生成用户公钥和私钥，将用户信息和用户公钥发送至移动银行服务器之前，移动终端与移动银行服务器和银行综合前置服务器多方进行验证，并在验证之后以数字证书的方式存储在移动银行服务器，保证用户公钥传输通路的安全性，增加攻击的难度。

5

图 3 为本发明另一个实施例的用户公钥证书生成方法的流程图。

如图 3 所示，根据本发明实施例的数字证书生成方法（即步骤 S101）包括下述步骤：

步骤 S301，移动终端获取移动银行服务器的公钥和银行综合前置服务器的公钥，对移动银行服务器的公钥和银行综合前置服务器的公钥进行验证，以及在验证通过之后根据注册指令与移动银行服务器建立连接，并生成用户公钥和私钥。

具体的，移动终端下载银行客户端软件，在安装客户端软件时，从所加载的软件中获取移动银行服务器的公钥和银行综合前置服务器的公钥，移动银行服务器的公钥和银行综合前置服务器的公钥的根证书提前预置在移动终端中，在发送注册请求时，可以根据预置的根证书验证移动银行服务器的公钥和银行综合前置服务器的公钥是否正确，其中在移动银行服务器的公钥和银行综合前置服务器的公钥正确时才可以继续执行下述步骤，在移动银行服务器的公钥和银行综合前置服务器的公钥错误时提示错误信息。

其中，移动银行服务端的私钥存储在移动银行服务器中，移动银行服务器的公钥和私钥用于对移动终端与移动银行服务端之间的通讯数据进行加密；银行服务端的私钥存储在银行综合前置服务器中，银行综合前置服务器的公钥和私钥用于对交易过程中的银行卡等敏感信息进行加密。

当然，本实施例中，可以在用户点击注册后，触发移动终端根据预设的非对称加密算法的密钥生成规则生成用户的公私钥对，移动终端生成用户的公私钥对以便后续执行交易时通过该公私钥对与移动银行服务器进行交互。

步骤 S302，移动终端根据移动银行服务器的公钥对账号信息、硬件信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器。

具体的，第一验证信息由移动银行服务器生成，并下发至移动终端并显示出来，以供用户查看并输入，该第一验证信息可以为图形验证码，从而可以防止攻击。移动终端接收用户输入的第一验证信息（例如图形验证码中的字符）。

另外，本实施例中，第一随机加密参数由移动终端随机生成。

账号信息包括：手机号码、银行卡号、注册完毕后的登录密码；或者账号信息包括：手机号码、银行卡号、注册完毕后的登录密码的哈希值。

硬件信息为：硬件特征信息或者硬件特征信息的哈希值，其中，硬件特征信息包括设备序列号和/或网卡的 MAC 地址。

- 5 具体地，移动终端提取移动终端自身的硬件特征信息（或者计算提取的硬件特征信息的哈希值），同时生成第一随机加密参数，接收用户录入的手机号码、银行卡号、登录密码（可以提示用户输入两次）、图形验证码显示的字符，通过点击提交之后移动终端通过移动银行服务器的公钥对获取的信息（包括手机号码、银行卡号、登录密码、硬件特征信息/硬件特征信息的哈希值、第一随机加密参数和图形验证码）进行加密并发送给移动银行服务
10 器。

当然，此时，移动终端还可以计算登录密码的哈希值，通过点击提交之后移动终端通过移动银行服务器的公钥对获取的信息（包括手机号码、银行卡号、登录密码的哈希值、硬件特征信息/硬件特征信息的哈希值、第一随机加密参数和图形验证码）进行加密并发送给移动银行服务器。

- 15 步骤 S303，移动银行服务器根据移动银行服务器的私钥对来自移动终端的信息进行解密，以获得账号信息、硬件信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器。

具体的，移动银行服务器验证移动终端发送的第一验证信息与自身生成的第一验证信息是否一致，一致则通过验证。

- 20 另外，移动银行服务器获取解密信息后，保存账号信息中的手机号码、硬件信息以及第一随机加密参数。

步骤 S304，银行综合前置服务器对来自移动银行服务器的账号信息进行验证，发送验证结果至移动银行服务器。

- 25 具体的，银行综合前置服务器验证账号信息中的手机号码和银行卡号是否正确，发送验证结果至移动银行服务器。

步骤 S305，在验证结果为正确时，移动银行服务器生成第二随机加密参数和第二验证信息，并将第二随机加密参数和第二验证信息发送至移动终端。

具体的，在验证结果为正确时，移动银行服务器根据第一随机加密参数对第二随机加密参数进行加密，并将加密后的第二随机加密参数发送至移动终端；并且利用存储的手机

号码将第二验证信息以短信的形式发送至移动终端。

步骤 S306, 移动终端根据第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成三验证信息, 并根据用户私钥对硬件信息进行签名以生成第一签名信息, 并将第三验证信息、用户公钥和第一签名信息发送至移动银行服务器。

5 具体的, 移动终端根据第一随机加密参数对加密后的第二随机加密参数进行解密, 获得第二随机加密参数; 并接收用户输入的第二验证信息; 移动终端再根据第一随机加密参数和第二随机加密参数对用户输入的第二验证信息和用户公钥进行加密以生成第三验证信息, 并根据用户私钥对硬件特征信息或者硬件特征信息的哈希值进行签名以生成第一签名信息, 将第三验证信息、用户公钥以及第一签名信息发送至移动银行服务器。

10 在本实施例中, 可以利用第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行分段做加密以生成第三验证信息, 例如使用 MAC 加密算法。

步骤 S307, 移动银行服务器对来自移动终端的第三验证信息和第一签名信息进行验证, 并在验证通过后将用户公钥发送至第三方电子商务认证服务器进行认证签名, 以生成用户公钥证书。

15 具体的, 移动银行服务器根据存储的第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成第四验证信息, 并根据用户公钥对第一签名信息进行验签, 并判断第三验证信息与第四验证信息是否一致, 第一签名信息是否通过验签; 如果一致且通过验签, 则验证通过。

20 第三方电子商务认证服务器对用户的公钥进行认证签名, 可以防止用户公钥被冒充, 并将签名之后的用户公钥储存在移动银行服务器中, 移动银行服务器存储签名的用户公钥之后提示用户公钥证书生成成功。

25 根据本发明实施例的数字证书生成方法, 在移动终端生成用户公钥和私钥, 将用户信息和用户公钥发送至移动银行服务器之前, 移动终端与移动银行服务器和银行综合前置服务器多方进行验证, 并在验证之后以数字证书的方式存储在移动银行服务器, 保证用户公钥传输通路的安全性, 增加攻击的难度。同时移动银行服务器经过对移动终端的硬件信息进行验证, 可以明确知道与自己通信的是哪个移动终端, 防止假冒移动终端与移动银行服务器进行交互, 保证了安全。

图 4 为本发明一个实施例的交易方法的流程图。

如图 4 所示, 根据本发明实施例的交易方法 (即步骤 S102) 包括下述步骤。

步骤 S401, 移动终端接收用户的交易信息, 并生成第一随机数。

具体地, 交易信息至少包括交易账号和交易金额。

5 步骤 S402, 移动终端根据第一随机数、移动终端的硬件信息、用户私钥、移动银行服务器的公钥及银行综合前置服务器的公钥对交易信息进行加密以生成交易报文, 并将交易报文发送至移动银行服务器, 其中, 硬件信息为硬件特征信息或硬件特征信息的哈希值, 硬件特征信息可以包括移动终端的设备序列号或网卡的 MAC 地址等。

