(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113630261 B
(45)授权公告日 2021.12.17

(21)申请号 202111189992.3

(22)申请日 2021.10.13

(65)同一申请的已公布的文献号
申请公布号 CN 113630261 A

(43)申请公布日 2021.11.09

(73)专利权人 环球数科集团有限公司
地址 518063 广东省深圳市南山区粤海街道高新南九道10号深圳湾科技生态园10栋B座17层01-03号

(72)发明人 张卫平 丁烨 张浩宇

(74)专利代理机构 北京清控智云知识产权代理事务所(特殊普通合伙) 11919
代理人 马肃

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G07B 11/00(2006.01)

(56)对比文件
EP 1363424 A2,2003.11.19
CN 109379185 A,2019.02.22
CN 103400418 A,2013.11.20
CN 103067164 A,2013.04.24
zhang qing,等.The large prime numbers generation of RSA algorithm based on genetic algorithm.《2011 International Conference on Intelligence Science and Information Engineering》.2011,
许可嘉等.基于离散对数签名的安全电子门票系统.《电脑知识与技术》.2017,(第16期),
雷超阳.基于RSA的数字签名技术研究与实现.《长沙通信职业技术学院学报》.2008,(第04期),

审查员 段燕辉

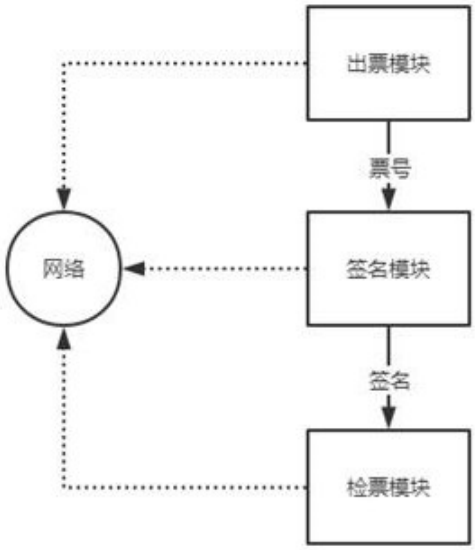
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于沙盒内签名和非对称加密技术的离线检测票务系统

(57)摘要

本发明提供了基于沙盒内签名和非对称加密技术的离线检测票务系统,包括签名模块、出票模块和检票模块,所述出票模块用于产生票号,所述签名模块和所述检票模块各自设有非对称加密技术中的公钥和私钥,所述签名模块和所述检票模块含有相同的中间数生成器,所述签名模块根据票号信息和中间数生成器生成中间数,并用公钥对所述中间数进行加密得到签名,所述检票模块对签名用私钥进行解密得到中间数,所述检票模块根据票号和中间数生成器生成中间数,并将两个中间数进行核对,核对无误后则检票成功;该系统保障安全性的前提下能够在离线状态下进行检票,降低在一些偏远地区的景区对网络的依赖度,降低部署检票机的复杂度。



CN 113630261 B

1.基于沙盒内签名和非对称加密技术的离线检测票务系统，其特征在于，包括签名模块、出票模块和检票模块，所述出票模块用于产生票号，所述签名模块和所述检票模块各自设有非对称加密技术中的公钥和私钥，所述签名模块和所述检票模块含有相同的中间数生成器，所述签名模块根据票号信息和中间数生成器生成中间数，并用公钥对所述中间数进行加密得到签名，所述检票模块对签名用私钥进行解密得到中间数，所述检票模块根据票号和中间数生成器生成中间数，并将两个中间数进行核对，核对无误后则检票成功；

