(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
2014 年 9 月 18 日 (18.09.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/139412 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2014/073225

(22) 国际申请日: 2014 年 3 月 11 日 (11.03.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310084397.2 2013 年 3 月 15 日 (15.03.2013) CN
201310084671.6 2013 年 3 月 15 日 (15.03.2013) CN
201310084673.5 2013 年 3 月 15 日 (15.03.2013) CN
201310084653.8 2013 年 3 月 15 日 (15.03.2013) CN
201310741949.2 2013 年 12 月 27 日 (27.12.2013) CN

(71) 申请人: **福建联迪商用设备有限公司 (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD)** [CN/CN]; 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。

(72) 发明人: **苏文龙 (SU, Wenlong)**; 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。 **孟陆强 (MENG, Luqiang)**; 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。 **陈瑞兵 (CHEN, Ruibing)**; 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。 **姚承勇 (YAO, Chengyong)**; 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。

(74) 代理人: **福州市鼓楼区博深专利代理事务所（普通合伙） (BORSAM INTELLECTUAL PROPERTY(FUZHOU))**; 中国福建省福州市鼓楼区湖滨路 66 号中福西湖花园 3#楼 3A 单元, Fujian 350003 (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, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, SA, SC, SD, SE, SG, SK, SL, SM,

[见续页]

(54) **Title**: METHOD AND SYSTEM FOR SECURED DOWNLOAD OF TERMINAL MASTER KEY (TMK)

(54) **发明名称** : 一种终端主密钥 TMK 安全下载方法系统

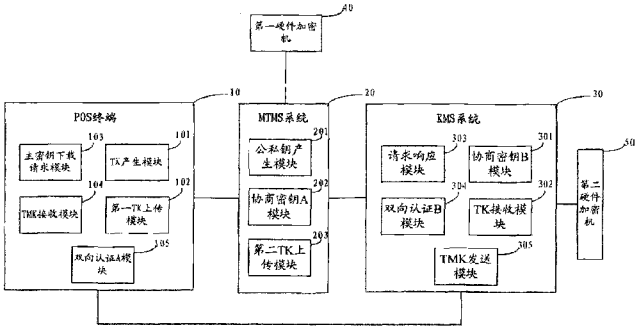

图 1 / FIG.1

10 POS TERMINAL	203 SECOND TK UPLOAD MODULE
101 TK GENERATING MODULE	30 KMS SYSTEM
102 FIRST TK UPLOAD MODULE	301 NEGOTIATION KEY MODULE B
103 MASTER KEY DOWNLOAD REQUESTOR MODULE	302 TK RECEIVER MODULE
104 TMK RECEIVER MODULE	303 REQUEST RESPONDER MODULE
105 TWO-WAY AUTHENTICATION MODULE A	304 TWO-WAY AUTHENTICATION MODULE B
20 MTMS SYSTEM	305 TMK TRANSMITTER MODULE
201 PUBLIC/PRIVATE KEY GENERATING MODULE	40 FIRST HARDWARE SECURITY MODULE
202 NEGOTIATION KEY MODULE A	50 SECOND HARDWARE SECURITY MODULE

(57) **Abstract**: Provided in the present invention is a method for secured download of a terminal master key (TMK), comprising the steps of: a POS terminal generates a transmission key (TK); an operating terminal collects the TK and uploads same to an MTMS system; the MTMS system centralizedly manages the TK and transmits the TK to a corresponding KMS system; the POS terminal activates remote download of the TMK; the POS terminal and the KMS system use AUK for two-way authentication, and upon successful authentication, the KMS system transmits the TMK to the POS terminal. The beneficial effects of the present invention are: remote download of the TMK is implemented by using the POS terminal in uploading the TK, management and uploading of the TK is greatly facilitated by the MTMS system, and transmission of the TK to the corresponding KMS system is ensured; also, the two-way authentication is performed between transmissions of the master key between the POS terminal and the KMS terminal, thus further enhancing download security of the master key.

(57) **摘要**:

[见续页]

WO 2014/139412 A1

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, KM, 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))。

本发明提供一种终端主密钥 TMK 安全下载方法，包括步骤：POS 终端产生传输密钥 TK；操作终端采集 TK 并上传给 MTMS 系统；MTMS 系统统一管理所述 TK 并将 TK 传送给相应的 KMS 系统；POS 终端启动远程下载终端主密钥 TMK；POS 终端与 KMS 系统使用 AUK 进行双向认证，认证通过后 KMS 系统将 TMK 传送给 POS 终端。本发明的有益效果为：通过 POS 终端上传传输密钥 TK 实现远程下载终端主密钥 TMK，通过 MTMS 系统大大方便了传输密钥 TK 的管理和上传，确保了传输密钥 TK 传输给对应的 KMS 系统。并且 POS 终端与 KMS 之间传输主密钥之间还进行了双向认证，进一步提高了主密钥的下载安全。

发明名称: 一种终端主密钥TMK安全下载方法系统

[1] 技术领域

[2] 本发明涉及电子支付领域，尤其涉及一种终端主密钥TMK安全下载方法及系统。

[3] 背景技术

[4] 银行卡（BANK Card）作为支付工具越来越普及，通常的银行卡支付系统包括销售点终端（Point Of Sale，POS）、POS收单系统（POSP）、密码键盘（PIN PAD）和硬件加密机（Hardware and Security Module，HSM）。其中POS终端能够接受银行卡信息，具有通讯功能，并接受柜员的指令完成金融交易信息和有关信息交换的设备；POS收单系统对POS终端进行集中管理，包括参数下载，密钥下载，接受、处理或转发POS终端的交易请求，并向POS终端回送交易结果信息，是集中管理和交易处理的系统；密码键盘（PIN PAD）是对各种金融交易相关的密钥进行安全存储保护，以及对PIN进行加密保护的安全设备；硬件加密机（HSM）是对传输数据进行加密的外围硬件设备，用于PIN的加密和解密、验证报文和文件来源的正确性以及存储密钥。个人标识码（Personal Identification Number，PIN），即个人密码，是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许以明文的方式出现；终端主密钥（Terminal Master Key，TMK），POS终端工作时，对工作密钥进行加密的主密钥，加密保存在系统数据库中；POS终端广泛应用于银行卡支付场合，比如厂商购物、酒店住宿等，是一种不可或缺的现代化支付手段，已经融入人们生活的各种场合。银行卡，特别是借记卡，一般都由持卡人设置了PIN，在进行支付过程中，POS终端除了上送银行卡的磁道信息等资料外，还要持卡人输入PIN供发卡银行验证持卡人的身份合法性，确保银行卡支付安全，保护持卡人的财产安全。为了防止PIN泄露或被破解，要求从终端到发卡银行整个信息交互过程中，全程对PIN进行安全加密保护，不允许在计算机网络系统的任何环节，PIN以明文的方式出现，因此目前接受输入PIN的POS终端都要求配备密钥管理体系。

[5] POS终端的密钥体系分成二级：终端主密钥（TMK）和工作密钥（WK）。其中TMK对WK进行加密保护。每台POS终端拥有唯一的TMK，必须要有安全保护，保证只能写入设备并参与计算，不能读取；TMK是一个很关键的根密钥，如果TMK被截取，工作密钥就比较容易被破解，将严重威胁银行卡支付安全。所以能否安全下载TMK到POS终端，成为整个POS终端安全性的关键。

