(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 106910068 A
(43)申请公布日 2017.06.30

(21)申请号 201710066524.4

(22)申请日 2017.02.07

(71)申请人 桂林理工大学
地址 541004 广西壮族自治区桂林市七星区建干路12号

(72)发明人 邓健志 周越菡 程小辉

(51)Int.Cl.
G06Q 20/38(2012.01)

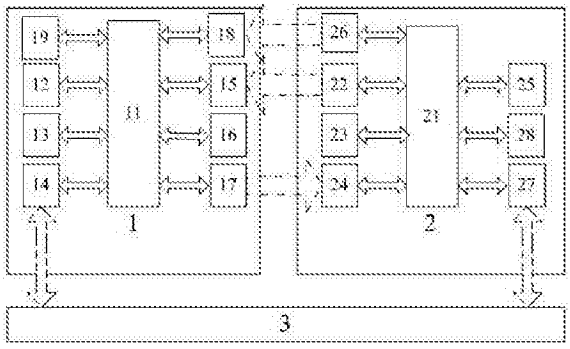
权利要求书5页 说明书10页 附图1页

(54)发明名称

多算法多密钥的光认证离线支付方法

(57)摘要

本发明公开了一种多算法多密钥的光认证离线支付方法。建立一套多算法多密钥的光认证离线消费装置，包括：电子钱包、消费机和服务器；采用消费机和电子钱包配备的可见光信号收发、条码显示及扫描装置构成信息通信信道，用条码和其他提示信息的显示装置的照明背光构造一个信息传输的隐藏信道，以可见光通信技术和条码扫描识别技术的相互验证，在支付过程中生成的多个随机数，随机的选择装置内的密码算法和加密解密密钥对传输的信息进行处理，并利用隐藏信道传输消息，使得支付过程传输的数据具有很强的随机性、完整性和不可否认性，从而提高了离线支付的安全性，为人们的购物、消费、转账等业务，提供了一种方便快捷、安全可靠的离线支付手段。



CN 106910068 A

1.一种多算法多密钥的光认证离线支付方法，其特征在于具体步骤为：

(1)建立一套多算法多密钥的光认证离线消费装置，包括：电子钱包、消费机和服务器；

电子钱包，包括：可见光发射模块、条码扫描模块、控制模块、钱包模块、输入模块、显示模块、数据接口、钱包光接收模块和密码处理模块；可见光发射模块，用于根据控制模块输入的信息，生成并发送可见光信号；条码扫描模块，用于扫描识别条码，并将识别的结果输出给控制模块；控制模块，用于：1、将待发送的信息进行处理，生成数据包，并输出给可见光发射模块，驱动可见光发射模块发送可见光信号；2、接收条码扫描模块的扫描结果输出，并对扫描结果进行验证；3、接收钱包光接收模块的结果输出，并予以识别、认证；4、根据收到的信息和生成的支付信息，生成需要通过可见光发射模块的信息；5、与钱包模块进行消费、充值、余额查询、操作日志信息的读写操作；6、能够通过数据接口与服务器进行数据交互；7、输入待加密的数据到密码处理模块，并接收密码处理模块加密后的数据输出；8、输入待解密的数据到密码处理模块，并接收密码处理模块解密后的数据输出；9、向密码处理模块输入密码算法和密钥的选择的指令；钱包模块，用于保存包括：用户账号信息、钱包余额、消费权限、查询密码、支付密码、操作日志、生产发行机构在内的信息；并可以验证输入的密码是否与钱包密码模块内保存的密码一致；输入模块，用于向控制模块输入包括支付金额、查询密码、支付密码、操作指令在内的信息；显示模块，用于显示支付金额、密码输入界面、操作指令以及提示信息；数据接口，用于提供电子钱包的联网功能，提供与服务器连接并进行数据交换、数据维护和升级的功能；钱包光接收模块，用于接收背光模块发送的可见光背光信号；密码处理模块，用于：1、为支付流程中电子钱包需要传输的信息，提供不止一种的密码算法；2、保存提供的密码算法中，将会使用到的密钥；3、根据所选择的密码算法和密钥，对支付流程中电子钱包需要发送的信息进行加密，并对电子钱包接收到的加密信息进行解密；

消费机，包括：可见光接收模块、条码显示模块、读写控制模块、收银箱模块、键盘模块、通信模块、密码协处理器和背光模块；可见光接收模块，用于接收可见光信号，并处理还原成对应的数字信号，还原成数据包；条码显示模块，用于：1、根据读写控制模块的输入信息，生成并显示出条码；2、显示交易金额、密码输入界面、操作指令以及提示信息；读写控制模块，用于：1、接收可见光接收模块的输出，并予以识别、认证；2、将待发送的信息进行处理，输出给条码显示模块；3、将需要通过光信号形式发送的信息进行处理，生成数据包，并输出给背光模块，驱动背光模块发送可见光信号； 4、与收银箱模块进行消费、充值、余额查询、操作日志信息的读写操作；5、提供数据接口，通过通信模块与服务器进行信息的上传和下载； 6、输入待加密的数据到密码协处理器，并接收密码协处理器加密后的数据输出；7、输入待解密的数据到密码协处理器，并接收密码协处理器解密后的数据输出；8、向密码协处理器输入密码算法和密钥的选择的指令；收银箱模块，用于保存包括：操作日志、收款消费权限、黑名单、收银余额、操作密码、有效期、生产发行机构在内的信息；键盘模块，用于向读写控制模块输入交易金额、交易密码、操作指令；通信模块，用于通过有线或者无线的方式，连接上位机或者接入网络，从而与服务器相连；背光模块，用于为条码显示模块提供显示的照明背光，同时利用背光发送可见光背光信号；密码协处理器，用于：1、为支付流程中消费机需要传输的信息，提供不止一种的密码算法；2、保存提供的密码算法中，将会使用到的密钥；3、根据所选择的密码算法和密钥，对支付流程中消费机需要发送的信息进行加密，并对

消费机接收到的加密信息进行解密；

服务器，用于：1、与消费机通过通信模块建立上传、下载的数据连接；2、与电子钱包通过数据接口建立上传、下载的数据连接；3、提供本离线支付方法的后台服务支持；4、提供整个离线支付装置与金融系统的资金流动的接口；5、为消费机、电子钱包发放或取消授权，提供包括：密钥更新、算法更新和升级、使用权限调整、有效期调整、电子钱包充值、消费机缴款、电子钱包和消费机公开信息查询在内的服务；6、保存包括：授权用户清单、黑名单、操作日志汇总、消费机清单在内的信息；

授权用户清单，用于保存包括：已经授权可以进行离线支付的电子钱包的身份标识、使用权限、有效期、电子钱包持有者的身份信息；黑名单，用于保存授权用户清单中，因欠费、挂失、有不正当使用记录而被拒绝支付交易的那部分电子钱包的身份标识信息；支付接口，用于提供整个离线支付装置与金融系统的资金流动的接口；操作日志汇总，用于保存包括所有消费机、电子钱包的查询、充值、消费的操作的时间、支付金额、支付过程数据参数在内的信息；消费机清单，用于保存包括：已经授权可以进行离线支付交易的消费机的身份标识、使用权限、有效期、消费机持有者的身份信息；服务器用于给包括上述消费机的模块及其功能的设备发放权限，使其具备接受装置内的电子钱包进行支付的功能；服务器用于给包括上述电子钱包的模块以及功能的设备发放权限，使其具备向装置内的消费机进行支付的功能；同时由服务器给用户发放一个授权，授权方式是发放一个授权实体硬件设备，或者是为已有设备的用户提供一个授权号；并为设备充值，写入电子钱包身份标识、使用权限、有效期、电子钱包的支付密码和查询密码、电子钱包持有者的身份信息；