所述签名模块进行签名的方法包括如下步骤：

S1、所述签名模块读取票号信息并转换为数值n(P)，所述数值n(P)为长度为32位的数；

S2、所述签名模块读取时间信息并转换为数值n(T)，所述n(T)为票号生效日的零点零分零秒与1970年1月1日零点零分零秒之间的秒数差；

S3、所述签名模块对所述票号信息和所述时间信息进行处理得到一段长为L的中间数n(N)；

S4、所述签名模块用公钥对所述中间数进行加密得到签名；

步骤S3中得到中间数n(N)的具体过程包括如下步骤：

S21、将所述数值n(T)用32位的二进制表示；

S22、读取所述数值n(T)中数值为1的位数形成数组a[i]，所述数组a[i]的成员个数为n_1，读取所述数值n(T)中数值为0的位数形成数组b[j]，所述数组b[j]的成员个数为n_2，$n_1+n_2=32$；

S23、将所述数值n(P)中位于数组a[i]中的数按顺序重新构成一个长度为n_1的数值P1，将所述数值n(P)中位于数组b[j]中的数按顺序重新构成一个长度为n_2的数值P2；

所述中间数生成器根据票号信息和时间信息生成一个大数Z：

$$Z=\left(P1\bullet\prod_{i=1}^{n_1}(a[i]+1)+1\right)\bullet\left(P2\bullet\prod_{j=1}^{n_2}(b[j]+1)-1\right)-1;$$

将所述大数Z因式分解得到：

$$Z=r\bullet\prod_{i=1}^{m}u_i^{x_i};$$

其中，$\{u_i\}$为升序排列的质数数列，x_i为大数Z中含有的某一质数u_i的个数，r为剩余数，m为质数的个数；

r和m需满足的条件为：

$$Long(r)+\sum_{i=1}^{m}Long(x_i)=L;$$

其中，Long()函数表示取数的位数，L为中间数的长度；

将数列$\{x_i\}$和r拼接成长度为L的中间数。

2.如权利要求1所述的基于沙盒内签名和非对称加密技术的离线检测票务系统，其特征在于，所述出票模块产生的票号包括两个字段，第一字段用于表示票号种类，第二部分用于表示票号序列，当票号是在联网状态下产生时，票号种类为连续票，其票号序列与上一个票号序列连续，当票号在断网状态下产生时，票号种类为随机票，其票号序列为随机产生。

3.如权利要求2所述的基于沙盒内签名和非对称加密技术的离线检测票务系统，其特

征在于,所述检票模块包括识别单元和解密单元,所述识别单元通过识别电子票或纸质票上的图像得到票号信息和签名信息,所述解密单元对所述签名信息进行解密得到中间数。

4.如权利要求3所述的基于沙盒内签名和非对称加密技术的离线检测票务系统,其特征在于,所述中间数生成器处于沙盒环境,无法通过读取代码来获知中间数生成器的内在逻辑。

基于沙盒内签名和非对称加密技术的离线检测票务系统

技术领域

[0001] 本发明涉及信息处理技术领域，尤其涉及基于沙盒内签名和非对称加密技术的离线检测票务系统。

背景技术

[0002] 当前景区的票务系统大部分是联网的，能够保证门票的真实性，但在一些网络不完善的景区，通过人工检票来识别门票的真实性，但这种方法存在安全漏洞，无法识别伪装程度高的假票，本发明提供了一种能够在离线状态下进行检票，同时具有高防伪性的票务系统。

[0003] 现在已经开发出了很多票务系统，经过我们大量的检索与参考，发现现有的票务系统有如公开号为KR100184696B1，KR100646066B1、CN107578479B和KR100263937B1所公开的系统，方法包括：票包括交互信息，交互信息包括检票信息和检票服务地址。检票装置读取票的交互信息，根据交互信息包括的检票服务地址，请求检票服务地址对应的检票服务。检票服务地址可以是多种检票地址的组合，从而实现了多种不同组合的检票服务，譬如各票务代理提供检票服务、票务代理联合提供检票服务、统一的检票服务和分类的检票服务等。票的检票服务地址为系统的纽带和桥梁，将票务代理、购票终端和检票服务联系起来。

