(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
2017 年 1 月 26 日 (26.01.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/012176 A1

(51) 国际专利分类号:
G06Q 20/00 (2012.01) *H04W 4/14* (2009.01)

(21) 国际申请号: PCT/CN2015/088477

(22) 国际申请日: 2015 年 8 月 30 日 (30.08.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510439444.X 2015 年 7 月 23 日 (23.07.2015) CN

(71) 申请人: **宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.)** [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: **周文容 (ZHOU, Wenrong)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: **北京友联知识产权代理事务所（普通合伙） (YOULINK INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区学清路 8 号科技财富中心 A 座 506 室尚志峰, Beijing 100192 (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, 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, 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, ST, 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))。

(54) **Title**: MOBILE PAYMENT METHOD AND DEVICE BASED ON HCE AND MOBILE TERMINAL

(54) **发明名称** : 基于 HCE 的移动支付方法及装置、移动终端

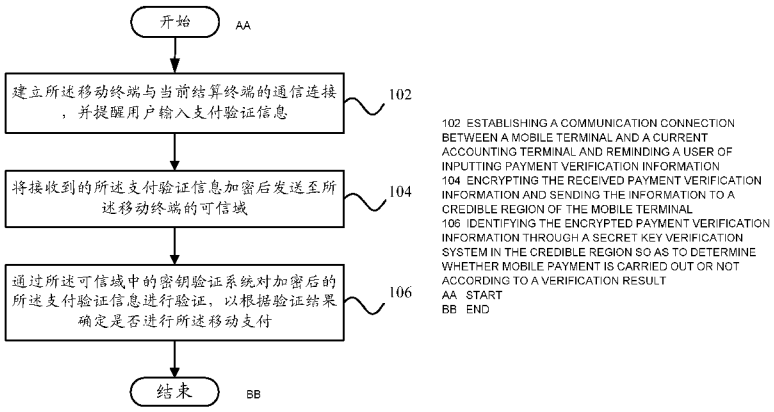

图 1

(57) **Abstract**: Proposed are a mobile payment method based on HCE, a mobile payment device based on HCE and a mobile terminal, wherein the mobile payment method based on HCE comprises: establishing a communication connection between the mobile terminal and a current accounting terminal and reminding a user of inputting payment verification information; encrypting the received payment verification information and sending the information to a credible region of the mobile terminal; and identifying the encrypted payment verification information through a secret key verification system in the credible region so as to determine whether mobile payment is carried out or not according to a verification result. In the solution, a secret key system of a mobile payment solution based on the HCE is stored in the credible region of the mobile terminal and the secret key system of the credible region is called to confirm the payment verification information when the payment proceeds, so that the secret key system can be effectively prevented from tracking and tampering and a safe and reliable payment environment is provided; and meanwhile, the mobile payment based on the HCE can also be normally realized under an off-line condition, thereby improving user experience.

(57) **摘要**:

[见续页]

WO 2017/012176 A1

本发明提出了一种基于 HCE 的移动支付方法、一种基于 HCE 的移动支付装置和一种移动终端，其中，基于 HCE 的移动支付方法包括：建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息；将接收到的所述支付验证信息加密后发送至所述移动终端的可信域；通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。该技术方案，通过将基于 HCE 的移动支付方案的密钥系统存储在移动终端的可信域中，支付时调用可信域的密钥系统对支付验证信息进行确认，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

基于 HCE 的移动支付方法及装置、移动终端

技术领域

本发明涉及通信技术领域，具体而言，涉及一种基于 HCE 的移动支付方法、一种基于 HCE 的移动支付装置和一种移动终端。

背景技术

随着移动支付在生活中越来越普及，基于HCE（Host-based Card Emulation，基于主机的卡模拟）技术的支付方案也在Android 5.0操作系统中被Google设置成了Android平台移动支付的默认支持方式，以及VISA、Bankinter、Privatbank等银行也已经开始支持使用HCE技术进行移动支付，HCE技术的安全性也已经显得越来越重要。

目前，现有的基于HCE的移动支付方案包括：（1）基于HCE的云端支付技术方案，通过云端技术的密钥系统，为基于HCE的移动支付提供安全保证；（2）基于HCE的前端支付技术方案，通过移动终端（比如，手机）的APP提供密钥系统，为基于HCE的移动支付提供安全保证。

但是，上述基于HCE的移动支付方案存在以下缺陷：（1）基于HCE的云端支付技术方案，需要实时联网才可以进行移动支付，在没有网络的情况下，将不能正常进行移动支付；（2）基于HCE的前端支付技术方案，密钥系统保存在移动终端中的APP中，很容易被跟踪和篡改，给移动支付的安全带来很大隐患，不利于用户体验。

