

(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 4 月 16 日 (16.04.2020)



(10) 国际公布号
WO 2020/073715 A1

(51) 国际专利分类号:
G06K 17/00 (2006.01)

(21) 国际申请号: PCT/CN2019/097095

(22) 国际申请日: 2019 年 7 月 22 日 (22.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811187031.7 2018年10月12日 (12.10.2018) 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)。

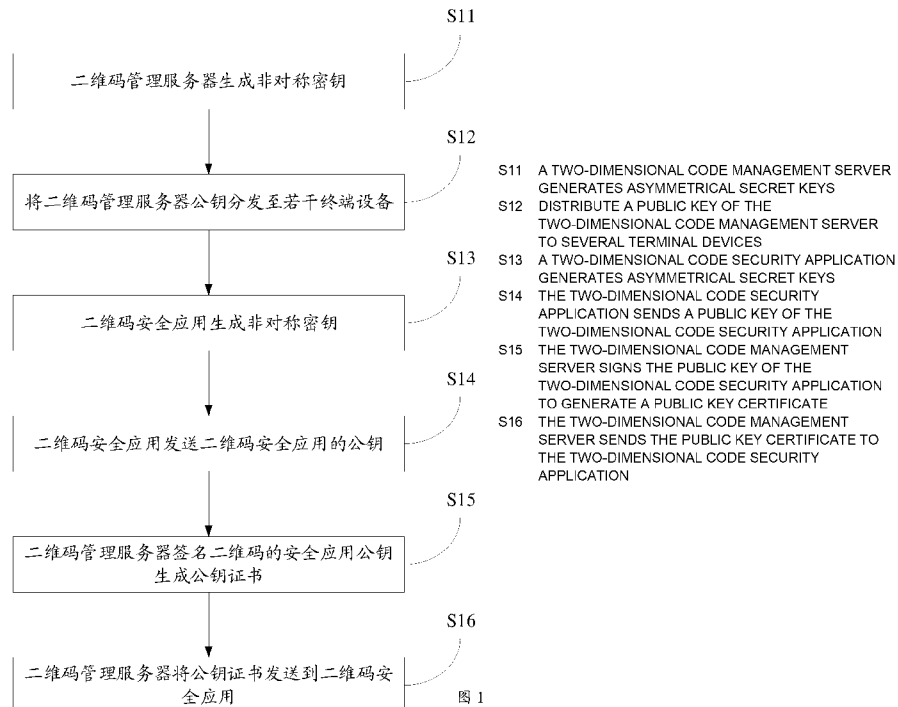
(72) 发明人: 孙曦(SUN, Xi); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 落红卫(LUO, Hongwei); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(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,

(54) Title: TWO-DIMENSIONAL CODE ANTI-COUNTERFEITING METHOD, DEVICE AND SYSTEM BASED ON SECURITY APPLICATION

(54) 发明名称: 基于安全应用的二维码防伪方法、设备及系统



(57) Abstract: Disclosed are a two-dimensional code anti-counterfeiting method, device and system based on a security application. The method comprises: a two-dimensional code security application receiving a request for generating two-dimensional code information data (S62); the two-dimensional code security application signing two-dimensional code service information according to a private key of the two-dimensional code security application (S63); and the two-dimensional code security application sending the two-dimensional information data (S64), wherein the two-dimensional code security application has asymmetrical secret keys composed of a public

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, 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))。

key of the two-dimensional code security application and the private key of the two-dimensional code security application, and the two-dimensional code information data includes the two-dimensional code service information and a signature of the two-dimensional code service information by the two-dimensional code security application.

(57) 摘要: 一种基于安全应用的二维码防伪方法、设备及系统。该方法包括: 二维码安全应用接收生成二维码信息数据的请求(S62); 二维码安全应用根据二维码安全应用的私钥对二维码业务信息进行签名(S63); 二维码安全应用发送二维码信息数据(S64); 其中, 二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥; 所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

基于安全应用的二维码防伪方法、设备及系统

技术领域

[01] 本申请涉及安全领域，尤其涉及基于安全应用的二维码防伪方法、设备及系统。

背景技术

- 5 [02] 随着移动互联网的发展，二维码得到了广泛的应用，例如扫码打开共享单车、扫描支付等等。为了提高二维码的安全性，也有些企业提供动态的二维码，动态二维码中的数据随着时间会进行更新，展示变化的二维码。但是，目前市场上的二维码验证解决方案，二维码信息本身没有防伪能力，即通过解码设备解析二维码以后，直接得到明文
10 的二维码数据，该二维码数据和业务信息数据一致，扫码设备无法在本地验证二维码信息的合法性。为了验证二维码信息的合法性，需要将二维码信息发送到后台服务器，依赖于后台服务器的风险控制能力进行安全防护。但在此过程中，有可能因为无法识别二维码中信息的合法性，导致访问恶意网站或者执行了恶意程序，进而对用户造成损害。

发明内容

- 15 [03] 本申请实施例提供一种基于安全应用的二维码防伪方法、设备及系统，用于解决二维码安全性低的问题。

[04] 本申请实施例采用下述技术方案：

[05] 本申请实施例提供了一种基于安全应用的二维码防伪方法，所述方法包括：

[06] 二维码安全应用接收生成二维码信息数据的请求；

[07] 二维码安全应用根据二维码安全应用的私钥对二维码业务信息进行签名；

- 20 [08] 二维码安全应用发送二维码信息数据；

[09] 其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

[10] 本申请实施例提供了一种二维码读取方法，所述方法包括：

- 25 [11] 扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的

签名;

[12] 验证所述二维码业务信息的签名, 确认所述二维码业务信息。

[13] 本申请提供了一种基于安全应用的二维码防伪方法, 所述方法包括:

[14] 二维码展示模块发送生成二维码信息数据的请求;

5 [15] 二维码安全应用接收生成二维码信息数据的请求;

[16] 二维码安全应用根据二维码安全应用的私钥对二维码业务信息进行签名;

[17] 二维码安全向所述二维码展示模块发送二维码信息数据;

[18] 所述二维码展示模块以二维码的方式展示所述二维码信息数据;

10 [19] 二维码读取设备扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名;

[20] 二维码读取设备验证所述二维码业务信息的签名, 确认所述二维码业务信息;

[21] 其中, 二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥; 所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

15 [22] 本申请提供了一种二维码防伪设备, 该设备包括二维码安全模块;

[23] 二维码安全模块, 还用于接收生成二维码信息数据的请求; 根据二维码安全应用的私钥对二维码业务信息进行签名; 发送二维码信息数据;

20 [24] 其中, 二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥; 所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

[25] 本申请实施例提供了一种二维码防伪设备, 该设备包括安全芯片和存储器, 所述存储器上存储有二维码安全程序;

[26] 所述安全芯片, 用于执行所述二维码安全程序以实现根据权利要求 1 所述的方法。

25 [27] 本申请实施例提供了一种二维码防伪设备, 该设备包括处理器和存储器, 所述存储器存储有二维码安全程序;

[28] 所述处理器, 用于执行所述二维码安全程序以实现所述的方法。

[29] 本申请实施例提供了一种二维码防伪设备，所述设备包括：

[30] 请求接收模块，用于接收生成二维码信息数据的请求；

[31] 二维码业务信息签名模块，用于根据二维码安全应用的私钥对二维码业务信息进行签名；

5 [32] 二维码信息数据发送模块，用于发送二维码信息数据；

[33] 其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

[34] 本申请实施例提供了一种二维码读取设备，该二维码读取设备包括：

10 [35] 扫描模块，用于扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名；

[36] 验证模块，用于验证所述二维码业务信息的签名，确认所述二维码业务信息。

[37] 本申请实施例提供了一种二维码读取设备，其特征在于，所述设备包括处理器和存储器，所述存储器上存储有程序；

15 [38] 所述处理器，用于执行所述程序以实现所述的方法。

[39] 本申请实施例提供了一种二维码防伪系统，该系统包括所述的设备以及所述的二维码读取设备。

[40] 本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：

20 [41] 本申请实施例通过安全芯片或者可信执行环境对二维码的业务数据进行签名，提高了二维码的安全性，并通过证书的使用可以使得二维码读取设备可以在本地对二维码的合法性进行验证，降低了风险发生的概率。

附图说明

[42] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

25 [43] 图 1 为本申请第一实施例提供的证书分发流程图；

[44] 图 2 为本申请第二实施例的二维码防伪方法示意图；

- [45] 图 3 为本申请第三实施例的二维码防伪方法示意图;
- [46] 图 4 为本申请第四实施例的二维码展示流程示意图;
- [47] 图 5 为本申请第五实施例的二维码读取流程示意图;
- [48] 图 6 为本申请第六实施例的二维码防伪方法示意图;
- 5 [49] 图 7 为本申请第七实施例的二维码防伪设备示意图;
- [50] 图 8 为本申请第八实施例的二维码防伪设备示意图;
- [51] 图 9 为本申请第九实施例的二维码防伪设备示意图;
- [52] 图 10 为本申请第十实施例的二维码防伪设备示意图;
- [53] 图 11 为本申请第十一实施例的二维码防伪设备示意图;
- 10 [54] 图 12 为本申请第十二实施例的二维码生成和展示系统示意图;
- [55] 图 13 为本申请第十三实施例的二维码防伪系统示意图。

具体实施方式

- [56] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申
- 15 请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[57] 以下结合附图，详细说明本申请实施例提供的技术方案。

[58] 第一实施例

[59] 如图 1 所示，本申请实施公开了一种用于二维码的证书分发方法，具体包括：

- 20 [60] 步骤 S11，二维码管理服务器生成非对称密钥，包括二维码管理服务器公钥 Public_Key_Server 和二维码管理服务器私钥 Private_Key_Server; 在实际应用的过程中，如果使用 RSA 算法来生成密钥，其一般由公钥和模值，以及私钥和模值组成，模值一般选择 1024 比特或者 2048 比特。