发明内容

[0004] 本发明的目的在于，针对所存在的不足，提出了基于沙盒内签名和非对称加密技术的离线检测票务系统，

[0005] 本发明采用如下技术方案：

[0006] 基于沙盒内签名和非对称加密技术的离线检测票务系统，包括签名模块、出票模块和检票模块，所述出票模块用于产生票号，所述签名模块和所述检票模块各自设有非对称加密技术中的公钥和私钥，所述签名模块和所述检票模块含有相同的中间数生成器，所述签名模块根据票号信息和中间数生成器生成中间数，并用公钥对所述中间数进行加密得到签名，所述检票模块对签名用私钥进行解密得到中间数，所述检票模块根据票号和中间数生成器生成中间数，并将两个中间数进行核对，核对无误后则检票成功；

[0007] 所述中间数生成器先根据票号信息和时间信息生成一个大数Z：

[0008] $$Z=\left(P1\bullet\prod_{i=1}^{n_1}(a[i]+1)+1\right)\bullet\left(P2\bullet\prod_{j=1}^{n_2}(b[j]+1)-1\right)-1;$$

[0009] 其中，P1和P2为由票号信息得的两个数，数组a[i]和b[j]为由时间信息得到的两个数组，n_1为数组a[i]的长度，n_2为数组b[j]的长度；

[0010] 将所述大数Z因式分解得到：

[0011] $$Z=r\bullet\prod_{i=1}^{m}u_i^{x_i};$$

[0012] 其中，$\{u_i\}$为升序排列的质数数列，x_i为大数Z中含有的某一质数u_i的个数，r为剩余数，m为质数的个数；

[0013] r和m需满足的条件为：

[0014] $$Long(r)+\sum_{i=1}^{m}Long(x_i)=L$$；

[0015] 其中，Long()函数表示取数的位数，L为中间数的长度；

[0016] 将数列$\{x_i\}$和r拼接成长度为L的中间数；

[0017] 进一步的，所述出票模块产生的票号包括两个字段，第一字段用于表示票号种类，第二部分用于表示票号序列，当票号是在联网状态下产生时，票号种类为连续票，其票号序列与上一个票号序列连续，当票号在断网状态下产生时，票号种类为随机票，其票号序列为随机产生；

[0018] 进一步的，所述检票模块包括识别单元和解密单元，所述识别单元通过识别电子票或纸质票上的图像得到票号信息和签名信息，所述解密单元对所述签名信息进行解密得到中间数；

[0019] 进一步的，所述中间数生成器处于沙盒环境，无法通过读取代码来获知中间数生成器的内在逻辑；

[0020] 进一步的，所述P1、P2的构建方法为：

[0021] 将时间信息用二进制表示，数值为1的位数形成数组a[i]，数值为0的位数形成数组b[i]，将票号信息中位于数组a[i]中的数按顺序重新构成一个长度为n_1的数值P1，将票号信息中位于数组b[i]中的数按顺序重新构成一个长度为n_2的数值P2。

[0022] 本发明所取得的有益效果是：

[0023] 本系统的签名模块对票号进行加密签名，检票模块对签名进行解密，从而实现高防伪性的离线检测效果，适合一些偏远景区，同时也可以减少检票端的网络设备，降低部署成本，本系统在加密和解密过程中添加了中间数概念，所述中间数与票号和时间相关，必须同时掌握中间数的生成逻辑和公私钥的加解密逻辑才能通过检票，加大了安全性能，本发明的出票模块也能够在断网模式下进行工作，方便游客在特殊环境下获取票号。

附图说明

[0024] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制，而是将重点放在示出实施例的原理上。在不同的视图中，相同的附图标记指定对应的部分。

[0025] 图1为整体结构框架示意图；

[0026] 图2为离线检票原理示意图；

[0027] 图3为P1、P2构建示例示意图；

[0028] 图4为游客操作流程示意图；

[0029] 图5为检票中对相同票号的处理流程示意图。

具体实施方式

[0030] 为了使得本发明的目的、技术方案及优点更加清楚明白，以下结合其实施例，对本发明进行进一步详细说明；应当理解，此处所描述的具体实施例仅用于解释本发明，并不用

于限定本发明。对于本领域技术人员而言，在查阅以下详细描述之后，本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内，包括在本发明的范围内，并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征，并且这些特征根据以下将详细描述将是显而易见的。

