

(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
2018 年 4 月 5 日 (05.04.2018)



(10) 国际公布号
WO 2018/059262 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2017/102076
- (22) 国际申请日: 2017 年 9 月 18 日 (18.09.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610870709.6 2016年9月30日 (30.09.2016) CN
- (71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY 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: 张栋 (ZHANG, Dong); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135

(CN)。 丁林润 (DING, Linrun); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 李春欢 (LI, Chunhuan); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 陆东东 (LU, Dongdong); 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香港湾仔港湾道 23 号鹰君中心 22 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, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) Title: DATA ENCRYPTION METHOD FOR HCE MODE

(54) 发明名称: 用于 HCE 模式的数据加密方法

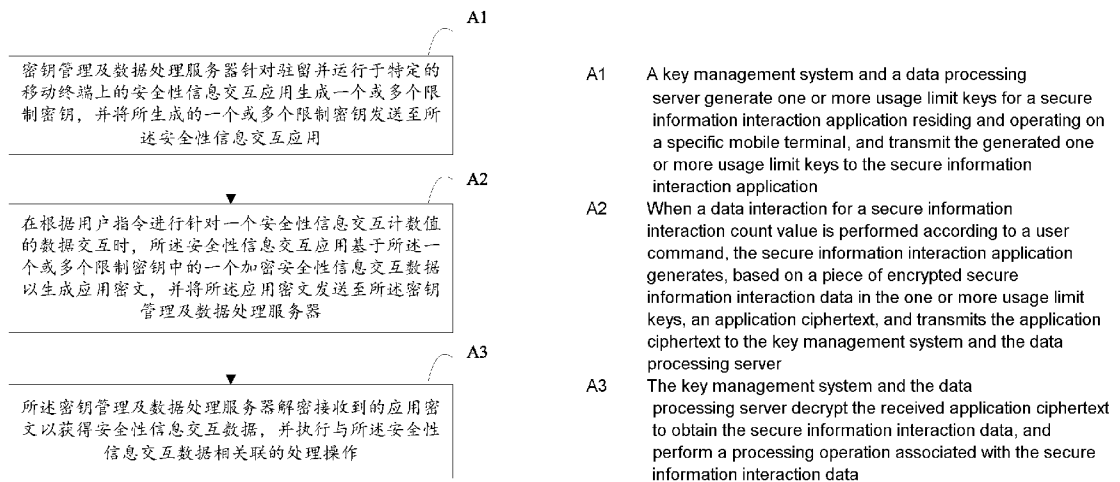


图 1

(57) Abstract: The present invention provides a data encryption method for an HCE mode. The method comprises: a key management system and a data processing server generating one or more usage limit keys for a secure information interaction application residing and operating on a specific mobile terminal, and transmitting the generated one or more usage limit keys to the secure information interaction application; when a data interaction for a secure information interaction count value is performed according to a user command, the secure information interaction application generating, based on a piece of encrypted secure information interaction data in the one or more usage limit keys, an application ciphertext, and transmitting the application ciphertext to the key management system and the data processing server; and, after the application ciphertext is received, the key management system and the data processing server verifying the validity and the legitimacy of the application ciphertext, and performing, after verification is completed, a subsequent



JO, JP, KE, KG, KH, KN, KP, KR, KW, 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))。

processing operation associated with the secure information interaction data. The method disclosed by the present invention achieves a high level of security.

(57) 摘要: 本发明提出了用于HCE模式的数据加密方法, 所述方法包括: 密钥管理及数据处理服务器针对驻留并运行于特定的移动终端上的安全性信息交互应用生成一个或多个限制密钥, 并将所生成的一个或多个限制密钥发送至安全性信息交互应用; 在根据用户指令进行针对一个安全性信息交互计数值的数据交互时, 安全性信息交互应用基于一个或多个限制密钥中的一个加密安全性信息交互数据以生成应用密文, 并将应用密文发送至密钥管理及数据处理服务器; 在接收到所述应用密文后, 密钥管理及数据处理服务器校验应用密文的有效性和合法性, 并在验证成功后执行后续的与所述安全性信息交互数据相关联的处理操作。本发明所公开的方法具有高的安全性。