因此，如何有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验，成为亟待解决的技术问题。

发明内容

本发明正是基于上述问题，提出了一种新的技术方案，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的

情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

有鉴于此，本发明的第一方面，提出了一种基于 HCE 的移动支付方法，用于移动终端，包括：建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息；将接收到的所述支付验证信息加密后发送至所述移动终端的可信域；通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。

在该技术方案中，首先建立移动终端与当前结算终端（比如 POS 机）的通信连接，并在建立完成后提醒用户输入支付验证信息，以及在接收到用户输入的支付验证信息进行加密处理后再发送至终端的可信域 Trustzone 中，以确保支付验证信息在传输过程的安全性，避免因支付验证信息泄漏而造成不必要的损失，然后，通过可信域 Trustzone 中存储的密钥验证系统对加密后的支付验证信息进行验证，从而确定是否继续完成此次移动支付过程，如此，通过将基于 HCE 的移动支付方案的密钥系统存储在移动终端的可信域中，支付时调用可信域的密钥系统对支付验证信息进行确认，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

在上述技术方案中，优选地，所述通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付，具体包括：通过所述密钥验证系统对加密后的所述支付验证信息进行解密；将所述支付验证信息与所述密钥验证系统中的预设验证信息进行匹配；根据匹配结果确定是否进行所述移动支付。

在该技术方案中，当将经过加密处理的支付验证信息发送至移动终端的可信域 Trustzone 后，首先通过可信域 Trustzone 中存储的密钥验证系统对其进行解密，进而将解密后的支付验证信息与密钥验证系统中的预设验证信息（可以有一个或多个）进行匹配，并进一步根据匹配结果确定是否继续完成此次移动支付过程，其中，Trustzone 是 ARM 针对消费电子设备安全提出的一种架构，提供了一种低成本的方案，在此架构下可以避免资讯从较可信的核心领域泄漏至较不安全的领域，如此，既可以有效地防止密钥系统被跟踪

和篡改，也可以确保产品的生产成本，以进一步提升用户体验。

在上述技术方案中，优选地，所述根据匹配结果确定是否进行所述移动支付，具体包括：当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配成功时，控制进行所述移动支付；当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配失败时，控制终止所述移动支付。

在该技术方案中，当用户输入的支付验证信息与存储在移动终端的可信域 Trustzone 中的密钥验证系统中的预设验证信息匹配成功时，则控制完成此次支付，否则终止交易，在有效提高移动支付安全性和可靠性的同时，也确保了移动支付不受是否联网的影响，可见，解决了现有的基于 HCE 的前端或云端支付技术方案中存在的问题，更利于用户体验。

在上述技术方案中，优选地，所述支付验证信息和所述预设验证信息包括：PIN 码、指纹验证信息和人脸验证信息。

在该技术方案中，用户输入的支付验证信息和可信域中的密钥验证系统中的预设验证信息包括但不限于 PIN 码（Personal Identification Number，个人识别密码，比如数字密码、图形密码等）、指纹验证信息和人脸验证信息，当然也可以包括虹膜验证信息等可以保证本申请的技术方案顺利实施的验证信息。

在上述技术方案中，优选地，在所述建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息之前，还包括：接收来自所述当前结算终端的应用选择 APDU 指令，以根据所述应用选择 APDU 指令和所述移动终端中的 AID 默认路由值建立与所述当前结算终端的通信连接。

在该技术方案中，通过接收来自当前结算终端的用于应用选择的 APDU（Application Protocol Data Unit，应用协议数据单元）指令，并根据该应用选择 APDU 指令在移动终端中的 AID 默认路由值中查找确定与该当前结算终端相匹配的支付路由值（支付路径），以进一步建立与当前结算终端的通信连接，即一个设备匹配识别的过程，为该技术方案的实现提供了必要的前提保障。

根据本发明的第二方面，提出了一种基于 HCE 的移动支付装置，用于移动终端，包括：通信模块，用于建立所述移动终端与当前结算终端的通信

连接，并提醒用户输入支付验证信息；加密模块，用于将接收到的所述支付验证信息加密后发送至所述移动终端的可信域；验证模块，用于通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。

在该技术方案中，首先建立移动终端与当前结算终端（比如，POS机）的通信连接，并在建立完成后提醒用户输入支付验证信息，以及在接收到用户输入的支付验证信息进行加密处理后再发送至终端的可信域Trustzone 中，以确保支付验证信息在传输过程的安全性，避免因支付验证信息泄漏而造成不必要的损失，然后，通过可信域 Trustzone 中存储的密钥验证系统对加密后的支付验证信息进行验证，从而确定是否继续完成此次移动支付过程，如此，通过将基于 HCE 的移动支付方案的密钥系统存储在移动终端的可信域中，支付时调用可信域的密钥系统对支付验证信息进行确认，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