- [61] 步骤 S12，二维码管理服务器将二维码管理服务器公钥分发至若干终端设备，例如
- 25 智能手机、平板电脑、计算机等，终端设备可以使用接收的二维码管理服务器公钥 Public_Key_Server 来加密数据或者验证签名；二维码管理服务器公钥 Public_Key_Server

的发送可以在没有建立二维码管理服务器和终端设备安全通道的情况下进行传输,例如二维码管理服务器直接根据终端设备的请求将二维码管理服务器公钥 Public_Key_Server 返回至终端设备,也可以在向终端设备返回二维码管理服务器公钥 Public_Key_Server 之前建立安全通道,例如采用安全套接层(Secure Sockets Layer, SSL)

5 协议建立安全通道,然后再将二维码管理服务器公钥 Public_Key_Server 返回至终端设备。对于非对称密钥,公钥用来加密数据和验证签名,私钥用来解密和签名。

[62] 步骤 S13,终端设备中的二维码安全应用生成非对称密钥,包括,二维码安全应用公钥 Public_Key_Client 和二维码安全应用私钥 Private_Key_Client;二维码安全应用生成的二维码安全应用公钥 Public_Key_Client 可以用于供二维码管理服务器生成证书,二
10 维码安全应用私钥 Private_Key_Client 可以用于生成签名;证书可以基于 X.509v3 证书标准,证书包含的信息一般包括:公钥值,公钥所有者的标识符信息,有效期,证书颁发者的标识符信息,证书颁发者的数字签名等。

[63] 步骤 S14,二维码安全应用将二维码安全应用的公钥 Public_Key_Client 发送到二维码管理服务器;同样地,二维码安全应用的公钥 Public_Key_Client 的发送可以在没有
15 建立终端设备和二维码管理服务器之间的安全通道的情况下进行传输,例如终端设备直接将二维码安全应用的公钥 Public_Key_Client 发送至二维码管理服务器,也可以在向二维码管理服务器发送二维码安全应用的公钥 Public_Key_Client 之前建立安全通道,例如采用 SSL 协议建立安全通道,然后再将二维码安全应用的公钥 Public_Key_Client 发送至二维码管理服务器。

20 [64] 步骤 S15,二维码管理服务器使用二维码管理服务器的私钥 Private_Key_Server 对二维码的安全应用公钥 Public_Key_Client 进行签名生成证书;在生成证书的过程中,可以直接对二维码安全应用公钥 Public_Key_Client 进行签名生成证书(public key certificate, PKC),也可以对二维码安全应用公钥 Public_Key_Client 进行哈希计算得到哈希值,再使用二维码管理服务器的私钥 Private_Key_Server 将该哈希值签名生成证书 PKC;作为
25 示例,证书包括:二维码的安全应用公钥(m,d),安全应用的标识 1001,有效期 2019 年 1 月 1 日,二维码管理服务器标识 0001,二维码的安全应用公钥的签名(m',d')。

(m,d)是通过密钥算法得到,(m',d')是通过二维码管理服务器的私钥对二维码的安全应用公钥(m,d)进行运算得到,例如对(m,d)进行哈希运算之后再使用二维码管理服务器的私钥对其进行幂指数运算和模运算,将模运算的结果作为签名。

30 [65] 步骤 S16,二维码管理服务器将证书发送到二维码安全应用;同样地,二维码管理

服务器可以在没有建立二维码管理服务器和终端设备安全通道的情况下进行传输,例如二维码管理服务器直接将证书 PKC 返回至终端设备,也可以在向终端设备返回证书 PKC 之前建立安全通道,例如采用安全套接层 (Secure Sockets Layer, SSL) 协议建立安全通道,然后再将证书 PKC 返回至终端设备。

- 5 [66] 通过上述的步骤,二维码管理服务器可以将证书分发至需要该证书的终端设备,从而为终端设备生成具有安全性的二维码时附上该证书完成了准备工作。终端设备可以使用证书作为二维码安全应用公钥 Public_Key_Client 的载体,在终端设备使用二维码安全应用私钥 Private_Key_Client 签名数据时,二维码读取设备可以通过对证书验证获得二维码安全应用公钥 Public_Key_Client,从而可以对使用二维码安全应用私钥 Private_Key_Client 所做的签名进行进一步的验证。需要说明的是,二维码读取设备保存有二维码管理服务器分发的二维码管理服务器的公钥。
- 10

- [67] 对于非对称密钥而言,用私钥可以用来解密或者签名,公钥可以用来加密或者验证签名。非对称密钥的算法可以包括 RSA、Elgamal、背包算法、Rabin、D-H、ECC 中的任一种。下面以 RSA 算法为例,分别说明公钥、私钥、签名证书以及签名生成的过程。
- 15

[68] 二维码管理服务器生成二维码管理服务器公钥 Public_Key_Server 和二维码管理服务器私钥 Private_Key_Server 的过程,具体包括:

[69] 步骤 (1), 令素数 $p=3$, 素数 $q=11$, 得到 $n=p \times q=33$, $f(n) = (p-1) \times (q-1) = 20$;

- 20 [70] 步骤 (2), 令 $e=3$, e 与 d 互质;

[71] 步骤 (3), 令 $e \times d \equiv 1 \pmod{f(n)}$, 即 $3 \times d \equiv 1 \pmod{20}$, 通过下表来选择 d:

d	$e \times d = 3 \times d$	$(e \times d) \pmod{(p-1)(q-1)}$ $= (3 \times d) \pmod{20}$
1	3	3
2	6	6
3	9	9
4	12	12
5	15	15
6	18	18
7	21	1
8	24	3
9	27	6

[72] 因此, 可以选择 $d=7$, 满足 $3 \times d \equiv 1 \pmod{20}$ 。

[73] 步骤 (4), 因此, 二维码管理服务器公钥 Public_Key_Server 可以为 (3,33), 二维码管理服务器私钥 $\text{Private_Key_Server}$ 可以为 (7,33)。

[74] 在获得上述的二维码管理服务器公钥 Public_Key_Server 和二维码管理服务器私钥 $\text{Private_Key_Server}$ 之后, 可以将二维码管理服务器公钥 Public_Key_Server 发送到终端设备, 二维码管理服务器保留二维码管理服务器私钥 $\text{Private_Key_Server}$ 。

[75] 二维码安全应用生成安全二维码安全应用公钥 Public_Key_Client 和二维码安全应用私钥 $\text{Private_Key_Client}$ 的过程, 具体包括:

[76] 步骤 (A), 令素数 $p=13$, 素数 $q=7$, 得到 $n=p \times q=91$, $f(n) = (p-1) \times (q-1) = 72$;

[77] 步骤 (B), 令 $e=7$, e 与 d 互质;

[78] 步骤 (C), 令 $e \times d \equiv 1 \pmod{f(n)}$, 即 $7 \times d \equiv 1 \pmod{72}$, $7 \times d$ 可以是 73, 145, 217 等。

[79] 因此, 为了满足上述恒等式, 可以选择 $d=31$, 满足 $7 \times d \equiv 1 \pmod{72}$ 。

[80] 步骤 (D), 因此, 二维码安全应用公钥 Public_Key_Client 可以为 (7,72), 二维

码安全应用私钥 Private_Key_Client 可以为 (31,72)。

[81] 在二维码安全应用在生成二维码安全应用公钥 Public_Key_Client 和二维码安全应用私钥 Private_Key_Client 以后, 可以将二维码安全应用公钥 Public_Key_Client 发送至二维码管理服务器, 由二维码管理服务器生成证书 PKC, 并发送至安装有二维码安全应用的终端设备。

[82] 二维码管理服务器生成证书的过程可以如下:

[83] 步骤(I), 二维码安全应用将二维码安全应用公钥 Public_Key_Client 发送至二维码管理服务器, 例如二维码安全应用公钥 Public_Key_Client 为 (7,72);

[84] 步骤(II), 二维码管理服务器收到二维码安全应用公钥 Public_Key_Client (7,72)

10 以后, 使用二维码管理服务器的 Private_Key_Server (7,33) 来生成证书。

[85] 例如, 通过计算 $7^7 \bmod 33=28$ 以及 $72^7 \bmod 33=30$ 得到证书中包含的证书内容为 (7,72,1001,20190101,0001, 28,30)。二维码读取设备在收到该证书以后, 可以确认公钥为 (7,72), 二维码安全应用的标识为 1001, 公钥的有效期为 2019 年 1 月 1 日, 二维码管理服务器的标识为 0001, 公钥的签名为 (28,30)。

15 [86] 可选地, 还可以对二维码安全应用公钥 Public_Key_Client (7,72) 进行散列, 例如将公钥中的 7 和 72 组合为 772, 然后模 16 后, 得到 4。此后, 可以使用二维码管理服务器的 Private_Key_Server (7,33) 来对 4 进行运算, $4^7 \bmod 33=16$, 得到数组 (7,72, 1001,20190101,0001,16), 作为证书的内容。

[87] 步骤(III), 二维码管理服务器将包含数组的证书发送至终端设备的安全应用, 20 例如证书的内容为数组 (7,72,1001,20190101,0001, 28,30) 或者 (7,72, 1001,20190101,0001,16)。

[88] 可选地, 在安装有二维码安全应用的终端设备保存有二维码管理服务器公钥 Public_Key_Server 的情况下, 二维码管理服务器还可以使用二维码管理服务器私钥 Private_Key_Server 对证书进一步签名, 将证书以及对证书的签名发送到安全应用, 安全应用可以进一步使用二维码管理服务器公钥 Public_Key_Server 验证证书的真实性。