[6] 为防范密钥泄露风险，终端主密钥的下载必须控制在管理中心的安全机房进行，通过人工集中下载终端主密钥。从而带来维护中心机房工作量大；设备出厂后需要运输到管理中心安全机房下载密钥才能部署到商户，运输成本上升；为了集中下装密钥，需要大量的人手和工作时间，维护成本大、维护周期长等问题。

[7] 发明内容

[8] 为解决上述技术问题，本发明采用的一个技术方案是：

[9] 一种终端主密钥TMK安全下载方法，包括步骤：S1、TK上传流程；S2、TMK下载流程；其中，步骤S1具体包括：S11、MTMS系统调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中；S12、MTMS系统调用第一硬件加密机、KMS 系统调用第二硬件加密机，分别在各自的硬件加密机中将MTMS系统权限分量及KMS 权限分量合成保护密钥PK 和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机和第二硬件加密机中；S13、POS终端调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；S14、POS终端调用密码键盘使用公钥Pu 加密传输密钥TK 生成第一传输密钥密文Ctk_Pu，并将传输第一密钥密文Ctk_Pu 和终端序列号SN发送至MTMS 系统；S15、MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu 关联地存储在MTMS系统数据库中；S16、MTMS系统调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN和第二传输密钥密文Ctk_pk 发送给KMS 系统；S17、KMS系统将MTMS系统发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在KMS 数据库中；步

骤S2具体包括：S21、POS 终端将终端序列号SN 和下载主密钥申请发送至KMS 系统；S22、KMS系统接收到POS 终端发送的终端序列号SN 和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk；S23、KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；S24、KMS 系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK 与POS 终端进行双向认证；S25、如果认证通过，KMS系统调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端；S26、POS终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[10] 本发明采用的另一个技术方案是：

[11] 一种终端主密钥TMK安全下载系统，包括：第一硬件加密机、第二硬件加密机、POS终端、与POS终端通信连接的MTMS系统以及与MTMS系统通信连接的KMS系统；所述POS终端包括TK产生模块、第一TK上传模块、主密钥下载请求模块、双向认证A模块以及TMK接收模块，所述MTMS系统包括公私钥产生模块、协商密钥A模块以及第二TK上传模块，所述KMS系统包括协商密钥B模块、TK接收模块、请求响应模块、双向认证B模块以及TMK发送模块；所述第一硬件加密机用于供MTMS 系统调用，所述第二硬件加密机用于供KMS 系统调用；公私钥产生模块用于调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中；协商密钥A模块和协商密钥B模块用于调用第一硬件加密机和第二硬件加密机，分别在各自的硬件加密机中将MTMS系统权限分量及KMS 权限分量合成保护密钥PK 和MAC 密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机和第二硬件加密机中；TK产生模块用于调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；第一TK上传模块用于调用密码键盘使用公钥Pu 加密传输密钥TK 生成第一传输密钥密文Ctk_Pu，

并将传输第一密钥密文Ctk_Pu 和终端序列号SN发送至MTMS 系统；第二TK上传模块用于将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu
关联地存储在MTMS系统数据库中；第二TK上传模块用于调用第一硬件加密机使用私钥Pr
解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN 和第二传输密钥密文Ctk_pk 发送给KMS 系统；TK接收模块用于将MTMS系统发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在KMS 数据库中；主密钥下载请求模块用于将终端序列号SN 和下载主密钥申请发送至KMS 系统；请求响应模块用于当KMS系统接收到POS 终端发送的终端序列号SN
和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk；请求响应模块用于调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；双向认证A模块和双向认证B模块用于当KMS 系统获得传输密钥TK后，调用第二硬件加密机使用认证密钥AUK 与POS 终端进行双向认证；TMK发送模块用于当认证通过时，调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端；TMK接收模块用于调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[12] 本发明的有益效果为：区别于现有技术的必需集中下载终端主密钥的技术缺陷，本发明通过POS终端上传传输密钥TK，由TK加密终端主密钥TMK后下载到POS终端，实现了远程下载终端主密钥TMK，避免了POS终端通过集中下载主密钥后再布放到商户，减少了物流成本和集中下载维护成本，并且POS终端与KMS之间传输主密钥之前还进行了双向认证，提高了主密钥的下载安全。进一步地，本发明通过 MTMS系统对TK进行统一采集与上传，方便了TK的采集与管理，同时，POS终端与KMS系统之间通过MTMS系统进行TK上传，避免了每台POS

终端与KMS系统直接通信，减轻了KMS系统的工作负担和难度，方便KMS系统识别与其通信连接对象的身份识别，提高了TK的准确传输以及KMS系统的工作效率。

[13] 附图说明

[14] 图1为本发明一实施方式一种终端主密钥TMK安全下载系统的结构框图；

[15] 图2为图1中双向认证A模块的结构框图；

[16] 图3为图1中双向认证B模块的结构框图；

[17] 图4为本发明一实施方式一种终端主密钥TMK安全下载方法的方法总流程图；

[18] 图5为图4中步骤S1的具体步骤流程图；

[19] 图6为图4中步骤S2的具体步骤流程图。

[20] 主要元件符号说明

[21] 10：POS终端； 20：MTMS系统； 30：KMS系统； 40：第一硬件加密机； 50：第二硬件加密机； 101：TK产生模块； 102：第一TK上传模块； 103：主密钥下载请求模块； 104：TMK接收模块； 105：双向认证A模块； 201：公私钥产生模块； 202：协商密钥A模块； 203：第二TK上传模块； 301：协商密钥B模块； 302：TK接收模块； 303：请求响应模块； 304：双向认证B模块；
305：TMK发送模块；1051：第一随机数产生单元； 1052：第一数据收发单元；
1053：第一加解密单元； 1054：第一判断单元； 3041：第二随机数产生单元；
3042：第二数据收发单元； 3043：第二加解密单元； 3044：第二判断单元。

[22] 具体实施方式

[23] 为详细说明本发明的技术内容、构造特征、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[24] 首先，对本发明涉及的缩略语和关键术语进行定义和说明：

[25] AUK：Authentication Key
的简称，即认证密钥，用于PINPAD与密钥管理系统KMS之间的双向认证；

[26] CA中心：所谓CA（Certificate Authority）中心，它是采用PKI（Public Key Infrastructure）公开密钥基础架构技术，专门提供网络身份认证服务，负责签发和管理数字证书，且具有权威性和公正性的第三方信任机构，它的作用就像我

们现实生活中颁发证件的公司，如护照办理机构；

[27] HSM：High Security Machine的简称，高安全设备，在该系统中为硬件加密机；

[28] KMS系统：Key Management System，密钥管理系统，用于管理终端主密钥TMK；

[29] MAK：Mac Key的简称，即MAC计算密钥， 与客户协商确定24字节对称密钥，用于MTMS系统与KMS系统之间TK的MAC值计算；

[30] MTMS：全称Material Tracking Management System，物料追溯管理系统，主要在工厂生产时使用；

[31] PIK：Pin Key的简称，即Pin加密密钥，是工作密钥的一种；

[32] PINPAD：密码键盘；

[33] PK：Protect Key 的简称，即保护密钥，与客户协商确定，24字节对称密钥。用于MTMS/TCS 与KMS之间TK的加密传输；

[34] POS：Point Of Sale 的简称，即销售终端

[35] SNpinpad：密码键盘的序列号，PINPAD是内置时，和POS终端序列号SNpos一致；

[36] SN：支付终端的序列号；

[37] TEK：Transmission Encrypt Key的简称，即传输加密密钥，24字节对称密钥，用于PINPAD与密钥管理系统KMS之间TMK的加密传输；

