(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 2 月 23 日 (23.02.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/028595 A1

(51) 国际专利分类号:
G06Q 20/40 (2012.01)

(21) 国际申请号: PCT/CN2016/084107

(22) 国际申请日: 2016 年 5 月 31 日 (31.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510508808.5 2015 年 8 月 18 日 (18.08.2015) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: 赵瑾 (ZHAO, Jin); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: 广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD.); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,

[见续页]

(54) Title: PAYMENT VERIFICATION METHOD, TERMINAL, AND SERVER

(54) 发明名称 : 支付验证方法、终端和服务器

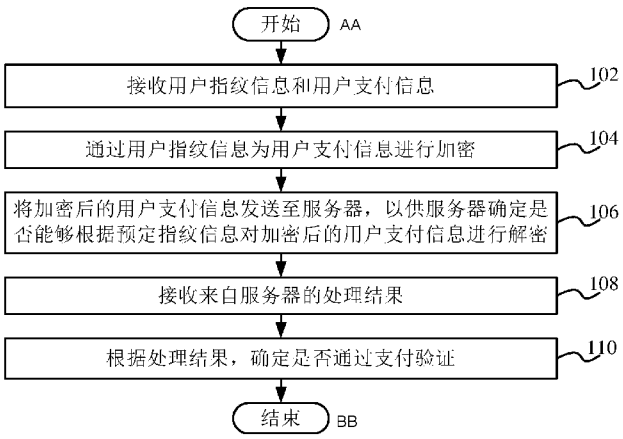


图 1

102 RECEIVE USER FINGERPRINT INFORMATION AND USER PAYMENT INFORMATION
104 ENCRYPT THE USER PAYMENT INFORMATION BY USING THE USER FINGERPRINT INFORMATION
106 SEND THE ENCRYPTED USER PAYMENT INFORMATION TO A SERVER, SUCH THAT THE SERVER DETERMINES WHETHER THE ENCRYPTED USER PAYMENT INFORMATION CAN BE DECRYPTED ACCORDING TO PREDETERMINED FINGERPRINT INFORMATION
108 RECEIVE A PROCESSING RESULT FROM THE SERVER
110 DETERMINE, ACCORDING TO THE PROCESSING RESULT, WHETHER PAYMENT VERIFICATION IS PASSED
AA START
BB END

(57) Abstract: A payment verification method, a terminal, and a server. The payment verification method comprises: receiving user fingerprint information and user payment information (102); encrypting the user payment information by using the user fingerprint information (104); sending the encrypted user payment information to a server, such that the server determines whether the encrypted user payment information can be decrypted according to predetermined fingerprint information (106); receiving a processing result from the server (108); and determining, according to the processing result, whether payment verification is passed (110). By encrypting user payment information by using user fingerprint information and decrypting the encrypted user payment information by using predetermined fingerprint information, it can be accurately determined whether an operation is performed by a user himself/herself, thus improving the security of user payment information and ensuring the security of user payment verification.

(57) 摘要:

[见续页]

WO 2017/028595 A1

IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种支付验证方法、一种终端和一种服务器，其中，支付验证方法包括：接收用户指纹信息和用户支付信息（102）；通过用户指纹信息为用户支付信息进行加密（104）；将加密后的用户支付信息发送至服务器，以供服务器确定是否能够根据预定指纹信息对加密后的用户支付信息进行解密（106）；以及接收来自服务器的处理结果（108）；根据处理结果，确定是否通过支付验证（110）。利用用户指纹信息对用户支付信息进行加密，通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

支付验证方法、终端和服务器

本申请要求于2015年08月18日提交中国专利局，申请号为201510508808.5、发明名称为“支付验证方法、终端和服务器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及终端技术领域，具体而言，涉及一种支付验证方法、一种终端和一种服务器。

背景技术

目前，在用户购买完商品进行付款时，终端都是利用扫描器扫描相应的付款二维码来获取用户的信息和商品的价格，然后，用户就可以输入相应的账号和密码等用户支付信息来进行支付验证。

但是，这种支付验证方式并不能保障用户的账号和信息的安全，另外，即使利用用户手机的动态密码来进行支付验证，也可能会导致用户的账号和信息被盗，同样不能保障用户的账号和信息的安全。

