

(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
2020 年 6 月 4 日 (04.06.2020)



(10) 国际公布号
WO 2020/108155 A1

(51) 国际专利分类号:
G06Q 20/16 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/32 (2012.01)

(21) 国际申请号: PCT/CN2019/111670

(22) 国际申请日: 2019 年 10 月 17 日 (17.10.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811457439.1 2018 年 11 月 30 日 (30.11.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛
大开曼资本大厦一座四层 847 号邮箱,
Grand Cayman (KY)。

(72) 发明人: 陈成 (CHEN, Cheng); 中国浙江省杭州市
市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴
集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL
PROPERTY LAW CORPORATION); 中国北京市
海淀区上地三街 9 号嘉华大厦 B 座 409,
Beijing 100085 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) Title: PAYMENT METHOD AND APPARATUS

(54) 发明名称: 支付方法和装置

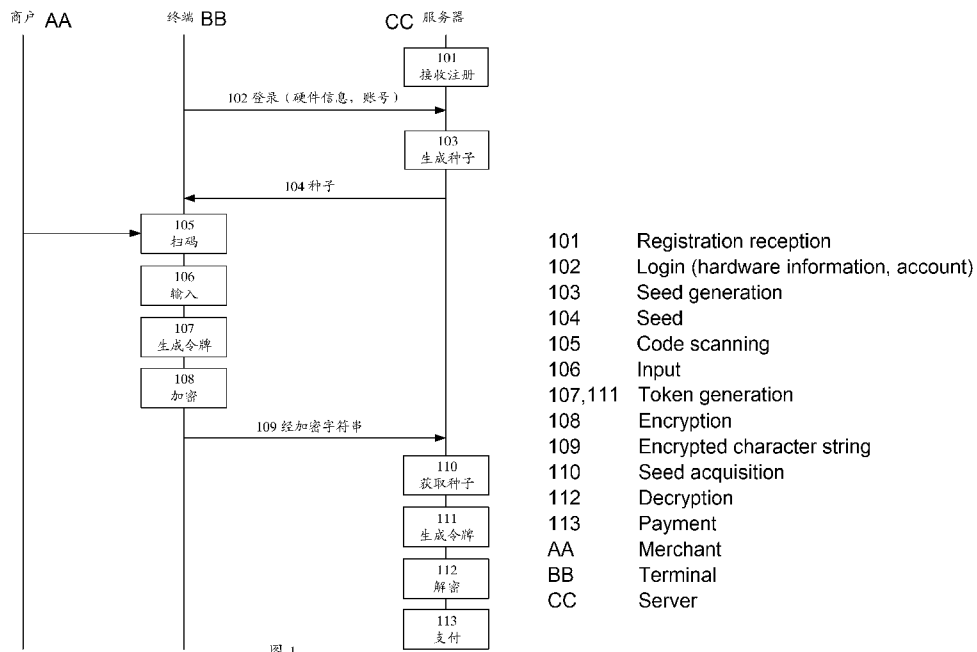


图 1

(57) Abstract: A method for payment, comprising receiving a seed from a server (202); generating a token (205); using the token to encrypt a character string comprising an entity ID and a transaction amount, so as to obtain an encrypted character string (206); and transmitting the encrypted character string using a short message or voice call (207). By means of the method, a user can successfully make a payment when the wireless network is unavailable or weak.

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, 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))。

(57) 摘要: 一种用于支付的方法, 包括: 接收来自服务器的种子(202); 生成令牌(205); 使用所述令牌对
包括实体ID和交易金额的字符串进行加密得到经加密字符串(206); 以及使用短信或语音呼叫来传送所述经
加密字符串(207)。使用所述方法, 在没有无线网络或者网络较弱的情况下, 用户也能成功进行支付。

支付方法和装置

技术领域

[01] 本发明主要涉及互联网应用技术领域，尤其涉及一种弱网环境下的支付方法。

背景技术

- 5 [02] 随着移动支付的不断发展和普及，越来越多的线下商户引入自助支付的方式。扫描付款码（例如，图形码）是一种常见的支付方式。扫码支付方式是用户终端扫描商户的图形码，获取商户的信息，进入支付页面，并在该支付页面中输入支付金额。用户终端将包含各种信息的支付请求通过无线网络（例如，3G、4G 通信网络）传给服务器进行支付。该方法也广泛应用于共享单车的扫码开锁。
- 10 [03] 但是有的时候，商户或共享单车所处位置的 3G、4G 通信网络信号较弱甚至没有信号，这给用户支付造成了不便。

发明内容

- [04] 本发明要解决的技术问题是提供一种在弱网环境下也能成功进行支付的方案。在网络环境不稳定时，用户终端通过短信或手机电话向服务器发送包含商户信息和金额信息
- 15 的字符串，服务器通过短信或电话识别出用户账号信息，由此创建交易。

[05] 为解决上述技术问题，本发明提供了一种用于支付的方法，包括：

[06] 接收来自服务器的种子；

[07] 使用所述种子、终端硬件信息和当前时间定时来生成令牌；

- [08] 使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串；以
- 20 及

[09] 使用短信或语音呼叫来传送所述经加密字符串。

[10] 可任选地，该方法进一步包括：

[11] 向所述服务器传送用户账号和所述终端硬件信息以供所述服务器生成所述种子。

[12] 可任选地，所述用户账号和所述终端硬件信息是使用无线网络传送的。

- 25 [13] 可任选地，该方法进一步包括：

[14]检测扫码指令;

[15]响应于所述扫码指令而使用摄像装置扫码商户的图形码; 以及

[16]对所述图形码进行解析以获取所述实体 ID。

[17]可任选地, 该方法进一步包括:

- 5 [18]响应于获取所述实体 ID 而展示支付界面, 所述支付界面包括输入框以供用户输入支付金额和/或密码。

[19]可任选地, 所述终端硬件信息包括 IMEI、或 IMSI。

[20]本发明还提供了一种用于支付的方法, 包括:

[21]通过短信或语音呼叫接收来自终端的经加密字符串;

- 10 [22]获取与所述终端相对应的种子;

[23]生成令牌; 以及

[24]使用所述令牌对所述经加密字符串进行解密。

[25]可任选地, 该方法进一步包括,

[26]接收来自所述终端的手机号、用户账号和终端硬件信息;

- 15 [27]使用所述终端硬件信息和当前时间定时生成种子; 以及

[28]将所述种子发送给所述终端。

[29]可任选地, 该方法进一步包括, 将所述种子与所述手机号和/或用户账号相关联地存储。

[30]可任选地, 该方法进一步包括, 将所生成的种子与所述手机号相关联地存储。

- 20 [31]可任选地, 所述获取与所述终端相对应的种子包括:

[32]识别所述终端的手机号; 以及

[33]根据所述手机号获取与所述终端相对应的种子。

[34]可任选地, 所述生成令牌包括:

[35]使用所述种子、所述终端硬件信息和当前时间定时来生成令牌。

- 25 [36]可任选地, 所述用户账号和所述终端硬件信息是使用无线网络从所述终端接收的。

[37]可任选地，所述终端硬件信息包括 IMEI、或 IMSI。

[38]本发明进一步提供了一种用于支付的设备，包括：

[39]用于接收来自服务器的种子的装置；

[40]用于使用所述种子、终端硬件信息和当前时间定时来生成令牌的装置；

5 [41]用于使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串的装置；以及

[42]用于使用短信或语音呼叫来传送所述经加密字符串的装置。

[43]可任选地，该设备进一步包括：

10 [44]用于向所述服务器传送用户账号和所述终端硬件信息以供所述服务器生成所述种子的装置。

[45]可任选地，所述用户账号和所述终端硬件信息是使用无线网络传送的。

[46]可任选地，该设备进一步包括：

[47]用于检测扫码指令的装置；

[48]用于响应于所述扫码指令而使用摄像装置扫码商户的图形码的装置；以及

15 [49]用于对所述图形码进行解析以获取所述实体 ID 的装置。

[50]可任选地，该设备进一步包括：

[51]用于响应于获取所述实体 ID 而展示支付界面，所述支付界面包括输入框以供用户输入支付金额和/或密码的装置。

[52]可任选地，所述终端硬件信息包括 IMEI、或 IMSI。

20 [53]本发明进一步提供了一种用于支付的设备，包括：

[54]用于通过短信或语音呼叫接收来自终端的经加密字符串的装置；

[55]用于获取与所述终端相对应的种子的装置；

[56]用于生成令牌的装置；以及

[57]用于使用所述令牌对所述经加密字符串进行解密的装置。

25 [58]可任选地，该设备进一步包括，

[59]用于接收来自所述终端的手机号、用户账号和终端硬件信息的装置;

[60]用于使用所述终端硬件信息和当前时间定时生成种子的装置; 以及

[61]用于将所述种子发送给所述终端的装置。

5 [62]可任选地, 该设备进一步包括, 用于将所述种子与所述手机号和/或用户账号相关联地存储的装置。

[63]可任选地, 该设备进一步包括, 用于将所生成的种子与所述手机号相关联地存储的装置。

[64]可任选地, 所述用于获取与所述终端相对应的种子的装置包括:

[65]用于识别所述终端的手机号的装置; 以及

10 [66]用于根据所述手机号获取与所述终端相对应的种子的装置。

[67]可任选地, 所述用于生成令牌的装置包括:

[68]用于使用所述种子、所述终端硬件信息和当前时间定时来生成令牌的装置。

[69]可任选地, 所述用户账号和所述终端硬件信息是使用无线网络从所述终端接收的。

[70]可任选地, 所述终端硬件信息包括 IMEI、或 IMSI。

15 [71]本发明又提供了一种用于支付的装置, 包括:

[72]处理器; 以及

[73]被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理器执行以下操作:

[74]向服务器传送手机号、用户账号和终端硬件信息;

20 [75]接收来自服务器的种子;

[76]生成令牌;

[77]使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串; 以及

[78]使用短信或语音呼叫来传送所述经加密字符串。

25 [79]本发明进一步提供了一种用于支付的装置, 包括:

[80]处理器; 以及

[81]被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[82]通过短信或语音呼叫接收来自终端的经加密字符串；

[83]获取与所述终端相对应的种子；

5 [84]生成令牌；以及

[85]使用所述令牌对所述经加密字符串进行解密。

附图说明

[86]图 1 示出了根据本发明的支付方法的消息流程图。

[87]图 2 示出了根据本发明的一方面的由终端执行的支付方法的流程图。

10 [88]图 3 示出了根据本发明的一方面的由服务器执行的支付方法的流程图。

[89]图 4 示出了根据本发明的各方面的由终端执行的支付方法的流程图。

[90]图 5 示出了根据本发明的各方面的由服务器执行的支付方法的流程图。

具体实施方式

[91]为了让本发明的上述目的、特征和优点能更明显易懂，以下结合附图对本发明的具体
15 实施方式作详细说明。

[92]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它不同于在此描述的其它方式来实施，因此本发明不受下面公开的具体实施例的限制。

[93]图 1 示出了根据本发明的支付方法的消息流程图。

20 [94]本发明的支付系统包括用户终端、服务器、以及实体（商户）设备。

[95]用户终端可以是移动终端（例如手机）。用户终端可具有摄像头以用于扫描图像码。用户终端可以发送文本信息（例如，短信）和进行语音呼叫，还可以通过无线网络（例如，WiFi、3G、4G 等）进行通信。

[96]服务器可以是支付后台，例如支付宝后台服务器。服务器可以接收来自用户终端的
25 支付请求，并执行终端向商户的支付（例如，向商户转账）。

[97] 商户设备可以是商户的图形码，该图形码包括商户信息，例如，商户 ID（标识符）。

[98] 以下描述根据本发明的在弱网环境下的支付方法的消息流程图。

[99] 在 101，服务器接收来自用户的注册消息。该注册消息中包括终端的手机号（移动电话 SIM 卡号码）和用户账号。

5 [100] 一般而言，用户在设备上安装应用（APP）客户端并且第一次启用该客户端之后，会向服务器发送注册消息，该注册消息可包括手机终端的手机号和用户申请的账号。该账号例如是用户自己定义的账号、邮箱、用户手机号等等。

[101] 该注册消息可以来自用户进行注册的设备，可以是手机终端，也可以是其它计算设备。

10 [102] 服务器接收到注册消息之后，可将手机号和用户账号相关联地进行存储。

[103] 在 102，终端向服务器发送终端硬件信息和用户账号。

[104] 例如，终端在用户初次登录应用客户端时，可通过无线网络向服务器发送终端硬件信息和用户账号。

[105] 该终端硬件信息是终端固有的特性，例如，对于终端而言唯一性的信息。终端
15 硬件信息可包括 IMEI（International Mobile Equipment Identity，国际移动设备识别码）、
IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码）等等。

[106] 服务器随后将终端硬件信息和用户账号相关联地存储起来。

[107] 在步骤 101 和 102 之后，服务器可将终端硬件信息与用户账号及手机号相关联地存储。

20 [108] 请注意，虽然图 1 中将步骤 101 和 102 分为两个步骤描述，但它们也可以合并成一个步骤。例如，在用户在终端上打开应用客户端注册时，可以同时向服务器发送终端的手机号、终端硬件信息和用户账号。由此服务器可以建立终端硬件信息和手机号、用户账号的映射。