25 [89] 通过上述的步骤, 可以完成证书的分发。

[90] 需要说明的是, 对于终端设备而言, 均可以接收并保存二维码管理服务器公钥 Public_Key_Server。如果终端设备安装有二维码安全应用, 则其既可以用来生成二维码,

也可以用来读取二维码。如果终端设备未安装有二维码安全应用，则其用来读取二维码，但不能用来按照本申请实施例提供的技术方案生成二维码，在其需要生成二维码时，其可以采用传统的方式来生成和展示二维码，例如可以通过应用程序本身内置的二维码生成和展示模块来生成和展示二维码。需要说明的是，应用程序内置二维码生成和展示模块来生成和展示二维码是现有技术，在此不再赘述。

[91] 第二实施例

[92] 在现实生活中，二维码可以应用于很多的场景，例如支付场景或者即时通信场景。下面以支付场景为例对二维码生成流程进行说明。

[93] 随着社会的进步，便利店越来越多，方便了人们的生活。便利店的扫码机可以通过扫描客户购买的商品上的条码来为客户结算，结算之后可以通过二维码展示，用户可以扫描该二维码进行支付。

[94] 商家在收费的终端设备上确认结算之后，该终端设备中的二维码展示模块会向二维码安全应用发送二维码信息数据生成请求，该请求中会包括结算的有关信息，例如收款方账号，金额等信息，二维码安全应用可以使用二维码安全应用私钥 Private_Key_Client 对该信息进行签名，并附上公约证书发送到二维码展示模块，供二维码展示模块按照二维码展示的规则展示包含二维码安全应用所发送信息的二维码。可选地，结算信息中可以包含日期信息，二维码安全应用还可以增加一些动态信息，例如随机数之类的信息。

[95] 图 2 示出了本申请实施例提供的二维码生成流程，具体包括：

[96] 步骤 S21，二维码安全应用接收生成二维码信息数据的请求；该请求可以来自于二维码展示模块；该二维码展示模块可以为商家计费系统内置的模块，也可以是针对二维码的应用外置的模块，主要是在用户确认结算金额之后，获取与结算有关的信息（例如可以称为二维码业务信息），例如订单信息，并发送到二维码安全应用；与结算有关的信息包括但不限于金额、商家账户标识等，甚至还可以包括用户购买商品的明细，购买日期等等；

[97] 步骤 S22，二维码安全应用根据二维码安全应用的私钥对订单信息进行签名；其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；二维码安全应用在收到二维码展示模块发送的二维码信息数据生成请求之后，可以使用二维码安全应用私钥 Private_Key_Client 签名订单信息。二维码业务信息以及二维

码安全应用的签名证书可以合称为二维码信息数据。可选地，二维码信息数据还可以包含证书。二维码安全应用使用私钥 Private_Key_Client 签名订单信息时，可以将订单信息进行哈希运算，然后对哈希运算得到的结果进行幂指数运算和取模运算，将取模的结果作为签名。

- 5 [98] 步骤 S23，二维码安全应用发送二维码信息数据；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述订单信息的签名；可选地，该二维码信息数据中还包含证书。证书可以是由二维码管理服务器提供的证书，是二维码管理服务器对二维码安全应用发送的公钥的签名证书。

10 [99] 为了便于说明，本申请实施例将二维码展示模块发送的二维码业务信息简化为仅包括金额数据，例如 2。

[100] 在二维码安全应用收到二维码业务信息之后，需要使用二维码安全应用私钥 Private_Key_Client(31,72)对二维码业务信息进行签名，例如通过计算 $2^{31} \bmod 72 = 56$ 。

[101] 如上所述，证书的内容为数组可以为 (7,72,1001,20190101,0001, 28,30) 或者 (7,72, 1001,20190101,0001,16)，因此安全应用可以生成如下的二维码信息数据：

- 15 [102] (2,56,7,72,1001,20190101,0001,28,30) 或者 (2,56,7,72, 1001,20190101,0001,16)。

[103] 二维码安全应用可以将上述的二维码信息数据发送到二维码展示模块，二维码展示模块按照编码规则，将二维码信息数据展示为二维码，例如 QR 码。

[104] 上述的流程可以实现支付场景下的二维码生成，该二维码中包含了二维码业务信息、安全应用签名以及证书。

- 20 [105] 二维码读取设备可以读取二维码，获取二维码信息数据，并可以通过对签名进行验证，从而确认二维码业务数据是否真实。

[106] 第三实施例

[107] 在现实生活中，二维码可以应用于很多的场景，例如支付场景或者即时通信场景。下面以即时通信场景为例对二维码生成流程进行说明。

- 25 [108] 随着移动互联网的发展，基于无线互联网技术的即时通信软件层出不穷，例如微信，钉钉等。即时通信软件一般都会提供通过扫描二维码来添加好友或者通过扫描二维码来加入群的功能。

[109] 现有技术中，二维码读取设备在扫描二维码获得相关数据时，不对其真实性进行

验证，存在安全隐患。

[110] 本申请中，用户在同意另一用户通过扫描自身的二维码来加为好友时，该另一用户所使用的终端设备中的二维码展示模块会向二维码安全应用发送二维码信息数据生成请求，该请求可以仅仅是一个展示二维码的请求，可以不包含任何信息，也可以包含用户的标识；如果该请求仅仅是一个展示二维码的请求，则二维码安全应用可以之前预先与即时通信软件进行交互获得用户的标识，在收到该请求之后，二维码安全应用可以使用二维码安全应用私钥 Private_Key_Client 对该用户的标识来进行签名；如果请求中包含有用户的标识（可以称为二维码业务信息），二维码安全应用可以使用二维码安全应用私钥 Private_Key_Client 对该信息进行签名；二维码安全应用在签名之后，可以将二维码业务信息、签名以及公约证书发送到二维码展示模块，供二维码展示模块按照二维码展示的规则展示包含二维码安全应用所发送信息的二维码。

[111] 图 3 示出了本申请实施例提供的二维码生成流程，具体包括：

[112] 步骤 S31，二维码安全应用接收生成二维码信息数据的请求；该请求可以来自于二维码展示模块；该二维码展示模块可以为即时通信软件中的二维码展示模块，例如二维码名片模块，主要是在用户点击之后获取用户的标识（例如可以称为二维码业务信息），并发送到二维码安全应用；当然，也可以仅发送空的请求，用户的标识预先保存在二维码安全应用中；

[113] 步骤 S32，二维码安全应用根据二维码安全应用的私钥对用户标识进行签名；其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；

[114] 步骤 S33，二维码安全应用发送二维码信息数据；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述用户标识的签名；可选地，该二维码信息数据中还包含证书。证书可以由二维码管理服务器提供的证书，是二维码管理服务器对二维码安全应用发送的公钥的签名证书。

[115] 为了便于说明，本申请实施例将用户的标识设为 2。

[116] 在二维码安全应用收到二维码信息数据生成请求之后，需要使用二维码安全应用私钥 Private_Key_Client (31,72) 对二维码业务信息（即用户的标识）进行签名，例如通过计算 $2^{31} \bmod 72 = 56$ 。

[117] 如上所述，证书的内容为数组可以为 (7,72,1001,20190101,0001, 28,30) 或者 (7,72,

1001,20190101,0001,16), 因此安全应用可以生成如下的二维码信息数据:

[118] (2,56,7,72,1001,20190101,0001,28,30) 或者 (2,56,7,72, 1001,20190101,0001,16)。

[119] 二维码安全应用可以将上述的二维码信息数据发送到二维码展示模块, 二维码展示模块按照编码规则, 将二维码信息数据展示为二维码, 例如 QR 码。

5 [120] 上述的流程可以实现即时通信场景下的二维码生成, 该二维码中包含了用户的标识。

[121] 二维码读取设备可以读取二维码, 获取二维码信息数据, 并可以通过对签名进行验证, 从而确认二维码业务数据是否真实。

[122] 第四实施例

10 [123] 相对于条形码, 二维码能包含更多的信息, 随着智能手机的普及, 二维码得到了广泛的应用。

[124] 比较常用的二维码是快速响应 (quick response, QR)。二维码中一般包含: 码定位图案、功能性数据、数据码和纠错码等几个部分。

15 [125] 码定位图案的功能主要用于矫正二维码的位置。用户使用智能手机在扫描二维码时, 可能无法对准, 可以通过码定位图案将二维码矫正, 从而便于解析出二维码中的各个像素。

[126] 功能性数据主要包括存放一些格式化数据, 以及二维码版本的信息。

[127] 数据码主要用于存放二维码信息数据。

[128] 纠错码主要用于存放对于二维码信息数据的前向纠错码。

20 [129] 图 4 示出了本申请实施例提供的二维码展示流程, 具体包括:

[130] 步骤 S41, 二维码展示模块向安全应用发送二维码信息数据生成请求;

[131] 该二维码展示模块可以为即时通信软件中的二维码展示模块, 例如二维码名片模块, 主要是在用户点击之后获取用户的标识 (例如可以称为二维码业务信息), 并发送到二维码安全应用; 当然, 也可以仅发送空的请求, 用户的标识预先保存在二维码安全应用中; 或者

25

[132] 该二维码展示模块可以为商家计费系统内置的模块, 也可以是针对二维码的应用外置的模块, 主要是在用户确认结算金额之后, 获取与结算有关的信息 (例如可以称为

二维码业务信息)，并发送到二维码安全应用；与结算有关的信息包括但不限于金额、商家账户标识等，甚至还可以包括用户购买商品的明细，购买日期等等；

[133] 步骤 S42，二维码展示模块接收二维码安全应用发送的二维码信息数据，并根据二维码编码规则展示二维码信息数据对应的二维码。

5 [134] 二维码安全应用在收到二维码展示模块发送的请求之后，可以使用二维码安全应用私钥 Private_Key_Client 对二维码业务信息进行签名，并附上证书发送至二维码展示模块。二维码业务信息，二维码安全应用的签名以及证书可以合称为二维码信息数据。