因此，需要一种新的技术方案，能够提高用户支付信息的安全性，以及保障用户进行支付验证的安全。

发明内容

本发明正是基于上述问题，提出了一种新的技术方案，能够提高用户支付信息的安全性，以及保障用户进行支付验证的安全。

有鉴于此，本发明的第一方面提出了一种支付验证方法，用于终端，包括：接收用户指纹信息和用户支付信息；通过所述用户指纹信息为所述用户支付信息进行加密；将加密后的用户支付信息发送至服务器，以供所述服务器确定是否能够根据预定指纹信息对所述加密后的用户支付信息进行解密；以及接收来自所述服务器的处理结果；根据所述处理结果，确定

是否通过支付验证。

在该技术方案中，能够利用用户指纹信息为用户支付信息进行加密，其中，所述用户指纹信息可为多指纹序列，这样，服务器就能够接收到加密后的用户支付信息，然后再根据预先设定的预定指纹信息对该加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，否则不能通过支付验证。其中，用户支付信息包括：用户的账号、支付密码、物品价格以及支付费用等。通过上述技术方案，能够利用用户指纹信息对用户支付信息进行加密，通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，所述用户指纹信息包括一个指纹信息或多个指纹信息，其中，当所述用户指纹信息包括所述多个指纹信息时，所述支付验证方法还包括：按照接收所述多个指纹信息的顺序，为所述多个指纹信息中的每个指纹信息设置顺序标识；以及所述通过所述用户指纹信息为所述用户支付信息进行加密，具体包括：使用具有所述顺序标识的所述多个指纹信息为所述用户支付信息进行加密，以供所述服务器确定是否能够根据具有预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

在该技术方案中，获取到的用户指纹信息可以是一个指纹信息也可以是多个指纹信息，为了进一步提升支付过程的安全性，往往需要获取多个指纹信息。此时，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

本发明的第二方面提出了一种用于支付验证的终端，包括：信息接收单元，接收用户指纹信息和用户支付信息；加密单元，通过所述用户指纹信息为所述用户支付信息进行加密；发送单元，将加密后的用户支付信息发送至服务器，以供所述服务器确定是否能够根据预定指纹信息对所述加密后的用户支付信息进行解密；以及处理结果接收单元，接收来自所述服务器的处理结果；确定单元，根据所述处理结果，确定是否通过支付验证。

在该技术方案中，能够利用用户指纹信息为用户支付信息进行加密，其中，所述用户指纹信息可为多指纹序列，这样，服务器就能够接收到加密后的用户支付信息，然后再根据预先设定的预定指纹信息对该加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，否则不能通过支付验证。其中，用户支付信息包括：用户的账号、支付密码、物品价格以及支付费用等。通过上述技术方案，能够利用用户指纹信息对用户支付信息进行加密，并通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，所述用户指纹信息包括一个指纹信息或多个指纹信息，以及所述终端还包括：顺序标识设置单元，当所述用户指纹信息包括所述多个指纹信息时，按照接收所述多个指纹信息的顺序，为所述多个指纹信息中的每个指纹信息设置顺序标识；以及所述加密单元具体用于：使用具有所述顺序标识的所述多个指纹信息为所述用户支付信息进行加密，以供所述服务器确定是否能够根据具有预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

在该技术方案中，获取到的用户指纹信息可以是一个指纹信息也可以是多个指纹信息，为了进一步提升支付过程的安全性，往往需要获取多个指纹信息。此时，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个

预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

本发明的第三方面提出了一种支付验证方法，用于服务器，所述服务器与上述第二方面中所述的终端相连，包括：接收来自所述终端的加密后的用户支付信息；通过预定指纹信息对所述加密后的用户支付信息进行解密；将解密后的处理结果发送至所述终端，以供所述终端根据所述处理结果确定是否通过支付验证。

在该技术方案中，能够根据用户预先设定的预定指纹信息对加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，如果解密失败，则不能通过支付验证。其中，所述预定指纹信息可为多指纹序列，通过上述技术方案，能够通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，在所述接收来自所述终端的加密后的用户支付信息之前，还包括：根据接收到的第一设置命令，设置一个所述预定指纹信息或多个所述预定指纹信息。

在该技术方案中，用户可以根据自己的实际需要设置一个预定指纹信息也可以设置多个预定指纹信息，其中，如果设置一个预定指纹信息，在进行支付验证时操作简单能够节省支付验证的时间，如果设置多个预定指纹信息，安全系数较高，更能保证在进行支付验证过程中的安全性。

