

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2013 年 5 月 23 日 (23.05.2013)



(10) 国际公布号
WO 2013/071858 A1

(51) 国际专利分类号:

G06Q 20/08 (2012.01) H04L 9/32 (2006.01)
H04L 29/06 (2006.01) H04L 9/30 (2006.01)
H04N 21/4623 (2011.01)

(21) 国际申请号: PCT/CN2012/084565

(22) 国际申请日: 2012 年 11 月 14 日 (14.11.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:

201110361720.7 2011 年 11 月 15 日 (15.11.2011) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNION-PAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 刘风军 (LIU, Fengjun); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 徐晓强 (XU, Xiaoqiang); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 杨建辉 (YANG, Jianhui); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(CN)。 肖波 (XIAO, Bo); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 刘源 (LIU, Yuan); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 徐蓉 (XU, Rong); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 孙立林 (SUN, Lilin); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 金正博 (JIN, Zhengbo); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 王春晖 (WANG, Chunhui); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 海涛 (HAI, Tao); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: 中国专利代理 (香港) 有限公司 (CHINA PATENT AGENT (HK) LTD.); 中国香港特别行政区湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,

[见续页]

(54) Title: PAYMENT SECRET KEY SYSTEM OF INTELLIGENT TV AND PAYMENT METHOD BASED ON INTELLIGENT TV

(54) 发明名称: 一种智能电视支付密钥系统以及基于智能电视的支付方法

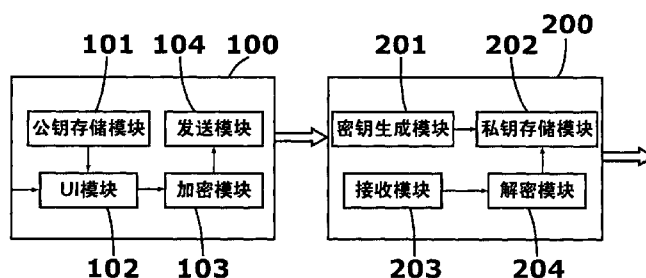


图1/Fig.1

101 PUBLIC KEY MEMORY MODULE
102 UI MODULE
103 ENCRYPTION MODULE
104 TRANSMISSION MODULE
201 SECRET KEY GENERATION MODULE
202 PRIVATE KEY MEMORY MODULE
203 RECEPTION MODULE
204 DECRYPTION MODULE

(57) Abstract: The present invention relates a payment secret key system of intelligent TV and a payment method based on intelligent TV. The payment system of the present invention includes a client terminal device (100) and a TVP (intelligent TV payment front device) encryption device (200), wherein, said payment client terminal device (100) has a public key memory module (101), a user interface module (102), an encryption module (103) and a transmission module (104), and said TVP encryption device (200) has a secret key generation module (201), a private key memory module (202), a reception module (203) and a decryption module (204). The payment secret key system of intelligent TV and a payment method based on intelligent TV using the present invention can improve security of the payment and save the cost.

(57) 摘要:

[见续页]



WO 2013/071858 A1



CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,

AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明涉及智能电视支付密钥系统和基于智能电视的支付方法。本发明的支付系统包括客户端装置(100)和 TVP 加密装置(200), 其中, 所述支付客户端装置(100)具备: 公钥存储模块(101)、用户界面模块(102)、加密模块(103)以及发送模块(104), 所述 TVP 加密装置(200)具备: 密钥生成模块(201)、私钥存储模块(202)、接收模块(203)、解密模块(204)。利用本发明的智能电视支付密钥系统和基于智能电视的支付方法能够提高支付安全性、节省成本。

一种智能电视支付密钥系统以及基于智能电视的支付方法

5 **技术领域**

本发明涉及一种智能电视支付密钥系统以及基于智能电视的支付方法，尤其涉及非对称密钥的智能电视支付密钥系统以及基于智能电视的支付方法。

10 **背景技术**

目前电视支付主要应用与两种场景：小额支付和大额支付。小额支付主要是电视用户用于购买影视剧视频服务的费用，电视服务运营商为用户提供一个虚拟账户，用户可以在账户中预先充值，当需要小额支付时，从这个虚拟的用户帐号扣除费用；大额支付一般
15 应用于电视商务、个人理财、缴费充值以及用户虚拟帐号的充值。电视支付基于无卡支付解决方案，持卡人通过遥控器操作对电视屏幕的菜单进行操作完成支付。用户能够通过智能电视终端的遥控器选择已绑定的银行卡卡号、输入个人密码或有效期或 CVN2（即校验码）等银行敏感信息实现无卡支付（事先绑定需要用户输入持卡人辅助认证信息送发卡方进行验证）；或者直接手动输入银行卡敏感信息和持卡人辅助认证信息等交易要素实现无卡交易。
20

图 N 是表示现有技术的电视支付系统的结构示意图。如图 N 所示，电视支付系统包括：支付客户端 801、支付通道前置系统（即 TPP）802、智能电视支付前置装置（即 TVP）803 及与之相关的内
25 容提供平台（也称为集成播控平台）804。整个电视支付系统在传输交易报文时对数据进行安全控制。

另一方面，市场上已出现的基于互联网模式的在线电视支付，其交易金融交易数据是通过 SSL 和 HTTPS 协议加密和传输。电视终端与服务器端通过数字证书相互认证，执行密钥交换；通过非对
30 称密钥对传送的数据进行加密和隐藏；达到数据的安全传输目的。

现有非对称加密技术应用更多的是终端只对用户 PIN 用公钥进行加密，在服务器端进行转加密。

在现有技术中存在以下的问题：不能绝对确保服务器自己是安全的。由于 SSL 和 HTTPS 协议加密算法及认证机制都是公开的，
5 且算法较简单，所以服务器端很容易被仿造；这点甚至已被攻击者利用，常见例子是模仿银行域名的钓鱼攻击。通过仿造服务器端模拟与客户端发生交易，获取银行卡号、交易密码等金融敏感信息。而如果通过双向认证的技术可以避免以上的缺陷，但却增加了开发和运营成本。另外，针对目前无卡支付的日益发展，发卡方更需要
10 对除 PIN 以外的其他要素进行验证，包括 CVN2、有效期等，甚至卡号，因此在交易通道中如何对这些要素进行安全传输是现有体系无法完全保障的。