消费机和电子钱包内，都存放有n种密码算法和m个加密解密密钥，其中n<m，且n和m都是不小于2的自然数；消费机将每次将要发送出去的数据，分成不少于两个部分，都分别采用不同的密码算法进行加密，然后再经由条码、背光这些不同的方式发送出去，电子钱包必须通过条码扫描模块和钱包光接收模块分别接收来自消费机显示的条码和可见光背光信号，并且只有把消费机显示的条码和可见光背光信号都接收到，才能使用电子钱包内的对应的密码算法和解密密钥，把消费机发出的数据完整的解密出来；

(2)在步骤(1)建立的多算法多密钥的光认证离线消费装置中，由电子钱包向消费机发起支付，支付流程包括以下步骤：

DM1，电子钱包生成一个支付请求码QQM1，支付请求码QQM1包括：电子钱包身份标识QID1、支付随机码QRD1、支付金额ZFR1，并由可见光发射模块采用可见光信号的方式向消费机发送支付请求码QQM1；

DM2，消费机通过可见光接收模块接收可见光信号形式的支付请求码QQM2，从中提取出电子钱包身份标识QID2、支付随机码QRD2、支付金额ZFR2；消费机生成一个应答随机码YDR2、一个光随机码GRD2；并根据应答随机码YDR2，选择一种密码算法SFn和一个加密密钥MYn；再根据光随机码GRD2，选择密码算法SFm和一个加密密钥MYm；

DM2.1，根据支付请求码QQM2、应答随机码YDR2、光随机码GRD2，生成一个收款应答码SKYD2，并运算得到收款码SKM2，收款码SKM2包括：收款金额SJR2、消费机身份标识SID2、收款应答码SKYD2、支付请求码QQM2、支付随机码QRD2；将收款码SKM2分成两个部分SKM2-1和SKM2-2，用密码算法SFn和一个加密密钥MYn对SKM2-1进行加密得到SFnSKM2-1，密码算法SFm和一个加密密钥MYm对SKM2-2和应答随机码YDR2进行加密得到SFmSKM2-2；

DM2.2,将SFnSKM2-1和SFmSKM2-2生成条码,通过条码显示模块显示出来;并通过背光模块,将光随机码GRD2以可见光信号的方式向电子钱包发送出去;

DM3,由电子钱包扫描消费机的条码显示模块显示的条码得到SFnSKM3-1、SFmSKM3-2,电子钱包利用钱包光接收模块接收光随机码GRD3;并根据光随机码GRD3,确定采用密码算法SFm和解密密钥JMm对SFmSKM3-2进行解密得到SKM3-2、应答随机码YDR3,再根据应答随机码YDR3确定选择密码算法SFn和一个解密密钥JMn对SFnSKM3-1进行解密得到SKM3-1;

DM3.1,合并SKM3-1和SKM3-2得到收款码SKM3;并从收款码SKM3提取出收款金额SJR3、消费机身份标识SID3、收款应答码SKYD3、支付随机码QRD3;并根据收款应答码SKYD3、应答随机码YDR3、光随机码GRD3,运算得到支付请求码QQM3、应答随机码YDR3;

DM3.2,进行以下的对比验证:

1)DM1中电子钱包生成的支付请求码QQM1和DM3中接收并提取得到的支付请求码QQM3;

2)DM1中电子钱包生成的支付金额ZFR1和DM3中接收并从收款码中提取得到的收款金额SJR3;

3)DM1中电子钱包生成的支付随机码QRD1和DM3中接收并从收款码中提取得到的支付随机码QRD3;

如果以上有一个不一致则退出支付流程,并在显示模块上显示支付请求错误的提示信息;如果一致就进入DM3.3;

DM3.3,电子钱包根据从收款码SKM3提取得到的收款金额SJR3、消费机身份标识SID3、收款应答码SKYD3、支付随机码QRD3以及收款应答码SKYD3、应答随机码YDR3、光随机码GRD3,运算得到支付确认码FKQR3,并生成支付码ZFM3,支付码ZFM3包括:收款码SKM3、电子钱包身份标识FID1、支付金额FJR1、支付确认码FKQR3,再根据应答随机码YDR3、光随机码GRD3选择密码算法SFa和一个加密密钥MYa对支付码ZFM3进行加密的到MYaZFM3,再把MYaZFM3以可见光信号的形式,由可见光发射模块发送出去;

DM4,消费机通过可见光接收模块接收可见光信号形式的信号,得到MYaZFM3,再根据应答随机码YDR2、光随机码GRD2选择密码算法SFb和一个加密密钥MYb对MYaZFM3进行解密得到支付码ZFM4,从中提取出收款码SKM4、电子钱包身份标识QID4、支付金额FJR4、支付确认码FKQR4,从SKM4提取出收款金额SJR4、消费机身份标识SID4、收款应答码SKYD4、收款金额SJR3、支付随机码QRD4;从支付确认码FKQR4运算得到收款应答码SKYD4、应答随机码YDR4、光随机码GRD4;

DM4.1,进行至少以下的对比验证:

1)对比DM2运算得到的收款码SKM2和DM4中提取出的收款码SKM4;

2)对比DM2中生成的应答随机码YDR2和DM4中从SKM4提取出的应答随机码YDR4;

3)对比DM2中生成的光随机码GRD2和DM4中从SKM4提取出的光随机码GRD4;

4)对比DM2中提取到的电子钱包身份标识QID2和DM4中从ZFM4提取出的电子钱包身份标识QID4;

5)对比DM2中得到的支付金额FJR2、收款金额SJR2和DM4中从ZFM4提取出的收款金额SJR4;

6)对比DM2中得到的支付随机码QRD2和DM4中从ZFM4提取出的支付随机码QRD4;

如果以上6个对比都分别一致,就进入DM4.2;否则就退出支付流程,并在条码显示模块

上显示验证出错的提示信息；

DM4.2，消费机生成一个光确认码GQR4，并根据电子钱包身份标识QID4、支付金额FJR4、消费机身份标识SID4、收款应答码SKYD4、应答随机码YDR4、光确认码GQR4、支付随机码QRD4，运算得到收款确认码SKQR4；将收款确认码SKQR分成两个部分SKQR4-1和SKQR4-2；

DM4.3，根据光确认码GQR4和应答随机码YDR2，选择一种密码算法SFp和一个加密密钥MYp；再根据光确认码GQR4和光随机码GRD2，选择密码算法SFq和一个加密密钥MYq；用密码算法SFp和一个加密密钥MYp对SKQR4-1进行加密得到SFpSKQR4-1，用密码算法SFq和一个加密密钥MYq对SKQR4-2和应答随机码YDR2进行加密得到SFqSKQR4-2；