[135] 为了便于说明，本申请实施例将二维码业务信息设为 2。

10 [136] 在二维码安全应用收到二维码信息数据生成请求之后，需要使用二维码安全应用私钥 Private_Key_Client (31,72) 对二维码业务信息（用户的标识或商家的结算信息）进行签名，例如通过计算 $2^{31} \bmod 72 = 56$ 。

[137] 如上所述，证书的内容为数组可以为 (7,72,1001,20190101,0001,28,30) 或者 (7,72,1001,20190101,0001,16)，因此安全应用可以生成如下的二维码信息数据：

[138] (2,56,7,72,1001,20190101,0001,28,30) 或者 (2,56,7,72,1001,20190101,0001,16)。

15 [139] 二维码安全应用可以将上述的二维码信息数据发送到二维码展示模块，二维码展示模块按照编码规则，将二维码信息数据展示为二维码，例如 QR 码。

[140] 二维码读取设备可以读取二维码，获取二维码信息数据，并可以通过对签名进行验证，从而确认二维码业务数据是否真实。

[141] 第五实施例

20 [142] 在终端设备展示二维码之后，二维码读取设备需要对二维码进行扫描，并验证二维码中的二维码业务信息是否真实。

[143] 图 5 示出了本申请实施例提供的二维码读取流程，具体包括：

25 [144] 步骤 S51，二维码读取设备扫描二维码，获取二维码信息数据。具体而言，二维码读取设备可以通过对二维码进行图像分析，解析出二维码中包含的二维码信息数据，例如 (2,56,7,72,1001,20190101,0001,28,30) 或者 (2,56,7,72,1001,20190101,0001,16)。

[145] 步骤 S52，二维码读取设备使用其存储的二维码管理服务器公钥 Public_Key_Server (3,33) 来验证证书，例如通过计算 $28^3 \bmod 33 = 7$ ， $30^3 \bmod 33 = 72$ ，从而验证二维码安全应用公钥 Public_Key_Client 可以为 (7,72)，与证书中的二维码安全应用公钥

Public_Key_Client 相同,从而验证二维码安全应用的公钥为 (7,72); 或者通过计算 $16^3 \bmod 33=4$, $772 \bmod 16=4$, 从而验证二维码安全应用的公钥为 (7,72)。

[146] 进一步地,二维码读取设备使用二维码安全应用公钥 Public_Key_Client 验证签名,例如通过计算 $2^7 \bmod 72=56$, 从而验证了二维码业务信息 2 的真实性。

5 [147] 步骤 S53,在对二维码业务信息验证通过以后,可以根据二维码业务信息完成后续业务流程。

[148] 例如,在支付场景下,可以向账务系统发起扣款请求,账务系统扣款后通知用户,并将所扣款项打入商家的账户;

10 [149] 又如,在即时通信场景下,可以向即时通信服务器发送好友添加请求,即时通信服务器将该好友添加请求发送到用户,用户同意该请求后,双方成为好友。

[150] 第六实施例

[151] 本申请提供的基于安全应用的二维码防伪方法如图 6 所示,具体包括:

15 [152] 步骤 S61,二维码展示模块发送生成二维码信息数据的请求;该请求中可以包括例如订单信息之类的二维码业务信息,也可以为空请求,例如二维码可以预先存储有例如用户标识之类的二维码业务信息;

[153] 步骤 S62,二维码安全应用接收生成二维码信息数据的请求;

[154] 步骤 S63,二维码安全应用根据二维码安全应用的私钥对二维码业务信息进行签名;

[155] 步骤 S64,二维码安全向所述二维码展示模块发送二维码信息数据;

[156] 步骤 S65,二维码展示模块以二维码的方式展示所述二维码信息数据;

20 [157] 步骤 S66,二维码读取设备扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名;

[158] 步骤 S67,二维码读取设备验证所述二维码业务信息的签名,确认所述二维码业务信息;

25 [159] 其中,二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥;所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

[160] 需要说明的是,安全应用还可以保存有二维码管理服务器发送的证书,该证书是

二维码管理服务器针对安全应用的公钥生成的签名证书。在安全应用发送二维码信息数据的时候，可以将该证书一并发送至二维码展示模块。相应地，二维码读取设备可以预先存储有二维码管理服务器发送的公钥，可以用来验证证书的真实性；在二维码读取设备验证二维码真实性以后，可以利用证书中的二维码安全应用的公钥来验证二维码业务信息签名的真实性，通过双重验证以后，可以对二维码业务信息进行处理，进行后续流程。可选地，也可以通过其他方式将安全应用的公钥发送到二维码读取设备，用来二维码业务信息签名的真实性。

[161] 第七实施例

[162] 本申请实施例提供了一种二维码信息数据生成设备，如图 7 所示，其可以为独立的实体，例如位于安全芯片中的二维码安全模块，或者为能够生成二维码信息数据的芯片。优选地，还包括二维码展示模块。

[163] 二维码安全模块可以利用位于安全芯片中的二维码安全应用来实现，二维码安全应用可以生成安全二维码安全应用公钥 `Public_Key_Client` 和二维码安全应用私钥 `Private_Key_Client`，具体生成的过程在此不再赘述。

[164] 在二维码安全应用在生成二维码安全应用公钥 `Public_Key_Client` 和二维码安全应用私钥 `Private_Key_Client` 以后，可以将二维码安全应用公钥 `Public_Key_Client` 发送至二维码管理服务器，由二维码管理服务器生成证书 PKC，并发送至安装有二维码安全应用的终端设备。

[165] 二维码安全应用在收到二维码展示模块发送的二维码信息数据生成请求之后，可以使用二维码安全应用私钥 `Private_Key_Client` 进行签名二维码业务信息，优选地，可以附上证书发送至二维码展示模块。二维码业务信息，以及二维码安全应用的签名可以合称为二维码信息数据。二维码信息数据还可以包括证书。二维码安全应用可以将二维码信息数据发送至二维码展示模块。

[166] 第八实施例

[167] 本申请实施例提供了一种二维码信息数据生成设备，如图 8 所示，其可以为独立的实体，例如二维码安全模块。优选地，还包括二维码展示模块。

[168] 二维码安全模块可以利用位于可信执行环境中的二维码安全应用来实现，二维码安全应用可以生成安全二维码安全应用公钥 `Public_Key_Client` 和二维码安全应用私钥 `Private_Key_Client`，具体生成的过程在此不再赘述。

[169] 在二维码安全应用在生成二维码安全应用公钥 Public_Key_Client 和二维码安全应用私钥 Private_Key_Client 以后, 可以将二维码安全应用公钥 Public_Key_Client 发送至二维码管理服务器, 由二维码管理服务器生成证书 PKC, 并发送至安装有二维码安全应用的终端设备。

5 [170] 二维码安全应用在收到二维码展示模块发送的二维码业务信息之后, 可以使用二维码安全应用私钥 Private_Key_Client 进行签名, 优选地, 可以附上证书发送至二维码展示模块。二维码业务信息, 以及二维码安全应用的签名可以合称为二维码信息数据。二维码信息数据还可以包括证书。二维码安全应用可以将二维码信息数据发送至二维码展示模块。

10 [171] 二维码展示模块可以通过二维码展示应用程序实现, 例如可以是账务系统或即时通信软件中的模块, 或者是独立于账务系统或即时通信软件的模块。

[172] 第九实施例

[173] 本申请实施例提供的信息数据生成设备, 如图 9 所示, 该设备包括: 请求接收模块, 二维码业务信息签名模块, 二维码信息数据发送模块。优选地, 该设备还可以包括
15 公钥发送模块和证书接收模块; 优选地, 还可以包括二维码展示模块。请求接收模块, 用于接收生成二维码信息数据的请求; 二维码业务信息签名模块, 用于根据二维码安全应用的私钥对二维码业务信息进行签名; 二维码信息数据发送模块, 用于发送二维码信息数据; 其中, 二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥; 所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述
20 二维码业务信息的签名。公钥发送模块, 用于将二维码安全应用的公钥发送至二维码管理服务器; 证书接收模块, 用于接收二维码安全应用的证书; 其中, 所述二维码信息数据还包含所述二维码安全应用的证书。二维码信息数据发送模块, 用于将所述二维码信息数据发送至所述二维码展示模块; 所述二维码展示模块, 用于以二维码的方式展示所述二维码信息数据。

25 [174] 第十实施例

[175] 本申请公开的二维码信息数据生成设备, 其可以为独立的物理实体, 如图 10 所示, 该设备包括处理器和存储器, 存储器可以分为两部分, 例如第一存储器和第二存储器, 优选地, 第一存储器上存储有二维码安全程序, 例如二维码安全应用, 第二存储器存储有二维码展示应用程序。

[176] 处理器，可以执行第一存储器上的二维码安全程序，实现本申请实施例提供的基于安全应用的二维码防伪方法。

[177] 第十一实施例

[178] 本申请公开的二维码信息数据生成设备，其可以为独立的物理实体，如图 11 所示，

- 5 该设备包括安全芯片和第一存储器，第一存储器上存储有二维码安全程序，例如二维码安全应用；优选地，该设备还包括处理器和第二存储器，第二存储器上存储有二维码展示程序。

[179] 安全芯片，可以执行第一存储器上的二维码安全程序，实现本申请实施例提供的基于安全应用的二维码防伪方法。

10 [180] 第十二实施例

[181] 本申请实施例提供的二维码读取设备示意图，如图 12 所示，该设备包括：扫描模块以及验证模块。扫描模块，用于扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名；验证模块，用于验证所述二维码业务信息的签名，确认所述二维码业务信息。