发明内容

15 本发明鉴于上述问题，旨在提供一种安全性高、节省成本的智能电视支付密钥系统以及基于智能电视的支付方法。

本发明的智能电视支付密钥系统，其特征在于，具备支付客户端装置和 TVP 加密装置，所述支付客户端装置具备：公钥存储模块，预置有下述的公钥；用户界面模块，获得交易信息和敏感数据，将
20 获得的交易信息生成报文体，并且从所述公钥存储模块调用公钥；加密模块，利用通过所述用户界面模块调用的公钥对所述敏感信息进行加密得到客户端加密数据；以及发送模块，将所述客户端加密数据和所述报文体作为交易报文体到所述 TVP 加密装置，所述 TVP 加密装置具备：密钥生成模块，用于生成私钥和与该私钥一一对应的
25 的公钥；私钥存储模块，用于存储所述私钥，接收模块，用于接收从所述支付客户端装置发送来的交易报文体；解密模块，调用存储在所述私钥存储模块中的私钥对所述交易报文体中的所述客户端加密数据进行解密。

优选地，所述发送模块具有对所述交易报文进行压缩和编码的
30 压缩编码单元和发送经压缩和编码的所述交易报文的发送单元，所

述接收模块具有接收所述交易报文的接收单元和对接所述交易报文进行解码和解压缩的解码解压缩单元。

优选地，所述加密模块利用所述公钥对所述敏感信息进行 RSA 非对称加密算法进行加密，所述解密模块利用所述私钥所述客户端加密数据进行非对称私钥解密。

优选地，所述支付客户端装置还具备：用于对所述交易报文体计算摘要值并且将计算出的摘要值作为所述敏感数据的第一摘要值计算模块，所述 TVP 加密装置还具备：用于对接收到的所述交易报文体计算摘要值的第二摘要值计算模块；摘要值比较模块，比较所述第二摘要值计算模块中计算得到的摘要值和由所述解码解压缩单元解码解压后得到的敏感数据中含有的摘要值是否一致。

优选地，所述第一摘要值计算模块和第二摘要值计算模块利用安全哈希算法对所述交易报文体计算摘要值。

优选地，所述摘要值比较模块在判断为所述摘要值不一致的情况下丢弃报文。

优选地，所述公钥为具有随时间推移的对应有效期并且强度随时间推移逐渐增强。

优选地，所述公钥为 3 把，分别为 1152 位、1408 位、1984 位。

优选地，所述私钥和所述公钥通过索引号对应。

优选地，所述发送模块还将所述索引号与所述交易报文体一起发送到所述 TVP 加密装置。

优选地，所述解密模块还用于利用对称密钥对解密后的 PIN BLOCK（密码格式）进行转加密。

优选地，所述 TVP 加密装置具备：动态码生成模块，根据来自所述支付客户端装置的请求生成动态码并且存储该动态码，并将该动态码发送给用户；动态码比较模块，比较所述动态码生成模块中已存储的动态码和所述交易报文体中包含的动态码。

优选地，所述动态码比较模块在判断所述动态码生成模块中已存储的动态码和所述交易报文体中的动态码不一致的情况下丢弃报文。

本发明的基于智能电视的支付方法，利用支付客户端装置和 TVP 加密装置进行电视支付，其特征在于，包括：获得交易信息和敏感数据的获取步骤；利用公钥对所述获取的敏感数据进行加密的加密步骤；将加密后的敏感数据和交易信息从所述支付客户端装置发送到所述 TVP 加密装置的发送步骤；接收从所述支付客户端装置发送来的敏感数据和交易信息的接收步骤；用与所述公钥一一对应的私钥对接收到的敏感数据进行解密的解密步骤。

优选地，在所述加密步骤中，利用公钥对所述敏感信息进行 RSA 非对称加密，在所述解密步骤中，利用私钥对所述敏感数据进行非对称称私钥解密。

优选地，在所述发送步骤中，对所述交易报文进行压缩和编码之后再发送，在所述接收步骤中，接收所述交易报文之后对接所述交易报文进行解码和解压缩。

优选地，本发明的基于智能电视的支付方法还具备：在所述支付客户端装置对所述交易报文体计算摘要值并且将计算出的摘要值作为所述敏感数据的第一摘要值计算步骤；在所述 TVP 加密装置对接收到的所述交易报文体计算摘要值的第二摘要值计算步骤；比较通过所述第二摘要值计算步骤中计算得到的摘要值和通过所述解码解步骤解密后得到的敏感数据中含有的摘要值是否一致的摘要值比较步骤。

优选地，在所述第一摘要值计算步骤和所述第二摘要值计算步骤中利用安全哈希算法对所述交易报文体计算摘要值。

优选地，在所述摘要值比较步骤中，在判断为所述摘要值不一致的情况下丢弃报文。

优选地，所述公钥为具有随时间推移的对应有效期并且强度随时间推移逐渐增强。

优选地，所述公钥为 3 把，分别为 1152 位、1408 位、1984 位。

优选地，所述私钥和所述公钥通过索引号一一对应。

优选地，在所述发送步骤中，还将所述索引号与所述交易报文体一起发送给所述 TVP 加密装置。

优选地，在所述解密步骤中，利用对称密钥对解密后的 PINBLOCK（密码格式）进行对称密钥加密的转加密步骤。

5 优选地，本发明的基于智能电视的支付方法还具备：根据来自所述支付客户端装置的请求生成动态码并且将该动态码存储在所述 TVP 加密装置，同时将该动态码发送给用户的动态码生成步骤；比较存储在所述 TVP 加密装置中的动态码和用户作为敏感数据输入到所述支付客户端并作为交易报文体发送到所述 TVP 加密装置中的动态码的动态码比较步骤。