DM4.4，消费机将SFpSKQR4-1和SFqSKQR4-2生成条码，通过条码显示模块显示出来；并通过背光模块，将光确认码GQR4以可见光信号的方式向电子钱包发送出去；

DM5，电子钱包扫描消费机条码显示模块显示的条码得到SFpSKQR5-1和SFqSKQR5-2，电子钱包利用钱包光接收模块接收光确认码GQR5；电子钱包根据光确认码GQR5和应答随机码YDR3，选择一种密码算法SFp和一个解密密钥JYp；再根据光确认码GQR5和光随机码GRD3，选择密码算法SFq和一个解密密钥JYq；采用密码算法SFp和解密密钥JYp对SFpSKQR5-1进行解密得到SKQR5-1，采用密码算法SFq和解密密钥JYq对SFqSKQR5-2得到SKQR5-2；合并SKQR5-1和SKQR5-2得到收款确认码SKQR5；再由收款确认码SKQR5运算得到电子钱包身份标识QID5、支付金额FJR5、消费机身份标识SID5、收款应答码SKYD5、光确认码GQR5、支付随机码QRD5；

DM5.1，进行至少以下的对比验证：

1)对比电子钱包身份标识QID1和从ZF5中运算得到的电子钱包身份标识QID5；

2)对比ZF1生成的支付金额FJR1和从ZF5中运算得到的支付金额FJR5；

3)对比ZF1生成的支付随机码QRD1和从ZF5中运算得到的支付随机码QRD5；

4)对比ZF3得到的消费机身份标识SID3和从ZF5中运算得到的消费机身份标识SID5；

5)对比ZF3生成的收款应答码SKYD3和从ZF5中运算得到的收款应答码SKYD5；

如果以上有一个对比不一致则退出支付流程，并在显示模块上显示验证错误的提示信息；如果一致就进入DM5.2；

DM5.2，电子钱包把光确认码GQR5、收款确认码SKQR5，以可见光信号的形式，由可见光发射模块发送出去；

DM5.3，更新钱包模块的钱包余额，用操作时间SJ、收款应答码SKYD5、支付金额FJR、消费机身份标识SID5、收款应答码SKYD5生成操作日志，并通过显示模块显示付款成功的提示信息；

DM6，消费机通过可见光接收模块接收可见光形式的信号，从中提取出光确认码GQR6、收款确认码SKQR6，将该操作时间SJ、电子钱包身份标识FID6、支付金额FJR6、支付码ZFM6、收款码SKM6写入收款箱模块，生成操作日志，并更新收款箱模块的余额信息，并通过条码显示模块显示收款成功的提示信息；

(3)在支付流程中，从电子钱包接收消费机发送的数据，以及从消费机接收电子钱包发送的数据，都可能在收发过程中存在无法识别的可能，所以在支付流程中，对于无法识别的数据，以及因为无法接收数据而导致无法识别的情况，装置都会在一个设定的等待时间超时后，单方面结束支付流程；

在支付流程中，如果在各解密的环节无法对待解密数据完成解密，都会结束支付流

程；

在支付流程中，从电子钱包向消费机发送的数据，以及从消费机向电子钱包发送的数据，可能在收发过程中存在数据的丢失、被篡改、伪造的风险，因此在支付流程中，对每次收到的关键数据，都假定当前收到的数据与支付流程的前面的步骤生成的或者接收到的数据不一样，需要对比验证，由此保证收发数据的真实、完整。

多算法多密钥的光认证离线支付方法

技术领域

[0001] 本发明属于光支付技术领域，特别涉及一种多算法多密钥的光认证离线支付方法。

背景技术

[0002] 传统的非现金交易手段都是在线交易，原有的磁卡系统就是典型的在线交易系统。离线支付是一种当网络、GPRS、3G、4G等通讯中断时，所进行的交易支付手段，RFID、NFC是目前比较常见的离线支付方式。

[0003] 离线支付可以在脱机状态下工作，不需在支付的过程中联机验证支付双方的真实有效，便可以完成支付，因此对支付双方以及支付流程的安全性有很高要求。

[0004] 可见光通信(Visible Light Communication，简称VLC)技术。VLC技术就是利用LED可以发出高频闪烁且人眼无法感知到的灯光闪烁的这一特点，在数据发送端用LED的高频闪烁来携带信号，在接收端用响应时间同样很快的感光元件进行信号的采集，从而实现无线通信的方法。

[0005] “扫码”是时下很流行的信息获取方式，“扫码支付”则是在“扫码”技术和微信、支付宝等技术的基础上发展起来的线上支付方式手段。然而，属于“扫码支付”的支付手段，仍然是一种离不开网络的在线支付方式，这样的方式还是不能如同离线支付一样，解决网络通讯中断无法支付的问题。

[0006] “扫码”的“码”通常是一个动态可变的“码”，需要在显示屏上的显示出来，现用的液晶屏、LED屏都是需要提供背光照明，而照明背光又是可见光通信的一个很好的载体。照明背光是一个容易被忽略的信息载体，将照明背光作为一个隐藏信号的传输载体，应用在光支付领域，可以提供一个隐藏通道，提高支付环节的安全性。

[0007] 本发明得到以上几个技术方式的启发，利用了摄像头、闪光灯、环境光感知传感模块这几个几乎是现代智能手机、平板电脑的标准配置，共同构造一个带有安全而隐蔽的离线支付方法，在支付过程中采用多个密码算法的随机组合，加大了交易密文的解密复杂度，让支付过程更加安全可靠。

发明内容

[0008] 本发明的目的在于提供一种多算法多密钥的光认证离线支付方法。

[0009] 具体步骤为：

(1)建立一套多算法多密钥的光认证离线消费装置，包括：电子钱包、消费机和服务器。

[0010] 电子钱包，包括：可见光发射模块、条码扫描模块、控制模块、钱包模块、输入模块、显示模块、数据接口、钱包光接收模块和密码处理模块；可见光发射模块，用于根据控制模块输入的信息，生成并发送可见光信号；条码扫描模块，用于扫描识别条码，并将识别的结果输出给控制模块；控制模块，用于：1、将待发送的信息进行处理，生成数据包，并输出给可见光发射模块，驱动可见光发射模块发送可见光信号；2、接收条码扫描模块的扫描结果输

出，并对扫描结果进行验证；3、接收钱包光接收模块的结果输出，并予以识别、认证；4、根据收到的信息和生成的支付信息，生成需要通过可见光发射模块的信息；5、与钱包模块进行消费、充值、余额查询、操作日志信息的读写操作；6、能够通过数据接口与服务器进行数据交互；7、输入待加密的数据到密码处理模块，并接收密码处理模块加密后的数据输出；8、输入待解密的数据到密码处理模块，并接收密码处理模块解密后的数据输出；9、向密码处理模块输入密码算法和密钥的选择的指令；钱包模块，用于保存包括：用户账号信息、钱包余额、消费权限、查询密码、支付密码、操作日志、生产发行机构在内的信息；并可以验证输入的密码是否与钱包密码模块内保存的密码一致；输入模块，用于向控制模块输入包括支付金额、查询密码、支付密码、操作指令在内的信息；显示模块，用于显示支付金额、密码输入界面、操作指令以及提示信息；数据接口，用于提供电子钱包的联网功能，提供与服务器连接并进行数据交换、数据维护和升级的功能；钱包光接收模块，用于接收背光模块发送的可见光背光信号；密码处理模块，用于：1、为支付流程中电子钱包需要传输的信息，提供不止一种的密码算法；2、保存提供的密码算法中，将会使用到的密钥；3、根据所选择的密码算法和密钥，对支付流程中电子钱包需要发送的信息进行加密，并对电子钱包接收到的加密信息进行解密。