[0031] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或组件必须具有特定的方位，以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制，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的具体含义。

[0032] 实施例一。

[0033] 本实施例提供了基于沙盒内签名和非对称加密技术的离线检测票务系统，结合图1和图2，包括签名模块、出票模块和检票模块，所述出票模块用于产生票号，所述签名模块和所述检票模块各自设有非对称加密技术中的公钥和私钥，所述签名模块和所述检票模块含有相同的中间数生成器，所述签名模块根据票号信息和中间数生成器生成中间数，并用公钥对所述中间数进行加密得到签名，所述检票模块对签名用私钥进行解密得到中间数，所述检票模块根据票号和中间数生成器生成中间数，并将两个中间数进行核对，核对无误后则检票成功；

[0034] 所述中间数生成器先根据票号信息和时间信息生成一个大数Z：

[0035] $$Z=\left(P1\bullet\prod_{i=1}^{n_1}(a[i]+1)+1\right)\bullet\left(P2\bullet\prod_{j=1}^{n_2}(b[j]+1)-1\right)-1;$$

[0036] 其中，P1和P2为由票号信息得的两个数，数组a[i]和b[j]为由时间信息得到的两个数组，n_1为数组a[i]的长度，n_2为数组b[j]的长度；

[0037] 将所述大数Z因式分解得到：

[0038] $$Z=r\bullet\prod_{i=1}^{m}u_i^{x_i};$$

[0039] 其中，$\{u_i\}$为升序排列的质数数列，x_i为大数Z中含有的某一质数u_i的个数，r为剩余数，m为质数的个数；

[0040] r和m需满足的条件为：

[0041] $$Long(r)+\sum_{i=1}^{m}Long(x_i)=L;$$

[0042] 其中，Long()函数表示取数的位数，L为中间数的长度；

[0043] 将数列$\{x_i\}$和r拼接成长度为L的中间数；

[0044] 所述出票模块产生的票号包括两个字段，第一字段用于表示票号种类，第二部分用于表示票号序列，当票号是在联网状态下产生时，票号种类为连续票，其票号序列与上一个票号序列连续，当票号在断网状态下产生时，票号种类为随机票，其票号序列为随机产生；

[0045] 所述检票模块包括识别单元和解密单元，所述识别单元通过识别电子票或纸质票上的图像得到票号信息和签名信息，所述解密单元对所述签名信息进行解密得到中间数；

[0046] 所述中间数生成器处于沙盒环境，无法通过读取代码来获知中间数生成器的内在逻辑；

[0047] 所述P1、P2的构建方法为：

[0048] 将时间信息用二进制表示，数值为1的位数形成数组a[i]，数值为0的位数形成数组b[i]，将票号信息中位于数组a[i]中的数按顺序重新构成一个长度为n_1的数值P1，将票号信息中位于数组b[i]中的数按顺序重新构成一个长度为n_2的数值P2

[0049] 实施例二。

[0050] 本实施例包含了实施例一的全部内容，本实施例提供了基于沙盒内签名和非对称加密技术的离线检测票务系统，包括签名模块、出票模块和检票模块，所述出票模块用于生成一个票号，所述签名模块根据票号生成签名信息，所述检票模块对所述签名信息和票号进行验证，上述三个模块互相处于离线状态以及沙盒环境，具有较强的独立性，不会对所处的系统造成影响；

[0051] 结合图4，游客通过登录APP或者登录网站访问所述出票模块，所述出票模块产生的票号具有两部分信息，一是票号特征，二是票号序列，所述票号特征分为连续票和随机票两类，为票号的首位数字，用不同的两个数字表示，当APP处于联网状态时，所述APP上的出票模块与所述网站上的出票模块产生的是连续票，所述连续票上的票号序列根据出票的先后顺序为连续的数列，当APP处于断网状态时，所述APP上的出票模块产生的时随机票，随机票上的票号序列为随机不连续的数列，当游客获得票号后，表示为预约状态；

