(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102509141 A
(43)申请公布日 2012.06.20

(21)申请号 201110335319.6

(22)申请日 2011.10.31

(71)申请人 广东商学院
地址 510320 广东省广州市海珠区赤沙路 21 号
申请人 梁英宏

(72)发明人 梁英宏 刘义春 张颖

(51)Int.Cl.
G06K 19/06(2006.01)
G06Q 30/00(2012.01)
H04L 9/32(2006.01)

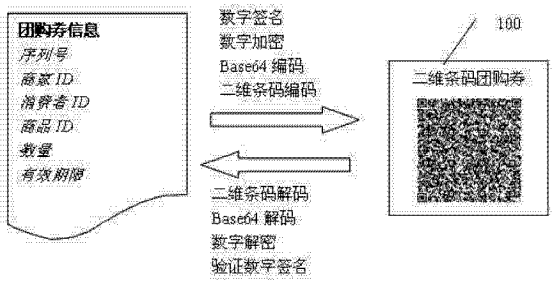
权利要求书 3 页 说明书 7 页 附图 6 页

(54)发明名称

一种电子团购券及其使用方法和系统

(57)摘要

本发明公开了一种二维条码团购券及其使用方法和系统，其二维条码团购券的形式为二维条码图像。将团购券信息转换成二维条码团购券的步骤包括数字签名、数字加密、Base64 编码和二维条码编码，利用二维条码团购券读取团购券信息的步骤包括二维条码解码、Base64 解码、数字解密和验证数字签名。其系统由二维条码团购券、商家计算机、消费者计算机、团购服务器、短信猫、消费者手机、移动存储介质、消费者打印机和二维条码阅读器组成。本发明的二维条码团购券信息容量大，读取方便，安全可靠并且可以离线使用，能够降低参与团购的商家的经营成本。



CN 102509141 A

1. 一种二维条码团购券，其特征在于，其形式为二维条码。

2. 一种采用二维条码团购券进行电子商务团购活动的方法，其特征在于，包括以下步骤：

（1）准备阶段：团购网站事先采用非对称密码算法为自己生成一对非对称密钥，包括公钥和私钥。商家在团购网站注册时，团购网站也采用非对称密码算法为该商家生成一对非对称密钥，保留该商家的公钥，将该商家的私钥以及团购网站的公钥交付给商家，同时为该商家生成一个商家 ID。商家注册完毕后可以发布商品，每一种商品有一个商品 ID。消费者在团购网站注册时，团购网站为消费者生成一个消费者 ID；

（2）网上下单：消费者在团购网站上对某个商品下单；

（3）生成团购券：团购网站确认订单后，生成包含序列号、商家 ID、商品 ID、消费者 ID、商品数量、有效期限等数据的团购券明文（团购券信息），然后利用自己的私钥对团购券明文进行数字签名，再利用该商品所属的商家的公钥对数字签名后的信息进行加密，最后生成二维条码图像，作为消费者的团购券；

（4）使用团购券：消费者携带该二维条码团购券（二维条码存放于手机彩信中或者打印在纸张上）到商家消费；

（5）读取团购券：商家首先使用二维条码阅读器阅读二维条码，然后使用自己的私钥进行解密，再利用团购网站公钥进行数字签名验证，验证通过后获取团购券信息明文，商家确认该券未使用后，根据团购券信息向消费者提供商品或服务；

（6）上传团购券：商家通过互联网实时传回团购券序列号，或者商家累计一定数量团购券，通过移动存储介质向团购网站批量上报团购券序列号数据，团购网站返回商家收入分成。

3. 根据权利要求 2 所述的一种采用二维条码团购券进行电子商务团购活动的方法，其特征在于，所述步骤（3）中团购网站生成团购券的流程包括以下子步骤：

（S301）首先根据订单信息创建团购券的明文，可以包括序列号、商家 ID、商品 ID、消费者 ID、商品数量、有效期限等信息，再使用团购网站私钥对原始数据进行数字签名，将数字签名附在明文后面，形成签名后的团购券信息；

（S302）利用商家公钥对签名后的团购券信息进行加密，形成二进制形式的加密团购券信息；

（S303）利用 Base64 字符编码对二进制的加密团购券数据进行字符编码，形成 Base64 编码形式的加密团购券信息；

（S304）利用二维条码编码算法对 Base64 编码形式的加密团购券信息进行编码，生成二维条码图像，该图像即为最终团购券。

4. 根据权利要求 2 所述的一种采用二维条码团购券进行电子商务团购活动的方法，其特征在于，所述步骤（5）中，商家读取团购券流程包括以下子步骤：

（S501）使用二维条码阅读器读取并解码团购券图像数据，形成 Base64 字符编码形式的加密团购券信息；

（S502）对 Base64 字符编码形式的加密团购券信息进行 Base64 字符编码的解码，形成二进制形式的加密团购券信息；

（S503）利用商家私钥对二进制数据进行解密，形成包含数字签名的已解密团购券信

息；

（S504）利用团购网站公钥对数字签名部分进行验证，验证成功后读取团购券明文数据，该数据为团购券的实际数据。

5. 一种采用二维条码团购券进行电子商务团购活动的系统，其特征在于，包括二维条码团购券（100）、商家计算机（200）、消费者计算机（300）、团购服务器（400）、短信猫（500）、消费者手机（600）、移动存储介质（700）、消费者打印机（800）和二维条码阅读器（900）组成，其中：

所述消费者计算机（300）通过互联网与团购服务器（400）通信，用于消费者浏览商品信息和进行团购下单；

所述短信猫（500）通过 RS-232 串口或者 USB 接口与团购服务器（400）相连，用于通过移动通信网络将二维条码团购券（100）以短信的方式发送到消费者手机（600）；

所述消费者打印机（800）通过并口或者 USB 接口与消费者计算机（300）相连，消费者计算机（300）可以控制费者打印机（800）打印从团购服务器（400）下载二维条码团购券（100）；

可选的，所述商家计算机（200）通过互联网与团购服务器（400）通信，用于发布商品信息以及实时传回团购券序列号；

所述二维条码阅读器（900）通过 RS-232 串口或者 USB 接口与商家计算机（200）相连，商家计算机（200）可以控制二维条码阅读器（900）读取消费者手机（600）中或者打印的二维条码团购券（100）；

所述商家计算机（200）可以将团购券序列号存储于移动存储介质（700），利用移动存储介质（700）将团购券序列号数据批量传送到团购服务器（400）。

6. 根据权利要求 5 所述的一种采用二维条码团购券进行电子商务团购活动的系统，其特征在于，所述团购服务器（400）包含用户界面模块（401）、商户数据上报模块（402）、数据库模块（403）、订单处理模块（404）和团购券生成模块（405），其中：

