基于 PKI 的二维条码电子消费券及其系统设计*

梁英宏，刘义春
（广东商学院 广东省电子商务市场应用技术重点实验室，广州 510320）

摘　要：目前在电子商务中主要采用序列号形式的电子消费券，信息容量小且安全性差。为解决该问题，将 PKI 与二维条码技术相结合，提出一种新型二维条码电子消费券及其使用流程和系统架构，该电子消费券的创建过程为：将原始的消费券信息利用 PKI 技术进行签名和加密后，再利用Base64编码进行字符编码，最后利用二维条码技术生成二维条码图像形式的电子消费券。实验证明，相比现有技术，该电子消费券信息容量大，数据安全且来源可靠，并可以支持离线使用，适用于团购等新的电子商务模式。

关键词：电子消费券；序列号；公钥基础设施；二维条码；团购
中图分类号：TP391　　**文献标志码**：A　　**文章编号**：1001-3695(2012)06-2161-04
doi:10.3969/j.issn.1001-3695.2012.06.042

PKI and 2D barcode based electronic voucher and its system design

LIANG Ying-hong, LIU Yi-chun
(*Guangdong Key Laboratory of Electronic Commerce*, *Guangdong University of Business Studies*, *Guangzhou* 510320, *China*)

Abstract: Currently serial numbers are the most commonly used electronic vouchers for e-commerce, which can not store information and have bad security. This paper proposed a PKI and 2D barcode based electronic voucher, as well as the processing flow and system architecture for supporting its applications. The generation process included three steps: the first step signed and encrypted the original voucher data using the PKI technology. The second step mapped the encrypted data to Base64 characters. Finally the characters were coded to a 2D barcode image with a 2D barcode algorithm. Experimental results prove that compared with the existing technologies, the new electronic voucher has more data capacity and security, and supports offline use, which is suitable for new e-commerce models such as group purchase.

Key words: electronic voucher; serial number; public key infrastructure; 2D barcode; group purchase

0　引言

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。一些商家利用电子消费券（折扣券、团购券）作为电子商务消费凭证，特别是在团购模式，电子消费券成为消费者到指定商家进行消费的唯一认证方式。

目前的电子商务团购流程为：团购网站发布商家打折商品的信息，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。这种序列号团购券技术简单、应用普遍，但也存在以下问题：

a）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并使用，同时也存在被他人掌握序列号生成规则的可能。

b）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。

c）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需要多个序列号，取货时商家也必须逐一验证，效率低下。

为了提高安全性和加快验证速度，也有部分商家采用二维条码作为电子消费券载体。将优惠券或票据信息通过二维条码进行编码形成图片发送到消费者手机，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。这种二维条码电子消费券与序列号电子消费券本质相同，但票据信息容量大、保密性更好。

在目前的二维条码电子消费券技术的基础上，本文考虑将基于 PKI 技术的加密和签名技术应用于电子消费券，相比序列号电子消费券能够记录更多信息，同时具备支持离线交易和安全性。

本文提出了一种用于电子商务的二维条码电子消费券以及其使用流程和系统架构，旨在解决现有技术存在的安全性差和不支持离线交易的问题，能够帮助商户方便地参与多个电子商务网站的营销活动。

收稿日期：2011-11-05；**修回日期**：2011-12-08　　**基金项目**：广东省科技计划资助项目(2009B090300347)；广东商学院校级课题资助项目(08YB52002)

作者简介：梁英宏(1978-)，男，安徽蚌埠人，副教授，博士，主要研究方向为商务智能与安全(lyhwin@yeah.net)；刘义春(1965-)，男，湖南岳阳人，副教授，主要研究方向为信息安全、商务智能.