[0052] 所述签名模块安装于网站或者位于景点的签名机上，所述签名模块在接收到票号信息以及付费信息后会生成签名信息，完成签名后会生成票据，所述票据上含有票号信息和签名信息，所述票号信息显示为数字，所述签名信息显示为图形，包括但不限于条形码，游客能够自行打印票据，或是在APP上生成电子票据，或是在签名机上打印出票据，需要注意的是，登录APP后需要联网才能产生付费信息，当游客在APP上进行签名时，所述APP会自动连接到位于网站上的签名模块进行签名，所述签名模块上含有非对称加密中的公钥，当游客获得票据后，表示为购票生效状态；

[0053] 所述检票模块安装于位于景点处的检票机上，所述检票模块包括识别单元和解密单元，所述识别单元能够识别出票据上的票号信息和签名信息，所述解密单元内含有私钥，所述解密单元利用私钥对签名信息进行处理得到票号信息，并与所述识别单元上的票号信息进行核对，核对无误后检票成功；

[0054] 所述签名模块上的公钥和所述检票模块上的私钥在出厂时进行配对设置；

[0055] 结合图3，所述签名模块进行签名的方法包括如下步骤：

[0056] S1、所述签名模块读取票号信息并转换为数值n(P)，所述数值n(P)为长度为32位的数；

[0057] S2、所述签名模块读取时间信息并转换为数值n(T)，所述n(T)为票号生效日的零点零分零秒与1970年1月1日零点零分零秒之间的秒数差；

[0058] S3、所述签名模块对所述票号信息和所述时间信息进行处理得到一段长为L的中间数n(N)；

[0059] S4、所述签名模块用公钥对所述中间数进行加密得到签名；

[0060] 步骤S3中得到中间数n(N)的具体过程包括如下步骤：

[0061] S21、将所述数值n(T)用32位的二进制表示；

[0062] S22、读取所述数值n(T)中数值为1的位数形成数组a[i]，所述数组a[i]的成员个数为n_1，读取所述数值n(T)中数值为0的位数形成数组b[i]，所述数组b[i]的成员个数为n_2，$n_1+n_2=32$；

[0063] S23、将所述数值n(P)中位于数组a[i]中的数按顺序重新构成一个长度为n_1的数值P1，将所述数值n(P)中位于数组b[i]中的数按顺序重新构成一个长度为n_2的数值P2；

[0064] S24、计算一个大数Z：

[0065] $$Z=\left(P1\bullet\prod_{i=1}^{n_1}(a[i]+1)+1\right)\bullet\left(P2\bullet\prod_{j=1}^{n_2}(b[j]+1)-1\right)-1;$$

[0066] S25、将所述大数Z因式分解得到：

[0067] $$Z=r\bullet\prod_{i=1}^{m}u_i^{x_i};$$

[0068] 其中，$\{u_i\}$为升序排列的质数数列，例如：$u_1=2$，$u_2=3$，$u_3=5$，$u_4=7$，...，x_i为大数Z中含有的某一质数u_i的个数，r为剩余数，m为质数的个数，需要注意的是，当大数的因数中不包含某一个质数u_i时，其对应的x_i记为零，而不是直接略过该因数；

[0069] r和m需满足的条件为：

[0070] $$Long(r)+\sum_{i=1}^{m}Long(x_i)=L;$$

[0071] 其中，Long()函数表示取数的位数；

[0072] S26、将所述数列x_i和r拼接成长度为L的中间数n(N)，其中，r置于中间数n(N)的末端；

[0073] 所述中间数作为明文通过公钥加密变成签名，所述签名作为密文在所述检票模块中通过私钥变成中间数，这两个过程均不可逆，而所述检票模块中根据票号信息和时间信息进行步骤S1至步骤S3过程得到中间数，所述检票模块将两个中间数进行对比，对比无误后通过检票；