[38] TK：Transmission Key的简称，即传输密钥。传输密钥是由传输加密密钥TEK和双向认证密钥AUK组成的；

[39] TMS：Terminal Management System 的简称，即终端管理系统，用于完成支付终端信息管理、软件与参数配置、远程下载、终端运行状态信息收集管理、远程诊断等功能；

[40] TMK：Terminal Master Key的简称，即终端主密钥，用于支付终端和支付收单系统之间工作密钥的加密传输；

[41] 安全房：具有较高安全级别，用于存放服务器的房间，该房间需要身份认证后才能进去。

[42] 智能IC卡：为CPU卡，卡内的集成电路包括中央处理器CPU、可编程只读存储器EEPROM、随机存储器RAM和固化在只读存储器ROM中的卡内操作系统COS(Chip Operating System)，卡中数据分为外部读取和内部处理部分。

[43] 对称密钥：发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括：DES、3DES、IDEA、FEAL、BLOWFISH等。

[44] 非对称密钥：非对称加密算法需要两个密钥：公开密钥（私钥Public key）和私有密钥（公钥Private key）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。甲方可以使用乙方的公钥对机密信息进行加密后再发送给乙方；乙方再用自己的私匙对加密后的信息进行解密。主要算法有RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）。

[45] RSA：一种非对称密钥算法。RSA公钥加密算法是1977年由Ron Rivest、Adi Shamirh 和Len Adleman 在（美国麻省理工学院）开发的。RSA 取名来自开发他们三者的名字。RSA 是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被 ISO 推荐为公钥数据加密标准。RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易。RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 是被研究得最广泛的公钥算法，从提出到现在的三十多年里，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

[46] TDES Triple-DES：DES是一种对称加密算法，密钥是8字节。TDES是基于DES的加密算法，其密钥是16 字节或者24 字节。TDES/3DES 是英文TripleDES的缩语（即三重数据加密标准），DES 则是英文Data Encryption Standard（数加密标

准）的缩语。DES 是一种对称密钥加密算法，即数据加密密钥与解密密钥相同的加密算法。DES 由IBM 公司在20 世纪70 年代开发并公开，随后为美国政府采用，并被美国国家标准局和美国国家标准协会 (ANSI)承认。TDES/3DES 是DES 加密算法的一种模式，它使用3条64 位的密钥对数据进行三次加密。是DES 的一个更安全的变形。

[47] 为解决背景技术中存在的技术问题，本发明采用一种新的主密钥下载方案，通过POS终端随机产生TK（Transmission Key，传输密钥），将产生后的TK保存于POS终端的密码键盘中，并将TK通过各种应用场景下所需的传输方式传送至KMS（Key Management System,密钥管理系统，用于管理终端主密钥TMK）中。

[48] 当POS终端申请下载终端主密钥TMK时，KMS系统使用TK加密终端主密钥TMK，并将加密后的终端主密钥密文发送给POS终端，POS终端接收后用TK对主密钥密文进行解密，得到终端主密钥TMK，并将终端主密钥TMK保存在密码键盘里。

[49] 如此，通过TK加密终端主密钥TMK，使TMK能够进行远程传输，方便TMK的安全下载。

[50] 上述通过POS终端采集传输密钥TK后发送至银行端对TMK进行加密，再通过POS终端远程下载经TK加密后的TMK的方法可以保证TMK的传输安全。但是，TK是通过POS终端零散上传的，每台POS终端都必需与KMS系统建立通信连接，因此大大增加了KMS系统的工作负担和难度，同时，也很难对TK上传进行管理和安全管控。

[51] 下面就对本发明克服上述问题的技术方案进行详细说明。

[52] 如图1所示，为本实施方式一种终端主密钥TMK安全下载系统的结构框图，该终端主密钥TMK安全下载系统包括：第一硬件加密机40、第二硬件加密机50、POS终端10、与POS终端10通信连接的MTMS系统20以及与MTMS系统20通信连接的KMS系统30；所述POS终端10包括TK产生模块101、第一TK上传模块102、主密钥下载请求模块103、双向认证A模块105以及TMK接收模块104，

[53] 所述MTMS系统20包括公私钥产生模块201、协商密钥A模块202以及第二TK上

传模块203，

[54] 所述KMS系统30包括协商密钥B模块301、TK接收模块302、请求响应模块303、双向认证B模块304以及TMK发送模块305；

[55] 所述第一硬件加密机40用于供MTMS 系统20调用，所述第二硬件加密机50用于供KMS 系统30调用；

[56] 公私钥产生模块201用于调用第一硬件加密机40产生公钥Pu和私钥Pr，将公钥Pu发送至POS终端10并存储在密码键盘中；

[57] 协商密钥A模块202和协商密钥B模块301用于调用第一硬件加密机40和第二硬件加密机50，分别在各自的硬件加密机中将MTMS系统20权限分量及KMS 权限分量合成保护密钥PK 和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机40和第二硬件加密机50中；

[58] TK产生模块101用于调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；

[59] 第一TK上传模块102用于调用密码键盘使用公钥Pu 加密传输密钥TK 生成第一传输密钥密文Ctk_Pu，并将传输第一密钥密文Ctk_Pu和终端序列号SN发送至MTMS 系统20；

[60] 第二TK上传模块203用于将接收到的终端序列号SN和第一传输密钥密文Ctk_Pu 关联地存储在MTMS系统数据库中；

[61] 第二TK上传模块203用于调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN和第二传输密钥密文Ctk_pk 发送给KMS 系统30；

[62] TK接收模块302用于将MTMS系统20发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在KMS 数据库中；

[63] 主密钥下载请求模块103用于将终端序列号SN 和下载主密钥申请发送至KMS系统30；

[64] 请求响应模块303用于当KMS系统30接收到POS 终端10发送的终端序列号SN

和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk；

[65] 请求响应模块303用于调用第二硬件加密机50使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk

获得传输密钥TK并将其存储在所述第二硬件加密机50中；

[66] 双向认证A模块105和双向认证B模块304用于当KMS 系统30获得传输密钥TK后，调用第二硬件加密机50使用认证密钥AUK 与POS 终端进行双向认证；

[67] TMK发送模块305用于当认证通过时，调用第二硬件加密机50使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端10；

[68] TMK接收模块104用于调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[69] 其中，所述MTMS系统20还包括数字摘要模块。

[70] 所述数字摘要模块用于将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu进行打包并生成第一数字摘要，将所述终端序列号SN

和第一传输密钥密文Ctk_Pu与所述第一数字摘要分开存储于MTMS系统数据库中；

[71] 以及用于提取所述打包的终端序列号SN 和第一传输密钥密文Ctk_Pu生成第二数字摘要，判断所述第二数字摘要与第一数字摘要是否相等，所述数字摘要模块还用于当第一数字摘要与第二数字摘要相等时，调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK。

[72] 通过所述数字摘要模块可以判断在MTMS系统20中所述TK是否被修改，从而保证从MTMS系统20上传的TK与POS终端10上传的TK一致。

[73] 请参阅图2和图3，图2为所述双向认证A模块的结构框图，图3为所述双向认证B模块的结构框图。其中，所述双向认证A模块105包括第一随机数产生单元1051、第一数据收发单元1052、第一加解密单元1053以及第一判断单元1054，所述双向认证B模块304包括第二随机数产生单元3041、第二数据收发单元3042、第二加解密单元3043以及第二判断单元3044。