[109] 在 103，服务器根据接收到的终端硬件信息和当前时间定时生成种子，并将种子
25 与用户账号和/或手机号相关联地进行存储。

[110] 服务器可以使用某种算法来生成种子。该算法例如是 hash 算法。

[111] 当前时间值可以是服务器在 103 生成种子的时间。

[112] 种子进一步可以定期更新。例如，种子可以按一定时间间隔生成，例如，每隔一分钟根据终端硬件信息和当前时间定时生成一次。

[113] 进一步，生成种子的算法也可定期更新，以保护种子的安全性，防止外部攻击。

5 [114] 服务器需要将种子与手机号的映射关系进行存储。例如，终端可通过终端硬件信息和手机号的映射关系查找与生成种子所使用的终端硬件信息相关联的手机号，将所生成的种子与手机号进行关联生成映射。

[115] 该映射关系可以存储在安全存储区中。该安全存储区可以是服务器中的某块存储单元，需保证该存储单元中存储的内容难以被该账号和/或手机号对应的客户端之外的其它装置窃取。

10 [116] 在 104，服务器向终端发送所生成的种子。服务器可通过无线网络向终端发送所生成的种子。

[117] 终端通过无线网络接收种子并存储所接收到的种子。

[118] 以上步骤 103-104 描述了服务器生成和分发种子的过程。

15 [119] 在用户在商铺中购物时，选购完商品进行结算时，可以扫描商户的图形码来完成支付过程。

[120] 在 105，终端检测到扫码指令之后，调用摄像装置来扫描商户的图形码，并对图形码进行解析，获取与图形码对应的商户 ID。

[121] 商户的图形码中编码有唯一的商户 ID。终端通过扫描图形码来获取商户 ID。

20 [122] 扫码指令可以是用户在客户端应用上点击“扫一扫”，当终端检测到扫码指令之际，即调用摄像应用来扫描图形码，以获取对应的商户 ID。图形码可以是二维码，包括但不限于，QR (Quick Response, 快速反应) 码、PDF417 (Portable Document Format 417, 便携式数据文件) 二维条码、Datamatrix (一种矩阵式二维条码) 二维条码等等。本发明的图形码是按照预设的图形编码规则对商户 ID 进行编码处理后获得的图形编码。例如，如果图形码是 QR 码，则该图形码为采用 QR 编码规则对商户 ID 进行编码处理
25 获得的图形编码。在另一示例中，如果图形码为 PDF417 码，则图形码为采用 PDF417 编码规则对商户 ID 进行编码处理获得的图形编码。

[123] 所述摄像应用可以是能够对图形码进行扫描和解析的应用。本发明实施例中，所述摄像应用可以为终端系统中的摄像应用，例如，手机系统自带的摄像头。本步骤中，

调用所述摄像应用扫描到完整的所述图形码后，所述摄像应用可以采用预设的编码规则所述图形码进行解析，获得商户 ID。例如，若所述图形码为 QR 码，所述摄像应用可根据 QR 编码规则对所述图形码进行解析，获得商户 ID；若所述图形码为 PDF417 码，所述摄像应用可根据 PDF417 编码规则对所述图形码进行解析，获得商户 ID。

5 [124] 在本说明书实施例中，为商户设置图形码。当用户需要向商户支付时，可以操作支付客户端扫描该商户的图形码。

[125] 支付客户端接收到购物扫描操作触发之后，调用摄像装置扫描商户的图形码，这里的购物扫描操作触发，可以是来自用户操作的触发，如将用户点击应用程序中的“扫一扫”按钮作为支付扫描操作触发。

10 [126] 在 106，终端响应于 105 的扫描操作而展示输入框以供用户输入。

[127] 终端通过扫码获取商户 ID 之后，可以进一步展示支付操作界面，以便用户进行支付。在一方面，该支付界面可显示商户标识和输入框，提示用户输入要向商户支付的金额。在交易需要支付密码的情况下，该支付界面还可提示用户输入密码。

15 [128] 请注意，以上描述了终端扫码商户二维码获得商户 ID，并且提示用户输入金额和密码（若需要）的方案。在替换实现中，也可以是商户在图形码生成设备上输入用户要支付的金额，从而所生成的图形码中既包括商户 ID、又包括用户需要支付的进而。终端可扫描该图形码来获得商户 ID 和金额信息。

[129] 如果商户将支付金额嵌入在图形码中并且支付不需要密码（即，免密码支付），则步骤 106 可省略。

20 [130] 在 107，终端根据存储的种子、终端硬件信息和时间定时来生成令牌（token）。

[131] 例如，终端可以使用合适的算法（例如，hash 算法等）将种子、终端硬件信息和当前时间定时计算得到令牌。

[132] 该当前时间定时可以是终端在 107 生成令牌的时间。

[133] 一般而言，仅仅终端和服务端可获得该令牌，其它设备难以获取该令牌。

25 [134] 在 108，终端使用商户 ID、输入的交易金额、以及所生成的令牌来生成经加密字符串。

[135] 具体而言，终端可以先将商户 ID 和输入的交易金额形成一字符串，使用所生成的令牌对该字符串加密以生成经加密字符串。

[136] 在需要支付密码的情况下，终端可将商户 ID、输入的交易金额和支付密码形成一字符串，使用所生成的令牌对该字符串加密以生成经加密字符串。加密算法可以是对称加密算法，例如，AES（Advanced Encryption Standard，高级加密标准）算法。

[137] 在 109，终端通过短信或手机呼叫将 108 处生成的经加密字符串发送给服务器。

5 [138] 终端可以通过短信将经加密的字符串发送给服务器。例如，用户在短信编辑框中输入字符串并通过短信发送。例如，终端可以响应于检测不到无线网络而自动调用短信接口，填入字符串，让用户确认是否发送或者自动发送。

[139] 替换地，终端也可以响应于检测不到无线网络而手机呼叫服务器端，人工输入字符串；用户还可以通过语音将字符串读出来，服务器进行语音识别以获得该字符串。

10 [140] 在 110，服务器识别出终端的手机号，并且根据手机号获取终端的种子。

[141] 例如，服务器可以根据手机号识别出用户的账号，然后根据账号得到所存储的终端的种子。

[142] 在 111，服务器使用获取的种子、终端硬件信息和当前时间定时来生成令牌。

15 [143] 例如，服务器可以使用与终端相同的算法、利用获取的种子、终端硬件信息和当前时间定时来生成令牌。

[144] 该当前时间定时可以是服务器在步骤 111 生成令牌的时间。

[145] 在 112，服务器使用所生成的令牌对接收到的经加密字符串解密，得到商户 ID 和交易金额。

20 [146] 服务器可使用终端在步骤 108 使用的相同的算法对经加密字符串解密。该算法可以是对称加密算法，例如，AES（Advanced Encryption Standard，高级加密标准）算法。