步骤 S403, 移动银行服务器根据移动银行服务器的私钥和存储的移动终端的硬件信息对交易报文进行解密, 并根据用户公钥证书进行验签。

10 步骤 S404, 如果通过验签, 移动银行服务器生成加密密钥, 并根据加密密钥、移动银行服务器的私钥、银行综合前置服务器的公钥和交易信息生成数字信封, 并将数字信封发送至银行综合前置服务器。其中如果未通过验签, 提示用户在移动银行服务器中验签失败。

15 步骤 S405, 银行综合前置服务器根据银行综合前置服务器的私钥和移动银行服务器的公钥对数字信封进行解密获取交易信息, 并根据移动银行服务器的公钥进行验签, 并在通过验签后, 完成交易。

根据本发明实施例的交易方法, 在移动终端根据第一随机数、移动终端的硬件信息、用户私钥和移动银行服务器的公钥对交易信息进行加密以获取交易报文, 并在移动银行服务器中对交易报文进行验证, 可以保证银行综合前置服务器接收到的交易信息是来自于用户使用的安全的终端, 同时保证交易信息在移动终端、移动银行服务器和银行综合前置服务器之间的安全传输, 保证移动支付的安全。

20

图 5 为本发明另一个实施例的交易方法的流程图。

如图 5 所示, 根据本发明实施例的交易方法 (即步骤 S102) 包括下述步骤。

步骤 S501, 移动终端接收用户的交易信息, 并生成第一随机数。

25 其中, 每次进行交易报文处理时均生成第一随机数, 且每次生成的第一随机数都不同。具体地, 交易信息至少包括交易账号和交易金额。

步骤 S502, 移动终端根据银行综合前置服务器的公钥对交易密码进行加密获得交易密码的密文, 并根据用户私钥对交易信息和交易密码的密文进行签名以生成第一数字签名。

其中, 交易密码的密文根据银行综合前置服务器的公钥对交易密码加密生成, 对交易

密码加密可以保证交易密码的安全，保证电子渠道的全程不落地。当然，本实施例中的移动终端还可根据银行综合前置服务器的公钥对交易密码的哈希值进行加密获得交易密码的密文。

步骤 S503，移动终端根据随机数和移动终端的硬件信息生成加密参数密钥，并根据加
5 密参数密钥对交易信息和交易密码的密文进行加密以生成第一报文密文。

具体地，移动终端提取移动终端的硬件特征信息并计算硬件特征信息的哈希值，利用
第一随机数和移动终端的硬件特征信息（或者硬件特征信息的哈希值）生成加密参数密钥，
根据加密参数密钥对交易信息和交易密码的密文进行加密以生成第一报文密文；其中移动
终端根据加密参数密钥，可以采用 3DES（Triple DES、三重数据加密算法）或者 AES
10 （Advanced Encryption Standard、高级加密标准）算法等加密交易信息和交易密码的密文以
生成第一报文密文。

步骤 S504，移动终端根据移动银行服务器的公钥对第一随机数进行加密以生成第一密
钥密文。

应理解，步骤 S502、S503 和 S504 的执行可以不分先后顺序。

15 步骤 S505，移动终端将第一数字签名、第一报文密文和第一密钥密文作为交易报文发
送至移动银行服务器。

上述步骤为移动终端将交易信息发送至移动银行服务器之前的加密处理流程，移动银
行服务器接收到移动终端发送的交易报文之后，进行以下处理，即移动银行服务器对移动
终端发送的交易报文进行解密处理。

20 步骤 S506，移动银行服务器根据移动银行服务器的私钥对第一密钥密文进行解密以获
取第一随机数。

步骤 S507，移动银行服务器根据第一随机数和存储的移动终端的硬件信息生成加密参
数密钥，并根据加密参数密钥对第一报文密文进行解密以获取交易信息和交易密码的密文。

具体地，移动银行服务器根据存储的移动终端的硬件特征信息和第一随机数，或者存
25 储的移动终端的硬件特征信息的哈希值和第一随机数，重新计算得到加密参数密钥，移动
银行服务器利用自己计算所得的加密参数密钥解密接收到的第一报文密文，得到交易信息
和交易密码的密文。

步骤 S508，移动银行服务器根据存储的用户公钥证书对第一数字签名进行验签。

具体地，移动银行服务器从用户公钥证书中获取用户公钥，利用用户公钥对第一数字

签名进行验签。

步骤 S509, 如果未通过验签, 提示用户在移动银行服务器中验签失败。

步骤 S510, 如果通过验签, 移动银行服务器生成加密密钥。

其中, 加密密钥使用对称加密密钥。

- 5 具体地, 如果通过验签, 说明是安全的移动终端发送的交易报文, 继续执行下述的步骤, 下述步骤为移动银行服务器对交易信息进行加密处理的流程。

步骤 S511, 移动银行服务器根据加密密钥对交易信息和交易密码的密文进行加密以生成第二报文密文。

- 10 步骤 S512, 移动银行服务器根据银行综合前置服务器的公钥对加密密钥进行加密以生成第二密钥密文。

其中, 该加密方式可以与移动终端对交易信息的加密方式相同。

步骤 S513, 移动银行服务器根据移动银行服务器的私钥对交易信息和交易密码的密文进行签名以生成第二数字签名。

- 15 步骤 S514, 移动银行服务器将第二数字签名、第二报文密文和第二密钥密文作为数字信封发送至银行综合前置服务器。

银行综合前置服务器接收到数字信封之后, 继续执行下述的步骤, 即银行综合前置服务器对移动银行服务器发送的信息进行解密处理的流程。

步骤 S515, 银行综合前置服务器根据银行综合前置服务器的私钥对第二密钥密文进行解密以获取加密密钥。

- 20 步骤 S516, 银行综合前置服务器根据加密密钥对第二报文密文进行解密以获取交易信息和交易密码的密文。

- 25 为了保证交易密码的安全, 保证电子渠道的全程不落地, 交易密码在经由移动终端、移动银行服务器发往银行综合前置服务器的过程中, 采用交易密码的密文的形式进行传输; 银行综合前置服务器解密获得交易密码的密文后, 可进一步根据银行综合前置服务器的私钥对交易密码的密文进行解密, 获得交易密码并发送至后端的银行系统中。

步骤 S517, 银行综合前置服务器根据移动银行服务器的公钥对第二数字签名进行验签。

步骤 S518, 如果通过验签, 则银行综合前置服务器根据交易信息完成交易。

步骤 S519, 如果未通过验签, 提示移动银行服务器验签失败并向移动终端发送验证失败信息。

根据本发明实施例的交易，进一步保证交易信息在移动终端、移动银行服务器和银行综合前置服务器之间的安全传输，保证移动支付的安全。

图 6 为本发明一个实施例的用户私钥的存储方法的流程图。

- 5 如图 6 所示，根据本发明实施例的用户私钥的存储方法（即步骤 S103）包括以下步骤：
步骤 S601，移动终端在预设区域加密存储由用户私钥生成的用户私钥文件。

其中，用户私钥文件包括用户私钥和移动终端的硬件信息；用户私钥保护密钥为由移动终端的硬件信息/硬件特征信息的哈希值的全部或部分信息、登录密码/登陆密码的哈希值的全部或部分信息和私钥保护参数生成。