[74] 第一随机数产生单元1051用于产生第一随机数Rnd1；第一数据收发单元用于将产生的第一随机数Rnd1发送至KMS系统；第二数据收发单元3042用于接收第一随机数Rnd1；第二随机数产生单元3041用于在接收到第一随机数Rnd1时，产生随机数第二Rnd2；第二加解密单元3043用于在接收到第一随机数Rnd1时，调用第二硬件加密机50使用传输认证密钥AUK加密第一随机数Rnd1获得第一随机数密文Crnd1；第二数据收发单元用于将第一随机数密文Crnd1和第二随机数Rnd2发送给POS终端；

[75] 第一加解密单元1053用于在接收到第一随机数密文Crnd1和第二随机数Rnd2时，使用传输认证密钥AUK解密接收到的第一随机数密文Crnd1获得第三随机数Rnd1’；第一判断单元1054用于判断第三随机数Rnd1’与第一随机数Rnd1是否一致；

[76] 第一加解密单元1053用于当所述第一判断单元判定第三随机数Rnd1’与第一随机数Rnd1一致时，使用传输认证密钥AUK加密第二随机数Rnd2生成第二随机数密文Crnd2；第一数据收发单元1052用于将第二随机数密文Crnd2发送给KMS系统30；

[77] 第二加解密单元3043用于在接收到第二随机数密文Crnd2时，调用硬件加密机使用传输认证密钥AUK解密接收到的第二随机数密文Crnd2获得第四随机数Rnd2’，第二判断单元3043用于判断第四随机数Rnd2’与第二随机数Rnd2是否一致，并当判定第四随机数Rnd2’与第二随机数Rnd2一致时，确认KMS系统30与POS终端10之间的双向认证通过。

[78] 请参阅图4，为本实施方式一种终端主密钥TMK安全下载方法的总流程图，该终端主密钥TMK安全下载方法包括：

[79] S1、TK上传流程；

[80] S2、TMK下载流程；

[81] 请参阅图5，为步骤S1的具体流程图，该步骤具体包括：

[82] S11、MTMS系统调用第一硬件加密机产生公钥Pu和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中；

[83] S12、MTMS系统调用第一硬件加密机、KMS 系统调用第二硬件加密机，分别

在各自的硬件加密机中将MTMS系统权限分量及KMS 权限分量合成保护密钥PK和MAC 密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机和第二硬件加密机中；

[84] S13、POS终端调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；

[85] S14、POS终端调用密码键盘使用公钥Pu 加密传输密钥TK 生成第一传输密钥密文Ctk_Pu，并将传输第一密钥密文Ctk_Pu 和终端序列号SN发送至MTMS 系统；

[86] S15、MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu 关联地存储在MTMS系统数据库中；

[87] S16、MTMS系统调用第一硬件加密机使用私钥Pr解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN 和第二传输密钥密文Ctk_pk 发送给KMS 系统；

[88] S17、KMS系统将MTMS系统发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在KMS 数据库中；

[89] 请参阅图6，为步骤S2的具体流程图，该步骤具体包括：

[90] S21、POS 终端将终端序列号SN 和下载主密钥申请发送至KMS 系统；

[91] S22、KMS系统接收到POS 终端发送的终端序列号SN 和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk；

[92] S23、KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；

[93] S24、KMS 系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK与POS 终端进行双向认证；

[94] S25、如果认证通过，KMS系统调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端；

[95] S26、POS终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得

终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[96] 其中，所述“MTMS系统调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中”具体包括：

[97] MTMS系统调用第一硬件加密机产生公钥Pu和私钥Pr，将公钥Pu发给CA中心；

[98] MTMS系统从CA中心获得生成的工作证书HsmWCRT并保存在数据库中，并将工作证书HsmWCRT发送至POS终端，工作证书HsmWCRT是使用根证书HsmRCRT对公钥Pu签名生成；

[99] POS终端使用烧片预装的根证书HsmRCRT验证工作证书HsmWCRT的合法性，并当验证通过后POS终端从工作证书HsmWCRT提取公钥Pu并存储在密码键盘中。

[100] 其中，所述“MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu关联地存储在MTMS系统数据库中”具体包括：

[101] MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu进行打包并生成第一数字摘要，将所述终端序列号SN 和第一传输密钥密文Ctk_Pu与所述第一数字摘要分开存储于MTMS系统数据库中；

[102] 所述“MTMS系统调用第一硬件加密机使用私钥Pr
解密第一传输密钥密文Ctk_Pu获得传输密钥TK”具体包括：

[103] MTMS系统提取所述打包的终端序列号SN 和第一传输密钥密文Ctk_Pu生成第二数字摘要；

[104] 判断所述第二数字摘要与第一数字摘要是否相等，如果相等，调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK。

[105] 其中，所述“KMS系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK与POS终端进行双向认证”具体包括：

[106] POS终端产生第一随机数Rnd1并将第一随机数Rnd1发送至KMS系统；

[107] KMS系统接收第一随机数Rnd1后产生随机数第二Rnd2，调用第二硬件加密机使用认证密钥AUK加密第一随机数Rnd1获得第一随机数密文Crnd1，将第一随机数密文Crnd1和第二随机数Rnd2发送给POS终端；

[108] POS终端使用认证密钥AUK解密接收到的第一随机数密文Crnd1获得第三随机数Rnd1’，判断第三随机数Rnd1’与第一随机数Rnd1是否一致：

[109] 如果第三随机数Rnd1’与第一随机数Rnd1一致，POS终端使用认证密钥AUK加密第二随机数Rnd2生成第二随机数密文Crnd2，并将第二随机数密文Crnd2发送给KMS系统；

[110] KMS系统调用第二硬件加密机使用认证密钥AUK解密接收到的第二随机数密文Crnd2获得第四随机数Rnd2’，判断第四随机数Rnd2’与第二随机数Rnd2是否一致；

[111] 如果第四随机数Rnd2’与第二随机数Rnd2一致，KMS系统与POS终端认证通过。

[112] 在本发明中，传输密钥TK产生时计算TK的原始希哈值，当每次存储、传输或使用TK时先校验TK的希哈值，当检验通过后才可以使用TK。通过校验TK的希哈值可以防止存储设备异常导致存储的数据错误，确定密钥是否正确。

[113] 本发明的有益效果为：区别于现有技术的必需集中下载终端主密钥的技术缺陷，本发明通过POS终端上传传输密钥TK，由TK加密终端主密钥TMK后下载到POS终端，实现了POS终端远程下载终端主密钥TMK，避免了POS终端通过集中下载主密钥后再布放到商户，减少了物流成本和集中下载维护成本，并且POS终端与KMS之间传输主密钥之前还进行了双向认证，提高了主密钥的下载安全。进一步地，本发明主密钥TMK是由KMS系统生成的，因此方便KMS系统对主密钥TMK的后续维护和管理。进一步地，本发明通过 MTMS系统对TK进行统一采集与上传，方便了TK的采集与管理，同时，POS终端与KMS系统之间通过MTMS系统进行TK上传，避免了每台POS终端与KMS系统直接通信，减轻了KMS系统的工作负担和难度，同时也方便KMS系统识别与其通信连接对象的身份和上传的TK的真实性，提高了TK的准确传输以及KMS系统的工作效率。

[114] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

[权利要求 1] 1、一种终端主密钥TMK安全下载方法，其特征在于，包括步骤：

S1、TK上传流程；

S2、TMK下载流程；

其中，步骤S1具体包括：

S11、MTMS系统调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中；

S12、MTMS系统调用第一硬件加密机、KMS 系统调用第二硬件加密机，分别在各自的硬件加密机中将MTMS系统权限分量及KMS 权限分量合成保护密钥PK 和MAC 密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机和第二硬件加密机中；

