(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 103714458 B
(45)授权公告日 2017.03.29

(21)申请号 201310703046.5

(22)申请日 2013.12.20

(65)同一申请的已公布的文献号
申请公布号 CN 103714458 A

(43)申请公布日 2014.04.09

(73)专利权人 江苏大学
地址 212013 江苏省镇江市京口区学府路301号

(72)发明人 韩牟 詹洋 马世典 孔令晶 王松浩

(74)专利代理机构 南京知识律师事务所 32207
代理人 汪旭东

(51)Int.Cl.
G06Q 20/40(2012.01)
G06Q 20/02(2012.01)
G06Q 30/06(2012.01)
H04L 9/32(2006.01)

(56)对比文件
CN 102842081 A,2012.12.26,
CN 101377838 A,2009.03.04,
CN 103208064 A,2013.07.17,
CN 102118710 A,2011.07.06,
CN 102842081 A,2012.12.26,
US 6856975 B1,2005.02.15,

审查员 谢珊珊

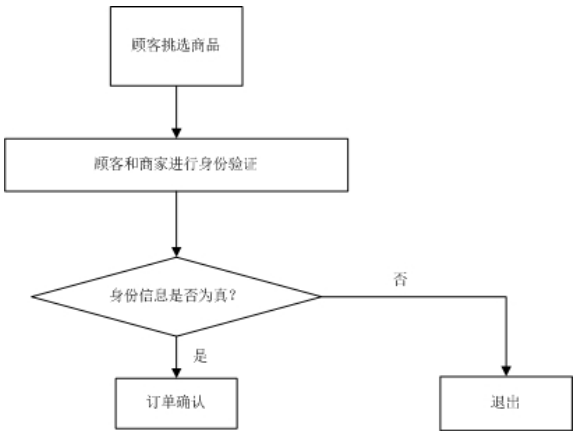
权利要求书2页 说明书4页 附图1页

(54)发明名称

基于二维码的移动终端交易加密方法

(57)摘要

本发明公开了一种基于二维码的移动终端交易加密方法，属于网络技术领域。本发明将二维码技术以及现有移动终端交易协议进行结合，在交易双方身份验证、订单确认以及支付过程中通过二维码进行相关信息的加密确保交易安全。本发明能够实现更加安全可靠的网上交易而不对移动终端装置带来太大的负担，保证移动端网上交易的安全性、保密性、不可抵赖性。



CN 103714458 B

1.基于二维码的移动终端交易加密方法,其特征在于,包括以下步骤:

1)顾客通过移动终端在商家的网上交易平台上选定商品后,交易双方进行身份验证,包括以下步骤:

1-1)顾客和商家的二维码芯片装置分别使用自己的私钥将当前时间戳信息加密,然后将密文生成二维码,并发送给第三方银行;

1-2)银行对发送过来的二维码分别解码,得到顾客和商家所生成的密文,并分别用顾客及商家的公钥进行解密,得到顾客用户及商家用户发送的时间戳,并比较两个时间戳是否相等;

1-3)若两个时间戳相等,银行进行交易双方的身份验证,并将对方身份信息分别用顾客和商家各自的公钥进行加密,将密文生成二维码,并分别发送给交易双方;顾客和商家的二维码芯片装置对银行发送的对方身份信息的二维码进行解码得到对方身份信息,从而确认对方的身份;

若两个时间戳不相等,银行将警告信息用顾客和商家各自的公钥加密,将密文生成二维码,并分别发送给交易双方;顾客和商家的二维码芯片装置对银行发送的警告信息的二维码进行解码得到警告信息,提示交易双方身份验证未通过,结束本方法;

2)如交易双方确认对方的身份,则进行订单确认,包括以下步骤:

2-1)顾客的二维码芯片装置将订单信息以及支付信息分别生成消息摘要,并与当前时间戳联合,用自己的私钥加密,然后分别用银行以及商家的公钥加密,并将密文生成二维码,利用移动终端分别发送给银行以及商家;所述订单信息为购买商品的详细信息;