[0074] 加密解密过程用下式表示：

[0075] 中间数$\xrightarrow{公钥}$签名$\xrightarrow{私钥}$中间数；

[0076] 在所述签名模块和所述检票模块中的用于生成中间数的代码处于沙盒环境且不可读，所以无法仅根据票号信息和时间信息得到正确的签名，加强了防伪安全性；

[0077] 所述检票模块在同一天时间内对同一票号信息和签名信息只能通过一次检票，所以无法通过复制有效的票号和签名信息来获得多张有效的票据；

[0078] 所述公私钥基于的非对称加密算法采用现有算法中的其中一种，但由于中间数不对外暴露，所以外界无法解析出采用的具体哪种算法；

[0079] 所述签名模块在联网模式下进行签名时，能够通过网络确认所有的连续票票号不重复，若发现有随机票的票号相同，会对后签名的随机票进行票号修改，确保随机票的票号

也不同；

[0080] 结合图5，当签名机上的签名模块在断网模式下进行签名时，所述签名模块会对签名信息添加标注信息，并且在步骤S1中对数值n(P)进行倒序排列，若发现是相同的随机票号时，则对倒序排列的数值n(P)再加1；

[0081] 当所述检票装置检测到标注信息时，在根据票号信息和时间信息进行中间数计算时，也会先对数值n(P)进行倒序排列，再进行中间数的核对，若核对无效，则对数值n(P)加1后重新计算中间数并核对；

[0082] 由于随机票号是随机生成的，在同一天内出现相同的随机票号的概率极低，出现三个相同随机票号的情况视为不可能，所以在对倒序排列的数值n(P)最多只加1进行重新核对。

[0083] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所描述的顺序不同的顺序执行方法，和/或可以添加，省略和/或组合各种部件。而且，关于某些配置描述的特征可以以各种其他配置组合，如可以以类似的方式组合配置的不同方面和元素。此外，随着技术发展其中的元素可以更新，即许多元素是示例，并不限制本公开或权利要求的范围。

[0084] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而，可以在没有这些具体细节的情况下实践配置例如，已经示出了众所周知的电路，过程，算法，结构和技术而没有不必要的细节，以避免模糊配置。该描述仅提供示例配置，并且不限制权利要求的范围，适用性或配置。相反，前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下，可以对元件的功能和布置进行各种改变。

[0085] 综上，其旨在上述详细描述被认为是例示性的而非限制性的，并且应当理解，以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