所述用户界面模块（401）与数据库模块（403）、订单处理模块（404）和团购券生成模块（405）交互，用于接收消费者的团购下单请求，将下单信息送入订单处理模块（404），提供消费者网上付款通道，并在团购券生成模块（405）中生成团购券，发送到消费者手机或者提供给消费者下载，所有的数据都存放在数据库模块（403）中；

所述商户数据上报模块（402）与数据库模块（403）交互，用于接收商家发送回来的团购券序列号，提供通过移动存储介质的批量上传和通过互联网的实时上传两种上传方式；

所述数据库模块（403）与用户界面模块（401）、商户数据上报模块（402）、订单处理模块（404）和团购券生成模块（405）交互，提供数据临时和长期存储功能；

所述订单处理模块（404）与用户界面模块（401）、数据库模块（403）和团购券生成模块（405）交互，用于根据消费者下单信息生成订单，将订单数据存放到数据库模块（403），并通知团购券生成模块（405）生成团购券，将团购券发送到消费者手机或者提供给消费者下载；

所述团购券生成模块（405）用于根据订单数据生成团购券。

7. 根据权利要求 5 所述的一种采用二维条码团购券进行电子商务团购活动的系统，其特征在于，所述团购券生成模块（405）包含数字签名子模块（4051）、数据加密子模块

(4052)和二维条码生成子模块(4053),其中:

所述数字签名子模块(4051)首先根据订单数据生成团购券数据,再采用团购网站私钥对团购券数据进行数字签名;

所述数据加密子模块(4052)利用商品所属商家的公钥对签名后的团购券数据进行加密,再使用 Base64 字符编码算法对二进制加密数据进行字符编码;

所述二维条码生成子模块(4053)采用二维条码编码算法对字符编码后的二进制加密团购券数据进行编码,生成二维条码图像。

8. 根据权利要求 5 所述的一种采用二维条码团购券进行电子商务团购活动的系统,其特征在于,所述商家计算机(200)包含用户界面模块(201)、数据记录模块(202)、数据解密模块(203)和数字签名验证模块(204),其中:

所述用户界面模块(201)与数据记录模块(202)交互,可以将二维条码阅读器所读取的数据录入数据记录模块(202),并且可以从数据记录模块(202)中获取解密后的团购券数据,还提供将团购券序列号批量装载到移动存储介质和通过互联网将团购券序列号实时上传的功能;

所述数据记录模块(202)与用户界面模块(201)和数据解密模块(203)交互,用于记录团购券解密前后的数据;

所述数据解密模块(203)与数据记录模块(202)交互,用于从数据记录模块(202)提取团购券解密前的数据再进行解密,解密过程:首先对解密前的团购券数据进行 Base64 解码,再利用商家自己的私钥对二进制数据进行解密,生成解密的团购券数据,传回数字签名验证模块(204);

所述数字签名验证模块(204)利用团购网站公钥对解密的团购券数据进行数字签名验证,如验证成功就将团购券明文存入数据记录模块(202),供用户界面模块(201)查询和调用。

一种电子团购券及其使用方法和系统

技术领域

[0001] 本发明涉及电子商务领域，更具体地说，涉及一种用于电子商务团购活动的电子团购券及其使用方法和系统。

背景技术

[0002] 随着互联网以及电子商务技术的发展，网上交易规模不断扩大，出现了大量的电子商务网站和交易平台，其中，团购成为一种新的电子商务营销模式。由于团购网站以大宗采购的名义与商家洽谈，商家往往会大幅降价出售商品，因而消费者通过团购网站能够以比平时低得多的价格购买商品，所以团购形式越来越得到消费者的喜爱，发展极为迅速。

[0003] 目前的电子商务团购方法过程为：团购网站发布商家打折让利商品的信息，并设定一个团购时间期限，消费者可以在该时间内通过团购网站下单并付款，团购网站确认订单后生成一个序列号通过短信发送到消费者手机，该序列号即代表团购券，消费者凭借该序列号到商家进行消费，商家将该序列号输入到团购网站进行验证，通过验证后向消费者发放商品或提供服务。为了避免消费者遗忘或丢失该序列号，有些团购网站提供团购券下载和打印功能，消费者可以自行打印包含序列号的团购券进行消费。目前这种团购方法存在以下问题：

1、仅使用序列号作为团购券的方法安全性差，序列号容易被他人窃取和使用，同时也存在被他人掌握序列号生成规则的可能。

[0004] 2、由于序列号本身不具备任何含义，因而不能离线使用，商家必须通过联网的方式将序列号传送给团购网站进行验证，商家必须准备一个用于团购消费的联网计算机，当团购量比较大时，还需要专人操作该计算机。

[0005] 3、单一序列号只能作为单个商品的凭证，消费者通过团购网站购买多个同一商品就获得多个序列号，取货时商家也必须逐一验证，效率低下。

[0006] 目前在其他电子商务模式中，也有部分商家采用二维条码作为电子优惠券载体，将优惠券信息通过二维条码进行编码形成图片后发送到消费者手机，商家验证时只需要采用二维条码阅读器对手机上的二维条码图像进行拍摄辨识，就可以自动读取票据信息。但是这种二维条码电子优惠券与序列号电子优惠券本质相同，尽管读取携带方便，但是安全性不高。

[0007] 因此在电子商务团购中需要一种新的电子团购券，能够记录更多信息，支持离线交易并具备安全性，为更多层次的消费者所接受。

发明内容

[0008] 本发明的目的在于提供一种用于电子商务团购活动的二维条码团购券及其使用方法和系统，旨在解决现有技术存在的安全性差，不支持离线交易，不能记录购买商品的类型和数量的问题。

[0009] 为了实现发明目的，所述二维条码团购券 100 的形式为二维条码，可以为 PDF417、

Maxi Code、QR Code、Data Matrix 等二维条码中的一种。

[0010] 将团购券信息转换成二维条码团购券 100 的步骤包括数字签名、数字加密、Base64 编码和二维条码编码。

[0011] 利用二维条码团购券 100 读取团购券信息的步骤包括二维条码解码、Base64 解码、数字解密和验证数字签名。

[0012] 所述团购券信息的内容可以包括但不限于以下内容：序列号、商家 ID、消费者 ID、商品 ID、数量和有效期限。

[0013] 所述序列号为团购券在团购网站中的唯一标识符，不同的二维条码团购券 100 中存储的序列号不能重复；

所述商家 ID、消费者 ID、商品 ID 分别是商家、消费者、商品在团购网站中的唯一标识符，不同的商家、消费者、商品的 ID 不能重复；

所述数量是团购券中商品的数量；

所述有效期限为团购券的使用期限。

[0014] 本发明的目的还在于提供一种采用二维条码团购券进行电子商务团购活动的方法，以更好地解决现有技术存在的问题。为了实现发明的目的，所述采用二维条码团购券进行电子商务团购活动的方法包括以下步骤：