[0011] 消费机，包括：可见光接收模块、条码显示模块、读写控制模块、收银箱模块、键盘模块、通信模块、密码协处理器和背光模块；可见光接收模块，用于接收可见光信号，并处理还原成对应的数字信号，还原成数据包；条码显示模块，用于：1、根据读写控制模块的输入信息，生成并显示出条码；2、显示交易金额、密码输入界面、操作指令以及提示信息；读写控制模块，用于：1、接收可见光接收模块的输出，并予以识别、认证；2、将待发送的信息进行处理，输出给条码显示模块；3、将需要通过光信号形式发送的信息进行处理，生成数据包，并输出给背光模块，驱动背光模块发送可见光信号； 4、与收银箱模块进行消费、充值、余额查询、操作日志信息的读写操作；5、提供数据接口，通过通信模块与服务器进行信息的上传和下载； 6、输入待加密的数据到密码协处理器，并接收密码协处理器加密后的数据输出；7、输入待解密的数据到密码协处理器，并接收密码协处理器解密后的数据输出；8、向密码协处理器输入密码算法和密钥的选择的指令；收银箱模块，用于保存包括：操作日志、收款消费权限、黑名单、收银余额、操作密码、有效期、生产发行机构在内的信息；键盘模块，用于向读写控制模块输入交易金额、交易密码、操作指令；通信模块，用于通过有线或者无线的方式，连接上位机或者接入网络，从而与服务器相连；背光模块，用于为条码显示模块提供显示的照明背光，同时利用背光发送可见光背光信号；密码协处理器，用于：1、为支付流程中消费机需要传输的信息，提供不止一种的密码算法；2、保存提供的密码算法中，将会使用到的密钥；3、根据所选择的密码算法和密钥，对支付流程中消费机需要发送的信息进行加密，并对消费机接收到的加密信息进行解密。

[0012] 服务器，用于：1、与消费机通过通信模块建立上传、下载的数据连接；2、与电子钱包通过数据接口建立上传、下载的数据连接；3、提供本离线支付方法的后台服务支持；4、提供整个离线支付装置与金融系统的资金流动的接口；5、为消费机、电子钱包发放或取消授权，提供包括：密钥更新、算法更新和升级、使用权限调整、有效期调整、电子钱包充值、消费机缴款、电子钱包和消费机公开信息查询在内的服务；6、保存包括：授权用户清单、黑名单、操作日志汇总、消费机清单在内的信息。

[0013] 授权用户清单，用于保存包括：已经授权可以进行离线支付的电子钱包的身份标识、使用权限、有效期、电子钱包持有者的身份信息；黑名单，用于保存授权用户清单中，因欠费、挂失、有不正当使用记录而被拒绝支付交易的那部分电子钱包的身份标识信息；支付接口，用于提供整个离线支付装置与金融系统的资金流动的接口；操作日志汇总，用于保存包括所有消费机、电子钱包的查询、充值、消费的操作的时间、支付金额、支付过程数据参数在内的信息；消费机清单，用于保存包括：已经授权可以进行离线支付交易的消费机的身份标识、使用权限、有效期、消费机持有者的身份信息；服务器用于给包括上述消费机的模块及其功能的设备发放权限，使其具备接受装置内的电子钱包进行支付的功能；服务器用于给包括上述电子钱包的模块以及功能的设备发放权限，使其具备向装置内的消费机进行支付的功能；同时由服务器给用户发放一个授权，授权方式是发放一个授权实体硬件设备，或者是为已有设备的用户提供一个授权号；并为设备充值，写入电子钱包身份标识、使用权限、有效期、电子钱包的支付密码和查询密码、电子钱包持有者的身份信息。

[0014] 消费机和电子钱包内，都存放有n种密码算法和m个加密解密密钥，其中n<m，且n和m都是不小于2的自然数。消费机将每次将要发送出去的数据，分成不少于两个部分，都分别采用不同的密码算法进行加密，然后再经由条码、背光这些不同的方式发送出去，电子钱包必须通过条码扫描模块和钱包光接收模块分别接收来自消费机显示的条码和可见光背光信号，并且只有把消费机显示的条码和可见光背光信号都接收到，才能使用电子钱包内的对应的密码算法和解密密钥，把消费机发出的数据完整的解密出来。

[0015] (2)在步骤(1)建立的多算法多密钥的光认证离线消费装置中，由电子钱包向消费机发起支付，支付流程包括以下步骤：

DM1，电子钱包生成一个支付请求码QQM1，支付请求码QQM1包括：电子钱包身份标识QID1、支付随机码QRD1、支付金额ZFR1，并由可见光发射模块采用可见光信号的方式向消费机发送支付请求码QQM1。

[0016] DM2，消费机通过可见光接收模块接收可见光信号形式的支付请求码QQM2，从中提取出电子钱包身份标识QID2、支付随机码QRD2、支付金额ZFR2；消费机生成一个应答随机码YDR2、一个光随机码GRD2；并根据应答随机码YDR2，选择一种密码算法SFn和一个加密密钥MYn；再根据光随机码GRD2，选择密码算法SFm和一个加密密钥MYm。

[0017] DM2.1，根据支付请求码QQM2、应答随机码YDR2、光随机码GRD2，生成一个收款应答码SKYD2，并运算得到收款码SKM2，收款码SKM2包括：收款金额SJR2、消费机身份标识SID2、收款应答码SKYD2、支付请求码QQM2、支付随机码QRD2；将收款码SKM2分成两个部分SKM2-1和SKM2-2，用密码算法SFn和一个加密密钥MYn对SKM2-1进行加密得到SFnSKM2-1，密码算法SFm和一个加密密钥MYm对SKM2-2和应答随机码YDR2进行加密得到SFmSKM2-2。

[0018] DM2.2，将SFnSKM2-1和SFmSKM2-2生成条码，通过条码显示模块显示出来；并通过背光模块，将光随机码GRD2以可见光信号的方式向电子钱包发送出去。

[0019] DM3，由电子钱包扫描消费机的条码显示模块显示的条码得到SFnSKM3-1、SFmSKM3-2，电子钱包利用钱包光接收模块接收光随机码GRD3；并根据光随机码GRD3，确定采用密码算法SFm和解密密钥JMm对SFmSKM3-2进行解密得到SKM3-2、应答随机码YDR3，再根据应答随机码YDR3确定选择密码算法SFn和一个解密密钥JMn对SFnSKM3-1进行解密得到SKM3-1。

[0020] DM3.1，合并SKM3-1和SKM3-2得到收款码SKM3；并从收款码SKM3提取出收款金额SJR3、消费机身份标识SID3、收款应答码SKYD3、支付随机码QRD3；并根据收款应答码SKYD3、应答随机码YDR3、光随机码GRD3，运算得到支付请求码QQM3、应答随机码YDR3。