在上述技术方案中，优选地，在所述接收来自所述终端的加密后的用户支付信息之前，当设置有多个所述预定指纹信息时，还包括：多个所述预定指纹信息中的每个所述预定指纹信息设置预定顺序标识；以及所述通过预定指纹信息对所述加密后的用户支付信息进行解密，具体包括：通过具有所述预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

在该技术方案中，在获取该多个用户指纹信息的过程中会有相应的顺

序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

本发明的第四方面提出了一种用于支付验证的服务器，所述服务器与上述第二方面中所述的终端相连，包括：加密信息接收单元，接收来自所述终端的加密后的用户支付信息；解密单元，通过预定指纹信息对所述加密后的用户支付信息进行解密；处理结果发送单元，将解密后的处理结果发送至所述终端，以供所述终端根据所述处理结果确定是否通过支付验证。在该技术方案中，能够根据用户预先设定的预定指纹信息对加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，如果解密失败，则不能通过支付验证。其中，所述预定指纹信息可为多指纹序列，通过上述技术方案，能够通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，还包括：第一设置单元，在所述接收来自所述终端的加密后的用户支付信息之前，根据接收到的第一设置命令，设置一个所述预定指纹信息或多个所述预定指纹信息。

在该技术方案中，用户可以根据自己的实际需要设置一个预定指纹信息也可以设置多个预定指纹信息，其中，如果设置一个预定指纹信息，在进行支付验证时操作简单能够节省支付验证的时间，如果设置多个预定指纹信息，安全系数较高，更能保证在进行支付验证过程中的安全性。

在上述技术方案中，优选地，还包括：第二设置单元，为多个所述预定指纹信息中的每个所述预定指纹信息设置预定顺序标识；以及所述解密单元具体用于：通过具有所述预定顺序标识的多个所述预定指纹信息对所

述加密后的用户支付信息进行解密。

在该技术方案中，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

通过本发明的技术方案，能够利用用户指纹信息对用户支付信息进行加密，通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

附图说明

图 1 示出了根据本发明的一个实施例的支付验证方法的流程图；

图 2 示出了根据本发明的一个实施例的终端的框图；

图 3 示出了根据本发明的另一个实施例的支付验证方法的流程图；

图 4 示出了根据本发明的一个实施例的服务器的框图；

图 5 示出了根据本发明的一个实施例的终端支付验证的流程图。

具体实施方式

为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的支付验证方法的流程图。

如图 1 所示，根据本发明的一个实施例的支付验证方法，用于终端，包括：

步骤 102，接收用户指纹信息和用户支付信息。

步骤 104，通过用户指纹信息为用户支付信息进行加密。

步骤 106，将加密后的用户支付信息发送至服务器，以供服务器确定是否能够根据预定指纹信息对加密后的用户支付信息进行解密。

步骤 108，接收来自服务器的处理结果。

步骤 110，根据处理结果，确定是否通过支付验证。

在该技术方案中，能够利用用户指纹信息为用户支付信息进行加密，其中，所述指纹信息可为多指纹序列，这样，服务器就能够接收到加密后的用户支付信息，然后再根据预先设定的预定指纹信息对该加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，否则不能通过支付验证。其中，用户支付信息包括：用户的账号、支付密码、物品价格以及支付费用等。通过上述技术方案，能够利用用户指纹信息对用户支付信息进行加密，通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，用户指纹信息包括一个指纹信息或多个指纹信息，其中，当用户指纹信息包括多个指纹信息时，支付验证方法还包括：按照接收多个指纹信息的顺序，为多个指纹信息中的每个指纹信息设置顺序标识；以及通过用户指纹信息为用户支付信息进行加密，具体包括：使用具有顺序标识的多个指纹信息为用户支付信息进行加密，以供服务器确定是否能够根据具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密。

在该技术方案中，获取到的用户指纹信息可以是一个指纹信息也可以是多个指纹信息，为了进一步提升支付过程的安全性，往往需要获取多个指纹信息。此时，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这

样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

图 2 示出了根据本发明的一个实施例的终端的框图。

如图 2 所示，根据本发明的一个实施例的终端 200，包括：信息接收单元 202，接收用户指纹信息和用户支付信息；加密单元 204，通过用户指纹信息为用户支付信息进行加密；发送单元 206，将加密后的用户支付信息发送至服务器，以供服务器确定是否能够根据预定指纹信息对加密后的用户支付信息进行解密；以及处理结果接收单元 208，接收来自服务器的处理结果；确定单元 210，根据处理结果，确定是否通过支付验证。