10 优选地，在所述动态码比较步骤中，动态码不一致的情况下丢弃报文。

15 本发明的智能电视支付密钥系统的支付客户端装置，其特征在于，公钥存储模块，用于预先储存公钥文件；用户界面模块，用于获得交易信息和敏感数据，将获得的交易信息生成报文体，并且用于从所述公钥存储模块调用公钥；加密模块，利用通过所述用户界面模块调用的公钥对所述敏感信息进行加密得到客户端加密数据；发送模块，发送所述客户端加密数据和所述报文体组成的交易报文。

优选地，该支付客户端装置还具备用于对所述交易报文体计算摘要值的摘要值计算模块。

20 优选地，所述摘要值计算模块利用安全哈希算法对所述交易报文体计算摘要值。

优选地，所述公钥为具有随时间推移的对应有效期并且强度随时间推移逐渐增强。

优选地，所述公钥为 3 把，分别为 1152 位、1408 位、1984 位。

25 优选地，所述加密模块采用所述公钥进行 RSA 非对称加密算法对所述敏感信息进行加密得到客户端加密数据。

优选地，所述加密模块对所述交易报文进行压缩和编码后再进行发送。

30 本发明的智能电视支付密钥系统中的 TVP 加密装置，其特征在于，密钥生成模块，用于生成私钥；私钥存储模块，用于存储所述

私钥；接收模块，用于接收包含客户端加密数据的交易报文体；解密模块，调用存储在所述私钥存储模块中的私钥对所述交易报文体中的客户端加密数据进行解密。

优选地，所述解密模块还用于利用对称密钥对解密后的 PIN BLOCK（密码格式）进行转加密。利用上述本发明的智能电视支付密钥系统、基于智能电视的支付方法，由于利用了公钥，因此即使交易报文在传输过程中被攻击者篡改，由于没有利用私钥，加密后的安全信息也无法被解密获取，提高了系统的安全性。而且，通过对报文计算摘要值，并进行比较，因此，即使交易报文在传输过程中被攻击者篡改，通过验证摘要值，就能够准确判断出交易报文是否被篡改。进一步，在验证摘要值的基础上，通过验证动态码，能够进一步保证持卡人身份的准确性。而且，在整个交易的各个环节中，交易密码都是密文状态，因此，确保了交易性息的安全性。另外，在本发明中采用了预置公钥的方式，公钥使用期长，加密密度强，能够兼顾安全性能和节省成本两方面。

附图说明

图 1 是表示本发明的智能电视支付密钥系统的示意构造图。

图 2 是表示本发明的智能电视支付密钥系统的进一步的示意构造图。

图 3 是表示本发明的基于智能电视的支付方法的流程图。

具体实施方式

下面介绍的是本发明的多个可能实施例中的一些，旨在提供对本发明的基本了解。并不旨在确认本发明的关键或决定性的要素或限定所要保护的范围。

为使本发明的目的、技术方案和优点更加清楚，下面结合附图对本发明作进一步的详细描述。

图 1 是表示本发明的智能电视支付密钥系统的示意构造图。

如图 1 所示，本发明的智能电视支付密钥系统由支付客户端装

置 100 (即电视终端) 和 TVP 加密装置 200 构成。支付客户端装置 100 主要包括公钥存储模块 101、用户界面模块 102 (图中简称为 UI 模块)、加密模块 103、发送模块 104, TVP 加密装置 200 主要包括密钥生成模块 201、私钥存储模块 202、接收模块 203、解密模块 204。

在支付客户端装置 100 中, 公钥存储模块 101 中预先被置入将在后面描述的公钥。用户界面模块 102 获得交易信息和敏感数据, 将获得的交易信息生成报文体, 并且从公钥存储模块调用公钥。

交易信息主要是指交易金额、交易内容、交易时间等与交易有关的信息。敏感数据包含银行卡帐号、交易密码、摘要值 (即 HASH 值, 将在后文进行描述)、银行卡校验位 (即 CVN2)、卡有效期、动态码 (将在后文进行描述) 等信息。

加密模块 103 利用通过用户界面模块 102 调用的公钥对敏感信息进行加密, 由此得到客户端加密数据。发送模块 104 将该客户端加密数据和所述报文体作为交易报文体到 TVP 加密装置 200。

这里, 加密模块 103 在对敏感信息进行加密时采用 RSA 非对称加密算法进行加密。RSA 非对称加密算法是最常用的非对称加密算法之一。

下面简单说明一下 RSA 非对称加密、解密的过程。

首先, RSA 密钥生成步骤包含以下三个步骤:

(1) 独立地选取两大素数 p 和 q , 计算 $n = p \times q$, 并且计算 $\varphi(n) = (p-1)(q-1)$;

(2) 选一整数 e , ($1 \leq e < \varphi(n)$, $\varphi(n)$ 与 e 互素)。在模 $\varphi(n)$ 下, e 有唯一逆元, 计算 $d = e^{-1} \bmod(\varphi(n))$;

(3) 取公钥为 (n, e) , 私钥为 (n, d) 并销毁 p, q 。

接着, RSA 加密和解密步骤如下:

加密消息前, 先将它分成比 n 小的数据分组, 再对每个分组加密。

加密: $C = M^e \pmod{n}$

解密: $M = C^d \pmod{n}$

又，在 TVP 加密装置 200 中，密钥生成模块 201 用于生成私钥和公钥。私钥存储模块 202 用于存储密钥生成模块 201 生成的私钥。接收模块 203 接收从支付客户端装置 100 发送来的交易报文体。解密模块 204 调用存储在私钥存储模块 202 中的私钥对交易报文体中的客户端加密数据进行非对称私钥解密。

在本发明中，密钥生成模块 201 生成的公钥和私钥是一一对应，它们可以通过一个索引号建立对应关系。私钥从外部不能够获得，公钥可以通过接口调用的方式由外部获得。在本发明中，通过将 TVP 加密装置 200 中生成的公钥转换成一个公钥文件预先置入到上述的支付客户端装置 100。这样，在支付客户端装置 100 对数据进行加密时，就由用户界面模块 102 调用出该公钥对数据进行加密。在此同时付客户端装置 100 的发送模块 104 也会将与公钥对应的索引号一起发送到 TVP 加密装置 200。这样，在 TVP 加密装置 200 中，根据该索引号就能够找到与该公钥一一对应的私钥。