(1)准备阶段：团购网站事先采用非对称密码算法为自己生成一对非对称密钥，包括公钥和私钥。商家在团购网站注册时，团购网站也采用非对称密码算法为该商家生成一对非对称密钥，保留该商家的公钥，将该商家的私钥以及团购网站的公钥交付给商家，同时为该商家生成一个商家 ID。商家注册完毕后可以发布商品，每一种商品有一个商品 ID。消费者在团购网站注册时，团购网站为消费者生成一个消费者 ID；

(2)网上下单：消费者在团购网站上对某个商品下单；

(3)生成团购券：团购网站确认订单后，生成包含序列号、商家 ID、商品 ID、消费者 ID、商品数量、有效期限等数据的团购券明文(团购券信息)，然后利用自己的私钥对团购券明文进行数字签名，再利用该商品所属的商家的公钥对数字签名后的信息进行加密，最后生成二维条码图像，作为消费者的团购券；

(4)使用团购券：消费者携带该二维条码团购券(二维条码存放于手机彩信中或者打印在纸张上)到商家消费；

(5)读取团购券：商家首先使用二维条码阅读器阅读二维条码，然后使用自己的私钥进行解密，再利用团购网站公钥进行数字签名验证，验证通过后获取团购券信息明文，商家确认该券未使用后，根据团购券信息向消费者提供商品或服务；

(6)上传团购券：商家通过互联网实时传回团购券序列号，或者商家累计一定数量团购券，通过移动存储介质向团购网站批量上报团购券序列号数据，团购网站返回商家收入分成。

[0015] 所述步骤(6)中，如果商家存在多个分店，则必须采用实时传回团购券序列号的方法，以保证数据的实时同步，避免单个团购券在多个分店被消费。

[0016] 上述方法中，商家可以与多个团购网站合作，只需保存所有合作的团购网站的公钥即可，定期或实时向团购网站上传团购券数据。

[0017] 本发明的目的还在于提供一种采用二维条码团购券进行电子商务团购活动的系

统，以更好地解决现有技术存在的问题。

[0018] 为了更好地实现发明的目的，所述系统包括二维条码团购券 100、商家计算机 200、消费者计算机 300、团购服务器 400、短信猫 500、消费者手机 600、移动存储介质 700、消费者打印机 800 和二维条码阅读器 900 组成，其中：

所述消费者计算机 300 通过互联网与团购服务器 400 通信，用于消费者浏览商品信息和进行团购下单；

所述短信猫 500 通过 RS-232 串口或者 USB 接口与团购服务器 400 相连，用于通过移动通信网络将二维条码团购券 100 以短信的方式发送到消费者手机 600；

所述消费者打印机 800 通过并口或者 USB 接口与消费者计算机 300 相连，消费者计算机 300 可以控制费者打印机 800 打印从团购服务器 400 下载二维条码团购券 100；

可选的，所述商家计算机 200 通过互联网与团购服务器 400 通信，用于发布商品信息以及实时传回团购券序列号；

所述二维条码阅读器 900 通过 RS-232 串口或者 USB 接口与商家计算机 200 相连，商家计算机 200 可以控制二维条码阅读器 900 读取消费者手机 600 中或者打印的二维条码团购券 100；

所述商家计算机 200 可以将团购券序列号存储于移动存储介质 700，利用移动存储介质 700 将团购券序列号数据批量传送到团购服务器 400。

[0019] 所述团购服务器 400 包含用户界面模块 401、商户数据上报模块 402、数据库模块 403、订单处理模块 404 和团购券生成模块 405，其中：

所述用户界面模块 401 与数据库模块 403、订单处理模块 404 和团购券生成模块 405 交互，用于接收消费者的团购下单请求，将下单信息送入订单处理模块 404，提供消费者网上付款通道，并在团购券生成模块 405 中生成团购券，发送到消费者手机或者提供给消费者下载，所有的数据都存放在数据库模块 403 中；

所述商户数据上报模块 402 与数据库模块 403 交互，用于接收商家发送回来的团购券序列号，提供通过移动存储介质的批量上传和通过互联网的实时上传两种上传方式；

所述数据库模块 403 与用户界面模块 401、商户数据上报模块 402、订单处理模块 404 和团购券生成模块 405 交互，提供数据临时和长期存储功能；

所述订单处理模块 404 与用户界面模块 401、数据库模块 403 和团购券生成模块 405 交互，用于根据消费者下单信息生成订单，将订单数据存放到数据库模块 403，并通知团购券生成模块 405 生成团购券，将团购券发送到消费者手机或者提供给消费者下载；

所述团购券生成模块 405 用于根据订单数据生成团购券，其中包含数字签名子模块 4051、数据加密子模块 4052 和二维条码生成子模块 4053：

所述数字签名子模块 4051 首先根据订单数据生成团购券数据，再采用团购网站私钥对团购券数据进行数字签名；

所述数据加密子模块 4052 利用商品所属商家的公钥对签名后的团购券数据进行加密，再使用 Base64 字符编码算法对二进制加密数据进行字符编码；

所述二维条码生成子模块 4053 采用二维条码编码算法对字符编码后的二进制加密团购券数据进行编码，生成二维条码图像。

[0020] 所述商家计算机 200 包含用户界面模块 201、数据记录模块 202、数据解密模块 203

和数字签名验证模块 204，其中：

所述用户界面模块 201 与数据记录模块 202 交互，可以将二维条码阅读器所读取的数据录入数据记录模块 202，并且可以从数据记录模块 202 中获取解密后的团购券数据，还提供将团购券序列号批量装载到移动存储介质和通过互联网将团购券序列号实时上传的功能；

所述数据记录模块 202 与用户界面模块 201 和数据解密模块 203 交互，用于记录团购券解密前后的数据；

所述数据解密模块 203 与数据记录模块 202 交互，用于从数据记录模块 202 提取团购券解密前的数据再进行解密，解密过程：首先对解密前的团购券数据进行 Base64 解码，再利用商家自己的私钥对二进制数据进行解密，生成解密的团购券数据，传回数字签名验证模块 204；

所述数字签名验证模块 204 利用团购网站公钥对解密的团购券数据进行数字签名验证，如验证成功就将团购券明文存入数据记录模块 202，供用户界面模块 201 查询和调用。