在该技术方案中，能够利用用户指纹信息为用户支付信息进行加密，其中，所述指纹信息可为多指纹序列，这样，服务器就能够接收到加密后的用户支付信息，然后再根据预先设定的预定指纹信息对该加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，否则不能通过支付验证。其中，用户支付信息包括：用户的账号、支付密码、物品价格以及支付费用等。通过上述技术方案，能够利用用户指纹信息对用户支付信息进行加密，并通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，用户指纹信息包括一个指纹信息或多个指纹信息，以及终端 200 还包括：顺序标识设置单元 212，当用户指纹信息包括多个指纹信息时，按照接收多个指纹信息的顺序，为多个指纹信息中的每个指纹信息设置顺序标识；以及加密单元 204 具体用于：使用具有顺序标识的多个指纹信息为用户支付信息进行加密，以供服务器确定是否能够根据具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息

进行解密。

在该技术方案中，获取到的用户指纹信息可以是一个指纹信息也可以是多个指纹信息，为了进一步提升支付过程的安全性，往往需要获取多个指纹信息。此时，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

图 3 示出了根据本发明的另一个实施例的支付验证方法的流程图。

如图 3 所示，根据本发明的另一个实施例的支付验证方法，用于服务器，服务器与图 2 示出的终端 200 相连，包括:

步骤 302，接收来自终端的加密后的用户支付信息。

步骤 304，通过预定指纹信息对加密后的用户支付信息进行解密。

步骤 306，将解密后的处理结果发送至终端，以供终端根据处理结果确定是否通过支付验证。

在该技术方案中，能够根据用户预先设定的预定指纹信息对加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，如果解密失败，则不能通过支付验证。其中，所述预定指纹信息可为多指纹序列，通过上述技术方案，能够通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，在步骤 302 之前，还包括：根据接收到的第一设置命令，设置一个预定指纹信息或多个预定指纹信息。

在该技术方案中，用户可以根据自己的实际需要设置一个预定指纹信息也可以设置多个预定指纹信息，其中，如果设置一个预定指纹信息，在

进行支付验证时操作简单能够节省支付验证的时间，如果设置多个预定指纹信息，安全系数较高，更能保证在进行支付验证过程中的安全性。

在上述技术方案中，优选地，在步骤 302 之前，当设置有多个预定指纹信息时，还包括：为多个预定指纹信息中的每个预定指纹信息设置预定顺序标识；以及步骤 304 具体包括：通过具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密。

在该技术方案中，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

图 4 示出了根据本发明的一个实施例的服务器的框图。

如图 4 所示，根据本发明的一个实施例的服务器 400，服务器 400 与图 2 示出的终端 200 相连，包括：加密信息接收单元 402，接收来自终端的加密后的用户支付信息；解密单元 404，通过预定指纹信息对加密后的用户支付信息进行解密；处理结果发送单元 406，将解密后的处理结果发送至终端，以供终端根据处理结果确定是否通过支付验证。

在该技术方案中，能够根据用户预先设定的预定指纹信息对加密后的用户支付信息进行解密，如果解密成功，则通过支付验证，如果解密失败，则不能通过支付验证。其中，所述预定指纹信息可为多指纹序列，通过上述技术方案，能够通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，保证了用户进行支付验证的安全性。

在上述技术方案中，优选地，还包括：第一设置单元 408，在接收来自终端的加密后的用户支付信息之前，根据接收到的第一设置命令，设置

一个预定指纹信息或多个预定指纹信息。

在该技术方案中，用户可以根据自己的实际需要设置一个预定指纹信息也可以设置多个预定指纹信息，其中，如果设置一个预定指纹信息，在进行支付验证时操作简单能够节省支付验证的时间，如果设置多个预定指纹信息，安全系数较高，更能保证在进行支付验证过程中的安全性。

在上述技术方案中，优选地，还包括：第二设置单元 410，为多个预定指纹信息中的每个预定指纹信息设置预定顺序标识；以及解密单元 404 具体用于：通过具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密。

在该技术方案中，在获取该多个用户指纹信息的过程中会有相应的顺序，就可以根据该顺序为获取到的每个用户指纹信息设置相应的顺序标识，这样就能够利用具有顺序标识的多个用户指纹信息为用户支付信息进行加密，然后，服务器就可以利用用户预先设定的具有预定顺序标识的多个预定指纹信息对加密后的用户支付信息进行解密，如果多个用户指纹信息与多个预定指纹信息一致，并且顺序标识与预定顺序标识也一致，则通过支付验证，否则不能通过支付验证。通过上述技术方案，能够为多个用户指纹信息设置相应的顺序标识，进一步提高了用户支付信息的安全性，以及保障了用户进行支付验证的安全。