为了避免公钥频繁升级，本发明的发明人提出一种在二进制格式的公钥文件中预设 3 把密钥的方式。在该方式中，每把公钥设置对应的有效期并且强度随时间推移逐渐增加。作为一个示例，可以设置分别为 1152 位、1408 位、1984 位的 3 把密钥。支付客户端装置 100 通过用户界面模块 102 提示用户输入银行卡敏感信息和验证要素，收集后根据当前日期所处哪个时间段从公钥文件中取出对应的公钥并由加密模块 103 进行加密处理。这样，不仅能够解决现有加密技术中需要频繁更新密钥的问题，还能够提供随时间推移保密性更高的密钥。

在支付客户端装置 100 中，发送模块 104 具体地包括：对所述交易报文进行压缩和 BASE64 编码的压缩编码单元和发送经压缩和编码的所述交易报文的发送单元（未图示）。

相应地，在 TVP 加密装置 200 中，接收模块 203 具体地包括：接收所述交易报文的接收单元和对接所述交易报文进行 BASE64 解码和解压缩的解码解压缩单元。

这里，TVP 加密装置 200 中的解密模块 204 还进一步利用对称

密钥和解密后的 PIN BLOCK (密码格式) 进行转加密。在本发明中, 需要进行转加密的原因是, 在金融系统中银行卡密码等敏感信息不允许在应用系统, 包括数据库、内存中驻留, 因此, 必须在 TVP 加密装置 200 中进行执行这一转加密过程。

5 图 2 是表示本发明的智能电视支付密钥系统的进一步的示意构造图。

为了保证信息传输的安全性, 在图 1 所示的结构基础上, 如图 2 所示, 在支付客户端装置 100 还具备: 用于对所述交易报文体计算摘要值 (即 HASH 值) 并且将计算出的摘要值作为所述敏感数据的第一摘要值计算模块 105。相应地。在 TVP 加密装置 200 还具备: 10 用于对接收到的交易报文体计算摘要值的第二摘要值计算模块 205; 摘要值比较模块 206, 比较第二摘要值计算模块中计算得到的摘要值和由解码解压缩单元解码解压后得到的敏感数据中含有的摘要值是否一致。这里, 作为计算摘要值的方法, 采用安全哈希算法。 15

这样, 在支付客户端装置 100, 由第一摘要值计算模块 105 对交易报文体计算摘要值, 并将该摘要值作为敏感信息进行上述加密。在 TVP 加密装置 200 利用第二摘要值计算模块 205 对接收到的报文体也计算摘要值, 同时由摘要值比较模块 206 对该计算出的摘要值与解密后的敏感信息中含有的摘要值进行比较, 如果两者不相 20 等, 则表明交易报文在传输过程中可能被篡改了, 则丢弃报文。

在此基础上, 为了再进一步保证信息传输的安全性, 除了利用摘要值进行比对之外, 还可以利用动态码的比对来进一步保证安全性。如图 2 所示, 具体地, TVP 加密装置 200 还可以进一步具备: 25 动态码生成模块 208 和动态码比较模块 209。动态码生成模块 208 根据来自支付客户端装置 100 的请求生成动态码并且存储该动态码, 同时将该动态码通过短信或者其他等的方式发送给用户。用户在支付时, 根据用户接口模块 102 的提示输入该动态码, 并将该动态码作为敏感信息, 通过加密模块 103 进行加密后由发送模块 104 30 发送到 TVP 加密装置 200。经 TVP 加密装置 200 中的接收模块 203

接收并由解密模块 204 解密后的动态码被输入到动态码比较模块 209，同时，动态码生成模块 208 中已存储的动态码（即最早由动态码生成模块 208 生成的动态码）也被输入动态码比较模块 209，由动态码比较模块 209 对两者进行，如果两者不相等，则表明交易
5 报文在传输过程中可能被篡改了，则丢弃报文。

在本发明的智能电视支付密钥系统中，利用了公钥而没有利用私钥，因此即使交易报文在传输过程中被攻击者篡改，加密后的安全信息也无法被解密获取，提高了系统的安全性。

而且，在本发明的智能电视支付密钥系统中，通过对报文计算
10 摘要值，并进行比较，因此，即使交易报文在传输过程中被攻击者篡改，通过验证摘要值，能够判断出交易报文是否被篡改，提高了系统的安全性。

而且，在本发明的智能电视支付密钥系统中，通过采用动态码验证机制，能够保证持卡人身份的准确性，提高了系统的安全性。

15 而且，在本发明智能电视支付密钥系统中，在整个交易的各个环节中，交易密码都是密文状态，都是不可见的，交易密码明文也不会记录在任何物理介质中，因此，进一步确保了交易性息的安全性，提高了系统的安全性。

而且，在本发明的智能电视支付密钥系统中，公钥使用期长，
20 加密密度强，能够在保证系统安全的基础上，节省成本。

下面对于本发明的基于智能电视的支付方法进行说明。

图 3 是表示本发明的基于智能电视的支付方法的流程图。

如图 3 所示，在支付客户端装置 100 侧，获取交易信息组成交易报文体，对报文体计算摘要值。其中，交易报文体由交易信息和
25 敏感数据。交易信息主要是指交易金额、交易内容、交易时间等与交易有关的信息。敏感数据包含银行卡帐号、交易密码、摘要值、银行卡校验位（即 CVN2）、卡有效期、动态码等信息。

在支付客户端装置 100 侧从获得银行卡卡号、交易密码等的其他敏感信息，将计算出的摘要值也作为敏感信息一起通过利用公钥
30 文件中存储的公钥进行 RSA 非对称加密，生成加密后的客户端名

感数据。接着，将加密后的客户端敏感数据和报文体作为交易报文一起发送到 TVP 加密装置 200。

在 TVP 加密装置 200 侧，在接收交易报文后，对发送来的加密后客户端敏感数据利用私钥进行非对称私钥解密，通过非对称私钥解密得到上送报文体的摘要值、上送的动态码、解密后敏感信息。

利用解密后的 PIN BLOCK（密码格式）和对称密钥进行对称密钥转加密，生成加密后的 PIN BLOCK（密码格式）。解密后敏感信息和加密后 PIN BLOCK（密码格式）可以被应用于交易处理。