[0021] 本发明与现有技术相比，具有如下优点和有益效果：

1、与只采用序列号的团购券相比，本发明的二维条码团购券信息容量大，可以存放更多的订单信息，并且可以通过二维条码阅读设备自动读取，方便快捷；

2、本发明的二维条码团购券采用了非对称密码技术，安全可靠，数据进过加密，来源经过验证；

3、本发明的二维条码团购券可离线使用，不要求商家的计算机一定要联网，降低参与团购的商家的经营成本；

4、与目前已有应用的二维条码电子消费券相比，本文提出的二维条码团购券由于对原始数据采用非对称密码技术进行签名和加密，因而增强了安全性，同时并没有增加新的硬件设备。

[0022] 附图说明

图 1 是本发明的二维条码团购券的生成和读取方法的示意图；

图 2 是本发明的采用二维条码团购券进行电子商务团购活动的系统的结构示意图；

图 3 是图 2 中团购服务器的模块图；

图 4 是图 3 中团购券生成模块的子模块图；

图 5 是图 2 中商家计算机的模块图；

图 6 是本发明的实施例中生成二维条码团购券的流程示意图；

图 7 是本发明的实施例中读取二维条码团购券的流程示意图。

[0023] 具体实施方式

下面结合实施例及附图，对本发明作进一步的详细说明，但本发明的实施方式不限于此。

[0024] 实施例 1

如图 1 所示，一种用于电子商务团购活动的二维条码团购券，所述二维条码团购券 100 的形式为二维条码，可以为 PDF417、Maxi Code、QR Code、Data Matrix 等二维条码中的一种。

[0025] 将团购券信息转换成二维条码团购券 100 的步骤包括数字签名、数字加密、

Base64 编码和二维条码编码。

[0026] 利用二维条码团购券 100 读取团购券信息的步骤包括二维条码解码、Base64 解码、数字解密和验证数字签名。

[0027] 所述团购券信息的内容可以包括但不限于以下内容 :序列号、商家 ID、消费者 ID、商品 ID、数量和有效期限。

[0028] 所述序列号为团购券在团购网站中的唯一标识符,不同的二维条码团购券 100 中存储的序列号不能重复 ;

所述商家 ID、消费者 ID、商品 ID 分别是商家、消费者、商品在团购网站中的唯一标识符,不同的商家、消费者、商品的 ID 不能重复 ;

所述数量是团购券中商品的数量 ;

所述有效期限为团购券的使用期限。

[0029] 如图 2 所示,使用该二维条码团购券进行电子商务团购活动的系统包括二维条码团购券 100、商家计算机 200、消费者计算机 300、团购服务器 400、短信猫 500、消费者手机 600、移动存储介质 700、消费者打印机 800 和二维条码阅读器 900 组成,其中 :

所述消费者计算机 300 通过互联网与团购服务器 400 通信,用于消费者浏览商品信息和进行团购下单 ;

所述短信猫 500 通过 RS-232 串口或者 USB 接口与团购服务器 400 相连,用于通过移动通信网络将二维条码团购券 100 以短信的方式发送到消费者手机 600 ;

所述消费者打印机 800 通过并口或者 USB 接口与消费者计算机 300 相连,消费者计算机 300 可以控制费者打印机 800 打印从团购服务器 400 下载二维条码团购券 100 ;

可选的,所述商家计算机 200 通过互联网与团购服务器 400 通信,用于发布商品信息以及实时传回团购券序列号 ;

所述二维条码阅读器 900 通过 RS-232 串口或者 USB 接口与商家计算机 200 相连,商家计算机 200 可以控制二维条码阅读器 900 读取消费者手机 600 中或者打印的二维条码团购券 100 ;

所述商家计算机 200 可以将团购券序列号存储于移动存储介质 700,利用移动存储介质 700 将团购券序列号数据批量传送到团购服务器 400。

[0030] 如图 3 所示,所述团购服务器 400 包含用户界面模块 401、商户数据上报模块 402、数据库模块 403、订单处理模块 404 和团购券生成模块 405,其中 :

所述用户界面模块 401 与数据库模块 403、订单处理模块 404 和团购券生成模块 405 交互,用于接收消费者的团购下单请求,将下单信息送入订单处理模块 404,提供消费者网上付款通道,并在团购券生成模块 405 中生成团购券,发送到消费者手机或者提供给消费者下载,所有的数据都存放在数据库模块 403 中 ;

所述商户数据上报模块 402 与数据库模块 403 交互,用于接收商家发送回来的团购券序列号,提供通过移动存储介质的批量上传和通过互联网的实时上传两种上传方式 ;

所述数据库模块 403 与用户界面模块 401、商户数据上报模块 402、订单处理模块 404 和团购券生成模块 405 交互,提供数据临时和长期存储功能 ;

所述订单处理模块 404 与用户界面模块 401、数据库模块 403 和团购券生成模块 405 交互,用于根据消费者下单信息生成订单,将订单数据存放到数据库模块 403,并通知团购券

生成模块 405 生成团购券，将团购券发送到消费者手机或者提供给消费者下载；

所述团购券生成模块 405 用于根据订单数据生成团购券，如图 4 所示，所述团购券生成模块 405 包含数字签名子模块 4051、数据加密子模块 4052 和二维条码生成子模块 4053，其中：

所述数字签名子模块 4051 首先根据订单数据生成团购券数据，再采用团购网站私钥对团购券数据进行数字签名；

所述数据加密子模块 4052 利用商品所属商家的公钥对签名后的团购券数据进行加密，再使用 Base64 字符编码算法对二进制加密数据进行字符编码；

所述二维条码生成子模块 4053 采用二维条码编码算法对字符编码后的二进制加密团购券数据进行编码，生成二维条码图像。

[0031] 如图 5 所示，所述商家计算机 200 包含用户界面模块 201、数据记录模块 202、数据解密模块 203 和数字签名验证模块 204，其中：

所述用户界面模块 201 与数据记录模块 202 交互，可以将二维条码阅读器所读取的数据录入数据记录模块 202，并且可以从数据记录模块 202 中获取解密后的团购券数据，还提供将团购券序列号批量装载到移动存储介质和通过互联网将团购券序列号实时上传的功能；

所述数据记录模块 202 与用户界面模块 201 和数据解密模块 203 交互，用于记录团购券解密前后的数据；

所述数据解密模块 203 与数据记录模块 202 交互，用于从数据记录模块 202 提取团购券解密前的数据再进行解密，解密过程：首先对解密前的团购券数据进行 Base64 解码，再利用商家自己的私钥对二进制数据进行解密，生成解密的团购券数据，传回数字签名验证模块 204；