[0021] DM3.2，进行以下的对比验证：

1)DM1中电子钱包生成的支付请求码QQM1和DM3中接收并提取得到的支付请求码QQM3。

[0022] 2)DM1中电子钱包生成的支付金额ZFR1和DM3中接收并从收款码中提取得到的收款金额SJR3。

[0023] 3)DM1中电子钱包生成的支付随机码QRD1和DM3中接收并从收款码中提取得到的支付随机码QRD3。

[0024] 如果以上有一个不一致则退出支付流程，并在显示模块上显示支付请求错误的提示信息；如果一致就进入DM3.3。

[0025] DM3.3，电子钱包根据从收款码SKM3提取得到的收款金额SJR3、消费机身份标识SID3、收款应答码SKYD3、支付随机码QRD3以及收款应答码SKYD3、应答随机码YDR3、光随机码GRD3，运算得到支付确认码FKQR3，并生成支付码ZFM3，支付码ZFM3包括:收款码SKM3、电子钱包身份标识FID1、支付金额FJR1、支付确认码FKQR3，再根据应答随机码YDR3、光随机码GRD3选择密码算法SFa和一个加密密钥MYa对支付码ZFM3进行加密的到MYaZFM3，再把MYaZFM3以可见光信号的形式，由可见光发射模块发送出去。

[0026] DM4，消费机通过可见光接收模块接收可见光信号形式的信号，得到MYaZFM3，再根据应答随机码YDR2、光随机码GRD2选择密码算法SFb和一个加密密钥MYb对MYaZFM3进行解密得到支付码ZFM4，从中提取出收款码SKM4、电子钱包身份标识QID4、支付金额FJR4、支付确认码FKQR4，从SKM4提取出收款金额SJR4、消费机身份标识SID4、收款应答码SKYD4、收款金额SJR3、支付随机码QRD4；从支付确认码FKQR4运算得到收款应答码SKYD4、应答随机码YDR4、光随机码GRD4。

[0027] DM4.1，进行至少以下的对比验证：

1)对比DM2运算得到的收款码SKM2和DM4中提取出的收款码SKM4。

[0028] 2)对比DM2中生成的应答随机码YDR2和DM4中从SKM4提取出的应答随机码YDR4。

[0029] 3)对比DM2中生成的光随机码GRD2和DM4中从SKM4提取出的光随机码GRD4。

[0030] 4)对比DM2中提取到的电子钱包身份标识QID2和DM4中从ZFM4提取出的电子钱包身份标识QID4。

[0031] 5)对比DM2中得到的支付金额FJR2、收款金额SJR2和DM4中从ZFM4提取出的收款金额SJR4。

[0032] 6)对比DM2中得到的支付随机码QRD2和DM4中从ZFM4提取出的支付随机码QRD4。

[0033] 如果以上6个对比都分别一致，就进入DM4.2；否则就退出支付流程，并在条码显示模块上显示验证出错的提示信息。

[0034] DM4.2，消费机生成一个光确认码GQR4，并根据电子钱包身份标识QID4、支付金额FJR4、消费机身份标识SID4、收款应答码SKYD4、应答随机码YDR4、光确认码GQR4、支付随机码QRD4，运算得到收款确认码SKQR4；将收款确认码SKQR分成两个部分SKQR4-1和SKQR4-2。

[0035] DM4.3，根据光确认码GQR4和应答随机码YDR2，选择一种密码算法SFp和一个加密密钥MYp；再根据光确认码GQR4和光随机码GRD2，选择密码算法SFq和一个加密密钥MYq；用

密码算法SFp和一个加密密钥MYp对SKQR4-1进行加密得到SFpSKQR4-1，用密码算法SFq和一个加密密钥MYq对SKQR4-2和应答随机码YDR2进行加密得到SFqSKQR4-2。

[0036] DM4.4，消费机将SFpSKQR4-1和SFqSKQR4-2生成条码，通过条码显示模块显示出来；并通过背光模块，将光确认码GQR4以可见光信号的方式向电子钱包发送出去。

[0037] DM5，电子钱包扫描消费机条码显示模块显示的条码得到SFpSKQR5-1和SFqSKQR5-2，电子钱包利用钱包光接收模块接收光确认码GQR5；电子钱包根据光确认码GQR5和应答随机码YDR3，选择一种密码算法SFp和一个解密密钥JYp；再根据光确认码GQR5和光随机码GRD3，选择密码算法SFq和一个解密密钥JYq；采用密码算法SFp和解密密钥JYp对SFpSKQR5-1进行解密得到SKQR5-1，采用密码算法SFq和解密密钥JYq对SFqSKQR5-2得到SKQR5-2；合并SKQR5-1 和SKQR5-2得到收款确认码SKQR5；再由收款确认码SKQR5运算得到电子钱包身份标识QID5、支付金额FJR5、消费机身份标识SID5、收款应答码SKYD5、光确认码GQR5、支付随机码QRD5。

[0038] DM5.1，进行至少以下的对比验证：

1)对比电子钱包身份标识QID1和从ZF5中运算得到的电子钱包身份标识QID5。

[0039] 2)对比ZF1生成的支付金额FJR1和从ZF5中运算得到的支付金额FJR5。

[0040] 3)对比ZF1生成的支付随机码QRD1和从ZF5中运算得到的支付随机码QRD5。

[0041] 4)对比ZF3得到的消费机身份标识SID3和从ZF5中运算得到的消费机身份标识SID5。

[0042] 5)对比ZF3生成的收款应答码SKYD3和从ZF5中运算得到的收款应答码SKYD5。

[0043] 如果以上有一个对比不一致则退出支付流程，并在显示模块上显示验证错误的提示信息；如果一致就进入DM5.2。

[0044] DM5.2，电子钱包把光确认码GQR5、收款确认码SKQR5，以可见光信号的形式，由可见光发射模块发送出去。

[0045] DM5.3，更新钱包模块的钱包余额，用操作时间SJ、收款应答码SKYD5、支付金额FJR、消费机身份标识SID5、收款应答码SKYD5生成操作日志，并通过显示模块显示付款成功的提示信息。

[0046] DM6，消费机通过可见光接收模块接收可见光形式的信号，从中提取出光确认码GQR6、收款确认码SKQR6，将该操作时间SJ、电子钱包身份标识FID6、支付金额FJR6、支付码ZFM6、收款码SKM6写入收款箱模块，生成操作日志，并更新收款箱模块的余额信息，并通过条码显示模块显示收款成功的提示信息。

[0047] (3)在支付流程中，从电子钱包接收消费机发送的数据，以及从消费机接收电子钱包发送的数据，都可能在收发过程中存在无法识别的可能，所以在支付流程中，对于无法识别的数据，以及因为无法接收数据而导致无法识别的情况，装置都会在一个设定的等待时间超时后，单方面结束支付流程。

[0048] 在支付流程中，如果在各解密的环节无法对待解密数据完成解密，都会结束支付流程。

[0049] 在支付流程中，从电子钱包向消费机发送的数据，以及从消费机向电子钱包发送的数据，可能在收发过程中存在数据的丢失、被篡改、伪造的风险，因此在支付流程中，对每次收到的关键数据，都假定当前收到的数据与支付流程的前面的步骤生成的或者接收到