另一方面，在接收交易报文后，对接收到的报文体计算摘要值。比较该计算得到的报文体的摘要值与上述上送报文体的摘要值，验证两者是否一致，在判断两者不一致的情况下，丢弃报文。在判断两者一致的情况下，继续处理。

在验证摘要值的基础上，进一步验证解密后的上送的动态码与 TVP 加密装置 200 已存储的动态码是否一致，在判断两者不一致的情况下，丢弃报文。在判断两者一致的情况下，继续交易处理。

本发明的基于智能电视的支付方法利用支付客户端 100 即电视终端和 TVP 加密装置 200 来实现，利用本发明的基于智能电视的支付方法，采用公钥，因此即使交易报文在传输过程中被攻击者篡改，由于没有采用私钥，加密后的安全信息也无法被解密获取，提高了系统的安全性。

而且，利用本发明的基于智能电视的支付方法，通过对报文计算摘要值，并进行比较，因此，即使交易报文在传输过程中被攻击者篡改，通过验证摘要值，能够判断出交易报文是否被篡改，提高了系统的安全性。

而且，利用本发明的基于智能电视的支付方法，通过采用动态码验证机制，能够保证持卡人身份的准确性，提高了系统的安全性。

而且，利用本发明的基于智能电视的支付方法，在整个交易的各个环节中，交易密码都是密文状态，都是不可见的，交易密码明

文也不会记录在任何物理介质中，因此，进一步确保了交易性息的安全性，提高了系统的安全性。

而且，利用本发明的基于智能电视的支付方法，公钥使用期长，加密密度强，能够在保证系统安全的基础上，节省成本。

- 5 以上例子主要说明了本发明的系统及各种应用方法。尽管只对其中一些本发明的实施方式进行了描述，但是本领域普通技术人员应当了解，本发明可以在不偏离其主旨与范围内以许多其他的形式实施。因此，所展示的例子与实施方式被视为示意性的而非限制性的，在不脱离如所附各权利要求所定义的本发明精神及范围的情况下，
10 下，本发明可能涵盖各种的修改与替换。

在不偏离本发明的精神和范围的情况下还可以构成许多有很大差别的实施例。应当理解，除了如所附的权利要求所限定的，本发明不限于在说明书中所述的具体实施例。

权利要求项

1.一种智能电视支付密钥系统，其特征在于，具备支付客户端装置（100）和 TVP 加密装置（200），

5 所述支付客户端装置（100）具备：

公钥存储模块（101），预置有下述的公钥；

用户界面模块（102），获得交易信息和敏感数据，将获得的交易信息生成报文体，并且从所述公钥存储模块调用所述公钥；

10 加密模块（103），利用通过所述用户界面模块调用的公钥，对所述敏感信息进行加密，得到客户端加密数据；以及

发送模块（104），将所述客户端加密数据和所述报文体作为交易报文体发送到所述 TVP 加密装置，

所述 TVP 加密装置（200）具备：

15 密钥生成模块（201），用于生成私钥和与该私钥一一对应的公钥；

私钥存储模块（202），用于存储所述私钥；

接收模块（203），用于接收从所述支付客户端装置发送来的交易报文体；

20 解密模块（204），调用存储在所述私钥存储模块中的私钥对所述交易报文体中的所述客户端加密数据进行解密。

2. 如权利要求 3 所述的智能电视支付密钥系统，其特征在于，所述发送模块（104）具有对所述交易报文进行压缩和编码的压缩编码单元和发送经压缩和编码的所述交易报文的发送单元，

25 所述接收模块（203）具有接收所述交易报文的接收单元和对所述交易报文进行解码和解压缩的解码解压缩单元。

3. 如权利要求 2 所述的智能电视支付密钥系统，其特征在于，所述加密模块（103）利用所述公钥对所述敏感信息进行 RSA 非对称加密算法进行加密，

30 所述解密模块（204）利用所述私钥所述客户端加密数据进行非对称私钥解密。

4.如权利要求 2 所述的智能电视支付密钥系统，其特征在于，
所述支付客户端装置（100）还具备：用于对所述交易报文体
计算摘要值并且将计算出的摘要值作为所述敏感数据的第一摘要
值计算模块（105），

5 所述 TVP 加密装置（200）还具备：

用于对接收到的所述交易报文体计算摘要值的第二摘要值计
算模块（205）；

摘要值比较模块（206），比较所述第二摘要值计算模块中计
算得到的摘要值和由所述解码解压缩单元解码解压后得到的敏感
10 数据中含有的摘要值是否一致。

5.如权利要求 4 所述的智能电视支付密钥系统，其特征在于，
所述第一摘要值计算模块（105）和第二摘要值计算模块（205）
利用安全哈希算法对所述交易报文体计算摘要值。

6. 如权利要求 5 所述的智能电视支付密钥系统，其特征在于，
15 所述摘要值比较模块（206）在判断为所述摘要值不一致的情
况下丢弃报文。

7 如权利要求 4 所述的智能电视支付密钥系统，其特征在于，
所述公钥为具有随时间推移的对应有效期并且强度随时间推
移逐渐增强。

20 8. 如权利要求 7 所述的智能电视支付密钥系统，其特征在于，
所述公钥为 3 把，分别为 1152 位、1408 位、1984 位。

9.如权利要求 1 所述的智能电视支付密钥系统，其特征在于，
所述私钥和所述公钥通过索引号一一对应。

所述发送模块（104）还将所述索引号与所述交易报文体一起
25 发送到所述 TVP 加密装置。

10.如权利要求 3 所述的智能电视支付密钥系统，其特征在于，
所述解密模块（204）还用于利用对称密钥对解密后的密码格
式进行转加密。

11. 如权利要求 3 所述的智能电视支付密钥系统，其特征在于，
30 所述 TVP 加密装置具备动态码生成模块（208），根据来自所

述支付客户端装置（100）的请求生成动态码并且存储该动态码，
同时也将该动态码发送给用户，

所述用户界面模块（102）作为敏感数据还获得通过用户输入的该动态码，由所述加密模块（103）将该动态码作为所述敏感信息
5 5 进行加密并由所述发送模块（104）将加密后的动态码作为所述客户端加密数据与
所述报文体作为交易报文体一起发送到所述 TVP 加密装置，