- 10 步骤 S602，移动终端在交易时进行用户身份验证，在验证通过之后生成第二随机数，根据第二随机数从移动银行服务器获取第一私钥保护参数和第二私钥保护参数。

具体地，在每次转账支付时，移动终端接收用户输入的支付信息，首先要根据支付信息验证用户身份；可通过短信验证码验证、动态口令验证、电子签名工具验证或交易密码验证等方式验证用户身份。

- 15 进一步，移动终端根据移动银行服务器的公钥对第二随机数进行加密，并将加密之后的第二随机数发送至移动银行服务器；移动银行服务器根据移动银行服务器的私钥对移动终端发送的加密信息进行解密以获取第二随机数；移动银行服务器根据第二随机数对第一私钥保护参数和第二私钥保护参数进行加密，并将加密之后的第一私钥保护参数和第二私钥保护参数发送至移动终端；移动终端根据第二随机数对移动银行服务器发送的信息进行
20 解密以获取第一私钥保护参数和第二私钥保护参数。

通过上述方式，能够保证移动终端与移动银行服务器之间传输私钥保护参数的安全。

其中，首次从移动银行服务器获取的第一私钥保护参数和第二私钥保护参数可以在注册时赋值相同。

- 25 步骤 S603，移动终端根据第二私钥保护参数解密存储的用户私钥文件，并验证解密之后的用户私钥文件。

当然，移动终端可以利用硬件信息验证解密之后的用户私钥文件，以提高安全性。

步骤 S604，如果用户私钥文件通过验证，则根据用户私钥文件执行交易，并更新私钥保护参数更新标识。

其中，根据解密用户私钥文件的第一私钥保护参数更新私钥保护参数更新标识。

步骤 S605, 如果用户私钥文件未通过验证, 则根据第一私钥保护参数解密存储的用户私钥文件, 并验证解密之后的用户私钥文件。

当然, 移动终端可以利用硬件信息验证解密之后的用户私钥文件, 以提高安全性。

步骤 S606, 如果用户私钥文件通过验证, 则根据用户私钥文件执行交易, 并更新私钥

5 保护参数更新标识。

根据解密用户私钥文件的第二私钥保护参数更新私钥保护参数更新标识。

此步骤中, 如果用户私钥文件未通过验证, 则反馈错误信息, 此时, 需要用户重新进行注册才能进行交易。

移动终端根据验证结果更新私钥保护参数更新标识, 进一步包括, 如果在利用第二私
10 钥保护参数解密用户私钥文件时, 解密后的用户私钥文件通过验证, 则可以根据解密用户私钥文件的第二私钥保护参数更新私钥保护参数更新标识, 例如将私钥保护参数更新标识更新为 2; 如果利用第一私钥保护参数解密用户私钥文件, 解密后的用户私钥文件通过验证, 则可以根据解密用户私钥文件的第一私钥保护参数更新私钥保护参数更新标识, 例如将私钥保护参数更新标识更新为 1。

15 步骤 S607, 移动终端根据接收到的交易结果生成更新私钥保护参数, 发送更新私钥保护参数及私钥保护参数更新标识至移动银行服务器。

其中, 无论交易结果是成功还是失败, 移动终端都生成更新私钥保护参数。

具体的, 移动终端还可以根据移动银行服务器的公钥对更新私钥保护参数和私钥保护参数更新标识进行加密, 并将加密之后的更新私钥保护参数和私钥保护参数更新标识发送
20 至移动银行服务器; 相应的, 移动银行服务器还根据移动银行服务器的私钥对移动终端发送的信息进行解密以获取更新私钥保护参数和私钥保护参数更新标识。通过加密传输的方式保证安全。

另外, 移动银行服务器还私钥保护参数更新标识对第一私钥保护参数和第二私钥保护参数进行更新, 具体的: 如果私钥保护参数更新标识为第二私钥保护参数对应的标识, 则
25 移动银行服务器根据更新私钥保护参数更新第二私钥保护参数, 并根据第二私钥保护参数更新第一私钥保护参数; 如果私钥保护参数更新标识为第一私钥保护参数对应的标识, 则移动银行服务器根据更新私钥保护参数更新第二私钥保护参数。

另外, 移动银行服务器在成功更新后, 还返回更新成功结果至移动终端。

步骤 S608, 移动终端根据移动银行服务的更新成功结果, 利用更新私钥保护参数对用

户私钥文件重新进行加密存储。

具体地，移动终端接收到更新成功结果之后，根据更新私钥保护参数、移动终端的硬件特征信息/硬件特征信息的哈希值的全部或部分信息、和登录密码/登陆密码的哈希值的全部或部分信息计算产生用户私钥保护密钥，并根据用户私钥保护密钥对用户私钥文件进行加密。

如果移动银行服务器更新失败，则移动终端根据移动银行服务器的更新失败结果，则不利用步骤 S607 生成的更新私钥保护参数对用户私钥文件进行加密存储，而仍采用原有的方式加密存储用户私钥文件，原有的方式可为步骤 S601 中根据用户私钥保护密钥对用户私钥文件进行加密并存储。

由此可见，根据本发明实施例的用户私钥的存储方法，移动终端从移动银行服务器获取私钥保护参数，并验证私钥保护参数能否成功解密用户私钥文件，在验证无误之后方可执行交易，使得用户私钥不易被破解，保证安全。

图 7 为根据本发明实施例的密钥保护系统的结构框图。

如图 7 所示，用户公钥证书生成系统包括：移动终端 10、移动银行服务器 20、银行综合前置服务器 30 和第三方电子商务认证服务器 40。

具体地，移动终端 10 用于接收注册指令，并根据注册指令生成用户公钥和私钥。具体地，移动终端 10 下载银行客户端软件，移动终端 10 通过银行客户端软件进行注册，当移动终端 10 接收到用户的注册指令之后，在移动终端 10 中生成用户公钥和私钥。

移动银行服务器 20 在移动终端 10 进行注册时，将用户公钥发送至第三方电子商务认证服务器 40 进行认证签名，以生成用户公钥证书并保存。其中，在注册的过程中移动银行服务器 20 和银行综合前置服务器 30 对移动终端 10 的身份进行认证，如果移动终端 10 的身份认证通过之后，移动银行服务器 20 将用户公钥发送至第三方电子商务认证服务器 40 进行认证签名，以生成用户公钥证书并保存，其中用户公钥证书存储在移动银行服务器 20。

移动银行服务器 20 根据用户数字证书对移动终端发送的加密的用户交易信息进行验证，并在验证通过之后，银行综合前置服务器 30 执行交易。其中，用户公钥证书生成之后，用户可以通过移动终端 10 进行交易，移动银行服务器 20 根据存储的用户公钥证书对移动终端 10 发送的加密的用户交易信息进行验证，在验证通过之后，银行综合前置服务器 30 执行交易。

移动终端 10 在交易执行之后生成更新私钥保护参数，并将更新私钥保护参数发送至移动银行服务器 20，移动终端 10 接收移动银行服务器 20 更新成功结果，根据更新私钥保护参数对用户私钥进行加密存储。