- 15 [182] 优选地，本申请实施例还提供了另一种二维码读取设备示意图，如图 10 所示，包括处理器和存储器，所述存储器上存储有程序，例如二维码读取应用程序；处理器，用于执行二维码读取应用程序实现本申请实施例提供的二维码读取方法。

[183] 优选地，上述二维码读取设备为移动智能终端或者计算机。

[184] 第十三实施例

- 20 [185] 本申请实施例提供的二维码系统，如图 13 所示，该系统包括二维码防伪设备和二维码读取设备；优选地，该系统还包括二维码管理服务器；该二维码防伪设备可以是本申请实施例提供的任何一种二维码防伪设备，二维码读取设备可以是本申请示例提供的任何一种二维码读取设备。

- 25 [186] 本申请实施例可以通过二维码管理服务器分发二维码管理服务器的公钥，并使用二维码管理服务器的私钥签名二维码安全应用的公钥，以及使用安全芯片或可信执行环境对二维码安全应用的私钥进行保护的方案，可以让二维码读取设备在本地就可以有效的对二维码安全应用的合法性进行验证，降低了风险发生的概率。

[187] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程

序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

- 5 [188] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令
- 10 产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

- [189] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。
- 15

[190] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

- 20 [191] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

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

- 25 [193] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他

内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

- 5 [194] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。
- 10 [195] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。
- 15 [196] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权利要求书

1、一种基于安全应用的二维码防伪方法，其特征在于，所述方法包括：

二维码安全应用接收生成二维码信息数据的请求；

二维码安全应用根据二维码安全应用的私钥对二维码业务信息进行签名；

5 二维码安全应用发送二维码信息数据；

其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

2、如权利要求 1 所述的方法，其特征在于，该方法还包括：

10 二维码安全应用将二维码安全应用的公钥发送至二维码管理服务器；

二维码安全应用接收二维码安全应用的证书；

其中，所述二维码信息数据还包含所述二维码安全应用的证书。

3、如权利要求 1 所述的方法，其特征在于，所述生成二维码信息数据的请求包含所述二维码业务信息；或者在所述二维码安全应用具有所述二维码业务信息的情况下，

15 所述生成二维码信息数据的请求为空请求。

4、如权利要求 1-3 任意一项所述的方法，其特征在于，所述发送二维码信息数据包括：

将所述二维码信息数据发送至所述二维码展示模块；

该方法还包括：

20 所述二维码展示模块以二维码的方式展示所述二维码信息数据。

5、如权利要求 2 所述的方法，其特征在于，所述方法还包括：

所述二维码管理服务器生成二维码管理服务器使用的非对称密钥，包括二维码管理服务器的公钥和二维码管理服务器的私钥；和/或

所述二维码管理服务器生成二维码管理服务器使用的对称密钥。

25 6、如权利要求 5 所述的方法，其特征在于，所述方法还包括：

所述二维码管理服务器将二维码管理服务器的公钥分发至二维码读取设备和/或二维码安全应用。

7、如权利要求 1 所述的方法，其特征在于，所述二维码安全应用根据二维码安全应用的私钥签名二维码业务信息包括：

30 所述二维码安全应用结合动态信息和所述业务信息得到更新后的业务信息；

所述二维码安全应用根据二维码安全应用的私钥签名所述更新的二维码业务信息。

8、一种二维码读取方法，其特征在于，所述方法包括：

扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名；

验证所述二维码业务信息的签名，确认所述二维码业务信息。

5 9、如权利要求 8 所述的方法，其特征在于，所述验证所述二维码业务信息的签名包括：

利用二维码安全应用的公钥验证所述二维码业务信息的签名。

10、如权利要求 8 所述的方法，其特征在于，该方法还包括：

扫描二维码以获得二维码安全应用的证书；

10 利用二维码管理服务器生成的密钥验证所述证书，确认所述证书包含的二维码安全应用的公钥；

所述验证所述签名，确认所述二维码业务信息包括：

利用证书包含的二维码安全应用的公钥验证所述二维码业务信息的签名，确认所述二维码业务信息。

15 11、如权利要求 8 所述的方法，其特征在于，该方法还包括：

二维安全应用将二维安全应用的公钥发送至二维码读取设备；或者

二维码管理服务器将二维安全应用的公钥发送至二维码读取设备；或者二维码管理服务器将二维码管理服务器生成的密钥发送至二维码读取设备，其中二维码管理服务器生成的密钥为非对称密钥或对称密钥。

20 12、一种基于安全应用的二维码防伪方法，其特征在于，所述方法包括：

二维码展示模块发送生成二维码信息数据的请求；

二维码安全应用接收生成二维码信息数据的请求；

二维码安全应用根据二维码安全应用的私钥对二维码业务信息进行签名；

二维码安全向所述二维码展示模块发送二维码信息数据；

25 所述二维码展示模块以二维码的方式展示所述二维码信息数据；

二维码读取设备扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名；

二维码读取设备验证所述二维码业务信息的签名，确认所述二维码业务信息；

其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

30

13、如权利要求 12 所述的方法，其特征在于，该方法还包括：

二维码安全应用将二维码安全应用的公钥发送至二维码管理服务器；

二维码安全应用接收二维码安全应用的证书；

其中，所述二维码信息数据还包含所述二维码安全应用的证书。

5 14、如权利要求 12 所述的方法，其特征在于，所述生成二维码信息数据的请求包含所述二维码业务信息；或者在所述二维码安全应用具有所述二维码业务信息的情况下，所述生成二维码信息数据的请求为空请求。

15、如权利要求 12 所述的方法，其特征在于，所述方法还包括：

10 所述二维码管理服务器生成二维码管理服务器使用的非对称密钥，包括二维码管理服务器的公钥和二维码管理服务器的私钥；和/或

所述二维码管理服务器生成二维码管理服务器使用的对称密钥。

16、如权利要求 15 所述的方法，其特征在于，所述方法还包括：

所述二维码管理服务器将二维码管理服务器的公钥分发至二维码读取设备和/或二维码安全应用。

15 17、如权利要求 12 所述的方法，其特征在于，所述二维码安全应用根据二维码安全应用的私钥签名二维码业务信息包括：

所述二维码安全应用结合动态信息和所述业务信息得到更新后的业务信息；

所述二维码安全应用根据二维码安全应用的私钥签名所述更新的二维码业务信息。

20 18、如权利要求 12 或 13 所述的方法，其特征在于，所述二维码读取设备验证所述二维码业务信息的签名包括：

二维码读取设备利用二维码安全应用的公钥验证所述二维码业务信息的签名。

19、如权利要求 18 所述的方法，其特征在于，该方法还包括：

扫描二维码以获得二维码安全应用的证书；

25 利用二维码管理服务器生成的密钥验证所述证书，确认所述证书包含的二维码安全应用的公钥。

20、如权利要求 12 所述的方法，其特征在于，该方法还包括：

二维安全应用将二维安全应用的公钥发送至二维码读取设备；或者

30 二维码管理服务器将二维安全应用的公钥发送至二维码读取设备；或者二维码管理服务器将二维码管理服务器生成的密钥发送至二维码读取设备，其中二维码管理服务器生成的密钥为非对称密钥或对称密钥。

21、一种二维码防伪设备，其特征在于，该设备包括二维码安全模块；

二维码安全模块，还用于接收生成二维码信息数据的请求；根据二维码安全应用的私钥对二维码业务信息进行签名；发送二维码信息数据；

其中，二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥；所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

22、如权利要求 21 所述的设备，其特征在于，二维码安全模块，还用于将二维码安全模块的公钥发送至二维码管理服务器；接收二维码安全模块的证书；

其中，所述二维码信息数据还包含所述二维码安全模块的证书。

23、如权利要求 21 所述的设备，其特征在于，所述生成二维码信息数据的请求包含所述二维码业务信息；或者在所述二维码安全应用具有所述二维码业务信息的情况下，所述生成二维码信息数据的请求为空请求。

24、如权利要求 21-23 任意一项所述的设备，其特征在于，二维码安全模块，还用于将所述二维码信息数据发送至所述二维码展示模块；以二维码的方式展示所述二维码信息数据。

25、如权利要求 22 所述的设备，其特征在于，所述二维码管理服务器，用于生成二维码管理服务器使用的非对称密钥，包括二维码管理服务器的公钥和二维码管理服务器的私钥；和/或

所述二维码管理服务器，用于生成二维码管理服务器使用的对称密钥。

26、如权利要求 25 所述的设备，其特征在于，所述二维码管理服务器，还用于将二维码管理服务器的公钥分发至二维码读取设备和/或二维码安全模块。

27、如权利要求 21 所述的设备，其特征在于，所述二维码安全模块，还用于结合动态信息和所述业务信息得到更新后的业务信息；根据二维码安全模块的私钥签名所述更新的二维码业务信息。

28、一种二维码防伪设备，其特征在于，该设备包括安全芯片和存储器，所述存储器上存储有二维码安全程序；

所述安全芯片，用于执行所述二维码安全程序以实现根据权利要求 1 所述的方法。

29、一种二维码防伪设备，其特征在于，该设备包括处理器和存储器，所述存储器存储有二维码安全程序；

所述处理器，用于执行所述二维码安全程序以实现根据权利要求 1 所述的方法。

30、一种二维码防伪设备，其特征在于，所述设备包括：
请求接收模块，用于接收生成二维码信息数据的请求；

二维码业务信息签名模块,用于根据二维码安全应用的私钥对二维码业务信息进行签名;

二维码信息数据发送模块,用于发送二维码信息数据;