所述 TVP 加密装置还具备动态码比较模块（209），比较所述
动态码生成模块（208）中已存储的所述动态码和所述交易报文体
10 10 中包含的动态码。

12. 如权利要求 11 所述的智能电视支付密钥系统，其特征在于，

所述动态码比较模块（209）在判断所述动态码生成模块（208）
中已存储的动态码和所述交易报文体中的动态码不一致的情况下
15 15 丢弃报文。

13. 一种基于智能电视的支付方法，利用支付客户端装置和 TVP
加密装置进行电视支付，其特征在于，包括：

获得交易信息和敏感数据的获取步骤；

利用公钥对所述获取的敏感数据进行加密的加密步骤；

20 20 将加密后的敏感数据和交易信息从所述支付客户终端装置发送到所述 TVP 加密装置的发送步骤；

接收从所述支付客户端装置发送来的敏感数据和交易信息的接收步骤；

用与所述公钥一一对应的私钥对接收到的敏感数据进行解密
25 25 的解密步骤。

14. 如权利要求 13 所述的基于智能电视的支付方法，其特征在于，

在所述加密步骤中，利用公钥对所述敏感信息进行 RSA 非对称加密，

30 30 在所述解密步骤中，利用私钥对所述敏感数据进行非对称解密

钥解密。

15.如权利要求 14 所述的基于智能电视的支付方法，其特征在于，

5 在所述发送步骤中，对所述交易报文进行压缩和编码之后再进
行发送，

在所述接收步骤中，接收所述交易报文之后对接所述交易报
文进行解码和解压缩。

16.如权利要求 15 的基于智能电视的支付方法，其特征在于，
还具备：

10 在所述支付客户端装置对所述交易报文体计算摘要值并且将
计算出的摘要值作为所述敏感数据的第一摘要值计算步骤；

在所述 TVP 加密装置对接收到的所述交易报文体计算摘要值
的第二摘要值计算步骤；

15 比较通过所述第二摘要值计算步骤中计算得到的摘要值和通
过所述解密步骤解密后得到的敏感数据中含有的摘要值是否一
致的摘要值比较步骤。

17.如权利要求 16 所述的基于智能电视的支付方法，其特征在
于，

20 在所述第一摘要值计算步骤和所述第二摘要值计算步骤中利
用安全哈希算法对所述交易报文体计算摘要值。

18.如权利要求 17 所述的基于智能电视的支付方法，其特征在
于，

在所述摘要值比较步骤中，在判断为所述摘要值不一致的情况
下丢弃报文。

25 19.如权利要求 18 所述的基于智能电视的支付方法，其特征在
于，在所述解密步骤中，利用对称密钥对解密后的密码格式进行转
加密。

20.如权利要求 19 所述的基于智能电视的支付方法，其特征在
于，还具备：

30 根据来自所述支付客户端装置的请求生成动态码并且将该动

态码存储在所述 TVP 加密装置,同时将该动态码发送给用户的动态码生成步骤;

比较存储在所述 TVP 加密装置中的动态码和用户作为敏感数据输入到所述支付客户端(100)并作为交易报文体发送到所述 TVP 加密装置(200)中的动态码的动态码比较步骤。

21.如权利要求 20 所述的基于智能电视的支付方法,其特征在于,

在所述动态码比较步骤中,动态码不一致的情况下丢弃报文。

22.如权利要求 13~21 任意一项所述的基于智能电视的支付方法,其特征在于,

所述公钥为具有随时间推移的对应有效期并且强度随时间推移逐渐增强。

23.如权利要求 22 所述的基于智能电视的支付方法,其特征在于,

所述公钥为 3 把,分别为 1152 位、1408 位、1984 位。

24.如权利要求 23 所述的基于智能电视的支付方法,其特征在于,

所述私钥和所述公钥通过索引号一一对应。

在所述发送步骤模块中,还将所述索引号与所述交易报文体一起发送给所述 TVP 加密装置。

25.一种智能电视支付密钥系统的支付客户端装置,其特征在于,公钥存储模块,用于预先储存公钥文件;

用户界面模块,用于获得交易信息和敏感数据,将获得的交易信息生成报文体,并且用于从所述公钥存储模块调用公钥;

25 加密模块,利用通过所述用户界面模块调用的公钥对所述敏感信息进行加密得到客户端加密数据;