根据本发明实施例的密钥保护系统，在移动终端生成用户公钥和私钥，并通过移动银行服务器和银行综合前置服务器多方对移动终端进行验证，并在验证之后移动银行服务器将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书，同时在交易时，移动银行服务器可以通过用户公钥证书进行验证，并在交易完成更新用户私钥的私钥保护参数，由此，在用户公钥证书的生成中移动银行服务器经过对移动终端进行验证，可以明确知道与自己通信的是哪个移动终端，防止假冒移动终端与移动银行服务器进行交互，保证了安全，增加攻击的难度，同时在交易的过程中通过用户公钥证书进行验证，可以保证交易安全性，且在交易执行之后更新私钥保护参数以对用户私钥进行加密存储，进一步保证安全性。

在密钥保护系统中，首先需要生成用户公钥证书，具体实施例如下：

移动终端 10 还用于获取移动银行服务器 20 的公钥和银行综合前置服务器 30 的公钥，对移动银行服务器 20 的公钥和银行综合前置服务器 30 的公钥进行验证，以及在验证通过之后根据注册指令与移动银行服务器 20 建立连接，并生成用户公钥和私钥，并根据移动银行服务器 20 的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至移动银行服务器 20。

移动银行服务器 20 还用于根据移动银行服务器 20 的私钥对来自移动终端 10 的信息进行解密，以获得账号信息、第一验证信息以及第一随机加密参数，并对第一验证信息进行验证，验证通过后将账号信息发送至银行综合前置服务器 20。

银行综合前置服务器 30 还用于对来自移动银行服务器 20 的账号信息进行验证，发送验证结果至移动银行服务器 20。

其中，在验证结果为正确时，移动银行服务器 20 还用于生成第二随机加密参数和第二验证信息，并将第二随机加密参数和第二验证信息发送至移动终端 10，移动终端 10 还用于根据第一随机加密参数和第二随机加密参数加密第二验证信息和用户公钥生成第三验证信息，并将第三验证信息发送至移动银行服务器 20，移动银行服务器 20 对来自移动终端 10 的第三验证信息进行验证，并在验证通过后将用户公钥发送至第三方电子商务认证服务

器 40 进行认证签名，以生成用户公钥证书。

移动终端 10 还用于根据移动银行服务器 20 的公钥对移动终端 10 的硬件信息进行加密，其中，硬件信息为硬件特征信息或硬件特征信息的哈希值，硬件特征信息包括设备序列号和/或网卡的 MAC 地址。

5 其中，账号信息包括手机号码、银行卡号和登录密码。

移动终端 10 还用于接收移动银行服务器 20 生成的第一验证信息，其中第一验证信息为图形验证码，以及根据移动银行服务器 20 的公钥对手机号码、银行卡号、计算得到的登录密码的哈希值、硬件信息、第一随机加密参数和第一验证信息进行加密，并将加密之后的信息发送至移动银行服务器 20，其中第一随机加密参数由移动终端 10 生成。

10 移动银行服务器 20 还用于根据第一随机加密参数对第二随机加密参数进行加密，并将加密后的第二随机加密参数发送至移动终端 10，以及将第二验证信息以短信的形式发送至移动终端 10。

将第二随机加密参数和第二验证信息发送至移动终端 10 的步骤之后，移动终端 10 还用于根据第一随机加密参数对加密后的第二随机加密参数进行解密，获得第二随机加密参
15 数；并接收用户输入的第二验证信息。

移动终端 10 还用于根据第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行加密以生成第三验证信息，并根据用户私钥对硬件信息进行签名以生成第一签名信息，并将第三验证信息、用户公钥和第一签名信息发送至移动银行服务器 20。

移动银行服务器 20 还用于根据存储的第一随机加密参数和第二随机加密参数对第二
20 验证信息和用户公钥进行加密以生成第四验证信息，并根据用户公钥对第一签名信息进行验签，并判断第三验证信息与第四验证信息是否一致，第一签名信息是否通过验签；如果一致并通过验签，则验证通过。

根据第一随机加密参数和第二随机加密参数对第二验证信息和用户公钥进行分段做加密，例如使用 MAC 加密算法。

25

在密钥保护系统中，在用户公钥证书之后执行交易，具体实施例如下：

移动终端 10 还用于接收用户的交易信息，并生成第一随机数，其中交易信息至少包括交易账号和交易金额，以及根据第一随机数、移动终端的硬件信息、用户私钥、移动银行服务器 20 的公钥及银行综合前置服务器 30 的公钥对交易信息进行加密以生成交易报文，

并将交易报文发送至移动银行服务器 20，其中硬件信息为硬件特征信息或硬件特征信息的哈希值。

移动银行服务器 20 还用于根据移动银行服务器 20 的私钥和存储的移动终端 10 的硬件信息对交易报文进行解密，并根据用户公钥证书进行验签，并在通过验签时，生成加密密
5 钥，并根据加密密钥、移动银行服务器 20 的私钥、银行综合前置服务器 30 的公钥和交易信息生成数字信封，并将数字信封发送至银行综合前置服务器 30。

银行综合前置服务器 30 还用于根据银行综合前置服务器 30 的私钥和移动银行服务器 20 的公钥对数字信封进行解密获取交易信息，并根据移动银行服务器 20 的公钥进行验签，并在通过验签后，完成交易。

10 在本发明实施例中，移动终端 10 还用于根据银行综合前置服务器 30 的公钥对交易密码或交易密码的哈希值进行加密获得交易密码的密文，并根据用户私钥对交易信息和交易密码的密文进行签名以生成第一数字签名，以及根据第一随机数和移动终端 10 的硬件信息生成加密参数密钥，并根据加密参数密钥对交易信息和交易密码的密文进行加密以生成第一报文密文，并根据移动银行服务器 20 的公钥对第一随机数进行加密以生成第一密钥密
15 文，以及将第一数字签名、第一报文密文和第一密钥密文作为交易报文发送至移动银行服务器 20。

移动银行服务器 20 还用于根据移动银行服务器 20 的私钥对第一密钥密文进行解密以获取第一随机数，并根据第一随机数和存储的移动终端 10 的硬件信息生成加密参数密钥，并根据加密参数密钥对第一报文密文进行解密以获取交易信息和交易密码的密文，以及根
20 据存储的用户公钥证书对第一数字签名进行验签。

移动银行服务器 20 还用于生成加密密钥，并根据加密密钥对交易信息和交易密码的密文进行加密以生成第二报文密文，以及根据银行综合前置服务器 30 的公钥对加密密钥进行加密以生成第二密钥密文，并根据移动银行服务器 20 的私钥对交易信息和交易密码的密文进行签名以生成第二数字签名，以及将第二数字签名、第二报文密文和第二密钥密文作为
25 数字信封发送至银行综合前置服务器 30。

银行综合前置服务器 30 还用于根据银行综合前置服务器 30 的私钥对第二密钥密文进行解密以获取加密密钥，并根据加密密钥对第二报文密文进行解密以获取交易信息和交易密码的密文，以及根据移动银行服务器 20 的公钥对第二数字签名进行验证，并在验证通过时，根据交易信息完成交易。

为了保证交易密码的安全，保证电子渠道的全程不落地，交易密码在经由移动终端 10、移动银行服务器 20 发往银行综合前置服务器 30 的过程中，采用交易密码的密文的形式进行传输；银行综合前置服务器 30 解密获得交易密码的密文后，可进一步根据银行综合前置服务器 30 的私钥对交易密码的密文进行解密，获得交易密码并发送至后端的银行系统中。