1 基于 PKI 和二维条码电子消费券的工作原理

PKI(public key infrastructure)是利用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施。基于 PKI 技术的二维条码电子消费券将原始的消费券信息利用 PKI 技术进行签名和加密后,再利用二维条码技术进行图像编码,最后生成二维条码图像形式的电子消费券,可以发送到消费者的移动终端或者提供给消费者下载打印。图 1 显示了基于 PKI 的二维条码电子消费券的创建和读取原理。

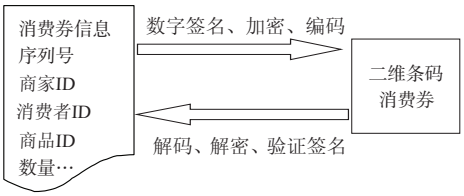

图 1 基于 PKI 的二维条码电子消费券的创建和读取原理

1.1 采用 PKI 技术对电子消费券数据进行签名和加密

PKI 采用公钥加密技术,提供一整套安全的基础平台。在公钥密码技术中,每个用户拥有一对相匹配的公私钥。其中的公钥对外公开,私钥由用户自己安全保管[1~3]。

电子消费券的安全性包括两方面:

a)信息加密,即电子消费券的信息只能被应该享有信息的商家所获取,消费者携带电子消费券到哪个商家去消费,该商家才应该获取信息,他人不应当获取该信息。

b)来源的真实性,即电子消费券应当是消费者通过合法渠道获得的,以团购为例,商家应当识别电子消费券是否为自己注册(授权)的团购网站所发行,特别是当一个商家在多个团购网站进行营销活动时,能够识别电子消费券来自于哪一家团购网站。

以上的安全可以利用 PKI 技术进行解决。为团购网站和商家分别生成一对密钥——公钥和私钥,双方持有各自的私钥和对方的公钥。

a)团购网站生成电子消费券时,利用自己的私钥对商家的电子消费券信息进行数字签名,再利用商家公钥加密签名后的数据。

b)商家读取电子消费券时,利用自己的私钥解密电子消费券,再利用团购网站的公钥鉴定数字签名真实性,确认电子消费券来自哪家团购网站,最后获取真实的电子消费券信息。

通过以上流程,电子消费券既得到加密,又能够被确认来源。以上流程也是目前电子商务交易数据传递的安全基础,但是目前只是一种虚拟的数据安全传送方式,并不能通过实物化展现,因此就考虑使用二维条码作为加密数据载体。

1.2 采用二维条码对加密数据进行图像编码

团购网站生成签名和加密后的电子消费券后,采用二维条码技术对数据进行编码,生成二维条码图像。该图像即为电子消费券的最终形式,可以存储于消费者的手机等移动终端设备,也可以打印成纸张优惠券。

商家验证电子消费券时,首先利用相应的二维条码阅读器读取二维条码的加密数据,然后再进行数据解密和签名验证,最终获取真实数据。

值得注意的是,由于经过签名和加密的电子消费券信息是二进制数据,需要通过 Base64 编码[4](或其他二进制数据转换为可打印字符的编码)对二进制数据进行编码,生成的字符编码才可用于二维条码编码。读取电子消费券时相反,也要经过 Base64解码过程。