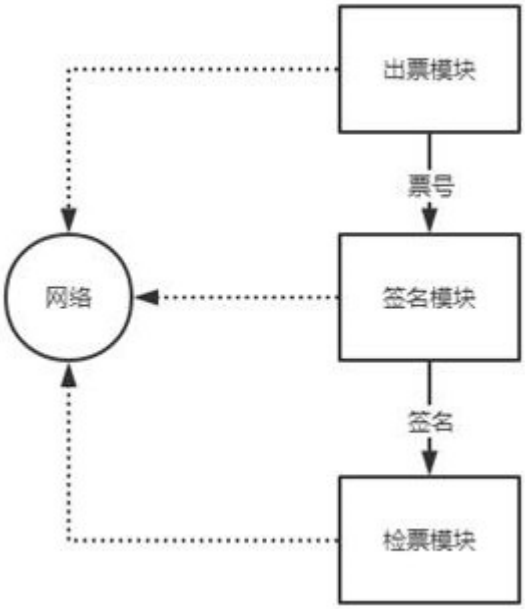

出票模块
票号
网络
签名模块
签名
检票模块

图1

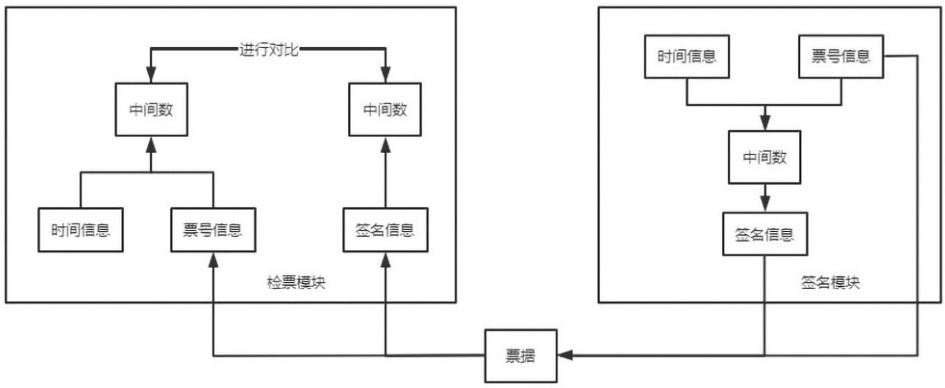

进行对比
中间数
中间数
时间信息
票号信息
签名信息
检票模块
时间信息
票号信息
中间数
签名信息
签名模块
票据

图2

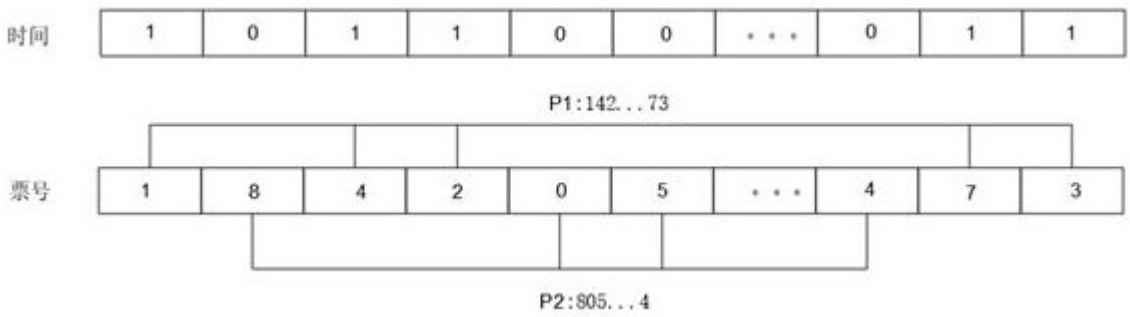

时间
1 0 1 1 0 0 . . . 0 1 1
P1:142...73
票号
1 8 4 2 0 5 . . . 4 7 3
P2:805...4

图3

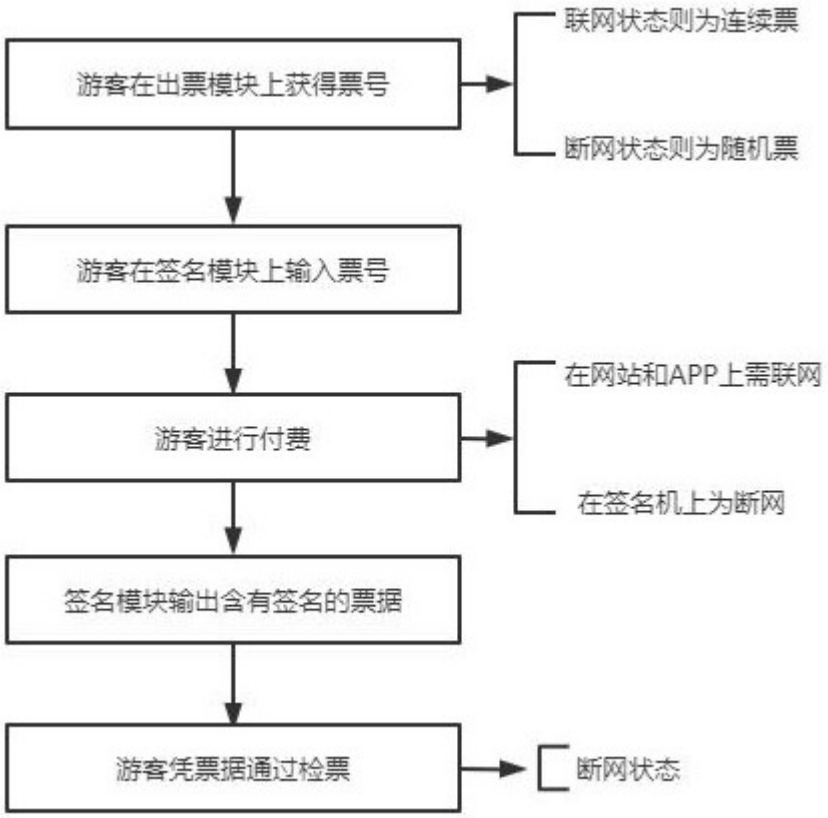

游客在出票模块上获得票号
联网状态则为连续票
断网状态则为随机票
游客在签名模块上输入票号
游客进行付费
在网站和APP上需联网
在签名机上为断网
签名模块输出含有签名的票据
游客凭票据通过检票
断网状态