2-2)商家的二维码芯片装置将顾客发送过来的二维码解码,并用自己的私钥解密后得到商品信息摘要以及支付信息摘要,并就自己已经知晓的用户购买的商品详细信息生成商品信息摘要,与顾客发送过来的商品信息摘要进行比较,若一致,就将顾客发送过来的已解密的消息用自己的私钥加密并用银行公钥加密后,将密文生成二维码发送给银行;否则,向银行发送订单信息出错信息;

2-3)如果银行收到商家发送的订单信息出错信息或者比较商家和顾客发送过来的订单信息时发现不一致,则订单确认未通过,银行将订单确认未通过信息发送给顾客,结束本方法;

如果银行确认商家和顾客发送过来的订单信息一致,则订单确认通过,银行将订单确认通过信息发送给顾客;

3)如果订单确认通过,则进行支付,包括以下步骤:

3-1)顾客通过移动终端进入支付页面,二维码芯片装置被触发,要求用户输入相应的进入口令;

3-2)顾客输入进入口令后,二维码芯片装置将该口令加密并生成二维码发送给银行;银行通过解析二维码获得加密过的进入口令,核实顾客进入口令是否正确;如正确则通知顾客进行支付,否则通知顾客重新输入进入口令;如果三次进入口令输入出错,二维码芯片装置启动保护功能,强制退出,结束本方法;

3-3)顾客得到银行进行支付的通知后,进行支付操作,该支付操作信息同样经由二维码芯片装置加密后以二维码形式发给银行;

3-4)收到顾客的支付操作信息后,银行要求顾客确认支付信息并要求顾客输入支付密

码，该要求经过银行服务器以顾客公钥加密后以二维码形式发送至顾客；

3-5)顾客的二维码芯片装置对收到的二维码信息进行解码，并将相关提示信息输出到移动终端，提示顾客输入支付密码；如顾客输入支付密码，则顾客的二维码芯片装置对支付密码加密并进行二维码编码后发送给银行，否则结束本方法；

3-6)银行收到顾客的支付密码后，进行转账操作，完成支付。

2.根据权利要求1所述的基于二维码的移动终端交易加密方法，其特征在于，所述购买商品的详细信息以及支付信息通过MD5算法生成消息摘要。

3.根据权利要求1所述的基于二维码的移动终端交易加密方法，其特征在于，所述加密、解密采用RSA算法。

基于二维码的移动终端交易加密方法

技术领域

[0001] 本发明属于网络技术领域，更准确地说，本发明涉及一种基于二维码的移动终端交易加密方法。

背景技术

[0002] 随着移动通信及网络技术的进步，移动终端应用已经深入到日常生活的各各角落。但由于移动终端支付中存在的安全性以及隐私保护等问题，使得其应用遭遇瓶颈。目前，在移动终端支付领域，绝大多数方案均是仅仅通过加解密算法来实现信息的保密性以及对用户进行身份认证，但却没有考虑到移动终端本身的不安全性以及信息的传输效率。

[0003] 二维码是用特定的几何图形按一定规律在平面(二维方向上)分布的黑白相间的矩形方阵记录数据符号信息的新一代条码技术具有信息量大，纠错能力强，识读速度快，保密性高，追踪性高，抗损性强，备援性大，成本便宜等特性。手机二维码是二维码技术在手机上的应用，目前已经广泛应用于请柬，海报，签到，名片，指示牌，宣传广告等各种场合。若使用二维码在某些重要场合传递具有身份信息、时效要求较高的数据时，需要对其加解密算法进行优化设计。

[0004] MD5(消息摘要算法)等加密技术已广泛用于对各种信息进行加密，该加密及时具有单向不可逆性(即只能通过加密得到密文，而不可由密文反向得到明文)，可用于生成消息摘要，且在手机平台上也易于实现。RSA算法已经在传统电子商务中进行了广泛应用，并且其既可实现通过私钥进行签名，又可实现通过公钥进行加密，在目前计算能力下是安全的，且基于该技术的芯片已经实现了商业化生产。