图 5 示出了根据本发明的一个实施例的终端支付验证的流程图。

步骤 502，扫描器扫描二维码进行支付。

步骤 504，发出提示信息，提示用户需要输入多指纹序列，其中，多指纹序列指具有预定顺序的多个指纹信息。

步骤 506，获取用户输入的支付账号和密码信息。

步骤 508，通过多指纹序列对用户账户和密码信息进行加密，并将加密后的用户账户和密码信息发送到银行端（即服务器）。

步骤 510，银行端通过用户预先设定的预定多指纹序列，对加密后的用户的账号和密码信息进行解密。其中，预定多指纹序列，用户可以根据自己的实际需要进行自由组合。

步骤 512，判断解密是否成功，当判断结果为是时，进入步骤 514，当

判断结果为否时，进入步骤 516。

步骤 514，支付验证成功。

步骤 516，支付验证失败。

以上结合附图详细说明了本发明的技术方案，通过本发明的技术方案，能够利用用户指纹信息对用户支付信息进行加密，通过预定指纹信息对加密后的用户支付信息进行解密，进而能够准确地确定是否是用户本人进行操作，提高了用户支付信息的安全性，保证了用户进行支付验证的安全性。

在本发明中，术语“第一”、“第二”、“第三”、“第四”仅用于描述的目的，而不能理解为指示或暗示相对重要性；术语“多个”表示两个或两个以上；术语“相连”、“连接”等均应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是直接相连，也可以通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。

在本说明书的描述中，术语“一个实施例”、“另一个实施例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或特点包含于本实用新型的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或实例。而且，描述的具体特征、结构、材料或特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求

1. 一种支付验证方法，用于终端，其特征在于，包括:

接收用户指纹信息和用户支付信息;

通过所述用户指纹信息为所述用户支付信息进行加密;

将加密后的用户支付信息发送至服务器，以供所述服务器确定是否能够根据预定指纹信息对所述加密后的用户支付信息进行解密; 以及

接收来自所述服务器的处理结果;

根据所述处理结果，确定是否通过支付验证。

2. 根据权利要求 1 所述的支付验证方法，其特征在于，所述用户指纹信息包括一个指纹信息或多个指纹信息，其中，当所述用户指纹信息包括所述多个指纹信息时，所述支付验证方法还包括:

按照接收所述多个指纹信息的顺序，为所述多个指纹信息中的每个指纹信息设置顺序标识; 以及

所述通过所述用户指纹信息为所述用户支付信息进行加密，具体包括:

使用具有所述顺序标识的所述多个指纹信息为所述用户支付信息进行加密，以供所述服务器确定是否能够根据具有预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

3. 一种用于支付验证的终端，其特征在于，包括:

信息接收单元，接收用户指纹信息和用户支付信息;

加密单元，通过所述用户指纹信息为所述用户支付信息进行加密;

发送单元，将加密后的用户支付信息发送至服务器，以供所述服务器确定是否能够根据预定指纹信息对所述加密后的用户支付信息进行解密; 以及

处理结果接收单元，接收来自所述服务器的处理结果;

确定单元，根据所述处理结果，确定是否通过支付验证。

4. 根据权利要求 3 所述的终端，其特征在于，所述用户指纹信息包括一个指纹信息或多个指纹信息，以及

所述终端还包括:

顺序标识设置单元，当所述用户指纹信息包括所述多个指纹信息时，按照接收所述多个指纹信息的顺序，为所述多个指纹信息中的每个指纹信息设置顺序标识；以及

所述加密单元具体用于：

使用具有所述顺序标识的所述多个指纹信息为所述用户支付信息进行加密，以供所述服务器确定是否能够根据具有预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