在上述技术方案中，优选地，所述验证模块具体包括：解密模块，用于通过所述密钥验证系统对加密后的所述支付验证信息进行解密；匹配模块，用于将所述支付验证信息与所述密钥验证系统中的预设验证信息进行匹配；控制模块，用于根据匹配结果确定是否进行所述移动支付。

在该技术方案中，当将经过加密处理的支付验证信息发送至移动终端的可信域 Trustzone 后，首先通过可信域 Trustzone 中存储的密钥验证系统对其进行解密，进而将解密后的支付验证信息与密钥验证系统中的预设验证信息（可以有一个或多个）进行匹配，并进一步根据匹配结果确定是否继续完成此次移动支付过程，其中，Trustzone 是 ARM 针对消费电子设备安全提出的一种架构，提供了一种低成本的方案，在此架构下可以避免资讯从较可信的核心领域泄漏至较不安全的领域，如此，既可以有效地防止密钥系统被跟踪和篡改，也可以确保产品的生产成本，以进一步提升用户体验。

在上述技术方案中，优选地，所述控制模块具体用于：当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配成功时，控制进行所

述移动支付；当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配失败时，控制终止所述移动支付。

在该技术方案中，当用户输入的支付验证信息与存储在移动终端的可信域 Trustzone 中的密钥验证系统中的预设验证信息匹配成功时，则控制完成此次支付，否则终止交易，在有效提高移动支付安全性和可靠性的同时，也确保了移动支付不受是否联网的影响，可见，解决了现有的基于 HCE 的前端或云端支付技术方案中存在的问题，更利于用户体验。

在上述技术方案中，优选地，所述支付验证信息和所述预设验证信息包括：PIN 码、指纹验证信息和人脸验证信息。

在该技术方案中，用户输入的支付验证信息和可信域中的密钥验证系统中的预设验证信息包括但不限于 PIN 码（Personal Identification Number，个人识别密码，比如数字密码、图形密码等）、指纹验证信息和人脸验证信息，当然也可以包括虹膜验证信息等可以保证本申请的技术方案顺利实施的验证信息。

在上述技术方案中，优选地，还包括：接收模块，用于在所述建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息之前，接收来自所述当前结算终端的应用选择 APDU 指令，以根据所述应用选择 APDU 指令和所述移动终端中的 AID 默认路由值建立与所述当前结算终端的通信连接。

在该技术方案中，通过接收来自当前结算终端的用于应用选择的 APDU（Application Protocol Data Unit，应用协议数据单元）指令，并根据该应用选择 APDU 指令在移动终端中的 AID 默认路由值中查找确定与该当前结算终端相匹配的支付路由值（支付路径），以进一步建立与当前结算终端的通信连接，即一个设备匹配识别的过程，为该技术方案的实现提供了必要的前提保障。

根据本发明的第三方面，提出了一种移动终端，包括：如上述技术方案中任一项所述的基于 HCE 的移动支付装置，因此，该移动终端具有上述技术方案中任一项所述的基于 HCE 的移动支付装置的所有有益效果，在此不再赘述。

通过本发明的技术方案，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于HCE的移动支付，从而提升用户体验。

附图说明

图 1 示出了根据本发明的一个实施例的基于 HCE 的移动支付方法的流程示意图；

图 2 示出了根据本发明的一个实施例的基于 HCE 的移动支付装置的框图；

图 3 示出了根据本发明的一个实施例的移动终端的框图；

图 4 示出了根据本发明的另一个实施例的基于 HCE 的移动支付方法的流程示意图。

具体实施方式

为了可以更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的基于 HCE 的移动支付方法的流程示意图。

如图 1 所示，根据本发明的一个实施例的基于 HCE 的移动支付方法，用于移动终端，包括：步骤 102，建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息；步骤 104，将接收到的所述支付验证信息加密后发送至所述移动终端的可信域；步骤 106，通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。

在该技术方案中，首先建立移动终端与当前结算终端（比如，POS机）的通信连接，并在建立完成后提醒用户输入支付验证信息，以及在接

收到用户输入的支付验证信息进行加密处理后再发送至终端的可信域 Trustzone 中，以确保支付验证信息在传输过程的安全性，避免因支付验证信息泄漏而造成不必要的损失，然后，通过可信域 Trustzone 中存储的密钥验证系统对加密后的支付验证信息进行验证，从而确定是否继续完成此次移动支付过程，如此，通过将基于 HCE 的移动支付方案的密钥系统存储在移动终端的可信域中，支付时调用可信域的密钥系统对支付验证信息进行确认，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

在上述技术方案中，优选地，所述步骤 106 具体包括：通过所述密钥验证系统对加密后的所述支付验证信息进行解密；将所述支付验证信息与所述密钥验证系统中的预设验证信息进行匹配；根据匹配结果确定是否进行所述移动支付。