的数据不一样，需要对比验证，由此保证收发数据的真实、完整。

[0050] 本发明以可见光通信技术和条码扫描识别技术两者相结合为前提，并利用条码和其他提示信息的显示装置的照明背光，构造了一个隐藏信道，并在支付过程中引入了在多密码算法和多密钥对数据进行密码运算，以提高支付过程的安全性，从而提出的一种多算法多密钥的光认证离线支付方法，本发明把时下最流行的智能手机、平板电脑作为电子钱包的载体，利用其摄像头、闪光灯、环境光感知器件等常见配置作为通信工具，实现了一个离线支付方法，解决了线上支付无法脱离网络的弊端。

附图说明

[0051] 图1是本发明方法的结构示意图。

[0052] 图2是本发明的实施例中装置的结构图。

[0053] 图中标记：1-电子钱包；2-消费机；3-服务器； 11-控制模块；12-输入模块；13-显示模块；14-数据接口；15-条码扫描模块；16-钱包模块；17-可见光发射模块；18-钱包光接收模块；19-密码处理模块；21-读写控制模块；22-条码显示模块；23-收银箱模块；24-可见光接收模块；25-键盘模块；26-背光模块；27-通信模块；28-密码协处理器。

具体实施方式

[0054] 实施例：

本发明的一种多算法多密钥的光认证离线支付方法，具体实施步骤如下：

建立一套多算法多密钥的光认证离线消费装置，包括：电子钱包1、消费机2、服务器3。

[0055] 电子钱包1，包括：可见光发射模块17、条码扫描模块15、控制模块11、钱包模块16、输入模块12、显示模块13、数据接口14、钱包光接收模块18、密码处理模块19。

[0056] 可见光发射模块17，用于根据控制模块11输入的信息，生成并发送可见光信号。

[0057] 条码扫描模块15，用于扫描识别条码，并将识别的结果输出给控制模块11。

[0058] 控制模块11，用于：1、将待发送的信息进行处理，生成数据包，并输出给可见光发射模块17，驱动可见光发射模块17发送可见光信号；2、接收条码扫描模块15的扫描结果输出，并对扫描结果进行验证；3、与钱包模块16进行消费、充值、余额查询、操作日志信息的读写操作；4、根据收到的信息和生成的支付信息，生成需要通过可见光发射模块17发送的信息；5、能够通过数据接口14与服务器3进行数据交互；6、接收钱包光接收模块18的结果输出，并予以识别、认证；7、输入待加密的数据到密码处理模块19，并接收密码处理模块19加密后的数据输出；8、输入待解密的数据到密码处理模块19，并接收密码处理模块19解密后的数据输出；9、向密码处理模块19输入密码算法和密钥的选择的指令。

[0059] 钱包模块16，用于保存包括：用户账号信息、钱包余额、消费权限、查询密码、支付密码、操作日志、生产发行机构在内的信息；并可以验证输入的密码是否与钱包密码模块内保存的密码一致；该模块使用手机sim卡实现。

[0060] 输入模块12，用于向控制模块11输入支付金额、查询密码、支付密码、操作指令。

[0061] 显示模块13，用于显示支付金额、密码输入界面、操作指令以及提示信息。

[0062] 数据接口14，用于提供电子钱包1的联网功能，提供与服务器3连接，并进行数据交换、数据维护和升级的功能。

[0063] 钱包光接收模块18，用于接收背光模块26发送的可见光背光信号。

[0064] 密码处理模块19，用于：1、为支付流程中电子钱包1需要传输的信息，提供不止一种的密码算法；2、保存提供的密码算法中，将会使用到的密钥；3、根据所选择的密码算法和密钥，对支付流程中电子钱包1需要发送的信息进行加密，并对电子钱包1接收到的加密信息进行解密。

[0065] 电子钱包1采用配置了闪光灯、光电感知器件和摄像头的智能手机实现。

[0066] 消费机2，包括：可见光接收模块24、条码显示模块22、读写控制模块21、收银箱模块23、键盘模块25、条码显示模块22、通信模块27、背光模块26、密码协处理器28。

[0067] 可见光接收模块24，用于接收可见光信号，并处理还原成对应的数字信号，还原成数据包。

[0068] 条码显示模块22，用于：1、根据读写控制模块21的输入信息，生成并显示出条码；2、显示交易金额、密码输入界面、操作指令以及提示信息。

[0069] 读写控制模块21，用于：1、接收可见光接收模块24的输出，并予以认证；2、将待发送的信息进行处理，输出给条码显示模块22；3、与收银箱模块23进行消费、充值、余额查询、操作日志信息的读写操作；4、提供通信接口，通过通信模块27与服务器3进行信息的上传和下载；5、将需要通过光信号形式发送的信息进行处理，生成数据包，并输出给背光模块26，驱动背光模块26发送可见光信号；6、输入待加密的数据到密码协处理器28，并接收密码协处理器28加密后的数据输出；7、输入待解密的数据到密码协处理器28，并接收密码协处理器28解密后的数据输出；8、向密码协处理器28输入密码算法和密钥的选择的指令。

[0070] 收银箱模块23，用于保存包括：操作日志、收款消费权限、黑名单、收银余额、操作密码、有效期、生产发行机构在内的信息。

[0071] 键盘模块25，用于向读写控制模块21输入交易金额、交易密码、操作指令。

[0072] 通信模块27，用于通过有线或者无线的方式，连接上位机或者接入网络，从而与服务器3相连。

[0073] 背光模块26，用于为条码显示模块22提供显示的照明背光，同时利用背光发送可见光背光信号。

[0074] 密码协处理器28，用于：1、为支付流程中消费机需要传输的信息，提供不止一种的密码算法；2、保存提供的密码算法中，将会使用到的密钥；3、根据所选择的密码算法和密钥，对支付流程中消费机2需要发送的信息进行加密，并对消费机2接收到的加密信息进行解密。

[0075] 服务器3，用于：1、与消费机2通过通信模块27建立上传、下载的数据连接；2、与电子钱包1通过数据接口14建立上传、下载的数据连接；3、提供本离线支付方法的后台服务支持；4、提供整个离线支付装置与金融系统的资金流动的接口；5、为消费机2以及电子钱包1发放或取消授权，提供包括：密钥更新、算法更新和升级、使用权限调整、有效期调整、电子钱包充值、消费机缴款、电子钱包1和消费机2公开信息查询在内的服务；6、保存包括：授权用户清单、黑名单、操作日志、消费机清单在内的信息。

[0076] 授权用户清单，用于保存包括：已经授权可以进行离线支付的电子钱包身份标识、使用权限、有效期、电子钱包持有者的身份信息。

[0077] 黑名单，用于保存授权用户清单中，因欠费、挂失、有不正当使用记录而被拒绝支

付交易的那部分电子钱包的身份标识信息。

[0078] 支付接口，用于提供整个离线支付装置与金融系统的资金流动的接口。

[0079] 操作日志汇总，用于保存包括所有消费机、电子钱包的查询、充值、消费的操作的时间、支付金额、支付过程数据参数在内的信息。

[0080] 消费机清单，用于保存已经授权可以进行离线支付交易的消费机终端的信息、使用权限、有效期。

[0081] 电子钱包的发行过程包括：由服务器给用户发放一个授权，授权方式可以是发放一个授权实体硬件设备，也可以是为用户已有的配备本发明的设备提供一个授权号；并为设备充值，写入电子钱包身份标识、使用权限、有效期、电子钱包的支付密码和查询密码、电子钱包持有者的身份信息。