图4

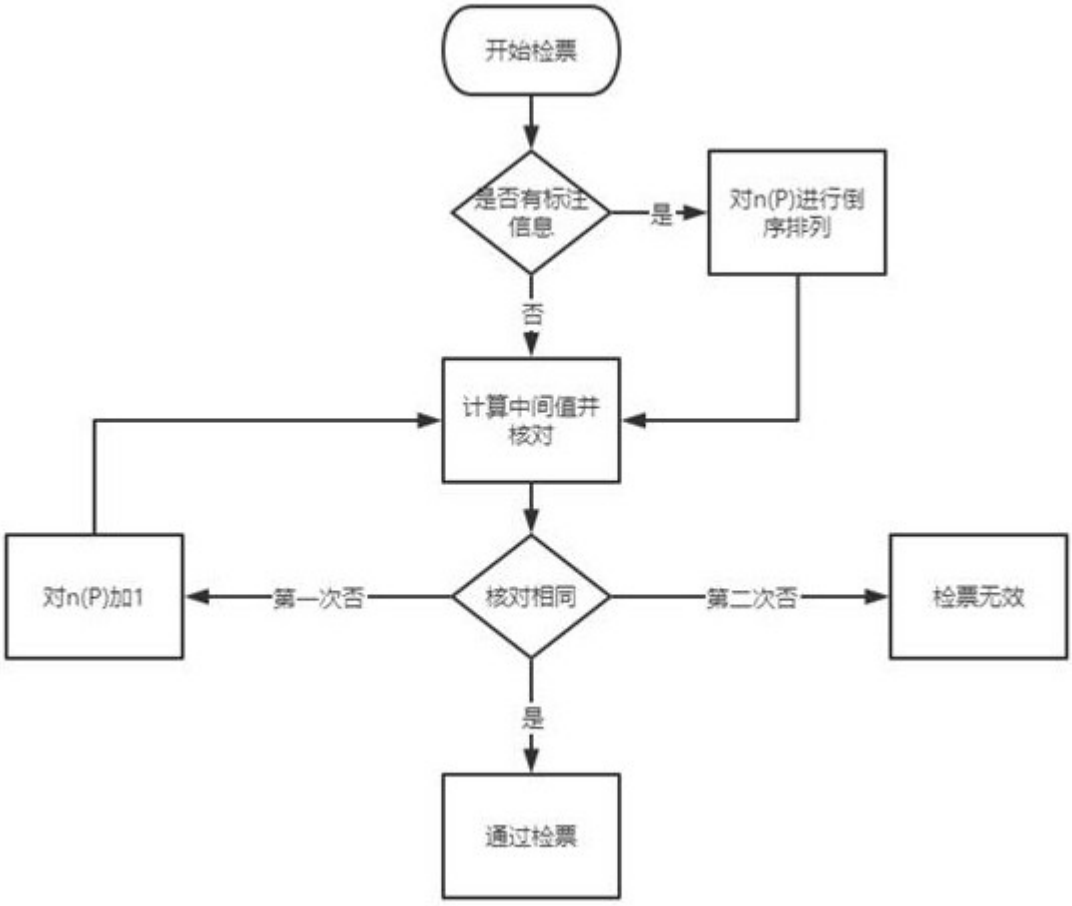

开始检票
是否有标注信息
是
对n(P)进行倒序排列
否
计算中间值并核对
对n(P)加1
第一次否
核对相同
第二次否
检票无效
是
通过检票

图5