在该技术方案中，当将经过加密处理的支付验证信息发送至移动终端的可信域 Trustzone 后，首先通过可信域 Trustzone 中存储的密钥验证系统对其进行解密，进而将解密后的支付验证信息与密钥验证系统中的预设验证信息（可以有一个或多个）进行匹配，并进一步根据匹配结果确定是否继续完成此次移动支付过程，其中，Trustzone 是 ARM 针对消费电子设备安全提出的一种架构，提供了一种低成本的方案，在此架构下可以避免资讯从较可信的核心领域泄漏至较不安全的领域，如此，既可以有效地防止密钥系统被跟踪和篡改，也可以确保产品的生产成本，以进一步提升用户体验。

在上述技术方案中，优选地，所述根据匹配结果确定是否进行所述移动支付，具体包括：当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配成功时，控制进行所述移动支付；当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配失败时，控制终止所述移动支付。

在该技术方案中，当用户输入的支付验证信息与存储在移动终端的可信域 Trustzone 中的密钥验证系统中的预设验证信息匹配成功时，则控制完成此次支付，否则终止交易，在有效提高移动支付安全性和可靠性的同时，也确保了移动支付不受是否联网的影响，可见，解决了现有的基于 HCE 的前端或云端支付技术方案中存在的问题，更利于用户体验。

在上述技术方案中，优选地，所述支付验证信息和所述预设验证信息包括：PIN 码、指纹验证信息和人脸验证信息。

在该技术方案中，用户输入的支付验证信息和可信域中的密钥验证系统中的预设验证信息包括但不限于 PIN 码（Personal Identification Number，个人识别密码，比如数字密码、图形密码等）、指纹验证信息和人脸验证信息，当然也可以包括虹膜验证信息等可以保证本申请的技术方案顺利实施的验证信息。

在上述技术方案中，优选地，在所述步骤 102 之前，还包括：接收来自所述当前结算终端的应用选择 APDU（Application Protocol Data Unit，应用协议数据单元）指令，以根据所述应用选择 APDU 指令和所述移动终端中的 AID 默认路由值建立与所述当前结算终端的通信连接。

在该技术方案中，通过接收来自当前结算终端的用于应用选择的 APDU 指令，并根据该应用选择 APDU 指令在移动终端中的 AID 默认路由值中查找确定与该当前结算终端相匹配的支付路由值（支付路径），以进一步建立与当前结算终端的通信连接，即一个设备匹配识别的过程，为该技术方案的实现提供了必要的前提保障。

图 2 示出了根据本发明的一个实施例的基于 HCE 的移动支付装置的框图。

如图 2 所示，根据本发明的一个实施例的基于 HCE 的移动支付装置 200，用于移动终端，包括：通信模块 202，用于建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息；加密模块 204，用于将接收到的所述支付验证信息加密后发送至所述移动终端的可信域；验证模块 206，用于通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。

在该技术方案中，首先建立移动终端与当前结算终端（比如，POS 机）的通信连接，并在建立完成后提醒用户输入支付验证信息，以及在接收到用户输入的支付验证信息进行加密处理后再发送至终端的可信域 Trustzone 中，以确保支付验证信息在传输过程的安全性，避免因支付验证信息泄漏而造成不必要的损失，然后，通过可信域 Trustzone 中存储的密钥验证系统对加密后的支付验证信息进行验证，从而确定是否继续完成此

次移动支付过程，如此，通过将基于 HCE 的移动支付方案的密钥系统存储在移动终端的可信域中，支付时调用可信域的密钥系统对支付验证信息进行确认，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

在上述技术方案中，优选地，所述验证模块 206 具体包括：解密模块 2062，用于通过所述密钥验证系统对加密后的所述支付验证信息进行解密；匹配模块 2064，用于将所述支付验证信息与所述密钥验证系统中的预设验证信息进行匹配；控制模块 2066，用于根据匹配结果确定是否进行所述移动支付。

在该技术方案中，当将经过加密处理的支付验证信息发送至移动终端的可信域 Trustzone 后，首先通过可信域 Trustzone 中存储的密钥验证系统对其进行解密，进而将解密后的支付验证信息与密钥验证系统中的预设验证信息（可以有一个或多个）进行匹配，并进一步根据匹配结果确定是否继续完成此次移动支付过程，其中，Trustzone 是 ARM 针对消费电子设备安全提出的一种架构，提供了一种低成本的方案，在此架构下可以避免资讯从较可信的核心领域泄漏至较不安全的领域，如此，既可以有效地防止密钥系统被跟踪和篡改，也可以确保产品的生产成本，以进一步提升用户体验。

在上述技术方案中，优选地，所述控制模块 2066 具体用于：当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配成功时，控制进行所述移动支付；当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配失败时，控制终止所述移动支付。