5 进一步，加密密钥为对称加密密钥。

在密钥保护系统中，在执行交易之后，更新私钥保护参数对用户私钥进行加密存储，具体实施例如下：

移动终端 10 还用于在预设区域加密存储由用户私钥生成的用户私钥文件，并在交易时
10 进行用户身份验证，并在验证通过之后生成第二随机数，根据第二随机数从移动银行服务器 20 获取第一私钥保护参数和第二私钥保护参数，并根据第二私钥保护参数解密存储的用户私钥文件，并验证解密之后的用户私钥文件，以及在用户私钥文件通过验证时根据用户私钥文件执行交易，并更新私钥保护参数更新标识，在用户私钥文件未通过验证时根据第一私钥保护参数解密存储的用户私钥文件，并验证解密之后的用户私钥文件，以及在用户
15 私钥文件通过验证时根据用户私钥文件执行交易，并更新私钥保护参数更新标识，并根据接收到的交易结果生成更新私钥保护参数，发送更新私钥保护参数及私钥保护参数更新标识至移动银行服务器 20，以及根据移动银行服务器 20 的更新成功结果，利用更新私钥保护参数对用户私钥重新进行加密存储。

如果移动银行服务器更新失败，则移动终端 10 根据移动银行服务器 20 的更新失败结
20 果，则不利用生成的更新私钥保护参数对用户私钥文件进行加密存储，而仍采用原有的方式加密存储用户私钥文件，原有的方式可为根据用户私钥保护密钥对用户私钥文件进行加密并存储。

另外，移动终端 10 根据两次验证均不通过的结果，重新执行注册流程。

在本发明的实施例中，移动终端 10 还用于根据用户私钥保护密钥对用户私钥文件进行
25 加密并存储，用户私钥文件包括用户私钥和移动终端 10 的硬件信息，以及用户私钥保护密钥为由移动终端 10 的硬件信息/硬件特征信息的哈希值的全部或部分信息、登录密码/登陆密码的哈希值的全部或部分信息和私钥保护参数生成。

进一步，根据解密用户私钥文件的第一私钥保护参数或第二私钥保护参数更新私钥保护参数更新标识。

如果私钥保护参数更新标识为第二私钥保护参数对应的标识，则移动银行服务器 20 根据更新私钥保护参数更新第二私钥保护参数，并根据第二私钥保护参数更新第一私钥保护参数；如果私钥保护参数更新标识为第一私钥保护参数对应的标识，则移动银行服务器 20 根据更新私钥保护参数更新第二私钥保护参数；移动银行服务器 20 返回更新成功结果至移动终端 10。

移动终端 10 还用于根据移动银行服务器 20 的公钥对更新私钥保护参数和私钥保护参数更新标识进行加密，并将加密之后的更新私钥保护参数和私钥保护参数更新标识发送至移动银行服务器 20；移动银行服务器 20 还用于根据移动银行服务器 20 的私钥对移动终端 10 发送的信息进行解密以获取更新私钥保护参数和私钥保护参数更新标识。

移动终端 10 还用于利用硬件信息验证解密之后的用户私钥文件。

移动终端 10 还用于根据移动银行服务器 20 的公钥对第二随机数进行加密，并将加密之后的第二随机数发送至移动银行服务器 20；移动银行服务器 20 还用于根据移动银行服务器 20 的私钥对移动终端 10 发送的加密信息进行解密以获取第二随机数，并根据第二随机数对第一私钥保护参数和第二私钥保护参数进行加密，并将加密之后的第一私钥保护参数和第二私钥保护参数发送至移动终端 10；移动终端 10 还用于根据第二随机数对移动银行服务器 20 发送的信息进行解密以获取第一私钥保护参数和第二私钥保护参数。

移动银行服务器 20 与移动终端 10 之间通过短信验证码验证、动态口令验证、电子签名工具验证或交易密码验证的方式验证用户身份。

应理解，应理解，本发明的系统实施例中的各个设备的具体操作过程可与方法实施例中的描述相同，此处不再详细描述。

尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同限定。

权利要求书

1、一种密钥保护方法，其特征在于，该方法包括：

a、移动终端接收注册指令，并根据所述注册指令生成用户公钥和私钥，以及在所述移动终端通过移动银行服务器和银行综合前置服务器的身份认证时，所述移动银行服务器将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成所述用户公钥证书并保存；

b、所述移动银行服务器根据所述用户公钥证书对所述移动终端发送的加密的用户交易信息进行验证，在验证通过之后，所述银行综合前置服务器执行交易；以及

10 c、所述移动终端在所述交易执行之后生成更新私钥保护参数，并将所述更新私钥保护参数发送至所述移动银行服务器，所述移动终端接收所述移动银行服务器更新成功结果，根据更新私钥保护参数对所述用户私钥进行加密存储。

2、根据权利要求1所述的方法，其特征在于，所述步骤a包括：

15 a1、所述移动终端获取移动银行服务器的公钥和银行综合前置服务器的公钥，对所述移动银行服务器的公钥和所述银行综合前置服务器的公钥进行验证，以及在验证通过之后根据所述注册指令与所述移动银行服务器建立连接，并生成所述用户公钥和私钥；

a2、所述移动终端根据所述移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至所述移动银行服务器；

20 a3、所述移动银行服务器根据所述移动银行服务器的私钥对来自所述移动终端的信息进行解密，以获得所述账号信息、第一验证信息以及第一随机加密参数，并对所述第一验证信息进行验证，验证通过后将所述账号信息发送至银行综合前置服务器；

a4、所述银行综合前置服务器对来自所述移动银行服务器的所述账号信息进行验证，发送验证结果至所述移动银行服务器；

25 a5、在所述验证结果为正确时，所述移动银行服务器生成第二随机加密参数和第二验证信息，并将所述第二随机加密参数和第二验证信息发送至所述移动终端；

a6、所述移动终端根据所述第一随机加密参数和第二随机加密参数加密所述第二验证信息和用户公钥生成第三验证信息，并将所述第三验证信息发送至所述移动银行服务器；以及

a7、所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证，并在验证通过后将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成所述用户公钥证书。

3、根据权利要求2所述的方法，其特征在于，所述步骤a2还包括：

5 所述移动终端根据所述移动银行服务器的公钥对所述移动终端的硬件信息进行加密，其中，所述硬件信息为硬件特征信息或硬件特征信息的哈希值，所述硬件特征信息包括设备序列号和/或网卡的MAC地址。

4、根据权利要求3所述的方法，其特征在于，所述账号信息包括手机号码、银行卡号和登录密码，所述步骤a2包括：

10 所述移动终端接收所述移动银行服务器生成的所述第一验证信息，其中所述第一验证信息为图形验证码；以及

所述移动终端根据所述移动银行服务器的公钥对所述手机号码、银行卡号、计算得到的登录密码的哈希值、硬件信息、第一随机加密参数和第一验证信息进行加密，并将加密之后的信息发送至所述移动银行服务器，其中所述第一随机加密参数由所述移动终端生成。

15 5、根据权利要求2所述的方法，其特征在于，所述步骤a5中将所述第二随机加密参数和所述第二验证信息发送至所述移动终端的步骤包括：

所述移动银行服务器根据所述第一随机加密参数对所述第二随机加密参数进行加密，并将加密后的所述第二随机加密参数发送至所述移动终端，以及将所述第二验证信息以短信的形式发送至所述移动终端。