其中,二维码安全应用具有二维码安全应用的公钥和二维码安全应用的私钥构成的非对称密钥;所述二维码信息数据包含二维码业务信息以及二维码安全应用对所述二维码业务信息的签名。

31、如权利要求 30 所述的设备,其特征在于,该设备还包括:

公钥发送模块,用于将二维码安全应用的公钥发送至二维码管理服务器;

证书接收模块,用于接收二维码安全应用的证书;

10 其中,所述二维码信息数据还包含所述二维码安全应用的证书。

32、如权利要求 30 所述的设备,其特征在于,所述生成二维码信息数据的请求包含所述二维码业务信息;或者在所述二维码安全应用具有所述二维码业务信息的情况下,所述生成二维码信息数据的请求为空请求。

15 33、如权利要求 30-32 任意一项所述的设备,其特征在于,该设备还包括二维码展示模块;

所述二维码信息数据响应发送模块,用于将所述二维码信息数据发送至所述二维码展示模块;

所述二维码展示模块,用于以二维码的方式展示所述二维码信息数据。

20 34、如权利要求 31 所述的设备,其特征在于,所述二维码管理服务器生成二维码管理服务器使用的非对称密钥,包括二维码管理服务器的公钥和二维码管理服务器的私钥;和/或

所述二维码管理服务器生成二维码管理服务器使用的对称密钥。

35、如权利要求 34 所述的设备,其特征在于,所述二维码管理服务器将二维码管理服务器的公钥分发至二维码读取设备和/或二维码安全应用。

25 36、如权利要求 30 所述的设备,其特征在于,二维码业务信息签名模块,还用于结合动态信息和所述业务信息得到更新后的业务信息;根据二维码安全应用的私钥签名所述更新的二维码业务信息。

37、一种二维码读取设备,其特征在于,该二维码读取设备包括:

30 扫描模块,用于扫描二维码以获得二维码业务信息以及二维码安全应用对所述二维码业务信息的签名;