5. 一种支付验证方法，用于服务器，所述服务器与如权利要求 3 或 4 所述的终端相连，其特征在于，包括：

接收来自所述终端的加密后的用户支付信息；

通过预定指纹信息对所述加密后的用户支付信息进行解密；

将解密后的处理结果发送至所述终端，以供所述终端根据所述处理结果确定是否通过支付验证。

6. 根据权利要求 5 所述的支付验证方法，其特征在于，在所述接收来自所述终端的加密后的用户支付信息之前，包括：

根据接收到的第一设置命令，设置一个所述预定指纹信息或多个所述预定指纹信息。

7. 根据权利要求 6 所述的支付验证方法，其特征在于，在所述接收来自所述终端的加密后的用户支付信息之前，当设置有多个所述预定指纹信息时，还包括：

为多个所述预定指纹信息中的每个所述预定指纹信息设置预定顺序标识；以及

所述通过预定指纹信息对所述加密后的用户支付信息进行解密，具体包括：

通过具有所述预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

8. 一种用于支付验证的服务器，所述服务器与如权利要求 3 或 4 所述的终端相连，其特征在于，包括：

加密信息接收单元，接收来自所述终端的加密后的用户支付信息；

解密单元，通过预定指纹信息对所述加密后的用户支付信息进行解密；

处理结果发送单元，将解密后的处理结果发送至所述终端，以供所述终端根据所述处理结果确定是否通过支付验证。

9. 根据权利要求 8 所述的服务器，其特征在于，还包括：

第一设置单元，在所述接收来自所述终端的加密后的用户支付信息之前，根据接收到的第一设置命令，设置一个所述预定指纹信息或多个所述预定指纹信息。

10. 根据权利要求 9 所述的服务器，其特征在于，还包括：

第二设置单元，为多个所述预定指纹信息中的每个所述预定指纹信息设置预定顺序标识；以及

所述解密单元具体用于：

通过具有所述预定顺序标识的多个所述预定指纹信息对所述加密后的用户支付信息进行解密。

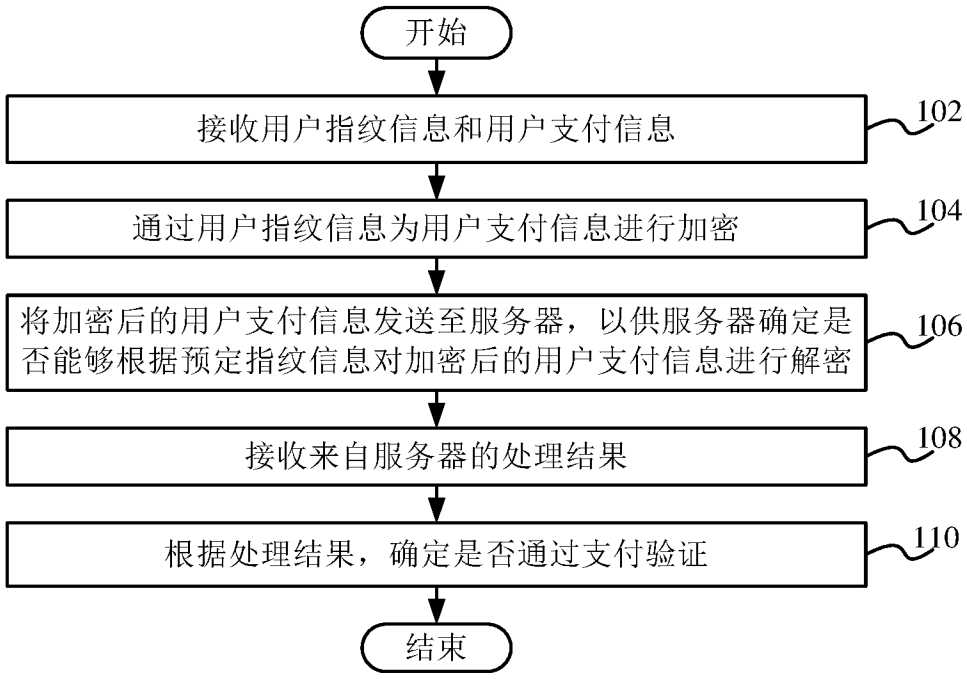

开始
接收用户指纹信息和用户支付信息
102
通过用户指纹信息为用户支付信息进行加密
104
将加密后的用户支付信息发送至服务器，以供服务器确定是否能够根据预定指纹信息对加密后的用户支付信息进行解密
106
接收来自服务器的处理结果
108
根据处理结果，确定是否通过支付验证
110
结束