20 6、根据权利要求5所述的方法，其特征在于，将所述第二随机加密参数和所述第二验证信息发送至所述移动终端的步骤之后，步骤a6之前，所述方法还包括：

所述移动终端根据所述第一随机加密参数对加密后的所述第二随机加密参数进行解密，获得所述第二随机加密参数；并接收用户输入的第二验证信息。

7、根据权利要求3所述的方法，其特征在于，所述步骤a6包括：

25 所述移动终端根据所述第一随机加密参数和第二随机加密参数对所述第二验证信息和用户公钥进行加密以生成所述第三验证信息，并根据所述用户私钥对所述硬件信息进行签名以生成第一签名信息，并将所述第三验证信息、用户公钥和第一签名信息发送至所述移动银行服务器。

8、根据权利要求7所述的方法，其特征在于，所述步骤a7中所述移动银行服务器对

来自所述移动终端的所述第三验证信息进行验证的步骤包括：

所述移动银行服务器根据存储的所述第一随机加密参数和第二随机加密参数对所述第二验证信息和用户公钥进行加密以生成第四验证信息，并根据所述用户公钥对所述第一签名信息进行验签，并判断所述第三验证信息与所述第四验证信息是否一致，所述第一签名信息是否通过验签；如果一致并通过验签，则验证通过。

9、根据权利要求 2 或 7 所述的方法，其特征在于，步骤 a6 中所述生成第三验证信息的步骤包括：

根据所述第一随机加密参数和所述第二随机加密参数对所述第二验证信息和用户公钥进行分段做加密。

10、根据权利要求 1 所述的方法，其特征在于，所述步骤 b 包括：

b1、移动终端接收用户的交易信息，并生成第一随机数，其中所述交易信息至少包括交易账号和交易金额；

b2、所述移动终端根据所述第一随机数、移动终端的硬件信息、用户私钥、移动银行服务器的公钥及银行综合前置服务器的公钥对所述交易信息进行加密以生成交易报文，并将所述交易报文发送至所述移动银行服务器，其中所述硬件信息为硬件特征信息或硬件特征信息的哈希值；

b3、所述移动银行服务器根据所述移动银行服务器的私钥和存储的所述移动终端的硬件信息对所述交易报文进行解密，并根据所述用户公钥证书进行验证；

b4、如果验证通过，所述移动银行服务器生成加密密钥，并根据所述加密密钥、移动银行服务器的私钥、银行综合前置服务器的公钥和交易信息生成数字信封，并将所述数字信封发送至所述银行综合前置服务器；以及

b5、所述银行综合前置服务器根据所述银行综合前置服务器的私钥和移动银行服务器的公钥对所述数字信封进行解密获取所述交易信息，并根据所述移动银行服务器的公钥进行验签，并在通过验签后，完成交易。

11、根据权利要求 10 方法，其特征在于，所述步骤 b2 包括：

所述移动终端根据所述银行综合前置服务器的公钥对交易密码或交易密码的哈希值进行加密获得交易密码的密文，并根据所述用户私钥对所述交易信息和所述交易密码的密文进行签名以生成第一数字签名；

所述移动终端根据所述第一随机数和所述移动终端的硬件信息生成加密参数密钥，并

根据所述加密参数密钥对所述交易信息和所述交易密码的密文进行加密以生成第一报文密文；

所述移动终端根据所述移动银行服务器的公钥对所述第一随机数进行加密以生成第一密钥密文；以及

- 5 所述移动终端将所述第一数字签名、所述第一报文密文和所述第一密钥密文作为所述交易报文发送至所述移动银行服务器。

12、根据权利要求 11 所述的方法，其特征在于，所述步骤 b3 包括以下步骤：

所述移动银行服务器根据所述移动银行服务器的私钥对所述第一密钥密文进行解密以获取所述第一随机数；

- 10 所述移动银行服务器根据所述第一随机数和存储的所述移动终端的硬件信息生成所述加密参数密钥，并根据所述加密参数密钥对所述第一报文密文进行解密以获取所述交易信息和所述交易密码的密文；以及

所述移动银行服务器根据存储的所述用户公钥证书对所述第一数字签名进行验签。

13、根据权利要求 12 所述的方法，其特征在于，所述步骤 b4 包括：

- 15 所述移动银行服务器生成所述加密密钥；

所述移动银行服务器根据所述加密密钥对所述交易信息和所述交易密码的密文进行加密以生成第二报文密文；

所述移动银行服务器根据所述银行综合前置服务器的公钥对所述加密密钥进行加密以生成第二密钥密文；

- 20 所述移动银行服务器根据所述移动银行服务器的私钥对所述交易信息和所述交易密码的密文进行签名以生成第二数字签名；以及

所述移动银行服务器将所述第二数字签名、所述第二报文密文和所述第二密钥密文作为所述数字信封发送至所述银行综合前置服务器。

14、根据权利要求 13 所述的方法，其特征在于，所述步骤 b5 包括：

- 25 所述银行综合前置服务器根据所述银行综合前置服务器的私钥对所述第二密钥密文进行解密以获取所述加密密钥；

所述银行综合前置服务器根据所述加密密钥对所述第二报文密文进行解密以获取所述交易信息和所述交易密码的密文；

所述银行综合前置服务器根据所述移动银行服务器的公钥对所述第二数字签名进行验

签；以及

如果通过验签，则所述银行综合前置服务器根据所述交易信息完成交易。

15、根据权利要求 12 所述的方法，其特征在于，所述加密密钥为对称加密密钥。

16、根据权利要求 1 所述的方法，其特征在于，所述步骤 c 包括：

5 c1、移动终端在预设区域加密存储由所述用户私钥生成的用户私钥文件；

c2、所述移动终端在所述交易时进行用户身份验证，并在验证通过之后生成第二随机数，根据所述第二随机数从所述移动银行服务器获取第一私钥保护参数和第二私钥保护参数；

10 c3、所述移动终端根据所述第二私钥保护参数解密所述存储的用户私钥文件，并验证解密之后的所述用户私钥文件；

c4、如果所述用户私钥文件通过验证，则根据所述用户私钥文件执行交易，并更新私钥保护参数更新标识；

c5、如果所述用户私钥文件未通过验证，则根据所述第一私钥保护参数解密所述存储的用户私钥文件，并验证解密之后的所述用户私钥文件；

15 c6、如果所述用户私钥文件通过验证，则根据所述用户私钥文件执行交易，并更新所述私钥保护参数更新标识；

c7、所述移动终端根据接收到的交易结果生成更新私钥保护参数，发送所述更新私钥保护参数及所述私钥保护参数更新标识至移动银行服务器；以及

20 c8、所述移动终端根据所述移动银行服务器的更新成功结果，利用更新私钥保护参数对所述用户私钥重新进行加密存储。

17、根据权利要求 16 所述的方法，其特征在于，所述步骤 c1 包括：

根据用户私钥保护密钥对所述用户私钥文件进行加密并存储；

所述用户私钥文件包括用户私钥和所述移动终端的硬件信息；以及

25 所述用户私钥保护密钥为由所述移动终端的硬件信息/硬件特征信息的哈希值的全部或部分信息、登录密码/登陆密码的哈希值的全部或部分信息和私钥保护参数生成。

18、根据权利要求 16 所述的方法，其特征在于，所述步骤 c4 或 c6 中更新所述私钥保护参数更新标识的步骤包括：

根据解密所述用户私钥文件的所述第一私钥保护参数或第二私钥保护参数更新所述私钥保护参数更新标识。

19、根据权利要求 16 所述的方法，其特征在于，所述步骤 c7 和所述步骤 c8 之间还包括：

如果所述私钥保护参数更新标识为所述第二私钥保护参数对应的标识，则所述移动银行服务器根据所述更新私钥保护参数更新所述第二私钥保护参数，并根据所述第二私钥保护参数更新所述第一私钥保护参数；