[147] 在 113，服务器可使用商户 ID、用户账号（在 110 处通过短信或手机呼叫的手机号识别出的）以及交易金额进行支付操作。

[148] 图 2 示出了根据本发明的一方面的由终端执行的支付方法的流程图。

25 [149] 在步骤 201，终端向服务器发送终端硬件信息和用户账号。

[150] 例如，终端在登录应用客户端时，可通过无线网络向服务器发送终端硬件信息和用户账号。

[151] 服务器一般在先前的注册消息中会接收到用户的终端手机号和用户账号并将终端手机号和用户账号相关联地存储。在接收到来自终端的终端硬件信息和用户账号，服务器可通过用户账号来建立终端手机号和终端硬件信息的映射。

[152] 在步骤 202，终端接收来自服务器的种子。

5 [153] 该种子可以是服务器使用终端硬件信息和当前时间定时来生成的。

[154] 在 203，终端检测到扫码指令之后，调用摄像装置来扫描商户的图形码。

[155] 终端可以对图形码进行解析，获取与图形码对应的商户 ID。商户的图形码中可编码有唯一的商户 ID。终端通过扫描商户的图形码来获取商户 ID。

[156] 在金额信息被编码在图形码的情形中，终端还可以从图形码中解析出金额信息。

10 [157] 在 204，终端响应于扫描操作而展示支付界面以供用户输入。

[158] 终端获取商户 ID 之后，可以进一步展示支付操作界面，以使用户进行支付。

[159] 例如，该支付界面可显示商户标识和输入框，提示用户输入要向商户支付的金额和支付密码（若需要）。

[160] 在 205，终端根据接收到的种子、终端硬件信息和当前时间定时来生成令牌。

15 [161] 例如，终端可以使用合适的算法（例如，hash 算法等）将种子、终端硬件信息和当前时间定时计算得到令牌。终端可将商户 ID、交易金额和支付密码（若需要）形成一字符串，使用所生成的令牌对该字符串加密以生成经加密字符串

[162] 一般而言，仅仅终端和服务端可获得该令牌，其它设备难以获取该令牌。

[163] 在 206，终端使用商户 ID、输入的交易金额、以及令牌来生成经加密字符串。

20 [164] 具体而言，该经加密字符串是使用令牌对商户 ID 和交易金额进行加密来生成的。

[165] 加密算法可以是对称加密算法，例如 AES（Advanced Encryption Standard，高级加密标准）算法。

[166] 在 207，终端将所生成的经加密字符串发送给服务器以进行支付。

25 [167] 终端可以通过短信将经加密的字符串发送给服务器。例如，用户在短信编辑框中输入字符串并通过短信发送。

[168] 替换地，终端也可以手机呼叫服务器端，人工输入字符串；用户还可以通过语音将字符串读出来，服务器进行语音识别获得字符串。

[169] 图 3 示出了根据本发明的一方面的由服务器执行的支付方法的流程图。

[170] 在步骤 301, 服务器接收终端手机号 (移动电话 SIM 卡号码) 和用户账号。

[171] 终端手机号 (移动电话 SIM 卡号码) 和用户账号例如可以在注册消息中接收。

5 [172] 一般而言, 用户在设备上安装应用 (APP) 客户端并第一次启用该客户端之后, 会向服务器发送注册消息, 该注册消息可包括终端的手机号和用户申请的账号。该注册消息可以来自用户进行注册的设备, 可以是手机终端, 也可以是其它计算设备。

[173] 在 302, 服务器接收来自终端的终端硬件信息和用户账号。

[174] 例如, 终端在登录应用客户端时, 可通过无线网络向服务器发送终端硬件信息和用户账号。

10 [175] 在 303, 服务器使用接收到的终端硬件信息和当前时间定时生成种子, 并将种子与账号和/或手机号相关联地进行存储。

[176] 服务器可以使用恰当的算法来生成种子。该算法例如是 hash 算法。当前时间值可以是服务器生成种子的时间。

15 [177] 种子可以定期更新。例如, 种子可以按一定时间间隔更新, 例如, 每隔一分钟根据终端硬件信息和当前时间定时生成一次。

[178] 进一步, 生成种子的算法也可定期更新, 以保护种子的安全性, 防止外部攻击。

[179] 服务器需要将种子与账号和/或手机号的映射关系进行存储, 例如存储在安全存储区, 该安全存储区可以是终端中的某块存储单元, 需保证该存储单元中存储的内容难以被该账号和/或手机号对应的客户端之外的其它装置窃取。

20 [180] 在 304, 服务器通过无线网络将所生成的种子发送给终端。

[181] 在 305, 服务器接收来自终端的经加密字符串。

[182] 具体而言, 服务器通过短信或手机呼叫接收来自终端的经加密字符串。

[183] 在 306, 服务器获取终端对应的种子。

25 [184] 具体而言, 服务器通过短信或手机呼叫提取出终端的手机号, 根据手机号来查找终端对应的种子。

[185] 在 307, 服务器使用种子、终端硬件信息和当前时间定时来生成令牌。

[186] 例如, 服务器可以使用与终端相同的算法, 利用种子、终端硬件信息和当前时

间定时来生成令牌。

[187] 在 308，服务器使用所生成的令牌对接收到的经加密字符串解密，得到商户 ID 和交易金额。

[188] 在 309，服务器可使用商户 ID、用户账号以及交易金额进行支付操作。

5 [189] 图 4 示出了根据本发明的各方面的由终端执行的支付方法的流程图。

[190] 在步骤 401，终端接收来自服务器的种子。

[191] 步骤 401 可对应于如图 1 所示的步骤 104。

[192] 该种子可以是服务器根据先前从终端接收到的终端硬件信息和当前时间定时生成的。

10 [193] 在步骤 402，终端生成令牌。

[194] 在一方面，终端可以使用接收到的种子、终端硬件信息和当前时间定时来生成令牌。

[195] 在步骤 403，终端使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串。

15 [196] 终端可以检测扫码指令，响应于检测到扫码指令而使用摄像装置扫码商户的图形码，以及对图形码进行解析以获取实体 ID 和/或交易金额。

[197] 终端也可以在输入框中接收用户输入的交易金额。进一步，终端可以在输入框中接收用户输入的支付密码。

20 [198] 终端可使用步骤 402 中生成的令牌对包括实体 ID、交易金额和支付密码（若需要）的字符串进行加密得到经加密字符串。

[199] 在步骤 404，终端使用短信或语音呼叫来传送经加密字符串。

[200] 图 5 示出了根据本发明的各方面的由服务器执行的支付方法的流程图。

[201] 在步骤 501，服务器通过短信或语音呼叫接收来自终端的经加密字符串。

[202] 在步骤 502，服务器获取与该终端相对应的种子。

25 [203] 服务器可以通过步骤 501 中的短信或语音呼叫终端的手机号，并且根据手机号获取与终端相对应的种子。

[204] 在步骤 503, 服务器生成令牌。

[205] 服务器可以使用种子、终端硬件信息和当前时间定时来生成令牌。

[206] 在步骤 504, 服务器使用令牌对经加密字符串进行解密。

5 [207] 可任选地, 在 501 之前, 服务器可以接收终端的手机号、用户账号和终端硬件信息; 使用终端硬件信息和当前时间定时生成种子; 以及将种子发送给所述终端以供终端生成经加密字符串。