S13、POS终端调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；

S14、POS终端调用密码键盘使用公钥Pu 加密传输密钥TK 生成第一传输密钥密文Ctk_Pu，并将传输第一密钥密文Ctk_Pu 和终端序列号SN发送至MTMS 系统；

S15、MTMS系统将接收到的终端序列号SN

和第一传输密钥密文Ctk_Pu 关联地存储在MTMS系统数据库中；

S16、MTMS系统调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN 和第二传输密钥密文Ctk_pk 发送给KMS 系统；

S17、KMS系统将MTMS系统发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在KMS 数据库中；

步骤S2具体包括：

S21、POS 终端将终端序列号SN 和下载主密钥申请发送至KMS 系

统；

S22、KMS系统接收到POS 终端发送的终端序列号SN 和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk；

S23、KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；

S24、KMS 系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK 与POS 终端进行双向认证；

S25、如果认证通过，KMS系统调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端；

S26、POS终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

2、根据权利要求1所述的一种终端主密钥TMK安全下载方法，其特征在于，所述“MTMS系统调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中”具体包括：

MTMS系统调用第一硬件加密机产生公钥Pu和私钥Pr，将公钥Pu发给CA中心；

MTMS系统从CA中心获得生成的工作证书HsmWCRT并保存在数据库中，并将工作证书HsmWCRT发送至POS终端，工作证书HsmWCRT是使用根证书HsmRCRT对公钥Pu签名生成；

POS终端使用烧片预装的根证书HsmRCRT验证工作证书HsmWCRT的合法性，并当验证通过后POS终端从工作证书HsmWCRT提取公钥Pu并存储在密码键盘中。

3、根据权利要求1所述的一种密钥管理方法，其特征在于，所述“

MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu关联地存储在MTMS系统数据库中”具体包括：

MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu进行打包并生成第一数字摘要，将所述终端序列号SN 和第一传输密钥密文Ctk_Pu与所述第一数字摘要分开存储于MTMS系统数据库中；

所述“MTMS系统调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK”具体包括：

MTMS系统提取所述打包的终端序列号SN

和第一传输密钥密文Ctk_Pu生成第二数字摘要；

判断所述第二数字摘要与第一数字摘要是否相等，如果相等，调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK。

4、根据权利要求1所述的一种密钥管理方法，其特征在于，所述“KMS系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK与POS终端进行双向认证”具体包括：

POS终端产生第一随机数Rnd1并将第一随机数Rnd1发送至KMS系统；

KMS系统接收第一随机数Rnd1后产生随机数第二Rnd2，调用第二硬件加密机使用认证密钥AUK加密第一随机数Rnd1获得第一随机数密文Crnd1，将第一随机数密文Crnd1和第二随机数Rnd2发送给POS终端；

POS终端使用认证密钥AUK解密接收到的第一随机数密文Crnd1获得第三随机数Rnd1’，判断第三随机数Rnd1’与第一随机数Rnd1是否一致：

如果第三随机数Rnd1’与第一随机数Rnd1一致，POS终端使用认证密钥AUK加密第二随机数Rnd2生成第二随机数密文Crnd2，并将第二随机数密文Crnd2发送给KMS系统；

KMS系统调用第二硬件加密机使用认证密钥AUK解密接收到的第二随机数密文Crnd2获得第四随机数Rnd2’，判断第四随机数Rnd2’与第二随机数Rnd2是否一致；

如果第四随机数Rnd2’与第二随机数Rnd2一致，KMS系统与POS终端认证通过。

5、一种终端主密钥TMK安全下载系统，其特征在于，包括：第一硬件加密机、第二硬件加密机、POS终端、与POS终端通信连接的MTMS系统以及与MTMS系统通信连接的KMS系统；所述POS终端包括TK产生模块、第一TK上传模块、主密钥下载请求模块、双向认证A模块以及TMK接收模块，

所述MTMS系统包括公私钥产生模块、协商密钥A模块以及第二TK上传模块，

所述KMS系统包括协商密钥B模块、TK接收模块、请求响应模块、双向认证B模块以及TMK发送模块；

所述第一硬件加密机用于供MTMS系统调用，所述第二硬件加密机用于供KMS 系统调用；

公私钥产生模块用于调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中；

协商密钥A模块和协商密钥B模块用于调用第一硬件加密机和第二硬件加密机，分别在各自的硬件加密机中将MTMS系统权限分量及KMS 权限分量合成保护密钥PK 和MAC 密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机和第二硬件加密机中；

TK产生模块用于调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；

第一TK上传模块用于调用密码键盘使用公钥Pu 加密传输密钥TK生成第一传输密钥密文Ctk_Pu，并将传输第一密钥密文Ctk_Pu 和终端序列号SN发送至MTMS 系统；

第二TK上传模块用于将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu 关联地存储在MTMS系统数据库中；

第二TK上传模块用于调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN

和第二传输密钥密文Ctk_pk 发送给KMS 系统；

TK接收模块用于将MTMS系统发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在KMS 数据库中；

主密钥下载请求模块用于将终端序列号SN 和下载主密钥申请发送至KMS 系统；

请求响应模块用于当KMS系统接收到POS

终端发送的终端序列号SN 和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk；

请求响应模块用于调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK 并将其存储在所述第二硬件加密机中；

双向认证A模块和双向认证B模块用于当KMS

系统获得传输密钥TK后，调用第二硬件加密机使用认证密钥AUK 与POS 终端进行双向认证；

TMK发送模块用于当认证通过时，调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端；

TMK接收模块用于调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

6、根据权利要求5所述的终端主密钥TMK安全下载系统，其特征

在于，所述MTMS系统还包括数字摘要模块；

所述数字摘要模块用于将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu进行打包并生成第一数字摘要，将所述终端序列号SN和第一传输密钥密文Ctk_Pu与所述第一数字摘要分开存储于MTMS系统数据库中；

以及用于提取所述打包的终端序列号SN

和第一传输密钥密文Ctk_Pu生成第二数字摘要，判断所述第二数字摘要与第一数字摘要是否相等，所述数字摘要模块还用于当第一数字摘要与第二数字摘要相等时，调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK。

7、根据权利要求5所述的终端主密钥TMK安全下载系统，其特征在于，所述双向认证A模块包括第一随机数产生单元、第一数据收发单元、第一加解密单元以及第一判断单元，

所述双向认证B模块包括第二随机数产生单元、第二数据收发单元、第二加解密单元以及第二判断单元；

第一随机数产生单元用于产生第一随机数Rnd1；第一数据收发单元用于将产生的第一随机数Rnd1发送至KMS系统；第二数据收发单元用于接收第一随机数Rnd1；第二随机数产生单元用于在接收到第一随机数Rnd1时，产生随机数第二Rnd2；第二加解密单元用于在接收到第一随机数Rnd1时，调用第二硬件加密机使用传输认证密钥AUK加密第一随机数Rnd1获得第一随机数密文Crnd1；第二数据收发单元用于将第一随机数密文Crnd1和第二随机数Rnd2发送给POS终端；

第一加解密单元用于在接收到第一随机数密文Crnd1和第二随机数Rnd2时，使用传输认证密钥AUK解密接收到的第一随机数密文Crnd1获得第三随机数Rnd1’；第一判断单元用于判断第三随机数Rnd1’与第一随机数Rnd1是否一致；