如果所述私钥保护参数更新标识为所述第一私钥保护参数对应的标识，则所述移动银行服务器根据所述更新私钥保护参数更新所述第二私钥保护参数；

所述移动银行服务器返回更新成功结果至所述移动终端。

20、根据权利要求 19 所述的方法，其特征在于，所述步骤 c7 所述发送所述更新私钥保护参数及所述私钥保护参数更新标识至移动银行服务器包括：

所述移动终端根据所述移动银行服务器的公钥对所述更新私钥保护参数和所述私钥保护参数更新标识进行加密，并将加密之后的所述更新私钥保护参数和所述私钥保护参数更新标识发送至所述移动银行服务器；

所述步骤 c7 和所述步骤 c8 之间还包括：所述移动银行服务器根据所述移动银行服务器的私钥对所述移动终端发送的信息进行解密以获取所述更新私钥保护参数和所述私钥保护参数更新标识。

21、根据权利要求 16 所述的方法，其特征在于，步骤 c3 中所述验证解密之后的所述用户私钥文件包括：

利用所述硬件信息验证解密之后的所述用户私钥文件。

22、根据权利要求 16-21 任一项所述的方法，其特征在于，步骤 c2 中所述根据所述第二随机数从移动银行服务器获取第一私钥保护参数和第二私钥保护参数的步骤包括：

所述移动终端根据所述移动银行服务器的公钥对所述第二随机数进行加密，并将加密之后的所述第二随机数发送至所述移动银行服务器；

所述移动银行服务器根据所述移动银行服务器的私钥对所述移动终端发送的加密信息进行解密以获取所述第二随机数；

所述移动银行服务器根据所述第二随机数对所述第一私钥保护参数和所述第二私钥保护参数进行加密，并将加密之后的所述第一私钥保护参数和第二私钥保护参数发送至所述移动终端；以及

所述移动终端根据所述第二随机数对所述移动银行服务器发送的信息进行解密以获取

所述第一私钥保护参数和第二私钥保护参数。

23、根据权利要求 16-21 任一项所述的方法，其特征在于，步骤 c2 中所述验证用户身份的步骤包括短信验证码验证、动态口令验证、电子签名工具验证或交易密码验证。

24、一种密钥保护系统，其特征在于，包括移动终端、移动银行服务器和银行综合前置服务器，其中，

所述移动终端，用于接收注册指令，并根据所述注册指令生成用户公钥和私钥；

所述移动银行服务器在移动终端进行注册时，将所述用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成所述用户公钥证书并保存；

所述移动银行服务器根据所述用户数字证书对所述移动终端发送的加密的用户交易信息进行验证，并在验证通过之后，所述银行综合前置服务器执行交易；

所述移动终端在所述交易执行之后生成更新私钥保护参数，并将所述更新私钥保护参数发送至所述移动银行服务器，所述移动终端接收所述移动银行服务器更新成功结果，根据更新私钥保护参数对所述用户私钥进行加密存储。

25、根据权利要求 24 所述的系统，其特征在于，

所述移动终端，还用于获取所述移动银行服务器的公钥和银行综合前置服务器的公钥，对所述移动银行服务器的公钥和所述银行综合前置服务器的公钥进行验证，以及在验证通过之后根据所述注册指令与所述移动银行服务器建立连接，并生成所述用户公钥和私钥，并根据所述移动银行服务器的公钥对账号信息、第一验证信息以及第一随机加密参数进行加密，并将加密之后的信息发送至所述移动银行服务器；

所述移动银行服务器，还用于根据所述移动银行服务器的私钥对来自所述移动终端的信息进行解密，以获得所述账号信息、第一验证信息以及第一随机加密参数，并对所述第一验证信息进行验证，验证通过后将所述账号信息发送至银行综合前置服务器；

所述银行综合前置服务器，还用于对来自所述移动银行服务器的所述账号信息进行验证，发送验证结果至所述移动银行服务器；

其中，在所述验证结果为正确时，所述移动银行服务器还用于生成第二随机加密参数和第二验证信息，并将所述第二随机加密参数和第二验证信息发送至所述移动终端，所述移动终端还用于根据所述第一随机加密参数和第二随机加密参数加密所述第二验证信息和用户公钥生成第三验证信息，并将所述第三验证信息发送至所述移动银行服务器，所述移动银行服务器对来自所述移动终端的所述第三验证信息进行验证，并在验证通过后将所述

用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成所述用户公钥证书。

26、根据权利要求 25 所述的系统，其特征在于，

所述移动终端，还用于根据所述移动银行服务器的公钥对所述移动终端的硬件信息进行加密，其中，所述硬件信息为硬件特征信息或硬件特征信息的哈希值，所述硬件特征信息包括设备序列号和/或网卡的 MAC 地址。

27、根据权利要求 26 所述的系统，其特征在于，所述账号信息包括手机号码、银行卡号和登录密码，

所述移动终端，还用于接收所述移动银行服务器生成的所述第一验证信息，其中所述第一验证信息为图形验证码，以及

根据所述移动银行服务器的公钥对所述手机号码、银行卡号、计算得到的登录密码的哈希值、硬件信息、第一随机加密参数和第一验证信息进行加密，并将加密之后的信息发送至所述移动银行服务器，其中所述第一随机加密参数由所述移动终端生成。

28、根据权利要求 25 所述的系统，其特征在于，

所述移动银行服务器，还用于根据所述第一随机加密参数对所述第二随机加密参数进行加密，并将加密后的所述第二随机加密参数发送至所述移动终端，以及将所述第二验证信息以短信的形式发送至所述移动终端。

29、根据权利要求 28 所述的系统，其特征在于，将所述第二随机加密参数和所述第二验证信息发送至所述移动终端的步骤之后，

所述移动终端，还用于根据所述第一随机加密参数对加密后的所述第二随机加密参数进行解密，获得所述第二随机加密参数；并接收用户输入的第二验证信息。

30、根据权利要求 26 所述的系统，其特征在于，

所述移动终端，还用于根据所述第一随机加密参数和第二随机加密参数对所述第二验证信息和用户公钥进行加密以生成所述第三验证信息，并根据所述用户私钥对所述硬件信息进行签名以生成第一签名信息，并将所述第三验证信息、用户公钥和第一签名信息发送至所述移动银行服务器。

31、根据权利要求 30 所述的系统，其特征在于，

所述移动银行服务器，还用于根据存储的所述第一随机加密参数和第二随机加密参数对所述第二验证信息和用户公钥进行加密以生成第四验证信息，并根据所述用户公钥对所述第一签名信息进行验签，并判断所述第三验证信息与所述第四验证信息是否一致，所述