所述数字签名验证模块 204 利用团购网站公钥对解密的团购券数据进行数字签名验证，如验证成功就将团购券明文存入数据记录模块 202，供用户界面模块 201 查询和调用。

[0032] 采用该二维条码团购券进行电子商务团购活动的方法包括以下步骤：

(1)准备阶段：团购网站事先采用非对称密码算法为自己生成一对非对称密钥，包括公钥和私钥。商家在团购网站注册时，团购网站也采用非对称密码算法为该商家生成一对非对称密钥，保留该商家的公钥，将该商家的私钥以及团购网站的公钥交付给商家，同时为该商家生成一个商家 ID。商家注册完毕后可以发布商品，每一种商品有一个商品 ID。消费者在团购网站注册时，团购网站为消费者生成一个消费者 ID；

(2) 网上下单：消费者在团购网站上对某个商品下单；

(3) 生成团购券：团购网站确认订单后，生成包含序列号、商家 ID、商品 ID、消费者 ID、商品数量、有效期限等数据的团购券明文(团购券信息)，然后利用自己的私钥对团购券明文进行数字签名，再利用该商品所属的商家的公钥对数字签名后的信息进行加密，最后生成二维条码图像，作为消费者的团购券；

(4)使用团购券：消费者携带该二维条码团购券(二维条码存放于手机彩信中或者打印在纸张上)到商家消费；

(5)读取团购券：商家首先使用二维条码阅读器阅读二维条码，然后使用自己的私钥进行解密，再利用团购网站公钥进行数字签名验证，验证通过后获取团购券信息明文，商家确

认该券未使用后，根据团购券信息向消费者提供商品或服务；

（6）上传团购券：商家通过互联网实时传回团购券序列号，或者商家累计一定数量团购券，通过移动存储介质向团购网站批量上报团购券序列号数据，团购网站返回商家收入分成。

[0033] 如图 6 所示，所述步骤（3）中团购网站生成团购券的流程包括以下子步骤：

（S301）首先根据订单信息创建团购券的明文，可以包括序列号、商家 ID、商品 ID、消费者 ID、商品数量、有效期限等信息，再使用团购网站私钥对原始数据进行数字签名，将数字签名附在明文后面，形成签名后的团购券信息；

（S302）利用商家公钥对签名后的团购券信息进行加密，形成二进制形式的加密团购券信息；

（S303）利用 Base64 字符编码对二进制的加密团购券数据进行字符编码，形成 Base64 编码形式的加密团购券信息；

（S304）利用二维条码编码算法对 Base64 编码形式的加密团购券信息进行编码，生成二维条码图像，该图像即为最终团购券。

[0034] 所述步骤（3）中，数字签名和加密的顺序不能颠倒，否则签名信息有可能被第三方所伪造，降低团购券安全性。

[0035] 如图 7 所示，所述步骤（5）中，商家读取团购券流程包括以下子步骤：

（S501）使用二维条码阅读器读取并解码团购券图像数据，形成 Base64 字符编码形式的加密团购券信息；

（S502）对 Base64 字符编码形式的加密团购券信息进行 Base64 字符编码的解码，形成二进制形式的加密团购券信息；

（S503）利用商家私钥对二进制数据进行解密，形成包含数字签名的已解密团购券信息；

（S504）利用团购网站公钥对数字签名部分进行验证，验证成功后读取团购券明文数据，该数据为团购券的实际数据。

[0036] 所述步骤（6）中，如果商家存在多个分店，则必须采用实时传回团购券序列号的方法，以保证数据的实时同步，避免单个团购券在多个分店被消费。

[0037] 上述方法中，商家可以与多个团购网站合作，只需保存所有合作的团购网站的公钥即可，定期或实时向团购网站上传团购券数据。

[0038] 如上所述，便可较好地实现本发明，上述实施例仅为本发明的较佳实施例，并非用来限定本发明的实施范围；即凡依本发明内容所作的均等变化与修饰，都为本发明权利要求所要求保护的范围所涵盖。

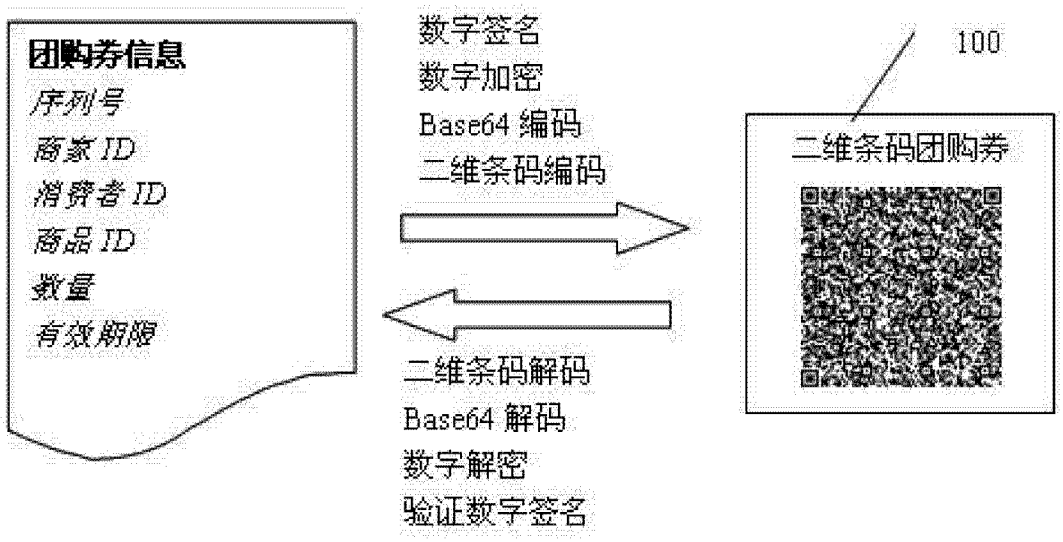

团购券信息
序列号
商家 ID
消费者 ID
商品 ID
数量
有效期限
数字签名
数字加密
Base64 编码
二维条码编码
二维条码解码
Base64 解码
数字解密
验证数字签名
100
二维条码团购券