10 [208] 本文结合附图阐述的说明描述了示例配置而不代表可被实现或者落在权利要求的范围内的所有示例。本文所使用的术语“示例性”意指“用作示例、实例或解说”, 而并不意指“优于”或“胜过其他示例”。本详细描述包括具体细节以提供对所描述的技术的理解。然而, 可以在没有这些具体细节的情况下实践这些技术。在一些实例中, 众所周知的结构和设备以框图形式示出以避免模糊所描述的示例的概念。

15 [209] 在附图中, 类似组件或特征可具有相同的附图标记。此外, 相同类型的各个组件可通过在附图标记后跟随短划线以及在类似组件之间进行区分的第二标记来加以区分。如果在说明书中仅使用第一附图标记, 则该描述可应用于具有相同的第一附图标记的类似组件中的任何一个组件而不论第二附图标记如何。

20 [210] 结合本文中的公开描述的各种解说性框以及模块可以用设计成执行本文中描述的功能的通用处理器、DSP、ASIC、FPGA 或其他可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合来实现或执行。通用处理器可以是微处理器, 但在替换方案中, 处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可被实现为计算设备的组合 (例如, DSP 与微处理器的组合、多个微处理器、与 DSP 核心协同的一个或多个微处理器, 或者任何其他此类配置)。

25 [211] 本文中所描述的功能可以在硬件、由处理器执行的软件、固件、或其任何组合中实现。如果在由处理器执行的软件中实现, 则各功能可以作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。其他示例和实现落在本公开及所附权利要求的范围内。例如, 由于软件的本质, 以上描述的功能可使用由处理器执行的软件、硬件、固件、硬连线或其任何组合来实现。实现功能的特征也可物理地位于各种位置, 包括被分布以使得功能的各部分在不同的物理位置处实现。另外, 如本文 (包括权利要求中) 所使用的, 在项目列举 (例如, 以附有诸如“中的至少一个”或“中的一个或多个”之类的措辞的项目列举) 中使用的“或”指示包含性列举, 以使得例如 A、B 或 C 中的至

少一个的列举意指 A 或 B 或 C 或 AB 或 AC 或 BC 或 ABC (即, A 和 B 和 C)。同样, 如本文所使用的, 短语“基于”不应被解读为引述封闭条件集。例如, 被描述为“基于条件 A”的示例性步骤可基于条件 A 和条件 B 两者而不脱离本公开的范围。换言之, 如本文所使用的, 短语“基于”应当以与短语“至少部分地基于”相同的方式来解读。

- 5 [212] 计算机可读介质包括非瞬态计算机存储介质和通信介质两者, 其包括促成计算机程序从一地向另一地转移的任何介质。非瞬态存储介质可以是能被通用或专用计算机访问的任何可用介质。作为示例而非限定, 非瞬态计算机可读介质可包括 RAM、ROM、电可擦除可编程只读存储器 (EEPROM)、压缩盘 (CD) ROM 或其他光盘存储、磁盘存储或其他磁存储设备、或能被用来携带或存储指令或数据结构形式的期望程序代码手
- 10 段且能被通用或专用计算机、或者通用或专用处理器访问的任何其他非瞬态介质。任何连接也被正当地称为计算机可读介质。例如, 如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线 (DSL)、或诸如红外、无线电、以及微波之类的无线技术从 web 网站、服务器、或其它远程源传送而来的, 则该同轴电缆、光纤电缆、双绞线、数字订户线 (DSL)、或诸如红外、无线电、以及微波之类的无线技术就被包括在介质的定义之
- 15 中。如本文所使用的盘 (disk) 和碟 (disc) 包括 CD、激光碟、光碟、数字通用碟 (DVD)、软盘和蓝光碟, 其中盘常常磁性地再现数据而碟用激光来光学地再现数据。以上介质的组合也被包括在计算机可读介质的范围内。

- [213] 提供本文的描述是为了使得本领域技术人员能够制作或使用本公开。对本公开的各种修改对于本领域技术人员将是显而易见的, 并且本文中定义的普适原理可被应用
- 20 于其他变形而不会脱离本公开的范围。由此, 本公开并非被限定于本文所描述的示例和设计, 而是应被授予与本文所公开的原理和新颖特征相一致的最广范围。

权利要求书

1. 一种用于支付的方法，包括：
接收来自服务器的种子；
使用所述种子、终端硬件信息和当前时间定时来生成令牌；
5 使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串；以及
使用短信或语音呼叫来传送所述经加密字符串。
2. 根据权利要求 1 所述的方法，其特征在于，进一步包括：
向所述服务器传送用户账号和所述终端硬件信息以供所述服务器生成所述种子。
- 10 3. 根据权利要求 2 所述的方法，其特征在于，所述用户账号和所述终端硬件信息是使用无线网络传送的。
4. 根据权利要求 1 所述的方法，其特征在于，进一步包括：
检测扫码指令；
响应于所述扫码指令而使用摄像装置扫码商户的图形码；以及
15 对所述图形码进行解析以获取所述实体 ID。
5. 根据权利要求 4 所述的方法，其特征在于，进一步包括：
响应于获取所述实体 ID 而展示支付界面，所述支付界面包括输入框以供用户输入
支付金额和/或密码。
6. 根据权利要求 1 所述的方法，其特征在于，所述终端硬件信息包括 IMEI、或 IMSI。
- 20 7. 一种用于支付的方法，包括：
通过短信或语音呼叫接收来自终端的经加密字符串；
获取与所述终端相对应的种子；
生成令牌；以及
使用所述令牌对所述经加密字符串进行解密。
- 25 8. 根据权利要求 7 所述的方法，其特征在于，进一步包括，
接收所述终端的手机号、用户账号和终端硬件信息；
使用所述终端硬件信息和当前时间定时生成种子；以及
将所述种子发送给所述终端。
9. 根据权利要求 8 所述的方法，其特征在于，进一步包括，将所述种子与所述手机
30 号和/或用户账号相关联地存储。
10. 根据权利要求 9 所述的方法，其特征在于，进一步包括，将所生成的种子与所

述手机号相关联地存储。

11. 根据权利要求 10 所述的方法, 其特征在于, 所述获取与所述终端相对应的种子包括:

识别所述终端的手机号; 以及

5 根据所述手机号获取与所述终端相对应的种子。

12. 根据权利要求 9 所述的方法, 其特征在于, 所述生成令牌包括:

使用所述种子、所述终端硬件信息和当前时间定时来生成令牌。

13. 根据权利要求 9 所述的方法, 其特征在于, 所述用户账号和所述终端硬件信息是使用无线网络从所述终端接收的。

10 14. 根据权利要求 9 所述的方法, 其特征在于, 所述终端硬件信息包括 IMEI、或 IMSI。

15. 一种用于支付的设备, 包括:

用于接收来自服务器的种子的装置;

用于使用所述种子、终端硬件信息和当前时间定时来生成令牌的装置;

用于使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串

15 的装置; 以及

用于使用短信或语音呼叫来传送所述经加密字符串的装置。

16. 根据权利要求 15 所述的设备, 其特征在于, 进一步包括:

用于向所述服务器传送用户账号和所述终端硬件信息以供所述服务器生成所述种子的装置。

20 17. 根据权利要求 16 所述的设备, 其特征在于, 所述用户账号和所述终端硬件信息是使用无线网络传送的。

18. 根据权利要求 15 所述的设备, 其特征在于, 进一步包括:

用于检测扫码指令的装置;

用于响应于所述扫码指令而使用摄像装置扫码商户的图形码的装置; 以及

25 用于对所述图形码进行解析以获取所述实体 ID 的装置。

19. 根据权利要求 18 所述的设备, 其特征在于, 进一步包括:

用于响应于获取所述实体 ID 而展示支付界面, 所述支付界面包括输入框以供用户输入支付金额和/或密码的装置。

30 20. 根据权利要求 15 所述的设备, 其特征在于, 所述终端硬件信息包括 IMEI、或 IMSI。

21. 一种用于支付的设备, 包括:

用于通过短信或语音呼叫接收来自终端的经加密字符串的装置；

用于获取与所述终端相对应的种子的装置；

用于生成令牌的装置；以及

用于使用所述令牌对所述经加密字符串进行解密的装置。

- 5 22. 根据权利要求 21 所述的设备，其特征在于，进一步包括，
用于接收来自所述终端的手机号、用户账号和终端硬件信息的装置；
用于使用所述终端硬件信息和当前时间定时生成种子的装置；以及
用于将所述种子发送给所述终端的装置。