第一签名信息是否通过验签；如果一致并通过验签，则验证通过。

32、根据权利要求 25 或 31 所述的系统，其特征在于，根据所述第一随机加密参数和所述第二随机加密参数对所述第二验证信息和用户公钥进行分段做加密。

33、根据权利要求 24 所述的系统，其特征在于，

5 所述移动终端，还用于接收用户的交易信息，并生成第一随机数，其中所述交易信息至少包括交易账号和交易金额，以及根据所述第一随机数、移动终端的硬件信息、用户私钥、移动银行服务器的公钥及银行综合前置服务器的公钥对所述交易信息进行加密以生成交易报文，并将所述交易报文发送至所述移动银行服务器，其中所述硬件信息为硬件特征信息或硬件特征信息的哈希值；

10 所述移动银行服务器，还用于根据所述移动银行服务器的私钥和存储的所述移动终端的硬件信息对所述交易报文进行解密，并根据所述用户公钥证书进行验签，并在通过验签时，生成加密密钥，并根据所述加密密钥、移动银行服务器的私钥、银行综合前置服务器的公钥和交易信息生成数字信封，并将所述数字信封发送至所述银行综合前置服务器；

15 所述银行综合前置服务器，还用于根据所述银行综合前置服务器的私钥和移动银行服务器的公钥对所述数字信封进行解密获取所述交易信息，并根据所述移动银行服务器的公钥进行验签，并在通过验签后，完成交易。

34、根据权利要求 33 所述的方法，其特征在于，

20 所述移动终端，还用于根据所述银行综合前置服务器的公钥对交易密码或交易密码的哈希值进行加密获得交易密码的密文，并根据所述用户私钥对所述交易信息和所述交易密码的密文进行签名以生成第一数字签名，以及根据所述第一随机数和所述移动终端的硬件信息生成加密参数密钥，并根据所述加密参数密钥对所述交易信息和所述交易密码的密文进行加密以生成第一报文密文，并根据所述移动银行服务器的公钥对所述第一随机数进行加密以生成第一密钥密文，以及将所述第一数字签名、所述第一报文密文和所述第一密钥密文作为所述交易报文发送至所述移动银行服务器。

25 35、根据权利要求 34 所述的系统，其特征在于，

所述移动银行服务器，还用于根据所述移动银行服务器的私钥对所述第一密钥密文进行解密以获取所述第一随机数，并根据所述第一随机数和存储的所述移动终端的硬件信息生成所述加密参数密钥，并根据所述加密参数密钥对所述第一报文密文进行解密以获取所述交易信息和所述交易密码的密文，以及根据存储的所述用户公钥证书对所述第一数字签

名进行验签。

36、根据权利要求 35 所述的系统，其特征在于，

所述移动银行服务器，还用于生成所述加密密钥，并根据所述加密密钥对所述交易信息
和所述交易密码的密文进行加密以生成第二报文密文，以及根据所述银行综合前置服务
5 器的公钥对所述加密密钥进行加密以生成第二密钥密文，并根据所述移动银行服务器的私
钥对所述交易信息和所述交易密码的密文进行签名以生成第二数字签名，以及将所述第二
数字签名、所述第二报文密文和所述第二密钥密文作为所述数字信封发送至所述银行综合
前置服务器。

37、根据权利要求 36 所述的系统，其特征在于，

10 所述银行综合前置服务器，还用于根据所述银行综合前置服务器的私钥对所述第二密
钥密文进行解密以获取所述加密密钥，并根据所述加密密钥对所述第二报文密文进行解密
以获取所述交易信息和所述交易密码的密文，以及根据所述移动银行服务器的公钥对所述
第二数字签名进行验签，并在通过验签时，根据所述交易信息完成交易。

38、根据权利要求 35 所述的系统，其特征在于，所述加密密钥为对称加密密钥。

15 39、根据权利要求 24 所述的系统，其特征在于，

所述移动终端，还用于在预设区域加密存储由所述用户私钥生成的用户私钥文件，并
在所述交易时进行用户身份验证，并在验证通过之后生成第二随机数，根据所述第二随机
数从所述移动银行服务器获取第一私钥保护参数和第二私钥保护参数，并根据所述第二私
钥保护参数解密所述存储的用户私钥文件，并验证解密之后的所述用户私钥文件，以及在
20 所述用户私钥文件通过验证时根据所述用户私钥文件执行交易，并更新私钥保护参数更新
标识，在所述用户私钥文件未通过验证时根据所述第一私钥保护参数解密所述存储的用户
私钥文件，并验证解密之后的所述用户私钥文件，以及在所述用户私钥文件通过验证时根
据所述用户私钥文件执行交易，并更新所述私钥保护参数更新标识，并根据接收到的交易
结果生成更新私钥保护参数，发送所述更新私钥保护参数及所述私钥保护参数更新标识至
25 移动银行服务器，以及根据所述移动银行服务器的更新成功结果，利用更新私钥保护参数
对所述用户私钥重新进行加密存储。

40、根据权利要求 39 所述的系统，其特征在于，

所述移动终端，还用于根据用户私钥保护密钥对所述用户私钥文件进行加密并存储，
所述用户私钥文件包括用户私钥和所述移动终端的硬件信息，以及所述用户私钥保护密钥

为由所述移动终端的硬件信息/硬件特征信息的哈希值的全部或部分信息、登录密码/登陆密码的哈希值的全部或部分信息和私钥保护参数生成。

41、根据权利要求 39 所述的系统，其特征在于，根据解密所述用户私钥文件的所述第一私钥保护参数或第二私钥保护参数更新所述私钥保护参数更新标识。

5 42、根据权利要求 39 所述的系统，其特征在于，

如果所述私钥保护参数更新标识为所述第二私钥保护参数对应的标识，则所述移动银行服务器根据所述更新私钥保护参数更新所述第二私钥保护参数，并根据所述第二私钥保护参数更新所述第一私钥保护参数；

10 如果所述私钥保护参数更新标识为所述第一私钥保护参数对应的标识，则所述移动银行服务器根据所述更新私钥保护参数更新所述第二私钥保护参数；

所述移动银行服务器返回更新成功结果至所述移动终端。

43、根据权利要求 42 所述的系统，其特征在于，

15 所述移动终端，还用于根据所述移动银行服务器的公钥对所述更新私钥保护参数和所述私钥保护参数更新标识进行加密，并将加密之后的所述更新私钥保护参数和所述私钥保护参数更新标识发送至所述移动银行服务器；

所述移动银行服务器，还用于根据所述移动银行服务器的私钥对所述移动终端发送的信息进行解密以获取所述更新私钥保护参数和所述私钥保护参数更新标识。

44、根据权利要求 39 所述的系统，其特征在于，所述移动终端还用于利用所述硬件信息验证解密之后的所述用户私钥文件。

20 45、根据权利要求 39-44 任一项所述的系统，其特征在于，

所述移动终端，还用于根据所述移动银行服务器的公钥对所述第二随机数进行加密，并将加密之后的所述第二随机数发送至所述移动银行服务器；

25 所述移动银行服务器，还用于根据所述移动银行服务器的私钥对所述移动终端发送的加密信息进行解密以获取所述第二随机数，并根据所述第二随机数对所述第一私钥保护参数和所述第二私钥保护参数进行加密，并将加密之后的所述第一私钥保护参数和第二私钥保护参数发送至所述移动终端；

所述移动终端，还用于根据所述第二随机数对所述移动银行服务器发送的信息进行解密以获取所述第一私钥保护参数和第二私钥保护参数。

46、根据权利要求 39-44 任一项所述的系统，其特征在于，所述移动银行服务器与所

述移动终端之间通过短信验证码验证、动态口令验证、电子签名工具验证或交易密码验证的方式验证用户身份。