图 1

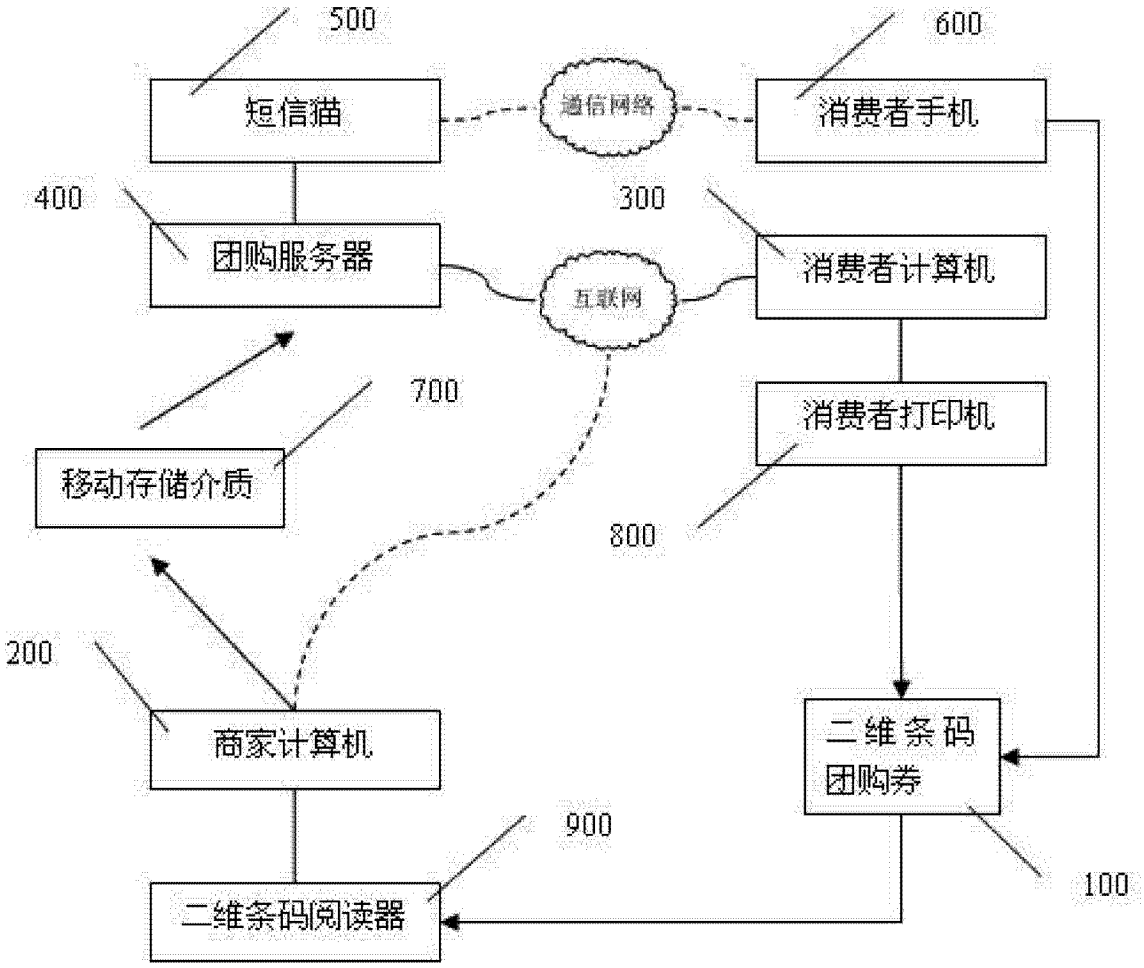

500
600
短信猫
通信网络
消费者手机
400
300
团购服务器
互联网
消费者计算机
700
消费者打印机
移动存储介质
800
200
商家计算机
二维条码
团购券
900
100
二维条码阅读器