第一加解密单元用于当所述第一判断单元判定第三随机数Rnd1’与

第一随机数Rnd1一致时，使用传输认证密钥AUK加密第二随机数Rnd2生成第二随机数密文Crnd2；第一数据收发单元用于将第二随机数密文Crnd2发送给KMS系统；

第二加解密单元用于在接收到第二随机数密文Crnd2时，调用硬件加密机使用传输认证密钥AUK解密接收到的第二随机数密文Crnd2获得第四随机数Rnd2'，第二判断单元用于判断第四随机数Rnd2'与第二随机数Rnd2是否一致，并当判定第四随机数Rnd2'与第二随机数Rnd2一致时，确认KMS系统与POS终端之间的双向认证通过。

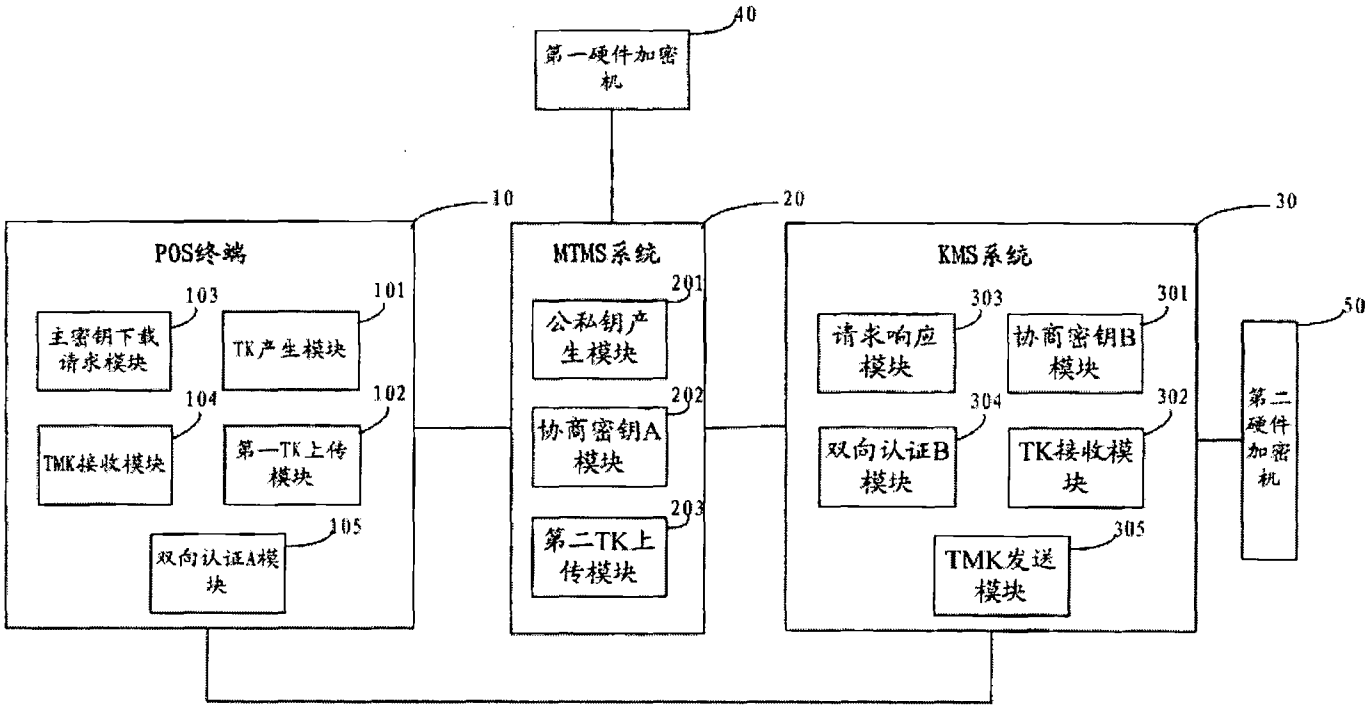
40
第一硬件加密机
10
POS终端
103
主密钥下载请求模块
101
TK产生模块
104
TMK接收模块
102
第一TK上传模块
105
双向认证A模块
20
MTMS系统
201
公私钥产生模块
202
协商密钥A模块
203
第二TK上传模块
30
KMS系统
303
请求响应模块
301
协商密钥B模块
304
双向认证B模块
302
TK接收模块
305
TMK发送模块
50
第二硬件加密机

图 1

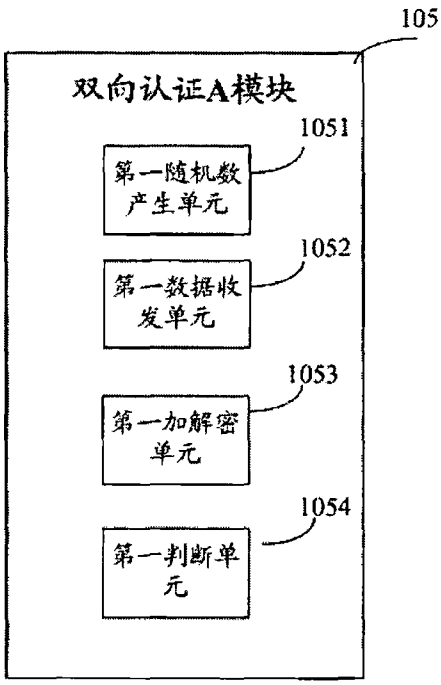
105
双向认证A模块
1051
第一随机数产生单元
1052
第一数据收发单元
1053
第一加解密单元
1054
第一判断单元

图 2

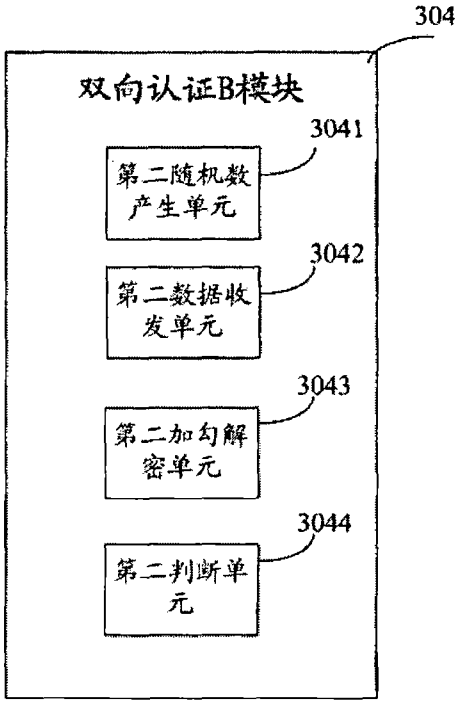
304
双向认证B模块
3041
第二随机数产生单元
3042
第二数据收发单元
3043
第二加勾解密单元
3044
第二判断单元