发送模块,发送所述客户端加密数据和所述报文体组成的交易报文。

26.如权利要求 25 所述的智能电视支付密钥系统的支付客户端装置,其特征在于,

该支付客户端装置还具备用于对所述交易报文体计算摘要值的摘要值计算模块。

27.如权利要求 4 所述的智能电视支付密钥系统的支付客户端装置，其特征在于，

5 所述摘要值计算模块利用安全哈希算法对所述交易报文体计算摘要值。

28.如权利要求 27 所述的智能电视支付密钥系统的支付客户端装置，其特征在于，

10 所述加密模块采用所述公钥进行 RSA 非对称加密算法对所述敏感信息进行加密得到客户端加密数据。

29. 如权利要求 28 所述的智能电视支付密钥系统的支付客户端装置，其特征在于，

所述加密模块对所述交易报文进行压缩和编码后再进行发送。

15 30.如权利要求 25~29 任意一项所述的智能电视支付密钥系统的支付客户端装置，其特征在于，

所述公钥为具有随时间推移的对应有效期并且强度随时间推移逐渐增强。

31.如权利要求 30 所述的智能电视支付密钥系统的支付客户端装置，其特征在于，

20 所述公钥为 3 把，分别为 1152 位、1408 位、1984 位。

32.一种智能电视支付密钥系统中的 TVP 加密装置，其特征在于，

密钥生成模块（201），用于生成私钥。

私钥存储模块（202），用于存储所述私钥，

25 接收模块（203），用于接收包含客户端加密数据的交易报文体；

解密模块（204），调用存储在所述私钥存储模块中的私钥对所述交易报文体中的客户端加密数据进行解密。

33.如权利要求 32 所述的智能电视支付密钥系统中的 TVP 加密装置，其特征在于，还具备：

30

所述解密模块（204）还用于利用对称密钥对解密后的密码格式进行转加密。

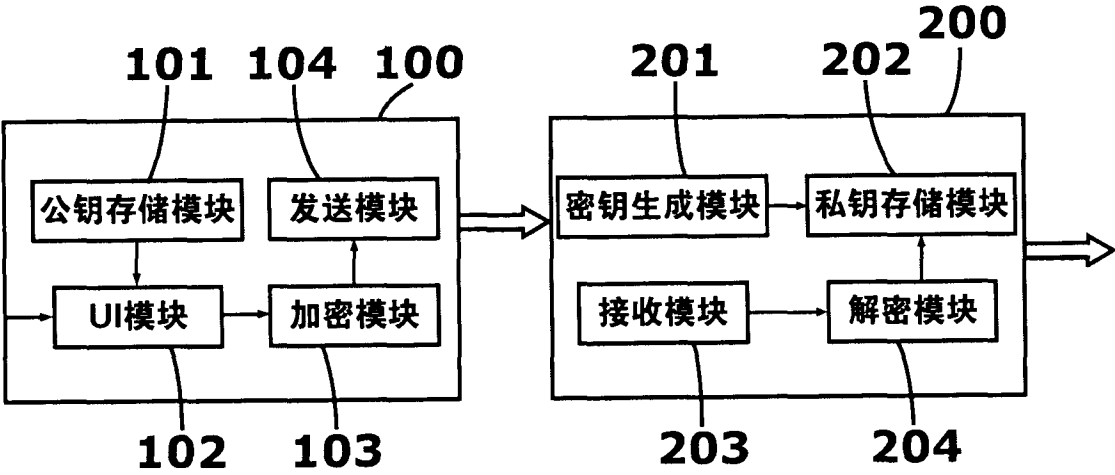


图 1

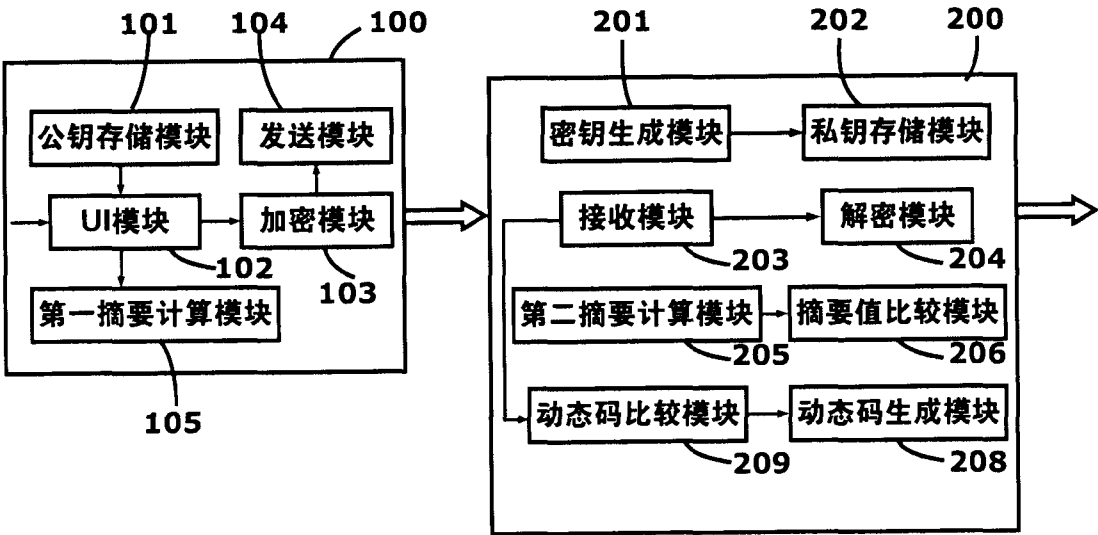


图 2

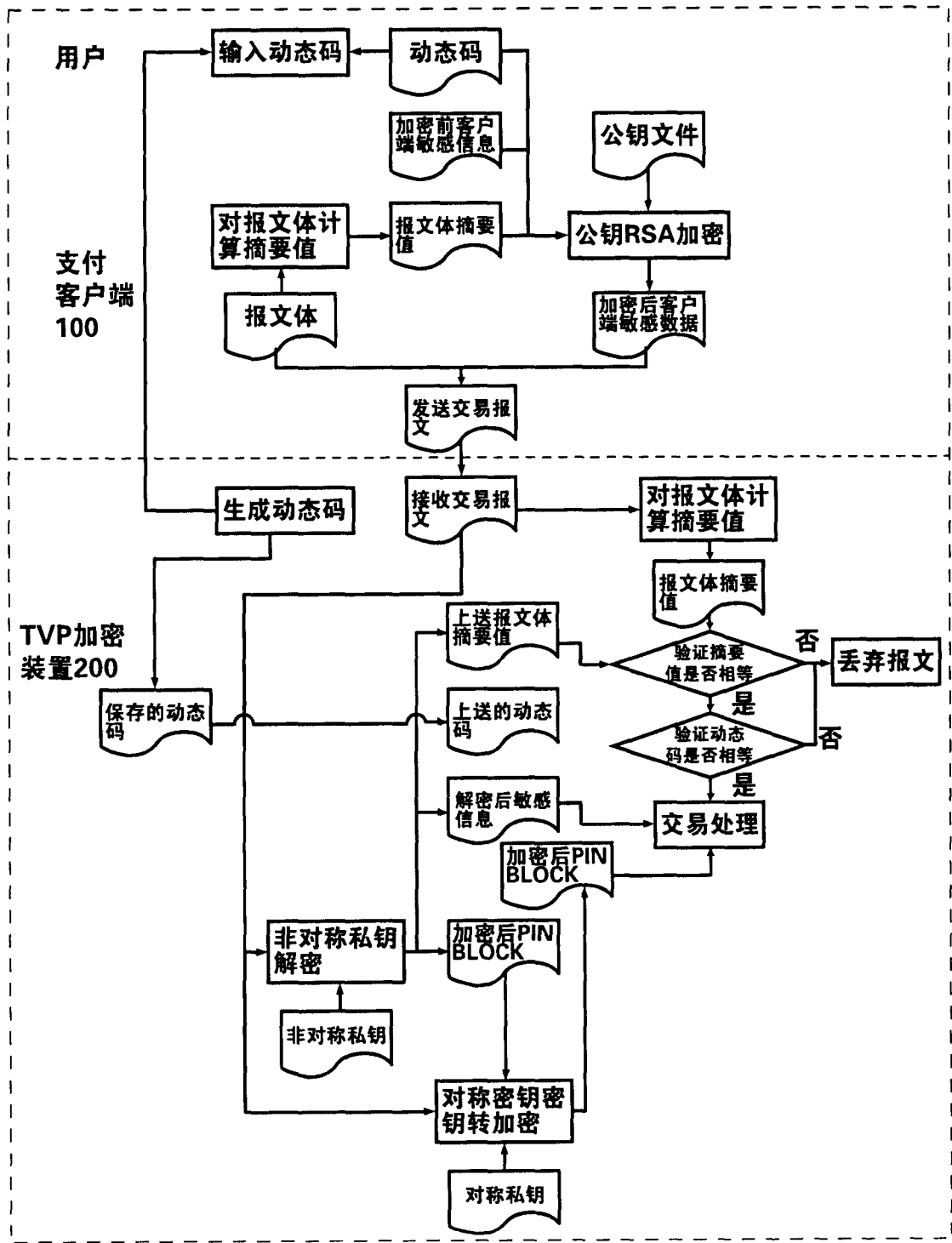


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2012/084565

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06Q20/-; H04L9/-; H04L29/-; H04N21/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
CPRSABS, CNTXT, CNKI, BAIDU: the Chinese words of "payment, purchase, TVP, intelligent TV payment, secret key, encrypt, public secret key"
VEN: pay+, purchas+, key, encrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101087189 A (JAY·C·CHEN)12 December. 2007 (12.12.2007) the description page 1 lines 13-18, page 3 line 24 – page 8 line 3, page 24 line 3 – page 31 line 21, figures 6A-6Q	1-33
A	CN 101098225 A (CHINA UNIONPAY CO., LTD.)02 January. 2008 (02.01.2008) the whole document	1-33
A	CN 1766920 A (GUANGZHOU HAOYILIAN PAYMENT NETWORK CO., LTD.) 03 May 2006 (03.05.2006)the whole document	1-33
A	CN 101853453 A (ZTE CORP.)06 October. 2010 (06.10.2010)the whole document	1-33

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 06 February. 2013 (06.02.2013)	Date of mailing of the international search report 28 February. 2013 (28.02.2013)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. 86-10-62019451	Authorized officer GUO, Xiaoyu Telephone No. (86-10)62411453

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/084565

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101087189 A	12.12.2007	WO 9957835 A1	11.11.1999
		AU 762708 B2	03.07.2003
		GB 2376337 A	11.12.2002
		JP 2005065315 A	10.03.2005