图 2

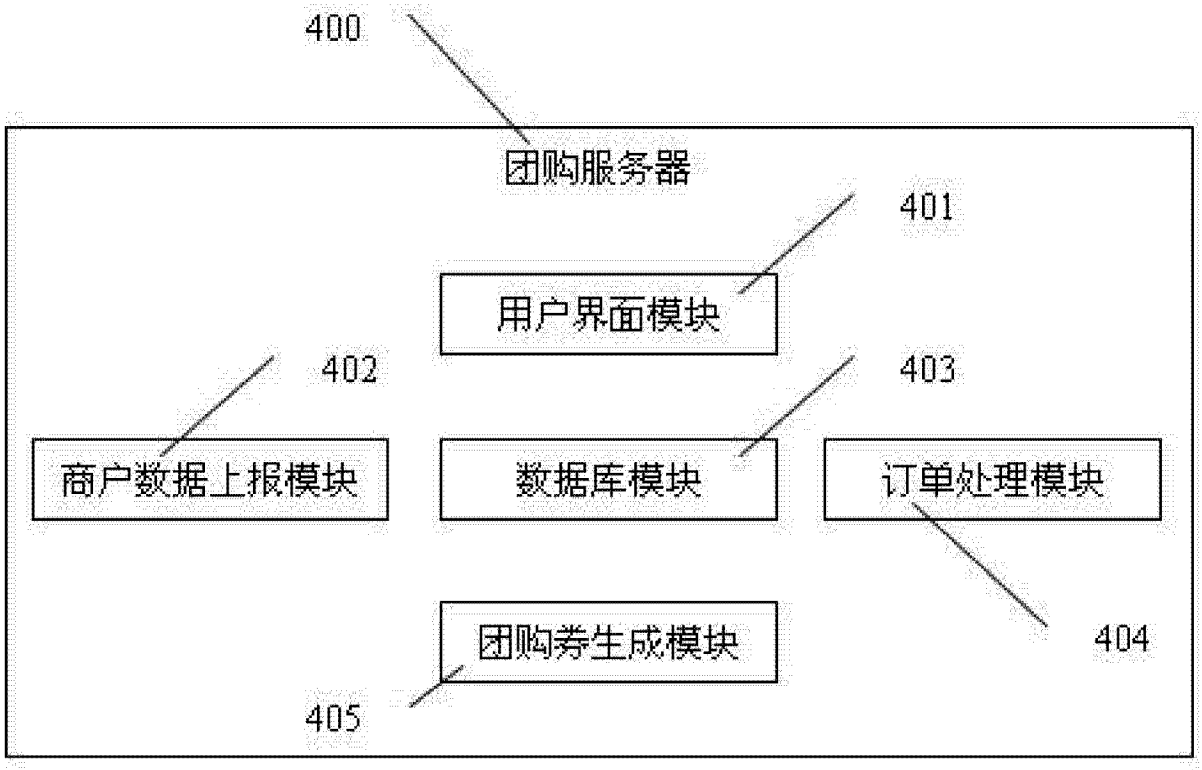

400
团购服务器
401
用户界面模块
402
商户数据上报模块
403
数据库模块
订单处理模块
404
团购券生成模块
405

图 3

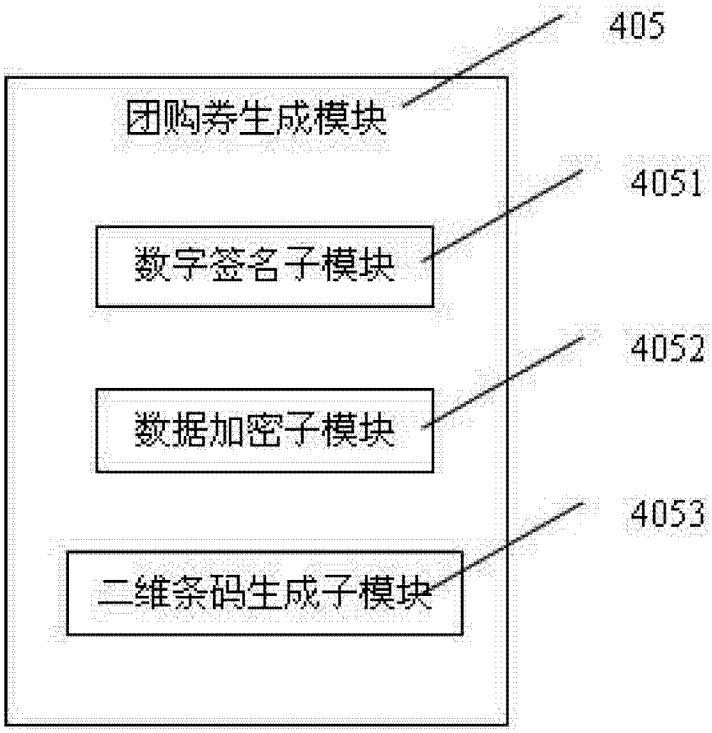

405
团购券生成模块
4051
数字签名子模块
4052
数据加密子模块
4053
二维条码生成子模块

图 4

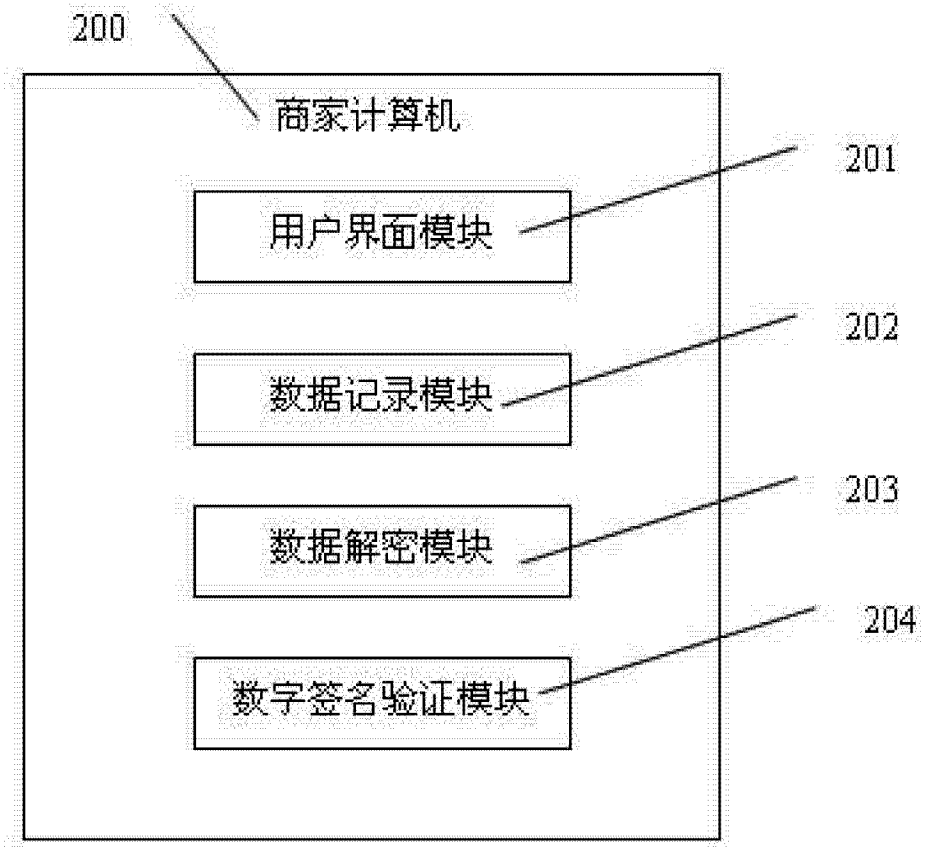


图 5

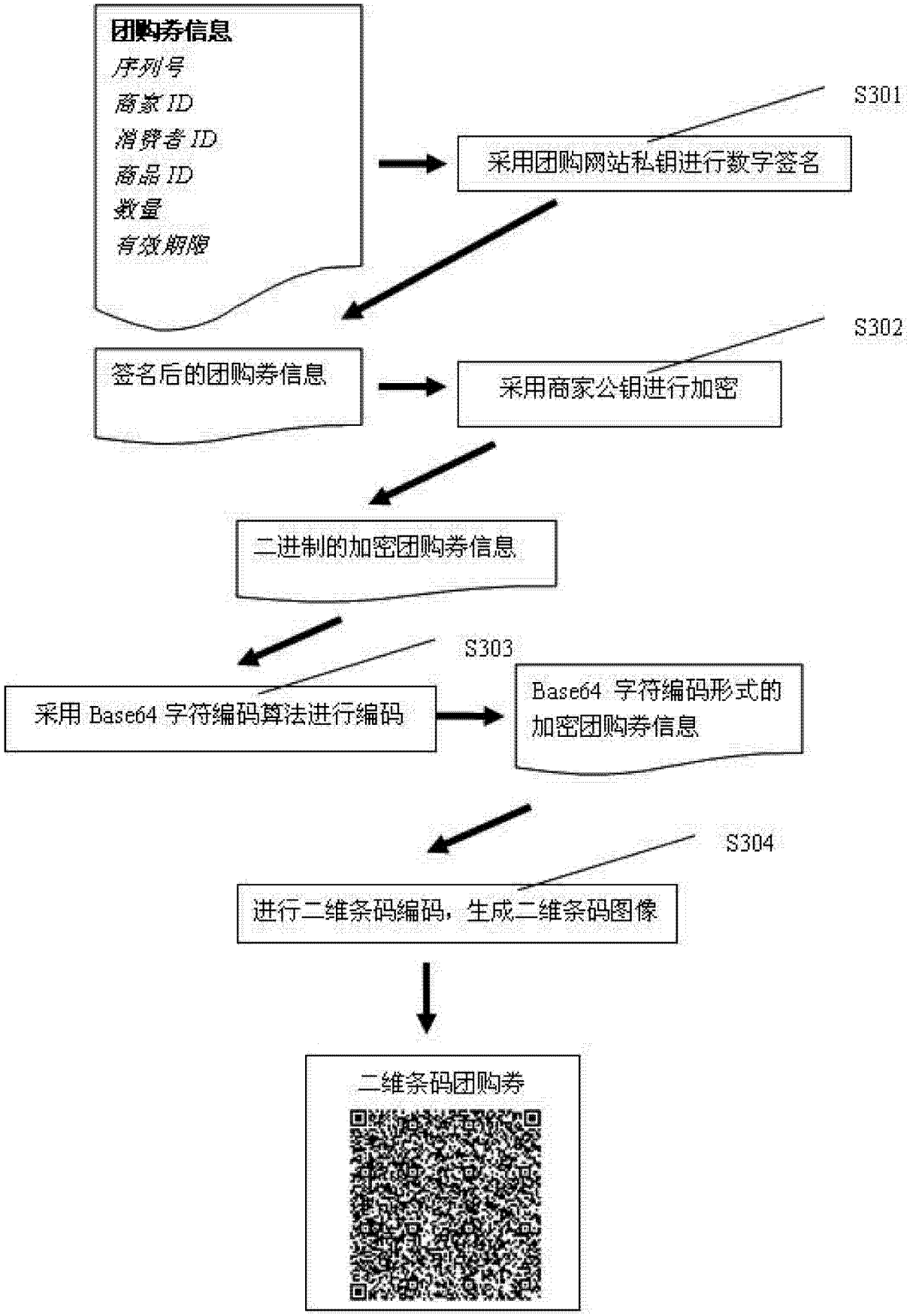

团购券信息
序列号
商家 ID
消费者 ID
商品 ID
数量
有效期限
S301
采用团购网站私钥进行数字签名