验证模块,用于验证所述二维码业务信息的签名,确认所述二维码业务信息。

38、一种二维码读取设备，其特征在于，所述设备包括处理器和存储器，所述存储器上存储有程序；

所述处理器，用于执行所述程序以实现根据权利要求 8 所述的方法。

39、一种二维码防伪系统，其特征在于，该系统包括根据权利要求 21-36 任意一项
5 所述的设备以及根据权利要求 37 或 38 所述的二维码读取设备。

40、根据权利要求 39 所述的系统，其特征在于，该系统还包括二维码管理服务器；

所述二维码管理服务器，用于向二维码读取设备发送密钥和/或生成证书并向根据权利要求 21-36 任意一项所述的设备发送所述证书。

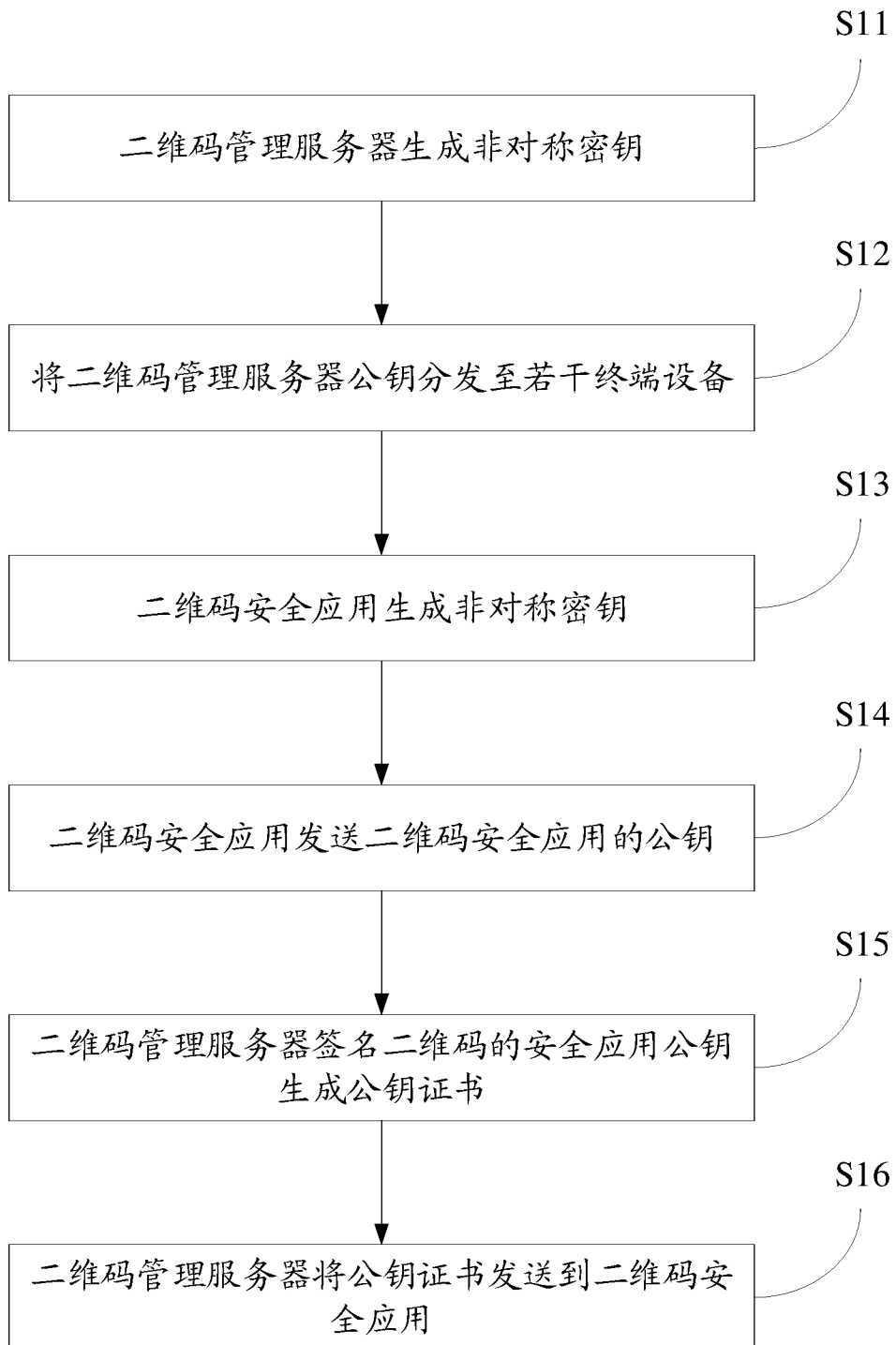


图 1

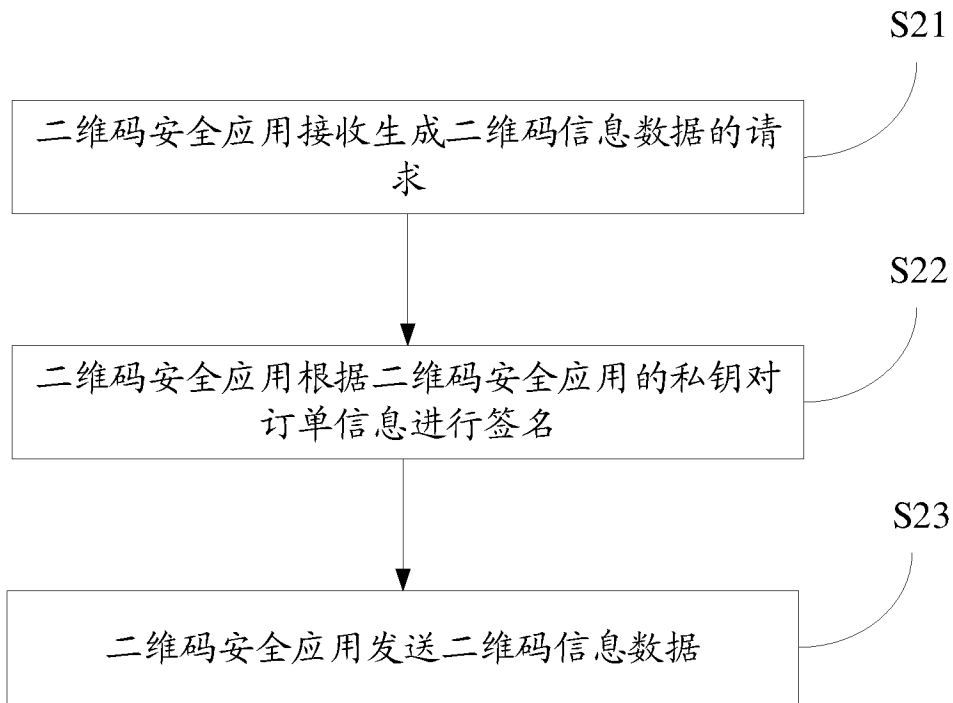


图 2

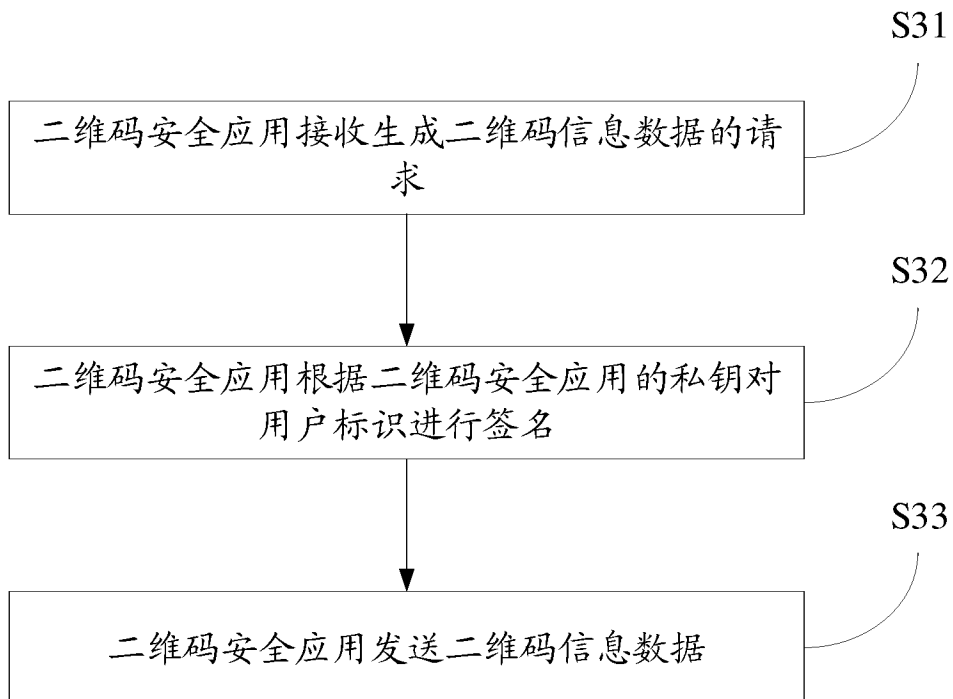


图 3

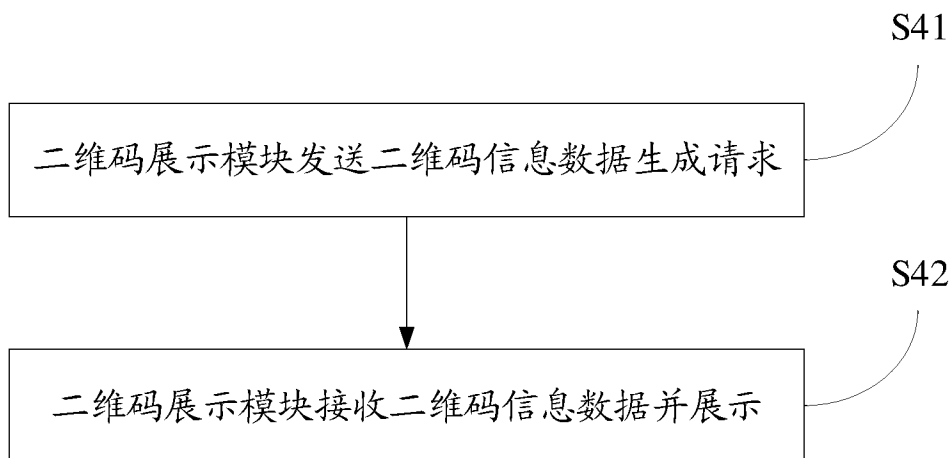


图 4

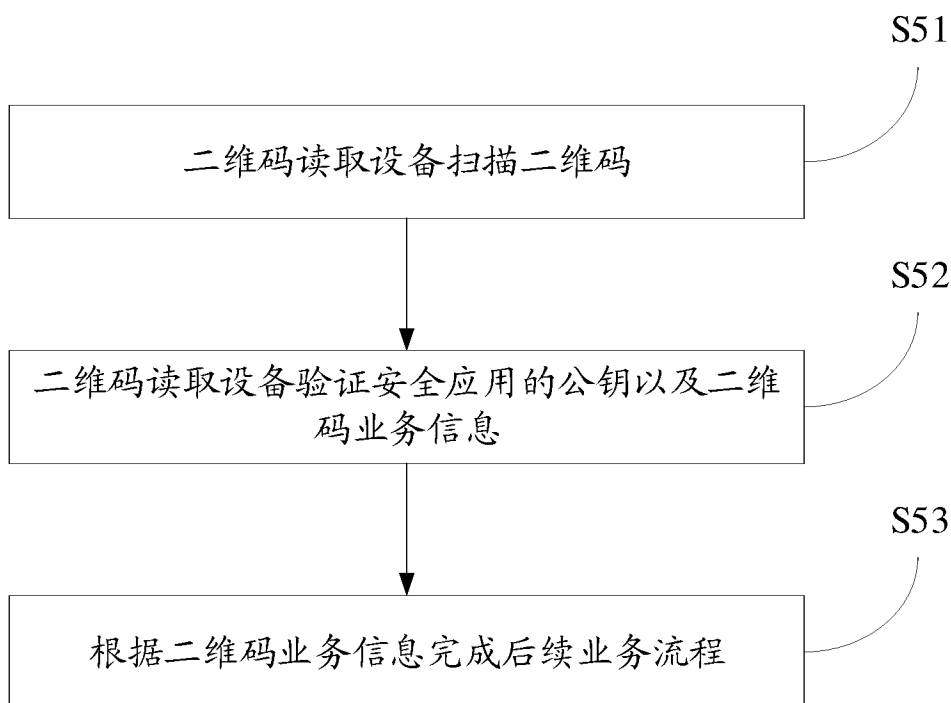


图 5

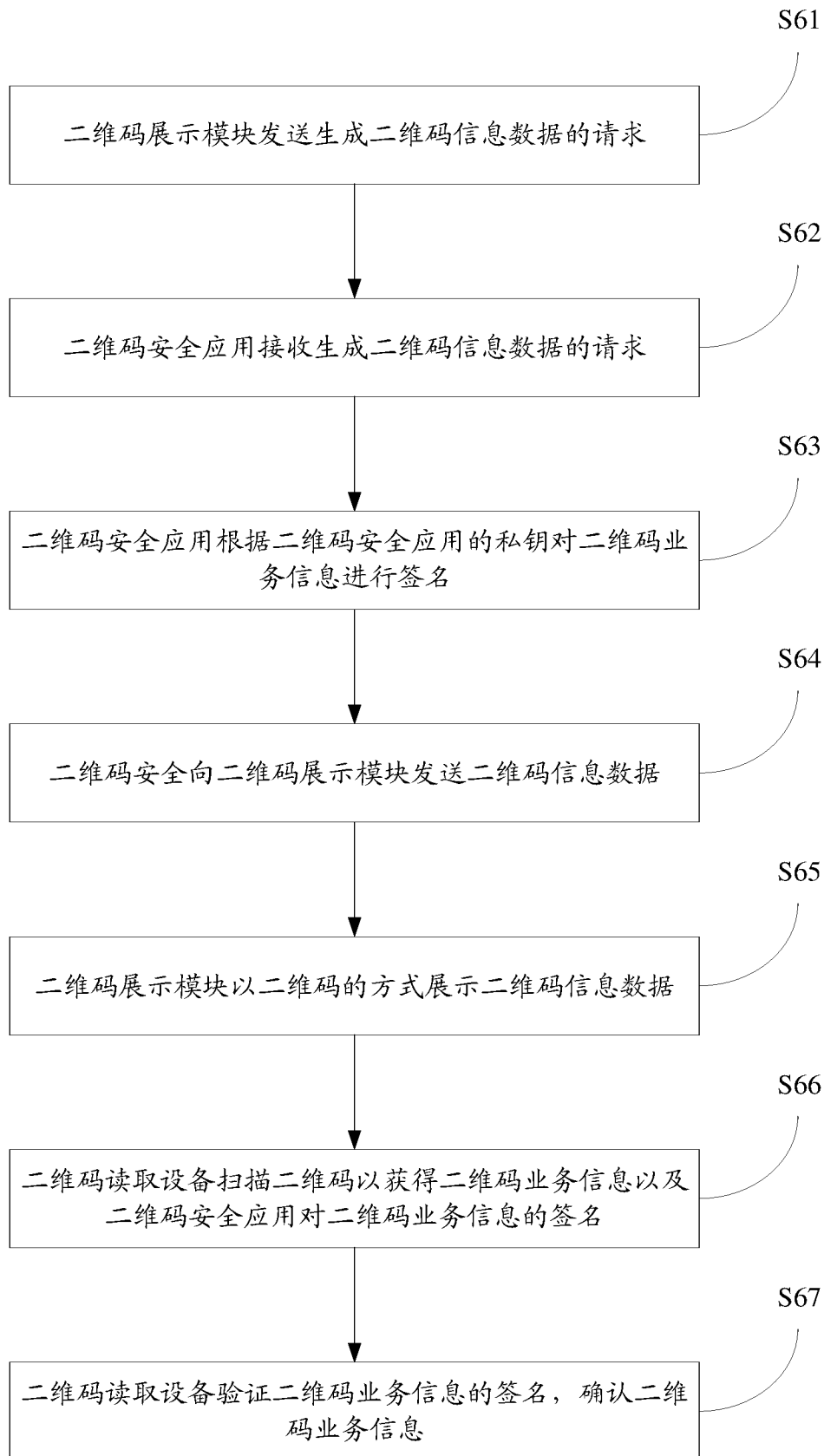


图 6



图 7



图 8

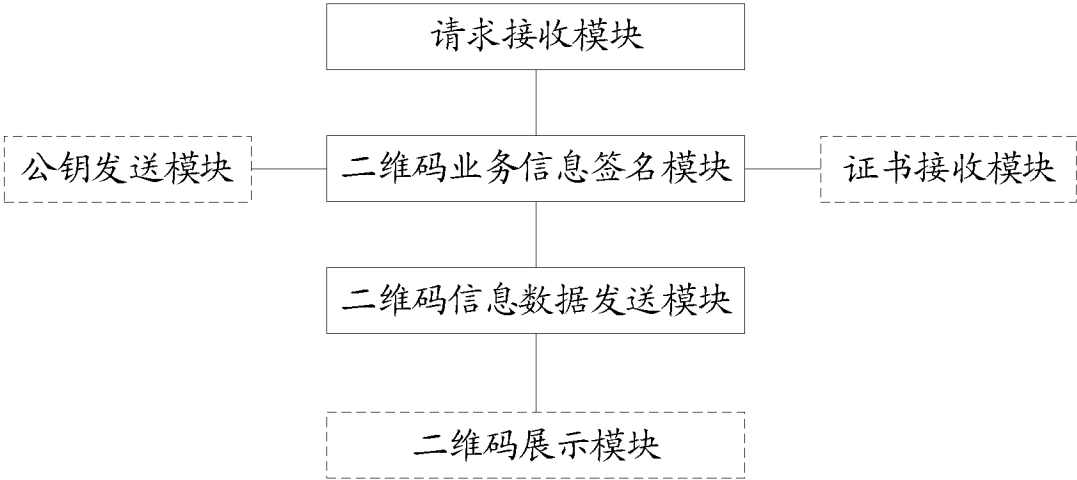


图 9

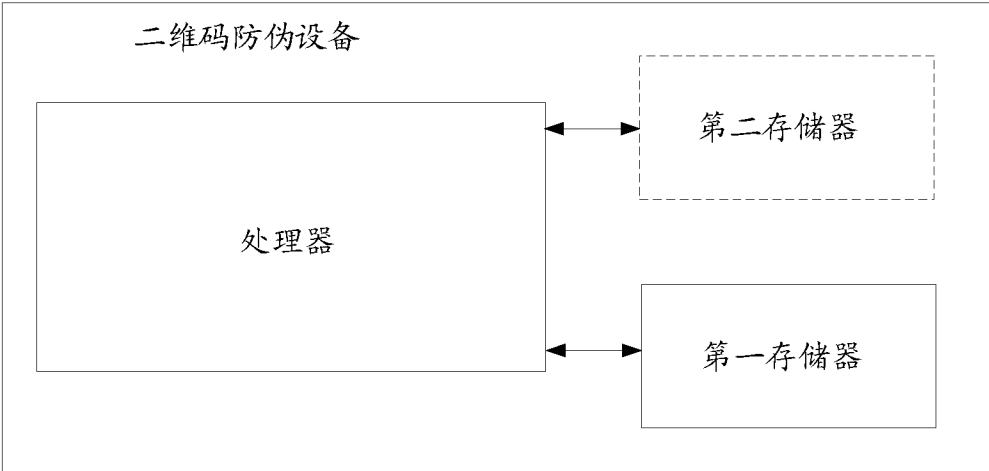


图 10

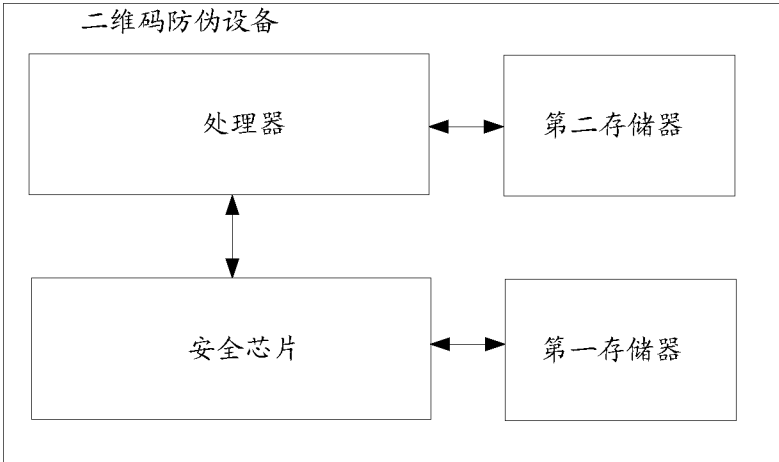


图 11



图 12

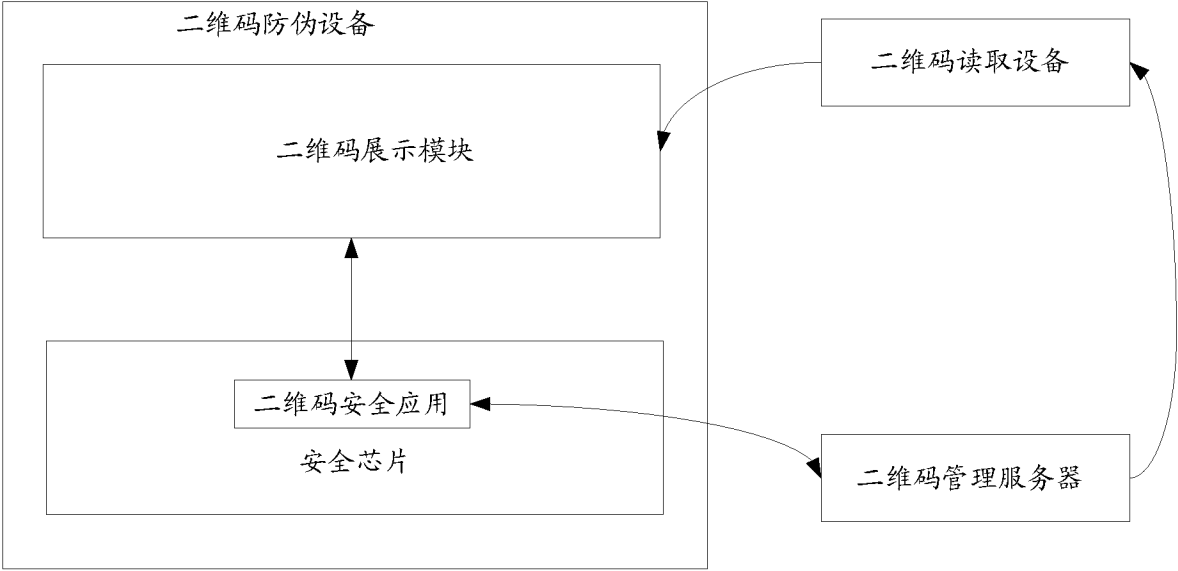


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/097095

A. CLASSIFICATION OF SUBJECT MATTER

G06K 17/00(2006.01)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)

G06K

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, WPI, EPODOC, IEEE, CNKI: 二维码, 安全, 私钥, 公钥, 密钥, 非对称, 证书, 签名, 扫描, 验证, 防伪, 应用, two-dimensional code, security, private key, public key, key, asymmetric, certificate, signature, scan, verification, application, anti-counterfeiting

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109615030 A (ALIBABA GROUP HOLDING LIMITED) 12 April 2019 (2019-04-12) claims 1-40, and description, paragraphs [0003]-[0041]	1-40
X	CN 104408502 A (QUANLIAN STAERCKE TECHNOLOGY CO., LTD.) 11 March 2015 (2015-03-11) description, paragraphs [0007]-[0041], [0079] and [0084]	1-40
X	CN 102932148 A (CHENGDU YIHENGXIN TECHNOLOGY CO., LTD.) 13 February 2013 (2013-02-13) description, paragraphs [0013]-[0021]	1-40
X	CN 103824202 A (CHENGDU YIHENGXIN TECHNOLOGY CO., LTD.) 28 May 2014 (2014-05-28) description, paragraphs [0005]-[0018]	1-40
A	CN 102201100 A (ZHU, QINGMING ET AL.) 28 September 2011 (2011-09-28) entire document	1-40
A	US 9338164 B1 (SYMANTEC CORPORATION) 10 May 2016 (2016-05-10) entire document	1-40

☐ 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