- 10 23. 根据权利要求 22 所述的设备，其特征在于，进一步包括，用于将所述种子与所
述手机号和/或用户账号相关联地存储的装置。

24. 根据权利要求 23 所述的设备，其特征在于，进一步包括，用于将所生成的种子
与所述手机号相关联地存储的装置。

25. 根据权利要求 24 所述的设备，其特征在于，所述用于获取与所述终端相对应的
种子的装置包括：

- 15 用于识别所述终端的手机号的装置；以及
用于根据所述手机号获取与所述终端相对应的种子的装置。

26. 根据权利要求 23 所述的设备，其特征在于，所述用于生成令牌的装置包括：
用于使用所述种子、所述终端硬件信息和当前时间定时来生成令牌的装置。

- 20 27. 根据权利要求 23 所述的设备，其特征在于，所述用户账号和所述终端硬件信息
是使用无线网络从所述终端接收的。

28. 根据权利要求 23 所述的设备，其特征在于，所述终端硬件信息包括 IMEI、或
IMSI。

29. 一种用于支付的装置，包括：

处理器；以及

- 25 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理
器执行以下操作：

接收来自服务器的种子；

生成令牌；

使用所述令牌对包括实体 ID 和交易金额的字符串进行加密得到经加密字符串；以

- 30 及

使用短信或语音呼叫来传送所述经加密字符串。

30. 一种用于支付的装置，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

- 5 通过短信或语音呼叫接收来自终端的经加密字符串；
- 获取与所述终端相对应的种子；
- 生成令牌；以及
- 使用所述令牌对所述经加密字符串进行解密。

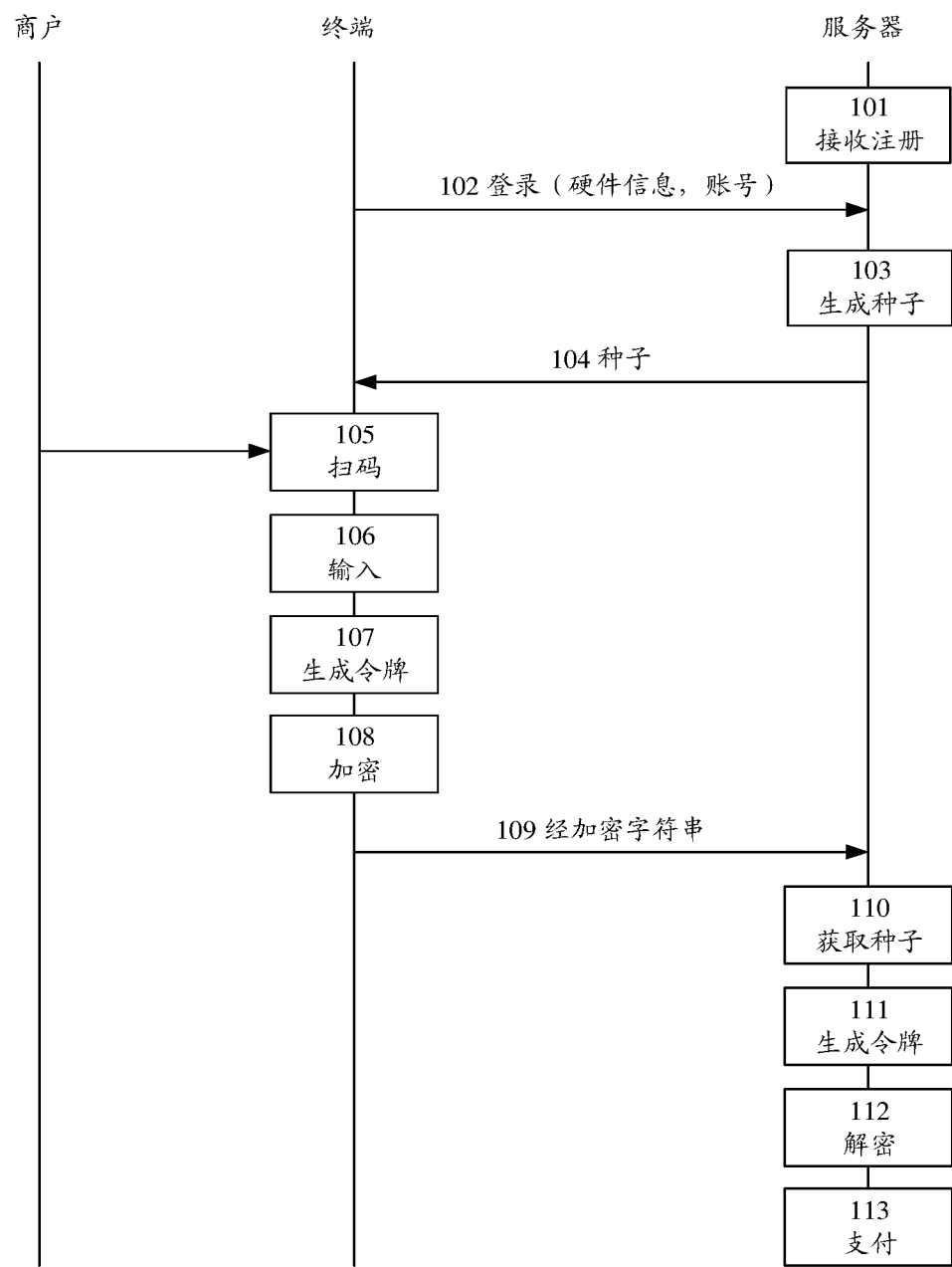


图 1

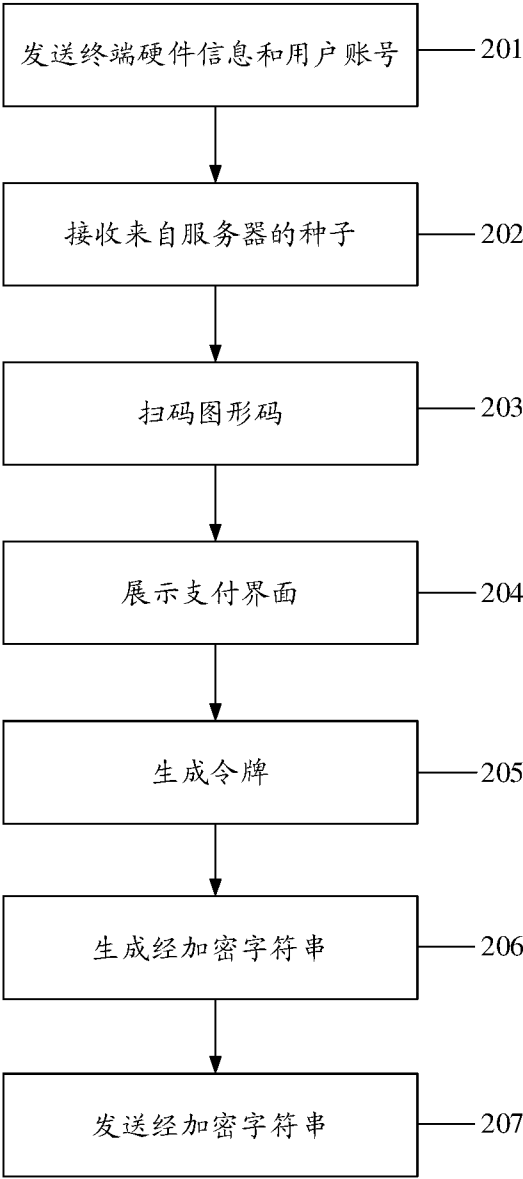


图 2

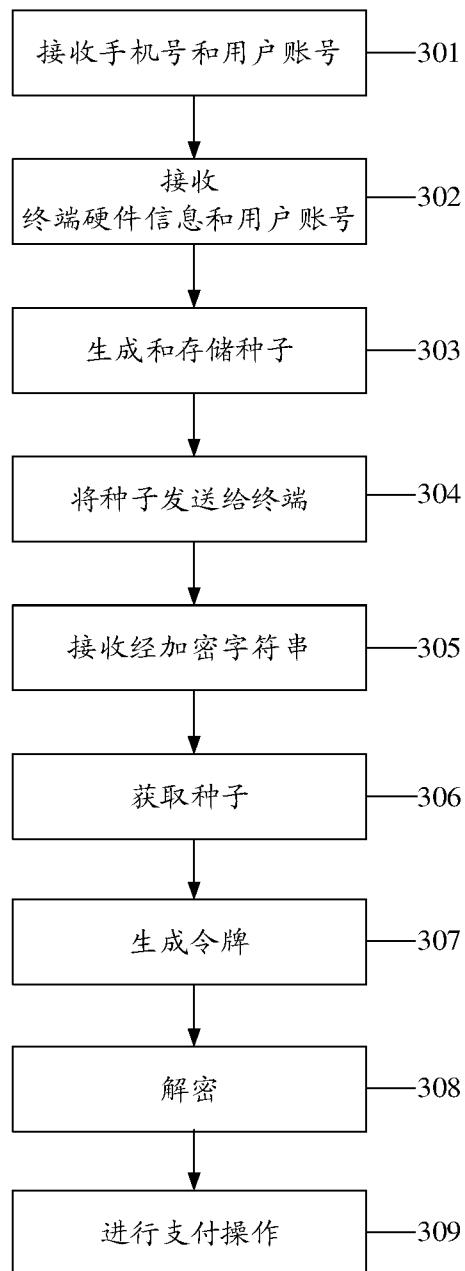


图 3

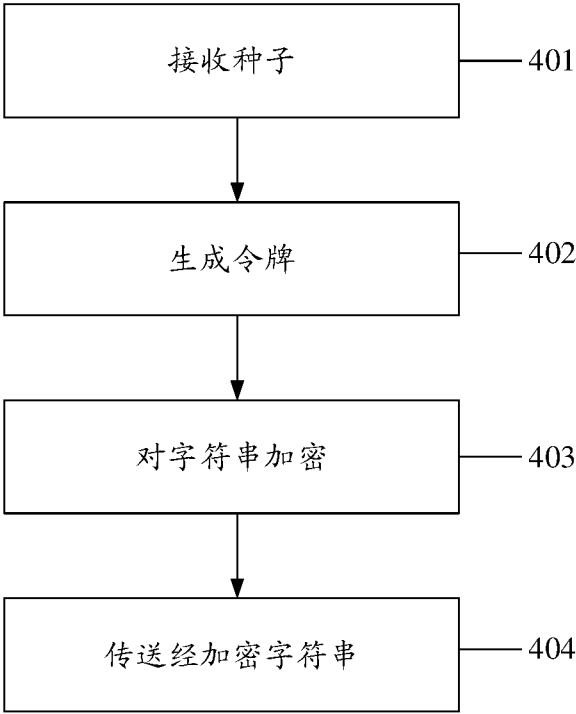


图 4

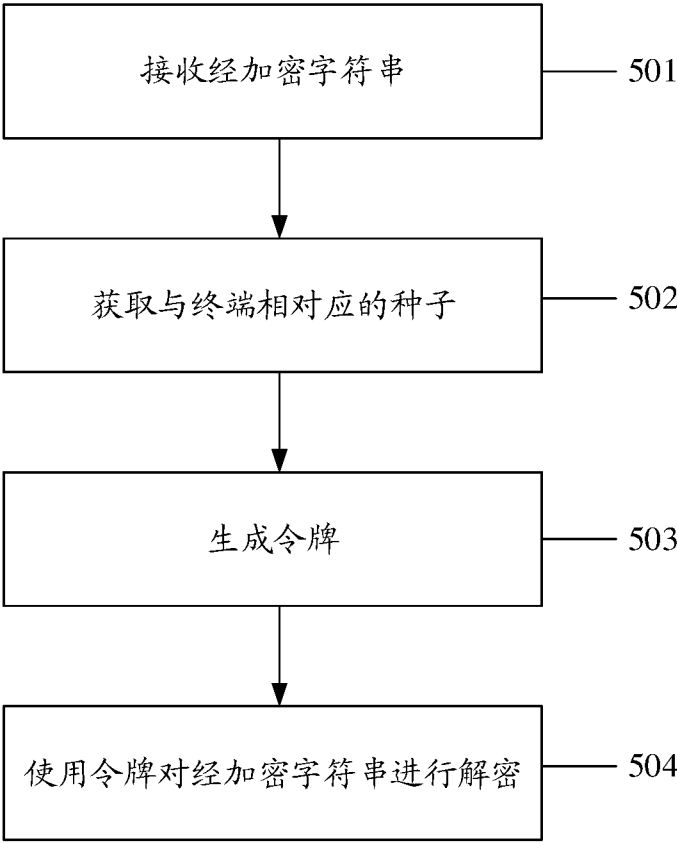


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/111670

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/16(2012.01)i; G06Q 20/32(2012.01)i; G06Q 20/38(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)

CNPAT, EPODOC, WPI, CNKI: 种子, 令牌, 动态, 口令, 验证, 随机数, 密钥, 加密, 短信, 短消息, 硬件识别码, seed, token, authority, random, key, rings, message, ID, IMEI, IMSI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109583872 A (ALIBABA GROUP HOLDING LIMITED) 05 April 2019 (2019-04-05) claims 1-30	1-30
Y	CN 104702580 A (BEIJING ANXUNBEN SCIENCE & TECH CO., LTD.) 10 June 2015 (2015-06-10) description, paragraphs [0010]-[0056], and figures 1 and 2	1-30
Y	CN 105099673 A (ALIBABA GROUP HOLDING LIMITED) 25 November 2015 (2015-11-25) description, paragraphs [0088]-[0125]	1-30
Y	CN 104331801 A (CHONGQING ZHITAO INFORMATION TECHNOLOGY CENTRE) 04 February 2015 (2015-02-04) description, paragraphs [0009]-[0015]	1-30
A	CN 101232631 A (ALIBABA CORPORATION) 30 July 2008 (2008-07-30) entire document	1-30
A	CN 103929402 A (SHENZHEN TENCENT COMPUTER SYSTEMS CO., LTD.) 16 July 2014 (2014-07-16) entire document	1-30



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

06 January 2020

Date of mailing of the international search report

15 January 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/111670

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109583872	A	05 April 2019	None			
CN	104702580	A	10 June 2015	TW	201524177	A	16 June 2015
CN	105099673	A	25 November 2015	WO	2015160711	A1	22 October 2015
				TW	201540040	A	16 October 2015