图 3

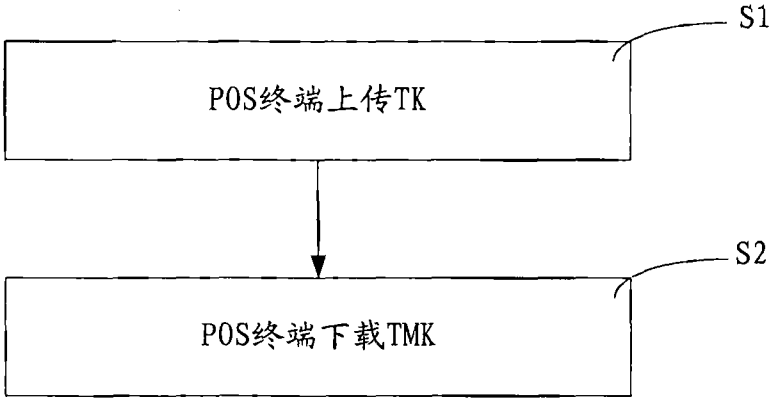
S1
POS终端上传TK
S2
POS终端下载TMK

图 4

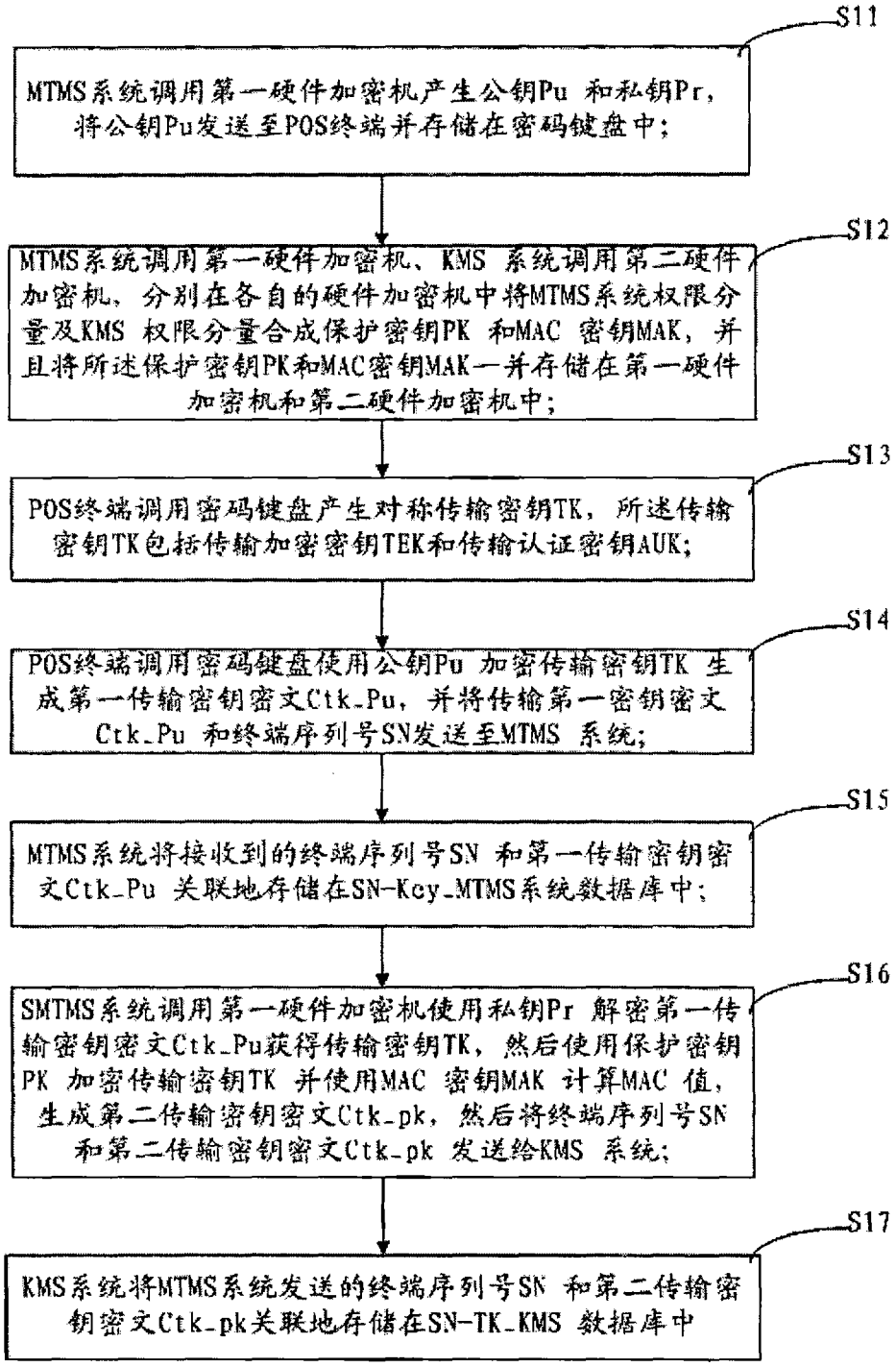
S11
MTMS系统调用第一硬件加密机产生公钥Pu 和私钥Pr，将公钥Pu发送至POS终端并存储在密码键盘中；
S12
MTMS系统调用第一硬件加密机、KMS 系统调用第二硬件加密机，分别在各自的硬件加密机中将MTMS系统权限分量及KMS 权限分量合成保护密钥PK 和MAC 密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并存储在第一硬件加密机和第二硬件加密机中；
S13
POS终端调用密码键盘产生对称传输密钥TK，所述传输密钥TK包括传输加密密钥TEK和传输认证密钥AUK；
S14
POS终端调用密码键盘使用公钥Pu 加密传输密钥TK 生成第一传输密钥密文Ctk_Pu，并将传输第一密钥密文Ctk_Pu 和终端序列号SN发送至MTMS 系统；
S15
MTMS系统将接收到的终端序列号SN 和第一传输密钥密文Ctk_Pu 关联地存储在SN-Key_MTMS系统数据库中；
S16
SMTMS系统调用第一硬件加密机使用私钥Pr 解密第一传输密钥密文Ctk_Pu获得传输密钥TK，然后使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，然后将终端序列号SN 和第二传输密钥密文Ctk_pk 发送给KMS 系统；
S17
KMS系统将MTMS系统发送的终端序列号SN 和第二传输密钥密文Ctk_pk关联地存储在SN-TK_KMS 数据库中