签名后的团购券信息
S302
采用商家公钥进行加密
二进制的加密团购券信息
S303
采用 Base64 字符编码算法进行编码
Base64 字符编码形式的加密团购券信息
S304
进行二维条码编码，生成二维条码图像
二维条码团购券

图 6

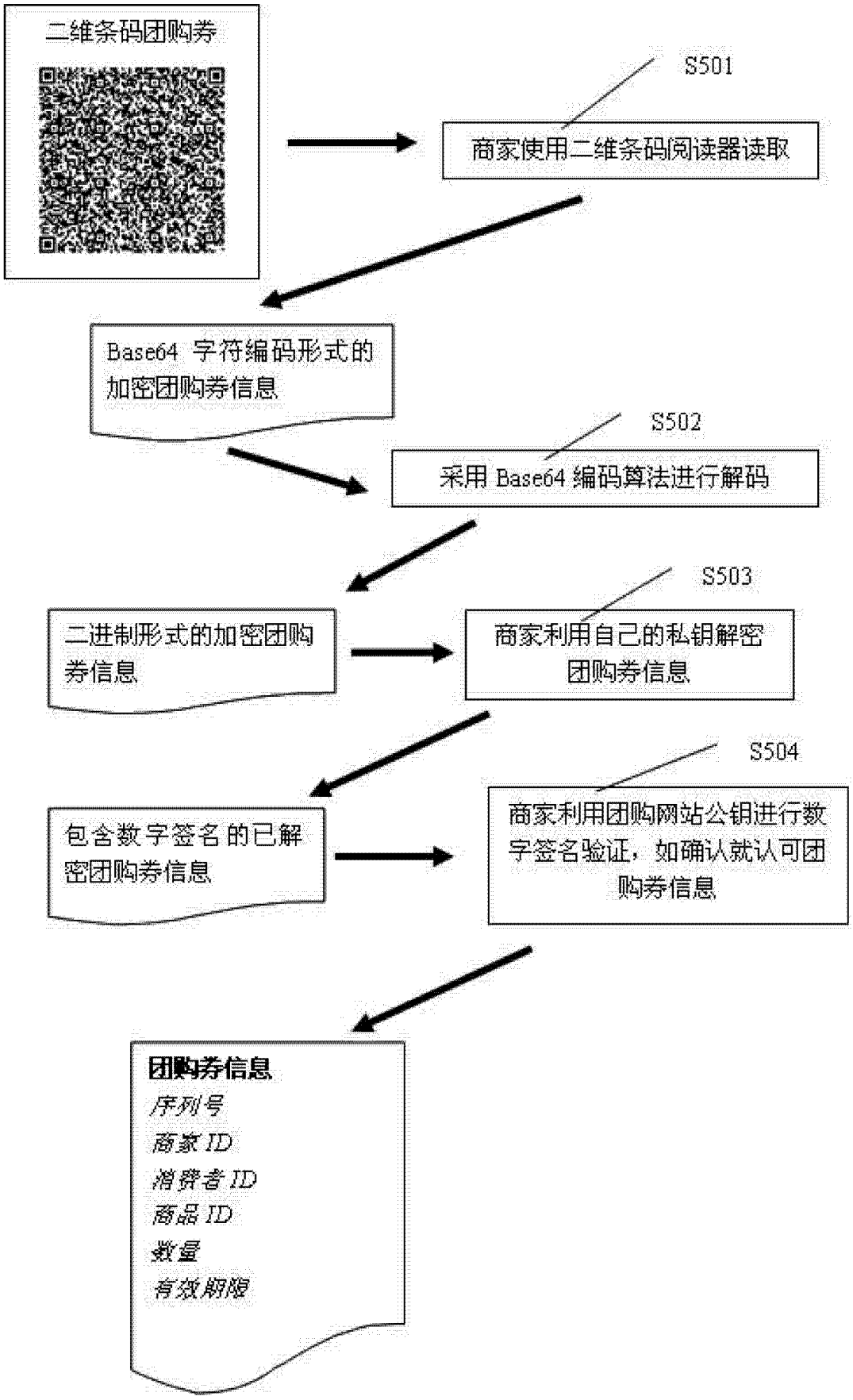

二维条码团购券
S501
商家使用二维条码阅读器读取
Base64 字符编码形式的加密团购券信息
S502
采用 Base64 编码算法进行解码
二进制形式的加密团购券信息
S503
商家利用自己的私钥解密团购券信息
包含数字签名的已解密团购券信息
S504
商家利用团购网站公钥进行数字签名验证，如确认就认可团购券信息
团购券信息
序列号
商家 ID
消费者 ID
商品 ID
数量
有效期限

图 7