发明内容

[0005] 本发明的目的是：针对现有技术中使用移动终端进行交易支付安全性不足的问题，提供一种基于二维码的移动终端交易加密方法，该方法将二维码技术以及现有移动终端交易协议进行结合，在交易双方身份验证、订单确认以及支付过程中通过二维码进行相关信息的加密确保交易安全，从而保证移动端网上交易的安全性、保密性、不可抵赖性。

[0006] 具体地说，本发明是采用以下的技术方案来实现的，包括以下步骤：

[0007] 1)顾客通过移动终端在商家的网上交易平台上选定商品后，交易双方进行身份验证，包括以下步骤：

[0008] 1-1)顾客和商家的二维码芯片装置分别使用自己的私钥将当前时间戳信息加密，然后将密文生成二维码，并发送给第三方银行；

[0009] 1-2)银行对发送过来的二维码分别解码，得到顾客和商家所生成的密文，并分别用顾客及商家的公钥进行解密，得到顾客用户及商家用户发送的时间戳，并比较两个时间戳是否相等；

[0010] 1-3)若两个时间戳相等，银行进行交易双方的身份验证，并将对方身份信息分别用顾客和商家各自的公钥进行加密，将密文生成二维码，并分别发送给交易双方；顾客和商

家的二维码芯片装置对银行发送的对方身份信息的二维码进行解码得到对方身份信息，从而确认对方的身份；

[0011] 若两个时间戳不相等，银行将警告信息用顾客和商家各自的公钥加密，将密文生成二维码，并分别发送给交易双方；顾客和商家的二维码芯片装置对银行发送的警告信息的二维码进行解码得到警告信息，提示交易双方身份验证未通过，结束本方法；

[0012] 2)如交易双方确认对方的身份，则进行订单确认，包括以下步骤：

[0013] 2-1)顾客的二维码芯片装置将信息订单以及支付信息分别生成消息摘要，并与当前时间戳联合，用自己的私钥加密，然后分别用银行以及商家的公钥加密，并将密文生成二维码，利用移动终端分别发送给银行以及商家；所述订单信息为购买商品的详细信息；

[0014] 2-2)商家的二维码芯片装置将顾客发送过来的二维码解码，并用自己的私钥解密后得到商品信息摘要以及支付信息摘要，并就自己已经知晓的用户购买的商品详细信息生成商品信息摘要，与顾客发送过来的商品信息摘要进行比较，若一致，就将顾客发送过来的已解密的消息用自己的私钥加密并用银行公钥加密后，将密文生成二维码发送给银行；否则，向银行发送订单信息出错信息；

[0015] 2-3)如果银行收到商家发送的订单信息出错信息或者比较商家和顾客发送过来的订单信息时发现不一致，则订单确认未通过，银行将订单确认未通过信息发送给顾客，结束本方法；

[0016] 如果银行确认商家和顾客发送过来的订单信息一致，则订单确认通过，银行将订单确认通过信息发送给顾客；

[0017] 3)如果订单确认通过，则进行支付，包括以下步骤：

[0018] 3-1)顾客通过移动终端进入支付页面，二维码芯片装置被触发，要求用户输入相应的进入口令；

[0019] 3-2)顾客输入进入口令后，二维码芯片装置将该口令加密并生成二维码发送给银行；银行通过解析二维码获得加密过的进入口令，核实顾客进入口令是否正确；如正确则通知顾客进行支付，否则通知顾客重新输入进入口令；如果三次进入口令输入出错，二维码芯片装置启动保护功能，强制退出，结束本方法；

[0020] 3-3)顾客得到银行进行支付的通知后，进行支付操作，该支付操作信息同样经由二维码芯片装置加密后以二维码形式发给银行；

[0021] 3-4)收到顾客的支付操作信息后，银行要求顾客确认支付信息并要求顾客输入支付密码，该要求经过银行服务器以顾客公钥加密后以二维码形式发送至顾客；

[0022] 3-5)顾客的二维码芯片装置对收到的二维码信息进行解码，并将相关提示信息输出到移动终端，提示顾客输入支付密码；如顾客输入支付密码，则顾客的二维码芯片装置对支付密码加密并进行二维码编码后发送给银行，否则结束本方法；