[0082] 由电子钱包1向消费机2发起支付，支付流程包括以下步骤：

DM1，电子钱包1生成一个支付请求码QQM1，支付请求码QQM1包括：电子钱包身份标识QID1、支付随机码QRD1、支付金额ZFR1，并由可见光发射模块17采用可见光信号的方式向消费机2发送支付请求码QQM1。

[0083] DM2，消费机2通过可见光接收模块24接收可见光信号形式的支付请求码QQM2，从中提取出电子钱包身份标识QID2、支付随机码QRD2、支付金额ZFR2；消费机生成一个应答随机码YDR2、一个光随机码GRD2；并根据应答随机码YDR2，选择一种密码算法SFn和一个加密密钥MYn；再根据光随机码GRD2，选择密码算法SFm和一个加密密钥MYm。

[0084] DM2.1，根据支付请求码QQM2、应答随机码YDR2、光随机码GRD2，生成一个收款应答码SKYD2，并运算得到收款码SKM2，收款码SKM2包括：收款金额SJR2、消费机身份标识SID2、收款应答码SKYD2、支付请求码QQM2、支付随机码QRD2；将收款码SKM2分成两个部分SKM2-1和SKM2-2，用密码算法SFn和一个加密密钥MYn对SKM2-1进行加密得到SFnSKM2-1，密码算法SFm和一个加密密钥MYm对SKM2-2和应答随机码YDR2进行加密得到SFmSKM2-2。

[0085] DM2.2，将SFnSKM2-1和SFmSKM2-2生成条码，通过条码显示模块22显示出来；并通过背光模块26，将光随机码GRD2以可见光信号的方式向电子钱包1发送出去。

[0086] DM3，由电子钱包1扫描消费机2的条码显示模块22显示的条码得到SFnSKM3-1、SFmSKM3-2，电子钱包1利用钱包光接收模块18接收光随机码GRD3；并根据光随机码GRD3，确定采用密码算法SFm和解密密钥JMm对SFmSKM3-2进行解密得到SKM3-2、应答随机码YDR3，再根据应答随机码YDR3确定选择密码算法SFn和一个解密密钥JMn对SFnSKM3-1进行解密得到SKM3-1。

[0087] DM3.1，合并SKM3-1和SKM3-2得到收款码SKM3；并从收款码SKM3提取出收款金额SJR3、消费机身份标识SID3、收款应答码SKYD3、支付随机码QRD3；并根据收款应答码SKYD3、应答随机码YDR3、光随机码GRD3，运算得到支付请求码QQM3、应答随机码YDR3。

[0088] DM3.2，进行以下的对比验证：

1）DM1中电子钱包1生成的支付请求码QQM1和DM3中接收并提取得到的支付请求码QQM3。

[0089] 2）DM1中电子钱包1生成的支付金额ZFR1和DM3中接收并从收款码中提取得到的收款金额SJR3。

[0090] 3）DM1中电子钱包1生成的支付随机码QRD1和DM3中接收并从收款码中提取得到的

支付随机码QRD3。

[0091] 如果以上有一个不一致则退出支付流程，并在显示模块13上显示支付请求错误的提示信息；如果一致就进入DM3.3。

[0092] DM3.3，电子钱包1根据从收款码SKM3提取得到的收款金额SJR3、消费机身份标识SID3、收款应答码SKYD3、支付随机码QRD3以及收款应答码SKYD3、应答随机码YDR3、光随机码GRD3，运算得到支付确认码FKQR3，并生成支付码ZFM3，支付码ZFM3包括：收款码SKM3、电子钱包身份标识FID1、支付金额FJR1、支付确认码FKQR3，再根据应答随机码YDR3、光随机码GRD3选择密码算法SFa和一个加密密钥MYa对支付码ZFM3进行加密的到MYaZFM3，再把MYaZFM3以可见光信号的形式，由可见光发射模块17发送出去。

[0093] DM4，消费机2通过可见光接收模块24接收可见光信号形式的信号，得到MYaZFM3，再根据应答随机码YDR2、光随机码GRD2选择密码算法SFb和一个加密密钥MYb对MYaZFM3进行解密得到支付码ZFM4，从中提取出收款码SKM4、电子钱包身份标识QID4、支付金额FJR4、支付确认码FKQR4，从SKM4提取出收款金额SJR4、消费机身份标识SID4、收款应答码SKYD4、收款金额SJR3、支付随机码QRD4；从支付确认码FKQR4运算得到收款应答码SKYD4、应答随机码YDR4、光随机码GRD4。

[0094] DM4.1，进行至少以下的对比验证：

1)对比DM2运算得到的收款码SKM2和DM4中提取出的收款码SKM4。

[0095] 2)对比DM2中生成的应答随机码YDR2和DM4中从SKM4提取出的应答随机码YDR4。

[0096] 3)对比DM2中生成的光随机码GRD2和DM4中从SKM4提取出的光随机码GRD4。

[0097] 4)对比DM2中提取到的电子钱包身份标识QID2和DM4中从ZFM4提取出的电子钱包身份标识QID4。

[0098] 5)对比DM2中得到的支付金额FJR2、收款金额SJR2和DM4中从ZFM4提取出的收款金额SJR4。

[0099] 6)对比DM2中得到的支付随机码QRD2和DM4中从ZFM4提取出的支付随机码QRD4。

[0100] 如果以上6个对比都分别一致，就进入DM4.2；否则就退出支付流程，并在条码显示模块上显示验证出错的提示信息。

[0101] DM4.2，消费机2生成一个光确认码GQR4，并根据电子钱包身份标识QID4、支付金额FJR4、消费机身份标识SID4、收款应答码SKYD4、应答随机码YDR4、光确认码GQR4、支付随机码QRD4，运算得到收款确认码SKQR4；将收款确认码SKQR分成两个部分SKQR4-1和SKQR4-2。

[0102] DM4.3，根据光确认码GQR4和应答随机码YDR2，选择一种密码算法SFp和一个加密密钥MYp；再根据光确认码GQR4和光随机码GRD2，选择密码算法SFq和一个加密密钥MYq；用密码算法SFp和一个加密密钥MYp对SKQR4-1进行加密得到SFpSKQR4-1，用密码算法SFq和一个加密密钥MYq对SKQR4-2和应答随机码YDR2进行加密得到SFqSKQR4-2。

[0103] DM4.4，消费机2将SFpSKQR4-1和SFqSKQR4-2生成条码，通过条码显示模块22显示出来；并通过背光模块26，将光确认码GQR4以可见光信号的方式向电子钱包1发送出去。

[0104] DM5，电子钱包1扫描消费机2的条码显示模块22显示的条码得到SFpSKQR5-1和SFqSKQR5-2，电子钱包1利用钱包光接收模块18接收光确认码GQR5；电子钱包1根据光确认码GQR5和应答随机码YDR3，选择一种密码算法SFp和一个解密密钥JYp；再根据光确认码GQR5和光随机码GRD3，选择密码算法SFq和一个解密密钥JYq；采用密码算法SFp和解密密钥