在该技术方案中，当用户输入的支付验证信息与存储在移动终端的可信域 Trustzone 中的密钥验证系统中的预设验证信息匹配成功时，则控制完成此次支付，否则终止交易，在有效提高移动支付安全性和可靠性的同时，也确保了移动支付不受是否联网的影响，可见，解决了现有的基于 HCE 的前端或云端支付技术方案中存在的问题，更利于用户体验。

在上述技术方案中，优选地，所述支付验证信息和所述预设验证信息包括：PIN 码、指纹验证信息和人脸验证信息。

在该技术方案中，用户输入的支付验证信息和可信域中的密钥验证系

统中的预设验证信息包括但不限于 PIN 码（Personal Identification Number，个人识别密码，比如数字密码、图形密码等）、指纹验证信息和人脸验证信息，当然也可以包括虹膜验证信息等可以保证本申请的技术方案顺利实施的验证信息。

在上述技术方案中，优选地，还包括：接收模块 208，用于在所述建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息之前，接收来自所述当前结算终端的应用选择 APDU 指令，以根据所述应用选择 APDU 指令和所述移动终端中的 AID 默认路由值建立与所述当前结算终端的通信连接。

在该技术方案中，通过接收来自当前结算终端的用于应用选择的 APDU（Application Protocol Data Unit，应用协议数据单元）指令，并根据该应用选择 APDU 指令在移动终端中的 AID 默认路由值中查找确定与该当前结算终端相匹配的支付路由值（支付路径），以进一步建立与当前结算终端的通信连接，即一个设备匹配识别的过程，为该技术方案的实现提供了必要的前提保障。

图 3 示出了根据本发明的一个实施例的移动终端的框图。

如图 3 所示，根据本发明的一个实施例的移动终端 300，包括：如上述技术方案中任一项所述的基于 HCE 的移动支付装置 200，因此，该移动终端 300 具有上述技术方案中任一项所述的基于 HCE 的移动支付装置 200 的所有有益效果，在此不再赘述。

图 4 示出了根据本发明的另一个实施例的基于 HCE 的移动支付方法的流程示意图。

如图 4 所示，根据本发明的另一个实施例的基于 HCE 的移动支付方法，通过 NFC（Near Field Communication，近场通信）技术的基于 HCE 的移动支付方案进行移动支付时，使用 Trustzone（可信域）为 APP 提供密钥系统认证，以确保移动支付的安全进行，具体地，当移动终端（比如，Andorid 手机、PC 机）将移动支付方式默认设置成基于 HCE 的支付方式后，用户持移动终端进行 POS 刷卡时，POS 机（结算终端）向移动终端发出应用选择的 APDU 指令，移动终端的 NFCC（NFC Controller，NFC 控制器）在收到 APDU 指令后，从 AID 默认路由值中选择相应的应

用（即建立移动终端与当前结算终端的通信连接），应用被选择后，则要求用户输入相应的 PIN 码（或者是指纹，脸部等认证信息）等认证信息（支付验证信息），然后，移动终端则会调用 Trustzone 中的密钥系统对认证信息进行解密和确认，当认证信息确认正确后则进行交易处理，否则终止交易，其中，可信域 Trustzone 是 ARM 针对消费电子设备安全提出的一种架构，提供了一种低成本的方案，针对系统单芯片内加入专属的安全核心，由硬件建构的存取控制方式支援两颗虚拟的处理器，使得应用程式核心能够在两个状态之间切换，在此架构下可以避免资讯从较可信的核心领域泄漏至较不安全的领域，其主要是能在一个缺乏安全性的环境下完整地执行操作系统，并可在可信的环境下能有更少的安全性的编码。

本技术方案提供了一种将 HCE 移动支付方案的密钥系统保存到移动终端的 Trustzone 中，进而使 Trustzone 中的密钥系统为进行移动支付的 APP 提供密钥认证。

本方案通过 Trustzone 对密钥系统进行保存，实现类似于基于 HCE 的前端支付技术的方案，有效地防止了密钥系统被跟踪和篡改，同时又避免了基于 HCE 的云端支付技术方案在未实时联网的情况下不能使用的技术瓶颈，在给用户进行移动支付的便捷性和安全性之间找到了一个很好的平衡点。

以上结合附图详细说明了本发明的技术方案，通过将基于 HCE 的移动支付方案的密钥系统存储在移动终端的可信域中，支付时调用可信域的密钥系统对支付验证信息进行确认，可以有效地防止密钥系统被跟踪和篡改，以提供安全可靠的支付环境的同时在不联网的情况也可以正常进行基于 HCE 的移动支付，从而提升用户体验。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种基于 HCE 的移动支付方法，用于移动终端，其特征在于，包括:

建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息;

将接收到的所述支付验证信息加密后发送至所述移动终端的可信域;

通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。

2. 根据权利要求 1 所述的基于 HCE 的移动支付方法，其特征在于，所述通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付，具体包括:

通过所述密钥验证系统对加密后的所述支付验证信息进行解密;

将所述支付验证信息与所述密钥验证系统中的预设验证信息进行匹配;

根据匹配结果确定是否进行所述移动支付。

3. 根据权利要求 2 所述的基于 HCE 的移动支付方法，其特征在于，所述根据匹配结果确定是否进行所述移动支付，具体包括:

当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配成功时，控制进行所述移动支付;

当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配失败时，控制终止所述移动支付。

4. 根据权利要求 2 或 3 所述的基于 HCE 的移动支付方法，其特征在于，所述支付验证信息和所述预设验证信息包括:

PIN 码、指纹验证信息和人脸验证信息。

5. 根据权利要求 1 至 3 中任一项所述的基于 HCE 的移动支付方法，其特征在于，在所述建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息之前，还包括:

接收来自所述当前结算终端的应用选择 APDU 指令，以根据所述应用选择 APDU 指令和所述移动终端中的 AID 默认路由值建立与所述当前结算终端

的通信连接。

6. 一种基于 HCE 的移动支付装置，用于移动终端，其特征在于，包括:

通信模块，用于建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息;

加密模块，用于将接收到的所述支付验证信息加密后发送至所述移动终端的可信域;

验证模块，用于通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付。

7. 根据权利要求 6 所述的基于 HCE 的移动支付装置，其特征在于，所述验证模块具体包括:

解密模块，用于通过所述密钥验证系统对加密后的所述支付验证信息进行解密;

匹配模块，用于将所述支付验证信息与所述密钥验证系统中的预设验证信息进行匹配;

控制模块，用于根据匹配结果确定是否进行所述移动支付。

8. 根据权利要求 7 所述的基于 HCE 的移动支付装置，其特征在于，所述控制模块具体用于:

当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配成功时，控制进行所述移动支付;

当所述支付验证信息与所述密钥验证系统中的所述预设验证信息匹配失败时，控制终止所述移动支付。

9. 根据权利要求 7 或 8 所述的基于 HCE 的移动支付装置，其特征在于，所述支付验证信息和所述预设验证信息包括:

PIN 码、指纹验证信息和人脸验证信息。

10. 根据权利要求 6 至 8 中任一项所述的基于 HCE 的移动支付装置，其特征在于，还包括:

接收模块，用于在所述建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息之前，接收来自所述当前结算终端的应用选择

APDU 指令，以根据所述应用选择 APDU 指令和所述移动终端中的 AID 默认路由值建立与所述当前结算终端的通信连接。

11. 一种移动终端，其特征在于，包括：如权利要求 6 至 10 中任一项所述的基于 HCE 的移动支付装置。

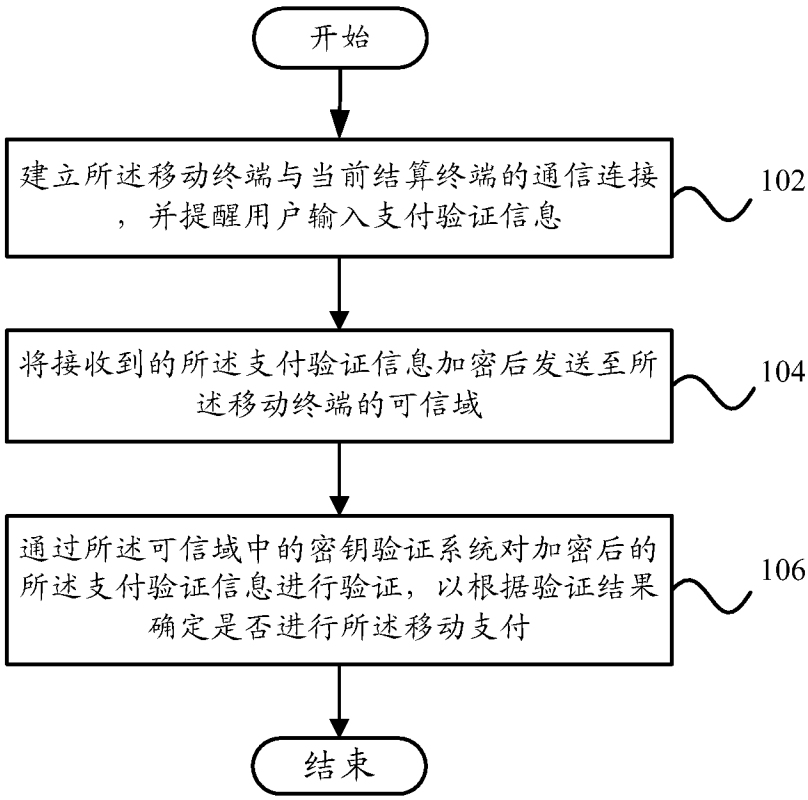
开始
建立所述移动终端与当前结算终端的通信连接，并提醒用户输入支付验证信息
102
将接收到的所述支付验证信息加密后发送至所述移动终端的可信域
104
通过所述可信域中的密钥验证系统对加密后的所述支付验证信息进行验证，以根据验证结果确定是否进行所述移动支付
106
结束