		CN 1307818 C	28.03.2007
		GB 2353623 A	28.02.2001
		JP 2002514839 T	21.05.2002
		GB 2353623 B	08.01.2003
		US 7096494 B1	22.08.2006
		AU 4307599 A	23.11.1999
		CN 1304602 A	18.07.2001
		GB 2376337 B	22.01.2003
		TW 476202 B	11.02.2002
		CA 2329032 C	13.04.2004
CN 101098225 A	02.01.2008	CN 101098225 B	25.07.2012
CN 1766920 A	03.05.2006	None	
CN 101853453 A	06.10.2010	None	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2012/084565

A. CLASSIFICATION OF SUBJECT MATTER

According to International Patent Classification (IPC) or to both national classification and IPC G06Q 20/08(2012.01)i

H04L 29/06 (2006.01) i

H04N 21/4623 (2011.01) i

H04L 9/32 (2006.01) i

H04L 9/30 (2006.01) i

国际检索报告

国际申请号

PCT/CN2012/084565

A. 主题的分类

见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06Q20/-; H04L9/-; H04L29/-; H04N21/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRSABS, CNTXT, CNKI, BAIDU: 支付, 付费, TVP, 智能电视支付, 密钥, 加密, 公钥

VEN: pay+, purchas+, key, encrypt+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN101087189A (杰伊·C·陈) 12.12 月 2007 年 (12.12.2007) 说明书第 1 页第 13-18 行, 第 3 页第 24 行-第 8 页第 3 行, 第 24 页第 3 行-第 31 页第 21 行, 图 6A-6Q	1-33
A	CN101098225A (中国银联股份有限公司) 02.1 月 2008 年 (02.01.2008) 全文	1-33
A	CN1766920A (广州好易联支付网络有限公司) 03.5 月 2006 年 (03.05.2006) 全文	1-33
A	CN101853453A (中兴通讯股份有限公司) 06.10 月 2010 (06.10.2010) 全文	1-33



其余文件在 C 栏的续页中列出。



见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

06.2 月 2013 (06.02.2013)

国际检索报告邮寄日期

28.2 月 2013 (28.02.2013)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

授权官员

郭晓宇

电话号码: (86-10) **62411453**

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2012/084565

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101087189A	12.12.2007	WO9957835A1	11.11.1999
		AU762708B2	03.07.2003
		GB2376337A	11.12.2002
		JP2005065315A	10.03.2005
		CN1307818C	28.03.2007
		GB2353623A	28.02.2001
		JP2002514839T	21.05.2002
		GB2353623B	08.01.2003
		US7096494B1	22.08.2006
		AU4307599A	23.11.1999
		CN1304602A	18.07.2001
		GB2376337B	22.01.2003
		TW476202B	11.02.2002
		CA2329032C	13.04.2004
CN101098225A	02.01.2008	CN101098225B	25.07.2012
CN1766920A	03.05.2006	无	
CN101853453A	06.10.2010	无	

A. 主题的分类

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

G06Q 20/08(2012.01)i

H04L 29/06(2006.01)i

H04N 21/4623(2011.01)i

H04L 9/32(2006.01)i

H04L 9/30(2006.01)i