用于 HCE 模式的数据加密方法

技术领域

[0001] 本发明涉及数据加密方法，更具体地，涉及用于 HCE 模式的数据加密方法。

背景技术

[0002] 目前，随着计算机和网络应用的日益广泛以及不同领域的业务种类的日益丰富，使用移动终端（例如智能手机）并经由近场通信技术（例如 NFC 技术）实施安全性信息交互过程（即对安全性要求较高的信息交互过程，诸如金融领域中的支付交易过程）变得越来越重要。

[0003] 在常规的基于 NFC 通信协议的移动式安全性信息交互方案中，移动终端典型地包括应用处理器、NFC 控制器以及安全单元（SE），所述安全单元例如是 SD 卡或 SE 芯片的形式。用于存储敏感信息（例如数据加密密钥等等）。

[0004] 然而，上述常规的移动式安全性信息交互方案存在如下问题：由于需要独立的硬件安全单元，故成本较高，并且兼容复杂性增高（例如，每增加一款安全载体需要回归测试所有应用，而每增加一款应用同样需要回归测试所有安全载体）。

[0005] 为了解决上述问题，基于 HCE（Host Card Emulation）模式的移动式安全性信息交互方案被提出，基于该方案，移动终端仅包括应用处理器和 NFC 控制器，并基于存储于移动终端处的安全性应用中的应用密文密钥（例如交易密钥 UDK）加密敏感信息（例如交易数据、应用交易计数器等等）来确保信息交互过程中的安全性。

[0006] 然而，上述基于 HCE 模式的移动式安全性信息交互方案存在如下问题：由于应用密文密钥被存储于移动终端处的安全性应用中且能够被无限使用，故存在潜在的被恶意盗用的风险，故安全性较低。

[0007] 因此，存在如下需求：提供具有高的安全性的用于 HCE 模式的数据加密方法。

发明内容

[0008] 为了解决上述现有技术方案所存在的问题，本发明提出了具有高的安全性的用于 HCE 模式的数据加密方法。

[0009] 本发明的目的是通过以下技术方案实现的：

一种用于 HCE 模式的数据加密方法，所述用于 HCE 模式的数据加密方法包括下列步骤：

(A1) 密钥管理及数据处理服务器针对驻留并运行于特定的移动终端上的安全性信息交互应用生成一个或多个限制密钥，并将所生成的一个或多个限制密钥发送至所述安全性信息交互应用；

(A2) 在根据用户指令进行针对一个安全性信息交互计数值的数据交互时，所述安全性信息交互应用基于所述一个或多个限制密钥中的一个加密安全性信息交互数据以生成应用密文，并将所述应用密文发送至所述密钥管理及数据处理服务器；

(A3) 在接收到所述应用密文后，所述密钥管理及数据处理服务器校验所述应用密文的有效性和合法性，并在验证成功后执行后续的与所述安全性信息交互数据相关联的处理操作。

[0010] 在上面所公开的方案中，优选地，所述步骤 (A1) 进一步包括：所述密钥管理及数据处理服务器基于所述安全性信息交互应用的请求或者周期性地根据安全性信息交互计数值的预设范围生成所述一个或多个限制密钥。

[0011] 在上面所公开的方案中，优选地，所述步骤 (A2) 进一步包括：所述安全性信息交互应用经由近场通信信道将所述应用密文发送至所述密钥管理及数据处理服务器。

[0012] 在上面所公开的方案中，优选地，所述步骤 (A1) 进一步包括：所述密钥管理及数据处理服务器存储与所述安全性信息交互应用相关联的应用密文密钥，并基于该应用密文密钥生成所述一个或多个限制密钥。

[0013] 在上面所公开的方案中，优选地，所述安全性信息交互应用在所述移动终端提供的可信执行环境或白盒加密库中存储所述一个或多个限制密钥。

[0014] 在上面所公开的方案中，优选地，所述一个或多个限制密钥中的每个与一个安全性信息交互计数值绑定，即所述安全性信息交互应用在发起基于当前安全性信息交互计数值的安全性信息交互时使用与该当前安全性信息交互计数值相