				US	2017223016	A1	03 August 2017
				KR	20160144991	A	19 December 2016
				US	2015295921	A1	15 October 2015
				JP	2017518559	A	06 July 2017
				HK	1213380	A1	30 June 2016
				EP	3132342	A1	22 February 2017
				IN	201617034547	A	17 February 2017
CN	104331801	A	04 February 2015	None			
CN	101232631	A	30 July 2008	WO	2008089684	A1	31 July 2008
				JP	2010517390	A	20 May 2010
				EP	2128808	A1	02 December 2009
				US	2010082462	A1	01 April 2010
				HK	1120982	A1	23 December 2011
CN	103929402	A	16 July 2014	US	2015312265	A1	29 October 2015
				WO	2014108003	A1	17 July 2014
				HK	1200989	A1	14 August 2015

国际检索报告

国际申请号

PCT/CN2019/111670

A. 主题的分类

G06Q 20/16(2012.01)i; G06Q 20/32(2012.01)i; G06Q 20/38(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))

CNPAT, EPDOC, WPI, CNKI:种子, 令牌, 动态, 口令, 验证, 随机数, 密钥, 加密, 短信, 短消息, 硬件识别码, seed, token, authority, random, key, rings, message, ID, IMEI, IMSI

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 109583872 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 权利要求1-30	1-30
Y	CN 104702580 A (北京安讯奔科技有限责任公司) 2015年 6月 10日 (2015 - 06 - 10) 说明书第[0010]-[0056]段, 附图1-2	1-30
Y	CN 105099673 A (阿里巴巴集团控股有限公司) 2015年 11月 25日 (2015 - 11 - 25) 说明书第[0088]-[0125]段	1-30
Y	CN 104331801 A (重庆智韬信息技术中心) 2015年 2月 4日 (2015 - 02 - 04) 说明书第[0009]-[0015]段	1-30
A	CN 101232631 A (阿里巴巴公司) 2008年 7月 30日 (2008 - 07 - 30) 全文	1-30
A	CN 103929402 A (深圳市腾讯计算机系统有限公司) 2014年 7月 16日 (2014 - 07 - 16) 全文	1-30

☐ 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

2020年 1月 6日

国际检索报告邮寄日期

2020年 1月 15日

ISA/CN的名称和邮寄地址

中国国家知识产权局(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

受权官员

孙娟

电话号码 (86-10)53961383

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/111670

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	109583872	A	2019年 4月 5日	无			
CN	104702580	A	2015年 6月 10日	TW	201524177	A	2015年 6月 16日
CN	105099673	A	2015年 11月 25日	WO	2015160711	A1	2015年 10月 22日
				TW	201540040	A	2015年 10月 16日
				US	2017223016	A1	2017年 8月 3日
				KR	20160144991	A	2016年 12月 19日
				US	2015295921	A1	2015年 10月 15日
				JP	2017518559	A	2017年 7月 6日
				HK	1213380	A1	2016年 6月 30日
				EP	3132342	A1	2017年 2月 22日
				IN	201617034547	A	2017年 2月 17日
CN	104331801	A	2015年 2月 4日	无			
CN	101232631	A	2008年 7月 30日	WO	2008089684	A1	2008年 7月 31日
				JP	2010517390	A	2010年 5月 20日
				EP	2128808	A1	2009年 12月 2日
				US	2010082462	A1	2010年 4月 1日
				HK	1120982	A1	2011年 12月 23日
CN	103929402	A	2014年 7月 16日	US	2015312265	A1	2015年 10月 29日
				WO	2014108003	A1	2014年 7月 17日
				HK	1200989	A1	2015年 8月 14日