[0023] 3-6)银行收到顾客的支付密码后，进行转账操作，完成支付。

[0024] 上述技术方案的进一步特征在于，所述购买商品的详细信息以及支付信息通过MD5算法生成消息摘要。

[0025] 上述技术方案的进一步特征在于，所述加密、解密采用RSA算法。

[0026] 本发明的有益效果如下：将二维码技术以及现有移动终端交易协议进行结合，在交易双方身份验证、订单确认以及支付过程中通过二维码进行相关信息的加密确保交易安

全。本发明能够实现更加安全可靠的网上交易而不对移动终端装置带来太大的负担，保证移动端网上交易的安全性、保密性、不可抵赖性。

附图说明

[0027] 图1为本发明方法中交易双方身份验证的流程图。

[0028] 图2为本发明方法中订单确认的流程图。

具体实施方式

[0029] 下面参照附图并结合实例对本发明作进一步详细描述。

[0030] 本发明方法基于二维码芯片装置，该二维码芯片装置具有以下功能：

[0031] (1)该二维码芯片装置在顾客即将进入移动终端支付交易平台时需要对顾客进行身份认证，也就是说，每次顾客转到移动终端支付页面，都需要输入进入口令，然后装置自动将该口令加密后发送给银行的代理服务器进行口令验证，只有通过口令验证，才能够继续使用。

[0032] (2)该二维码芯片装置还保存了顾客的身份验证证书，即唯一确认顾客身份的私钥，在顾客需要进行身份认证的时候，能够实现自动为信息签名。

[0033] (3)该二维码芯片装置可以识别二维码信息，即可以对所接收到的二维码可以进行解码并显示输出。

[0034] (4)该二维码芯片装置可以生成二维码，即可以对消息进行编码后以二维码的形式发送。

[0035] 本发明方法中，顾客和商家都需要配置自己的二维码芯片装置。顾客的二维码芯片装置与移动终端相连接，移动终端为二维码芯片装置提供必要的支持，主要提供电能、程序驱动等。顾客可以通过移动终端进行网上交易。

[0036] 二维码芯片装置由银行负责发放。顾客可以通过向银行申请移动支付服务以获得该装置。银行的密钥管理服务器随机从自己的密钥存储数据库中取出一个密钥，并将顾客身份信息、顾客设定的进入口令以及分配的私钥存入一个拥有唯一编号的二维码芯片装置，并将该芯片装置分配给顾客。该密钥就是顾客的私钥，以后顾客就可以用该私钥给自己的信息签名以及加密。商家获得该装置的过程与顾客相似，同样可以从银行获得属于自己的私钥进行信息签名及加密。

[0037] 如图1、图2所示，本发明的具体步骤如下：

[0038] 1)顾客通过移动终端在商家的网上交易平台上选定商品后，交易双方进行身份验证，包括以下步骤：

[0039] 1-1)顾客和商家的二维码芯片装置分别使用自己的私钥将当前时间戳信息通过RSA加密算法加密，然后将密文生成二维码，并发送给第三方银行；

[0040] 1-2)银行对发送过来的二维码分别解码，得到顾客和商家所生成的密文，并分别用顾客及商家的公钥进行解密，得到顾客用户及商家用户发送的时间戳，并比较两个时间戳是否相等；

[0041] 1-3)若两个时间戳相等，银行进行交易双方的身份验证，并将对方身份信息分别用顾客和商家各自的公钥通过RSA加密算法进行加密，将密文生成二维码，并分别发送给交

易双方;顾客和商家的二维码芯片装置对银行发送的对方身份信息的二维码进行解码得到对方身份信息,从而确认对方的身份;

[0042] 若两个时间戳不相等,银行将警告信息用顾客和商家各自的公钥通过RSA加密算法加密,将密文生成二维码,并分别发送给交易双方;顾客和商家的二维码芯片装置对银行发送的警告信息的二维码进行解码得到警告信息,提示交易双方身份验证未通过,结束本方法;

[0043] 2)如交易双方确认对方的身份,则进行订单确认,包括以下步骤:

[0044] 2-1)顾客的二维码芯片装置将订单信息以及支付信息分别通过MD5算法生成消息摘要,并与当前时间戳联合,用自己的私钥通过RSA加密算法加密,然后分别用银行以及商家的公钥通过RSA加密算法加密,并将密文生成二维码,利用移动终端分别发送给银行以及商家;所述订单信息为购买商品的详细信息;

[0045] 2-2)商家的二维码芯片装置将顾客发送过来的二维码解码,并用自己的私钥通过RSA解密后得到商品信息摘要以及支付信息摘要,并根据自己已经知晓的用户购买的商品详细信息通过MD5生成商品信息摘要,与顾客发送过来的商品信息摘要进行比较,若一致,就将顾客发送过来的已解密的消息用自己的私钥通过RSA签名并用银行公钥经RSA加密后,将密文生成二维码发送给银行;否则,向银行发送订单信息出错信息;

[0046] 2-3)如果银行收到商家发送的订单信息出错信息或者比较商家和顾客发送过来的订单信息时发现不一致,则订单确认未通过,银行将订单确认未通过信息发送给顾客,结束本方法;

[0047] 如果银行确认商家和顾客发送过来的订单信息一致,则订单确认通过,银行将订单确认通过信息发送给顾客;

[0048] 3)如果订单确认通过,则进行支付,包括以下步骤:

[0049] 3-1)顾客通过移动终端进入支付页面,二维码芯片装置被触发,要求用户输入相应的进入口令;

[0050] 3-2)顾客输入进入口令后,二维码芯片装置将该口令加密并生成二维码发送给银行;银行通过解析二维码获得加密过的进入口令,核实顾客进入口令是否正确;如正确则通知顾客进行支付,否则通知顾客重新输入进入口令;如果三次进入口令输入出错,二维码芯片装置启动保护功能,强制退出,结束本方法;

[0051] 3-3)顾客得到银行进行支付的通知后,进行支付操作,该支付操作信息同样经由二维码芯片装置加密后以二维码形式发给银行;

[0052] 3-4)收到顾客的支付操作信息后,银行要求顾客确认支付信息并要求顾客输入支付密码,该要求经过银行服务器以顾客公钥通过RSA进行加密后以二维码形式发送至顾客;

[0053] 3-5)顾客的二维码芯片装置对收到的二维码信息进行解码,并将相关提示信息输出到移动终端,提示顾客输入支付密码;如顾客输入支付密码,则顾客的二维码芯片装置对支付密码加密并进行二维码编码后发送给银行,否则结束本方法;

[0054] 3-6)银行收到顾客的支付密码后,进行转账操作,完成支付。

[0055] 虽然本发明已以较佳实施例公开如上,但实施例并不是用来限定本发明的。在不脱离本发明之精神和范围内,所做的任何等效变化或润饰,同样属于本发明之保护范围。因此本发明的保护范围应当以本申请的权利要求所界定的内容为标准。