图 1


信息接收单元202
处理结果接收单元208
加密单元204
确定单元210
发送单元206
顺序标识设置单元212
终端200

图 2

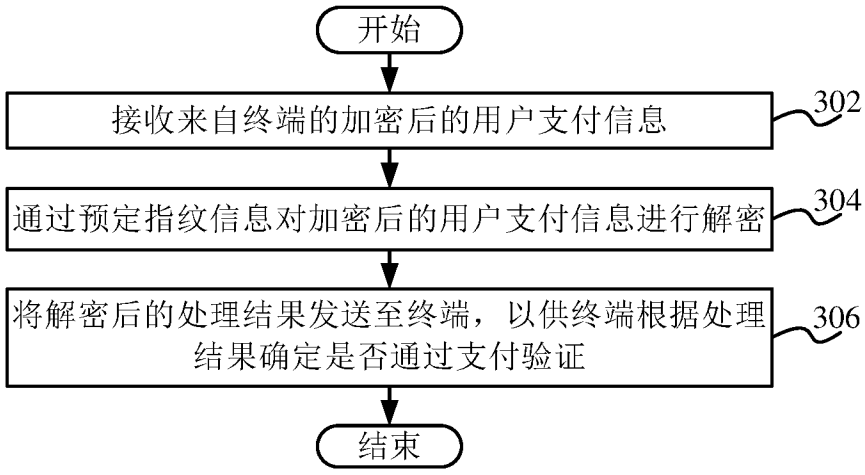

开始
接收来自终端的加密后的用户支付信息
302
通过预定指纹信息对加密后的用户支付信息进行解密
304
将解密后的处理结果发送至终端，以供终端根据处理结果确定是否通过支付验证
306
结束