图 5

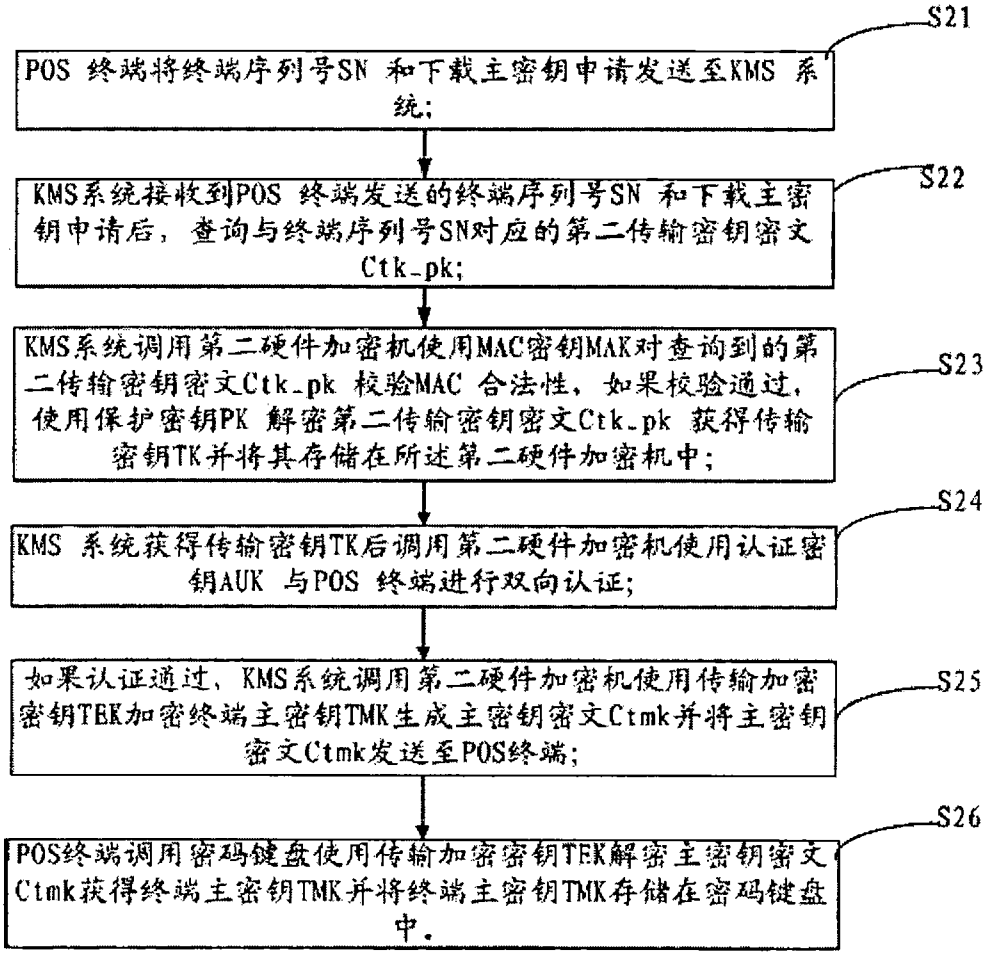
S21
POS 终端将终端序列号SN 和下载主密钥申请发送至KMS 系统;
S22
KMS系统接收到POS 终端发送的终端序列号SN 和下载主密钥申请后，查询与终端序列号SN对应的第二传输密钥密文Ctk_pk;
S23
KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中;
S24
KMS 系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK 与POS 终端进行双向认证;
S25
如果认证通过，KMS系统调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至POS终端;
S26
POS终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中.

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/073225

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i

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)

H04L, G06F

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)

CNABS; DWPI; CNKI; GOOGLE; WANFANG; IEEE: master key, terminal master key, bidirectional, authentication, pos machine, KMS management, private key, public key, remote, transmission key, two, TMK, key?, private, sale, MTMS, MAC, KMS, TMK, TK, POS, TEK, PK, manag+, master, download+, material, public, second, upload+, stor+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103237005 A (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD.), 07 August 2013 (07.08.2013), claims 1-10, description, paragraphs [0009]-[0071], and figures 1-2	1, 2, 4, 5, 7
A	CN 101930644 A (CHINA UNIONPAY CO., LTD.), 29 December 2010 (29.12.2010), claims 1-13, description, paragraphs [0032]-[0050], and figures 1-3	1-7
A	CN 102064939 A (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD.), 18 May 2011 (18.05.2011), the whole document	1-7

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 May 2014 (29.05.2014)	**23 June 2014 (23.06.2014)**
Name and mailing address of the ISA/CN: 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 **LI, Min** Telephone No.: (86-10) **62413700**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/073225

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103237005 A	07.08.2013	CN 103716168 A	09.04.2014
		CN 103701610 A	02.04.2014
		CN 103701812 A	02.04.2014
		CN 103701609 A	02.04.2014
		CN 103714641 A	09.04.2014
		CN 103716321 A	09.04.2014
		CN 103714640 A	09.04.2014
		CN 103716167 A	09.04.2014
		CN 103716155 A	09.04.2014
		CN 103714639 A	09.04.2014
		CN 103714638 A	09.04.2014
		CN 103716154 A	09.04.2014
		CN 103714637 A	09.04.2014
		CN 103714636 A	09.04.2014
		CN 103714635 A	09.04.2014
		CN 103714634 A	09.04.2014
		CN 103716153 A	09.04.2014
		CN 103716320 A	09.04.2014
		CN 103714633 A	09.04.2014
		CN 103731260 A	16.04.2014
		CN 103731259 A	16.04.2014
		CN 103729945 A	16.04.2014
		CN 103729944 A	16.04.2014
		CN 103729943 A	16.04.2014
		CN 103729942 A	16.04.2014
		CN 103729941 A	16.04.2014
		CN 103729940 A	16.04.2014
		CN 103745351 A	23.04.2014
		CN 103746800 A	23.04.2014
CN 101930644 A	29.12.2010	SG 177349 A1	28.02.2012
		WO 2010148646 A1	29.12.2010
		CA 2766491 A1	29.12.2010
CN 102064939 A	18.05.2011	None	

国际检索报告

国际申请号
PCT/CN2014/073225

A. 主题的分类

H04L 9/08 (2006.01) i

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)

H04L, G06F

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））

CNABS;DWPI;CNKI;GOOGLE;万方;IEEE:主密钥，终端主密钥，下载，上传，双向，认证，POS机，KMS管理，私钥，公钥，远程，传输密钥，两个，第二，存储，TMK，key?，private，sale，MTMS，MAC，KMS，TMK，TK，POS，TEK，PK，manag+，master，download+，material，public，second，upload+，stor+

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
PX	CN 103237005A（福建联迪商用设备有限公司）2013年 8月 07日 (2013-08-07) 权利要求1-10，说明书第[0009]-[0071]段，附图1-2	1，2，4，5，7
A	CN 101930644A（中国银联股份有限公司）2010年 12月 29日 (2010-12-29) 权利要求1-13，说明书第[0032]-[0050]段，附图1-3	1-7
A	CN 102064939A（福建联迪商用设备有限公司）2011年 5月 18日 (2011-05-18) 全文	1-7

☐ 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	国际检索报告邮寄日期
2014年 5月 29日	2014年 6月 23日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	李敏
传真号 (86-10)62019451	电话号码 (86-10)62413700

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/073225

检索报告引用的专利文件		公布日 (年/月/日)	同族专利		公布日 (年/月/日)
CN	103237005A	2013年 8月 07日	CN	103716168A	2014年 4月 09日
			CN	103701610A	2014年 4月 02日
			CN	103701812A	2014年 4月 02日
			CN	103701609A	2014年 4月 02日
			CN	103714641A	2014年 4月 09日
			CN	103716321A	2014年 4月 09日
			CN	103714640A	2014年 4月 09日
			CN	103716167A	2014年 4月 09日
			CN	103716155A	2014年 4月 09日
			CN	103714639A	2014年 4月 09日
			CN	103714638A	2014年 4月 09日
			CN	103716154A	2014年 4月 09日
			CN	103714637A	2014年 4月 09日
			CN	103714636A	2014年 4月 09日
			CN	103714635A	2014年 4月 09日
			CN	103714634A	2014年 4月 09日
			CN	103716153A	2014年 4月 09日
			CN	103716320A	2014年 4月 09日
			CN	103714633A	2014年 4月 09日
			CN	103731260A	2014年 4月 16日
			CN	103731259A	2014年 4月 16日
			CN	103729945A	2014年 4月 16日
			CN	103729944A	2014年 4月 16日
			CN	103729943A	2014年 4月 16日
			CN	103729942A	2014年 4月 16日
			CN	103729941A	2014年 4月 16日
			CN	103729940A	2014年 4月 16日
			CN	103745351A	2014年 4月 23日
			CN	103746800A	2014年 4月 23日
CN	101930644A	2010年 12月 29日	SG	177349A1	2012年 2月 28日
			WO	2010148646A1	2010年 12月 29日
			CA	2766491A1	2010年 12月 29日
CN	102064939A	2011年 5月 18日		无	