1.3 电子消费券的生成和验证流程

按照 1.1 和 1.2 节的原理描述,图 2 和 3 分别显示了基于 PKI 的二维条码电子消费券的生成和验证(读取)流程。

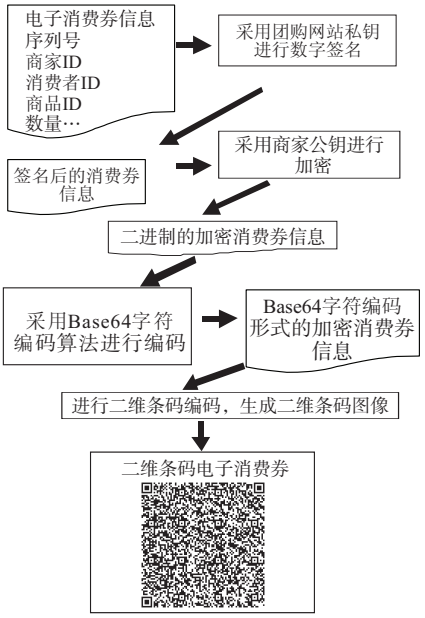

图 2 电子消费券的生成流程

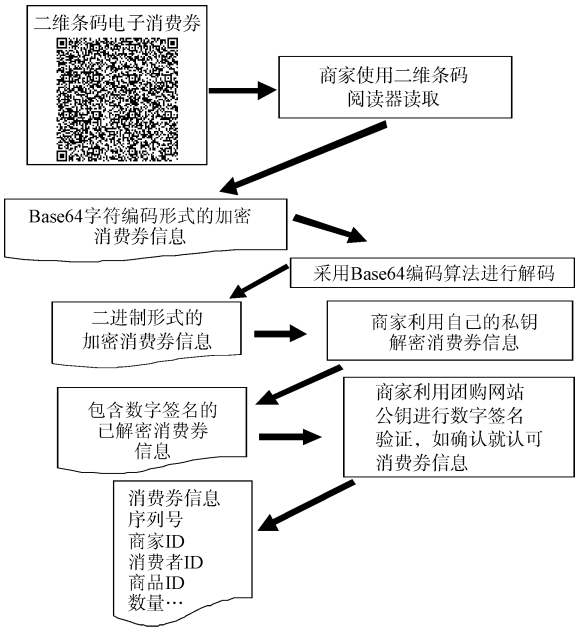

图3 电子消费券的验证流程

团购网站生成电子消费券流程:

a)根据订单信息创建电子消费券的明文,可以包括商家 ID、商品 ID、数量、使用期限等数据。

b)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。

c)利用商家公钥对签名后的数据进行加密,形成加密的二进制电子消费券数据。

d)利用Base64编码对二进制电子消费券数据进行字符编码,形成加密的电子消费券字符数据。

e)利用 QR 二维条码编码算法对电子消费券字符数据进

行编码,生成 QR 二维条码图像,该图像即为最终可显示的电子消费券。

商家验证电子消费券流程:

a)使用二维条码阅读器读取并解码电子消费券图像数据。

b)对所解码图像数据进行Base64解码,形成二进制数据。

c)利用商家私钥对二进制数据进行解密,形成包含签名的电子消费券数据。

d)利用团购网站公钥对数字签名部分进行验证。

e)验证成功后读取电子消费券明文数据,该数据为电子消费券的实际数据。

值得注意的是,在电子消费券生成过程中,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,降低电子消费券安全性。

2　基于 PKI 的二维条码电子消费券的使用流程

以团购为例,采用上述二维条码电子消费券进行电子商务团购活动的方法包括以下步骤:

a)准备阶段。商家在团购网站注册时,团购网站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。

b)网上下单。消费者在团购网站上对某个商品下单。

c)生成团购券(电子消费券)。团购网站确认订单后,利用自己的私钥对团购券进行数字签名,再利用该商品所属的商家的公钥对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。

d)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。

e)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。

f)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上报团购券序列号数据,团购网站返回商家收入分成。

所述步骤 f)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。

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,定期或实时地向团购网站上传团购券数据。

2.1　实例演示

本文采用 GnuPG 工具[5,6]生成密钥对,加密算法为 1024 bit的 RSA[7,8]算法,生成团购网站“Super Group Web”和商家“Berry Cake Shop”的密钥对。

1)团购网站生成团购券

a)团购券数据如图 4 所示。

```
0000101,230400000055,1
```

图4　团购券明文数据

图4 中,表示商家 ID 为 0000101,商品 ID 为 230400000055,数量为 1 个。采用团购网站 Super Group Web 的私钥进行数字签名,再利用商家 Berry Cake Shop 的公钥进行加密,加密后的数据为二进制数据(文本编辑器打开效果),如图 5 所示。