图 1

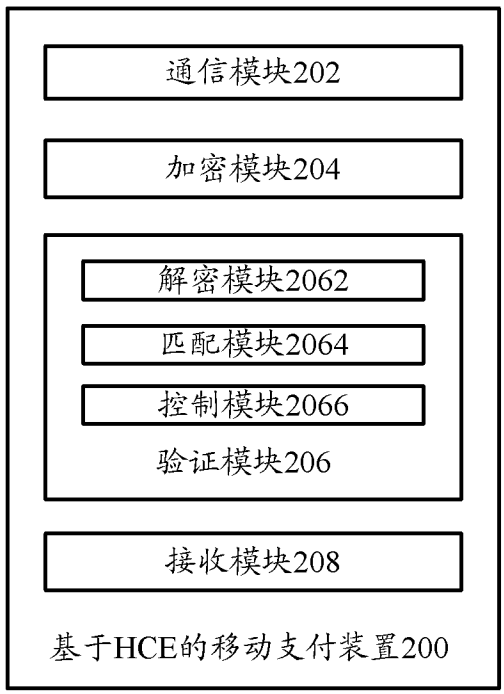
通信模块202
加密模块204
解密模块2062
匹配模块2064
控制模块2066
验证模块206
接收模块208
基于HCE的移动支付装置200

图 2

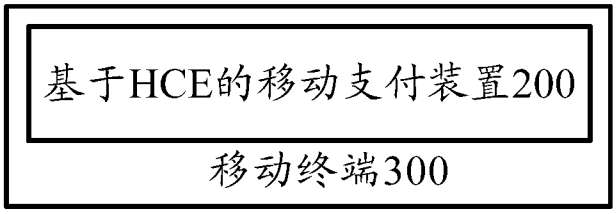
基于HCE的移动支付装置200
移动终端300

图 3

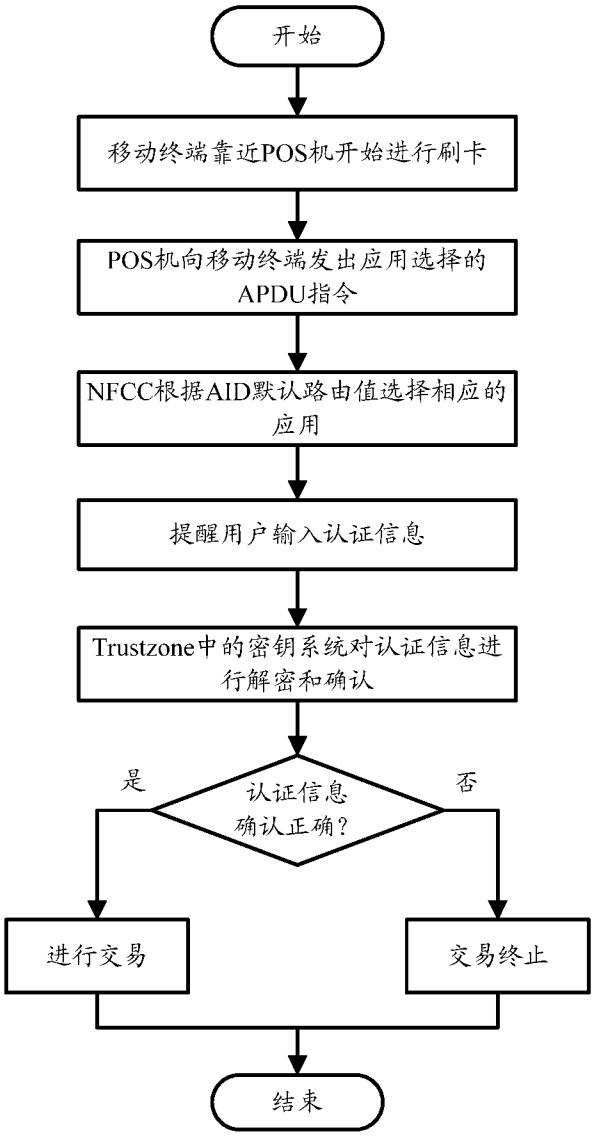
开始
移动终端靠近POS机开始进行刷卡
POS机向移动终端发出应用选择的APDU指令
NFCC根据AID默认路由值选择相应的应用
提醒用户输入认证信息
Trustzone中的密钥系统对认证信息进行解密和确认
认证信息确认正确？
是
否
进行交易
交易终止
结束

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/088477

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/00 (2012.01) i; H04W 4/14 (2009.01) 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)