图 3

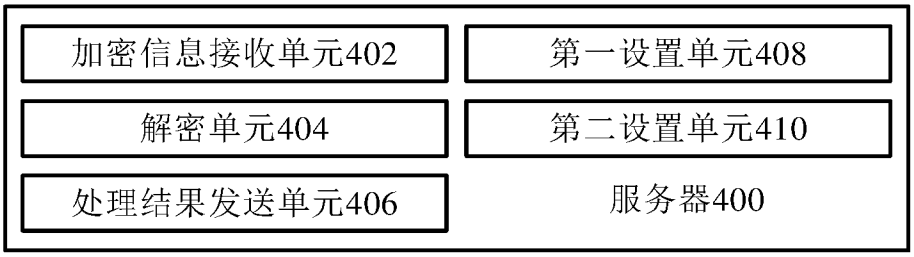

加密信息接收单元402
第一设置单元408
解密单元404
第二设置单元410
处理结果发送单元406
服务器400

图 4

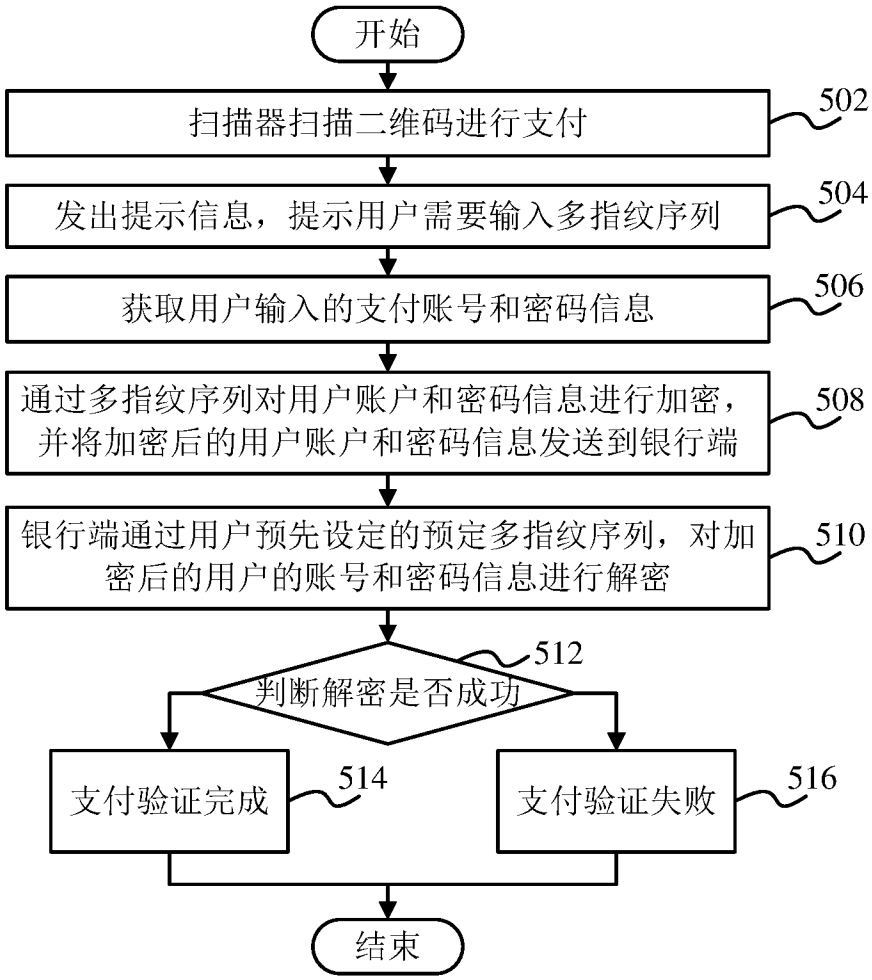

开始
扫描器扫描二维码进行支付
502
发出提示信息，提示用户需要输入多指纹序列
504
获取用户输入的支付账号和密码信息
506
通过多指纹序列对用户账户和密码信息进行加密，并将加密后的用户账户和密码信息发送到银行端
508
银行端通过用户预先设定的预定多指纹序列，对加密后的用户的账号和密码信息进行解密
510
判断解密是否成功
512
支付验证完成
514
支付验证失败
516
结束

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/084107

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: terminal, server, pay, authentication, verification, encipherment, fingerprint, sequential

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105139205 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 09 December 2015 (09.12.2015), claims 1-10	1-10
Y	CN 104580125 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 29 April 2015 (29.04.2015), description, paragraphs [0115]-[0135], and figures 4 and 6	1-10
Y	CN 103873260 A (LENOVO (BEIJING) CO., LTD.), 18 June 2014 (18.06.2014), description, paragraphs [0111]-[0117]	1-10
A	JP 2010055156 A (HITACHI SOFTWARE ENG.CO., LTD.), 11 March 2010 (11.03.2010), the whole document	1-10
A	KR 20140101322 A (LEE, D.H.), 19 August 2014 (19.08.2014), the whole document	1-10
A	US 8550339 B1 (BANK OF AMERICA CORPORATION), 08 October 2013 (08.10.2013), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 July 2016 (26.07.2016)	**30 August 2016 (30.08.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **SHI, Wenqing** Telephone No.: (86-10) **010-62413411**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/084107

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105139205 A	09 December 2015	None	
CN 104580125 A	29 April 2015	HK 1206886 A1	15 January 2016
		US 2015134530 A1	14 May 2015
		WO 2015062308 A1	07 May 2015
		TW 201516908 A	01 May 2015
CN 103873260 A	18 June 2014	None	
JP 2010055156 A	11 March 2010	None	
KR 20140101322 A	19 August 2014	WO 2016006924 A1	14 January 2016
US 8550339 B1	08 October 2013	None	

国际检索报告

国际申请号
PCT/CN2016/084107

A. 主题的分类

G06Q 20/40(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNKI,CNPAT,WPI,EPODOC:终端，服务器，支付，验证，加密，指纹，顺序，terminal, server, pay, authentication, verification, encipherment, fingerprint, sequential

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 105139205 A (宇龙计算机通信科技深圳有限公司) 2015年 12月 9日 (2015-12-09) 权利要求1-10	1-10
Y	CN 104580125 A (腾讯科技深圳有限公司) 2015年 4月 29日 (2015-04-29) 说明书第[0115]-[0135]段、附图4、6	1-10
Y	CN 103873260 A (联想北京有限公司) 2014年 6月 18日 (2014-06-18) 说明书第[0111]-[0117]段	1-10
A	JP 2010055156 A (HITACHI SOFTWARE ENG. CO., LTD.) 2010年 3月 11日 (2010-03-11) 全文	1-10
A	KR 20140101322 A (LEE, DO HUN) 2014年 8月 19日 (2014-08-19) 全文	1-10
A	US 8550339 B1 (BANK OF AMERICA CORPORATION) 2013年 10月 8日 (2013-10-08) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 7月 26日	2016年 8月 30日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	史文庆 电话号码 (86-10)010-62413411

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/084107

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105139205	A	2015年 12月 9日		无		
CN	104580125	A	2015年 4月 29日	HK	1206886	A1	2016年 1月 15日
				US	2015134530	A1	2015年 5月 14日
				WO	2015062308	A1	2015年 5月 7日
				TW	201516908	A	2015年 5月 1日
CN	103873260	A	2014年 6月 18日		无		
JP	2010055156	A	2010年 3月 11日		无		
KR	20140101322	A	2014年 8月 19日	WO	2016006924	A1	2016年 1月 14日
US	8550339	B1	2013年 10月 8日		无		