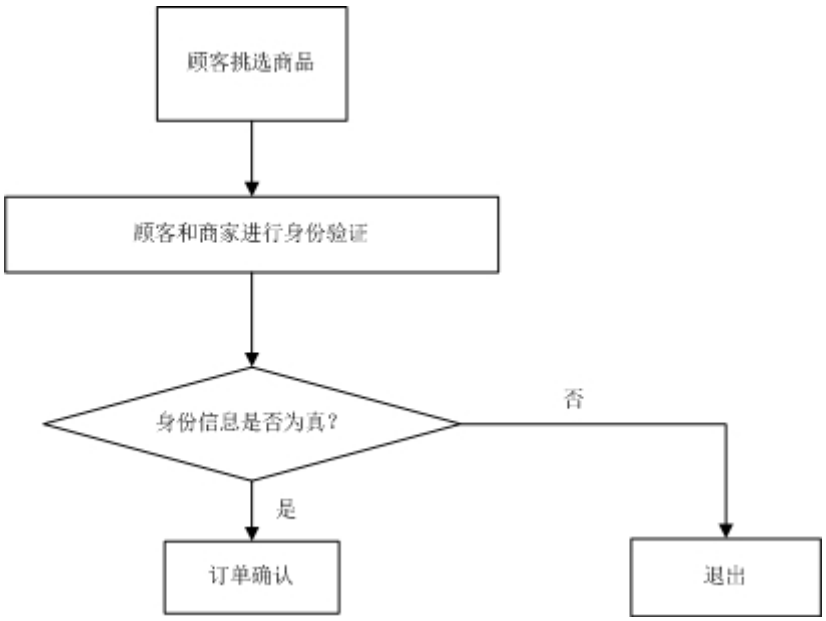

顾客挑选商品
顾客和商家进行身份验证
身份信息是否为真？
否
是
订单确认
退出

图1

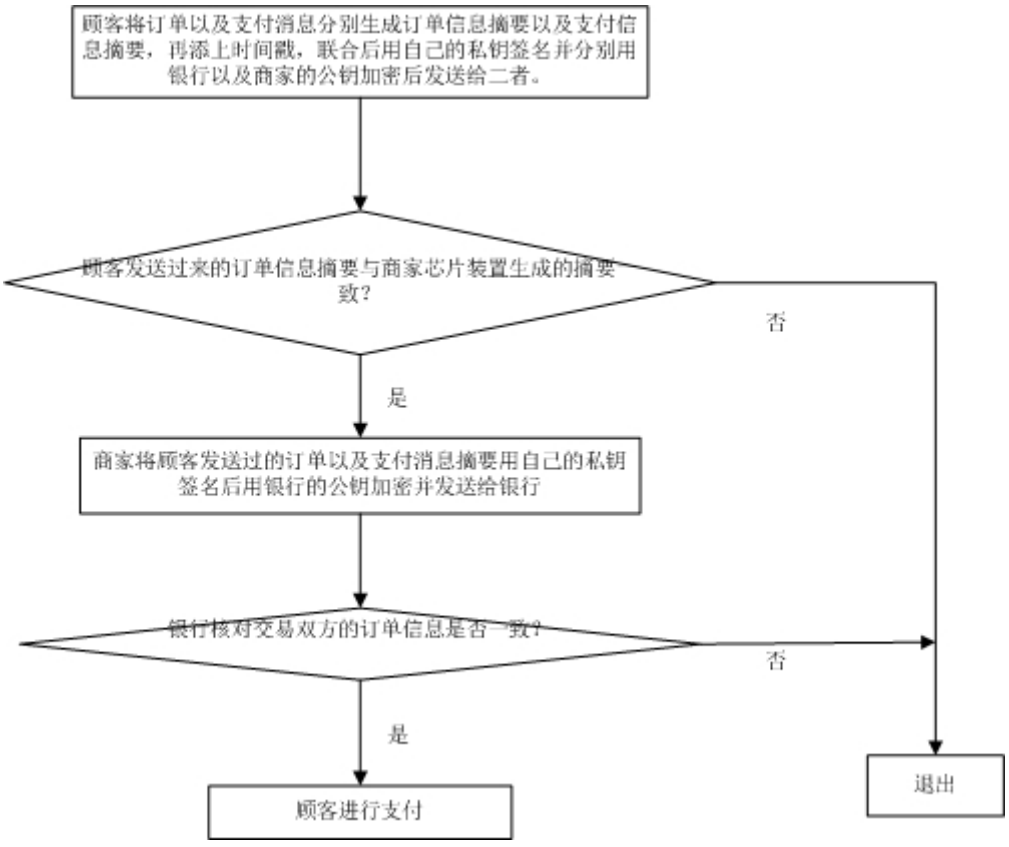

顾客将订单以及支付消息分别生成订单信息摘要以及支付信息摘要，再添上时间戳，联合后用自己的私钥签名并分别用银行以及商家的公钥加密后发送给二者。
顾客发送过来的订单信息摘要与商家芯片装置生成的摘要一致？
否
是
商家将顾客发送过的订单以及支付消息摘要用自己的私钥签名后用银行的公钥加密并发送给银行
银行核对交易双方的订单信息是否一致？
否
是
退出
顾客进行支付

图2