H04W; G06Q; H04L

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)

VEN, CNABS, CNTXT, CNKI: host-based card, emulation, pay, point of sale; HCE, Host-based Card Emulation, pay, transaction, POS, verification, encrypt, Trustzone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102057386 A (EBAY INC.), 11 May 2011 (11.05.2011), description, paragraphs 0044-0087, and figures 4, 6a and 6c	1-11
A	CN 104166914 A (WUHAN TIANYU INFORMATION INDUSTRY CO., LTD.), 26 November 2014 (26.11.2014), the whole document	1-11
A	CN 103544599 A (MAXIM INTEGRATED PRODUCTS, INC.), 29 January 2014 (29.01.2014), the whole document	1-11
A	KR 20140112785 A (SK PLANET CO., LTD.), 24 September 2014 (24.09.2014), abstract	1-11
A	US 2014025581 A1 (CALMAN, M.A. et al.), 23 January 2014 (23.01.2014), the whole document	1-11

☐ 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
28 March 2016 (28.03.2016)	**19 April 2016 (19.04.2016)**
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 **BIAN, Xiaofei** Telephone No.: (86-10) **62411330**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/088477

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102057386 A	11 May 2011	US 8150772 B2	03 April 2012
		US 2012089520 A1	12 April 2012
		EP 2308014 A4	06 November 2013
		US 8108318 B2	31 January 2012
		US 2013198086 A1	01 August 2013
		US 2015056957 A1	26 February 2015
		US 2009307142 A1	10 December 2009
		US 2009307139 A1	10 December 2009
		US 8417643 B2	09 April 2013
		US 2009307140 A1	10 December 2009
		US 2012173434 A1	05 July 2012
		CN 102057386 B	01 July 2015
		US 2009307778 A1	10 December 2009
		WO 2010002541 A1	07 January 2010
		CN 105046479 A	11 November 2015
		US 8554689 B2	08 October 2013
		EP 2308014 A1	13 April 2011
CN 104166914 A	26 November 2014	None	
CN 103544599 A	29 January 2014	DE 102013106295 A1	09 January 2014
		US 2014013406 A1	09 January 2014
KR 20140112785 A	24 September 2014	None	
US 2014025581 A1	23 January 2014	WO 2014014526 A1	23 January 2014

国际检索报告

国际申请号
PCT/CN2015/088477

A. 主题的分类

G06Q 20/00(2012.01)i; H04W 4/14(2009.01)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)

H04W; G06Q; H04L

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））

VEN,CNABS,CNTXT,CNKI: 主机卡，模拟，支付，交易，销售点，验证，加密，可信域; HCE, Host-based Card Emulation, pay, transaction, POS, verification, encrypt, Trustzone

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	CN 102057386 A (电子湾有限公司) 2011年 5月 11日 (2011-05-11) 说明书第0044-0087段，图4、6a、6c	1-11
A	CN 104166914 A (武汉天喻信息产业股份有限公司) 2014年 11月 26日 (2014-11-26) 全文	1-11
A	CN 103544599 A (马克西姆综合产品公司) 2014年 1月 29日 (2014-01-29) 全文	1-11
A	KR 20140112785 A (SK PLANET CO LTD) 2014年 9月 24日 (2014-09-24) 摘要	1-11
A	US 2014025581 A1 (CALMAN M.A.等) 2014年 1月 23日 (2014-01-23) 全文	1-11

☐ 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
2016年 3月 28日	2016年 4月 19日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 卞晓飞 电话号码 (86-10)62411330

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/CN2015/088477

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	102057386	A	2011年 5月 11日	US	8150772	B2	2012年 4月 3日
				US	2012089520	A1	2012年 4月 12日
				EP	2308014	A4	2013年 11月 6日
				US	8108318	B2	2012年 1月 31日
				US	2013198086	A1	2013年 8月 1日
				US	2015056957	A1	2015年 2月 26日
				US	2009307142	A1	2009年 12月 10日
				US	2009307139	A1	2009年 12月 10日
				US	8417643	B2	2013年 4月 9日
				US	2009307140	A1	2009年 12月 10日
				US	2012173434	A1	2012年 7月 5日
				CN	102057386	B	2015年 7月 1日
				US	2009307778	A1	2009年 12月 10日
				WO	2010002541	A1	2010年 1月 7日
				CN	105046479	A	2015年 11月 11日
				US	8554689	B2	2013年 10月 8日
				EP	2308014	A1	2011年 4月 13日
CN	104166914	A	2014年 11月 26日		无		
CN	103544599	A	2014年 1月 29日	DE	102013106295	A1	2014年 1月 9日
				US	2014013406	A1	2014年 1月 9日
KR	20140112785	A	2014年 9月 24日		无		
US	2014025581	A1	2014年 1月 23日	WO	2014014526	A1	2014年 1月 23日