JYp对SFpSKQR5-1进行解密得到SKQR5-1，采用密码算法SFq和解密密钥JYq对SFqSKQR5-2得到SKQR5-2；合并SKQR5-1 和SKQR5-2得到收款确认码SKQR5；再由收款确认码SKQR5运算得到电子钱包身份标识QID5、支付金额FJR5、消费机身份标识SID5、收款应答码SKYD5、光确认码GQR5、支付随机码QRD5。

[0105] DM5.1，进行至少以下的对比验证：

1)对比电子钱包身份标识QID1和从ZF5中运算得到的电子钱包身份标识QID5。

[0106] 2)对比ZF1生成的支付金额FJR1和从ZF5中运算得到的支付金额FJR5。

[0107] 3)对比ZF1生成的支付随机码QRD1和从ZF5中运算得到的支付随机码QRD5。

[0108] 4)对比ZF3得到的消费机身份标识SID3和从ZF5中运算得到的消费机身份标识SID5。

[0109] 5)对比ZF3生成的收款应答码SKYD3和从ZF5中运算得到的收款应答码SKYD5。

[0110] 如果以上有一个对比不一致则退出支付流程，并在显示模块13上显示验证错误的提示信息；如果一致就进入DM5.2。

[0111] DM5.2，电子钱包1把光确认码GQR5、收款确认码SKQR5，以可见光信号的形式，由可见光发射模块17发送出去。

[0112] DM5.3，更新钱包模块16的钱包余额，用操作时间SJ、收款应答码SKYD5、支付金额FJR、消费机身份标识SID5、收款应答码SKYD5生成操作日志，并通过显示模块显示付款成功的提示信息。

[0113] DM6，消费机2通过可见光接收模块24接收可见光形式的信号，从中提取出光确认码GQR6、收款确认码SKQR6，将该操作时间SJ、电子钱包身份标识FID6、支付金额FJR6、支付码ZFM6、收款码SKM6写入收款箱模块23，生成操作日志，并更新收款箱模块23的余额信息，并通过条码显示模块22显示收款成功的提示信息。

[0114] 在支付流程中，从电子钱包1接收消费机2发送的数据，以及从消费机2接收电子钱包1发送的数据，都可能在收发过程中存在无法识别的可能，所以在支付流程中，对于无法识别的数据，以及因为无法接收数据而导致无法识别的情况，装置都会在一个设定的等待时间超时后，单方面结束支付流程。

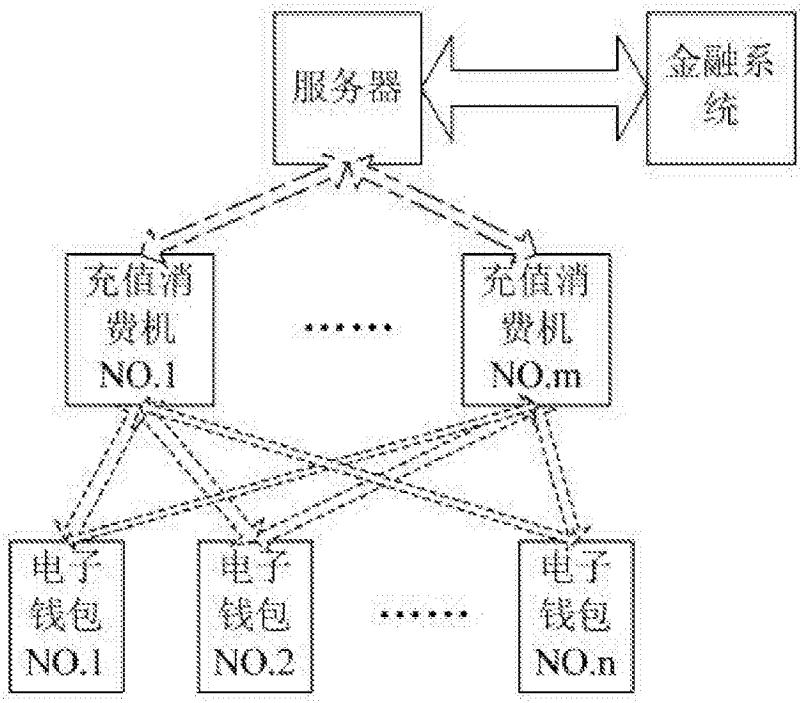

服务器
金融系统
充值消费机 NO.1
……
充值消费机 NO.m
电子钱包 NO.1
电子钱包 NO.2
……
电子钱包 NO.n

图 1

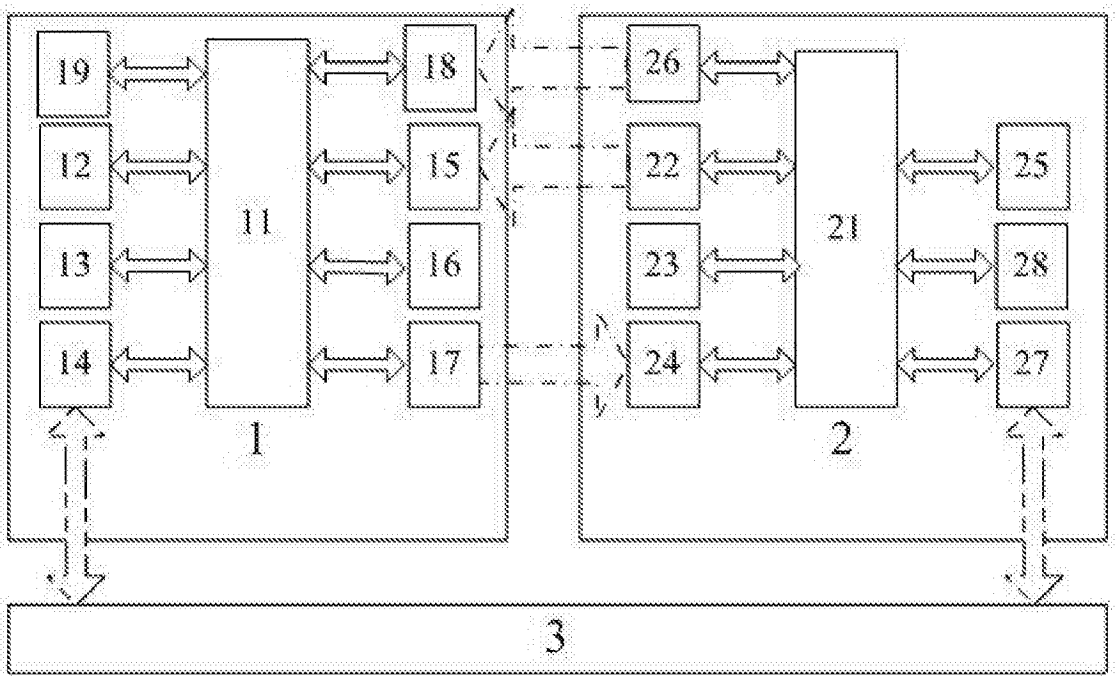

19
12
13
14
11
18
15
16
17
1
26
22
23
24
21
25
28
27
2
3

图 2