图5　签名和加密后的二进制团购券数据

b)采用Base64编码对二进制数据进行编码,形成可识别字符数据,如图 6 所示。

```
hIwDigahAi4Eo0QBA/9mK+hqolmPmjajUxzldFKtbL4Xs9NFaE3Hz3xMNhhdChCSHPcOEhEf19U3
bq8BzzDahYaqEcIS3nB75pHycXbPsz0eMd3WOhdWVT32MBu3ed9u7BA0n7ZXECRNibNE11xuzRss
Qxtb3soFF0AbnP5qsETtF+I9rute+Rh/+jzFrdLARAEj2kvnUp3WG//3M5Qdcs0yYIIEhdcwTRZp
FWKP49uFqCOaOvhicm9wMah4UGivEJ2Y7ILEhxSzh58+rFchbT3dYJ3014uIKOwMW9dR/4Sb0e69
rPvAYdAS5pBWs7+HyYPZE7heSpDBNrPkwK+8k1KMoYL+9Jvmr57U/am1UThsMOFAOt0dvajBjP4F
vFR3mvFzSo+6Y+cFSpBBrGG7AmpO9/WHqD+7Cm9dgZyK+Y13y1bJ2BFhNACOo50BFPztoly527BZ
cLAb+1ji3giMuQodnXE8zd0qv8q7PCKHr1ebVTDisqwzyYbBRnb5zg5S2DkHGJvyzc5V931z5e/K
ckqC17NR
```

图6　Base64编码后的团购券字符数据

c)利用 QR 码[9,10]进行二维条码编码,生成 QR 二维条码图像,如图 7 所示。

图7　QR 编码后的团购券图像

2)商家读取团购券

商家读取团购券的过程与生成过程正好相反,具体如下:

a)商家利用二维条码阅读器读取二维条码团购券的数据,读取的数据为Base64编码。

b)利用Base64解码,形成二进制加密数据。

c)商家利用自己的私钥进行解密,获得数字签名数据和团购券明文数据。

d)商家利用团购网站的公钥进行数字签名验证,验证团购券来源,如验证成功就认可团购券明文数据,根据团购券明文数据为消费者提供服务。

3　基于 PKI 的二维条码电子消费券的系统架构

为了使用本文提出的二维条码电子消费券,本文设计了支持基于 PKI 的二维条码电子消费券工作的系统,以团购电子商务为例,系统架构如图 8 所示。

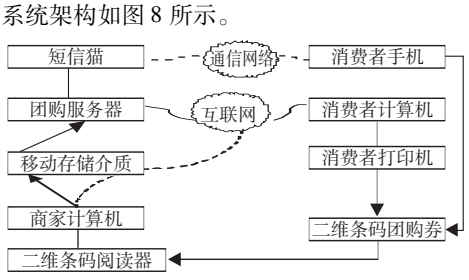

图8　基于 PKI 的二维条码电子消费券的系统架构

如图 8 所示,整个系统包括二维条码团购券、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。其具体过程如下:

a)消费者计算机通过互联网与团购服务器通信,用于消费者进行团购下单。

b)短信猫通过 RS-232 串口或者 USB 接口与团购服务器相连,用于通过移动通信网络将二维条码团购券以短信的方式发送到消费者手机。

c)消费者打印机通过并口或者 USB 接口与消费者计算机相连,消费者计算机可以控制消费者打印机打印从团购服务器下载二维条码团购券。

d)可选地,所述商家计算机通过互联网与团购服务器通信,用于发布商品信息,以及实时传回团购券序列号。

e)二维条码阅读器通过 RS-232 串口或者 USB 接口与商家计算机相连,商家计算机可以控制二维条码阅读器读取消费者手机中或者纸张上的二维条码团购券图像;

f)商家计算机可以将团购券序列号存储于移动存储介质,利用移动存储介质将团购券序列号数据传送到团购服务器。

如图9所示,团购服务器安装的程序模块包括用户界面、商户数据上报、数据库模块、订单处理和团购券生成模块。

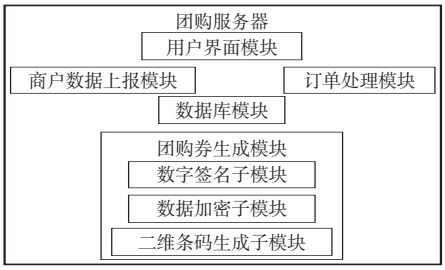

图9 团购服务器中程序的模块划分

a)用户界面模块与数据库模块、订单处理模块和团购券生成模块交互,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,提供消费者网上付款通道,并在团购券生成模块中生成团购券,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中。