02 September 2019

Date of mailing of the international search report

27 September 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
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/CN2019/097095

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	109615030	A	12 April 2019	None	
CN	104408502	A	11 March 2015	None	
CN	102932148	A	13 February 2013	CN	102932148
				B	11 May 2016
CN	103824202	A	21 January 2015	None	
CN	102201100	A	28 September 2011	CN	102201100
				B	24 April 2013
US	9338164	B1	10 May 2016	None	

国际检索报告

国际申请号

PCT/CN2019/097095

A. 主题的分类

G06K 17/00(2006.01)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)

G06K

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, WPI, EPODOC, IEEE, CNKI; 二维码, 安全, 私钥, 公钥, 密钥, 非对称, 证书, 签名, 扫描, 验证, 防伪, 应用, two-dimensional code, security, private key, public key, key, asymmetric, certificate, signature, scan, verification, application, anti-counterfeiting

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 109615030 A (阿里巴巴集团控股有限公司) 2019年 4月 12日 (2019 - 04 - 12) 权利要求1-40, 说明书第[0003]-[0041]段	1-40
X	CN 104408502 A (全联斯泰克科技有限公司) 2015年 3月 11日 (2015 - 03 - 11) 说明书第[0007]-[0041], [0079], [0084]段	1-40
X	CN 102932148 A (成都市易恒信科技有限公司) 2013年 2月 13日 (2013 - 02 - 13) 说明书第[0013]-[0021]段	1-40
X	CN 103824202 A (成都市易恒信科技有限公司) 2014年 5月 28日 (2014 - 05 - 28) 说明书第[0005]-[0018]段	1-40
A	CN 102201100 A (朱清明 等) 2011年 9月 28日 (2011 - 09 - 28) 全文	1-40
A	US 9338164 B1 (SYMANTEC CORPORATION) 2016年 5月 10日 (2016 - 05 - 10) 全文	1-40

☐ 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

2019年 9月 2日

国际检索报告邮寄日期

2019年 9月 27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

受权官员

石爽

传真号 (86-10)62019451

电话号码 86-(10)-53961413

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/097095

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	109615030	A	2019年 4月 12日	无	
CN	104408502	A	2015年 3月 11日	无	
CN	102932148	A	2013年 2月 13日	CN 102932148	B 2016年 5月 11日
CN	103824202	A	2015年 1月 21日	无	
CN	102201100	A	2011年 9月 28日	CN 102201100	B 2013年 4月 24日
US	9338164	B1	2016年 5月 10日	无	

表 PCT/ISA/210 (同族专利附件) (2015年1月)