b)商户数据上报模块与数据库模块交互,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。

c)数据库模块与用户界面模块、商户数据上报模块、订单处理模块和团购券生成模块交互,用于数据临时和长期存储功能。

d)订单处理模块与用户界面模块、数据库模块和团购券生成模块交互,用于根据消费者下单信息生成订单,将订单数据存放于数据库,并通知团购券生成模块生成团购券,将团购券发送到消费者手机或者提供给消费者下载。

e)团购券生成模块用于根据订单数据生成团购券,其中包含数字签名子模块、数据加密子模块和二维码生成子模块:

(a)数字签名子模块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签名。

(b)数据加密子模块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对二进制加密数据进行字符编码。

(c)二维码生成子模块采用二维码编码算法对字符编码后的二进制团购券数据进行编码,生成二维条码图像。

如图10所示,商家计算机安装的程序模块包括用户界面、数据记录、数字签名验证和数据解密模块。

a)用户界面模块与数据记录模块交互,可以将二维条码阅读器所读取的数据录入数据记录模块,并且可以从数据记录模块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。

b)数据记录模块与用户界面模块和数据解密模块交互,用于记录二维条码的解密前后的数据。

c)数据解密模块与数据记录模块交互,用于从数据记录模块提取二维条码解密前的数据。解密过程为: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。

d)数字签名验证模块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,供用户界面模块查询和调用。

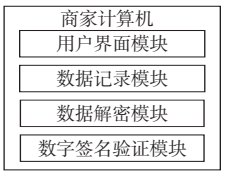

图10 商家计算机中程序的模块划分

4 结束语

本文将 PKI 技术与二维条码技术相结合,设计了一种能够以实物显示的加密电子消费券,并对其使用流程和支撑系统架构进行了设计;采用 GnuPG 软件和 QR 条码对本文设计的电子消费券进行了验证,该加密电子消费券及其使用方法和系统已经申请了国家发明专利(申请号:201110335319.6)。相比目前广泛采用的序列号电子消费券,本文提出的基于 PKI 的二维条码电子消费券的优势在于:a)信息容量大,读取方便;b)安全可靠,数据经过加密,来源经过验证;c)可离线使用。与目前已有应用的二维条码电子消费券相比,本文提出的新型电子消费券由于对原始数据采用非对称密码进行加密和签名,增强了安全性,同时并没有增加新的硬件设备。

参考文献:

[1] 张福泰,孙银霞,张磊,等. 无证书公钥密码体制研究[J]. 软件学报,2011,22(6):1316-1332.

[2] 张琳. 基于 PKI 的电子商务安全研究[J]. 电子科技大学学报,2009,38(S1):101-103.

[3] 吴振强,周彦伟,马建峰. 物联网安全传输模型[J]. 计算机学报,2011,34(8):1351-1364.

[4] 陈雅芳,徐从富. 基于Base64 编码的垃圾图片过滤方法[J]. 计算机工程,2011,37(8):194-196.

[5] JONCZY J, WUTHRICH M, HAENNI R. A probabilistic trust model for GnuPG[C]//Proc of the 23rd Chaos Communication Congress. Berlin: Chaos Computer Club, 2006: 61-66.

[6] 刘智莹,朱程荣. 基于 PHP 实现数据安全性的方法及比较[J]. 计算机工程与设计,2009,30(19):4387-4392.

[7] 司光东,杨加. RSA 算法中的代数结构[J]. 电子学报,2011,39(1):242-246.

[8] 魏福山,马传贵,程庆丰. 基于 RSA 的网关口令认证密钥交换协议[J]. 计算机学报,2011,34(1):38-45.

[9] 杨佳丽,高美凤. QR 码图像二值化的研究[J]. 计算机工程与应用,2009,45(35):176-178.

[10] 刘悦,刘明业. QR code 二维条码数据编码的研究[J]. 北京理工大学学报,2005,25(4):352-355.