绑定的一个限制密钥。

[0015] 在上面所公开的方案中，优选地，所述安全性信息交互应用在每次完成相关联的一组安全性信息交互过程后将其维护的安全性信息交互计数值加 1。

[0016] 在上面所公开的方案中，优选地，所述一个或多个限制密钥中的每个在被使用一次后均失效。

[0017] 在上面所公开的方案中，优选地，所述密钥管理及数据处理服务器基于每个安全性信息交互计数值生成与其相对应的限制密钥，并且所述安全性信息交互应用在发起基于当前安全性信息交互计数值的安全性信息交互时使用与该当前安全性信息交互计数值相绑定的一个限制密钥生成所述应用密文，以确保每个应用密文的唯一性。

[0018] 在上面所公开的方案中，优选地，所述步骤（A1）进一步包括：以如下方式生成所述一个或多个限制密钥：（1）使用与所述安全性信息交互应用相关联的应用密文密钥对预定字符串执行预定的运算操作以获得中间密钥；（2）使用所述中间密钥对特定范围的安全性信息交互计数值中的每个及其取反后的值执行预定的运算操作，以得到与所述特定范围的安全性信息交互计数值中的每个分别对应的限制密钥。

[0019] 在上面所公开的方案中，优选地，所述步骤（A2）进一步包括：为所述一个或多个限制密钥中的每个设定有效期，并且如果某个限制密钥超过有效期未被使用，则该限制密钥失效。

[0020] 在上面所公开的方案中，优选地，用户能够对所述安全性信息交互应用存储的所述一个或多个限制密钥增加基于生物识别和/或解锁口令的附加的加密操作。

[0021] 本发明所公开的用于 HCE 模式的数据加密方法具有以下优点：由于限制密钥仅能够使用一次，故其可以被存储在移动终端所提供的可信执行环境或白盒数据库中，而无需独立的硬件安全单元，故成本较低，并且能够避免或者减轻密钥被恶意盗用的风险，故具有高的安全性。

附图说明

[0022] 结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中：

图 1 是根据本发明的实施例的用于 HCE 模式的数据加密方法的流程图。

具体实施方式

[0023] 图 1 是根据本发明的实施例的用于 HCE 模式的数据加密方法的流程图。

如图 1 所示,本发明所公开的用于 HCE 模式的数据加密方法包括下列步骤:(A1) 密钥管理及数据处理服务器针对驻留并运行于特定的移动终端上的安全性信息交互应用生成一个或多个限制密钥(LUK),并将所生成的一个或多个限制密钥发送至所述安全性信息交互应用;(A2)在根据用户指令进行针对一个安全性信息交互计数值(例如应用交易计数器 ATC 的值)的数据交互时,所述安全性信息交互应用基于所述一个或多个限制密钥中的一个加密安全性信息交互数据(例如交易信息等等)以生成应用密文(例如金融领域中的 ARQC 密文),并将所述应用密文发送至所述密钥管理及数据处理服务器;(A3)在接收到所述应用密文后,所述密钥管理及数据处理服务器校验所述应用密文的有效性和合法性(例如以与步骤(A2)所采用的方式相同的方式生成应用密文副本,并随之将所接收的应用密文与应用密文副本相比对),并在验证成功后执行后续的与所述安全性信息交互数据相关联的处理操作。

[0024] 优选地,在本发明所公开的用于 HCE 模式的数据加密方法中,所述步骤(A1)进一步包括:所述密钥管理及数据处理服务器基于所述安全性信息交互应用的请求或者周期性地根据安全性信息交互计数值的预设范围生成所述一个或多个限制密钥。

[0025] 优选地,在本发明所公开的用于 HCE 模式的数据加密方法中,所述步骤(A2)进一步包括:所述安全性信息交互应用经由近场通信信道将所述应用密文发送至所述密钥管理及数据处理服务器。

[0026] 优选地,在本发明所公开的用于 HCE 模式的数据加密方法中,所述步骤(A1)进一步包括:所述密钥管理及数据处理服务器存储与所述安全性信息交互应用相关联的应用密文密钥(UDK),并基于该应用密文密钥生成所述一个或多个限制密钥。

[0027] 优选地,在本发明所公开的用于 HCE 模式的数据加密方法中,所述安全性信息交互应用在所述移动终端提供的可信执行环境或白盒加密库中存储所述一个或多个限制密钥。

[0028] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，所述一个或多个限制密钥中的每个与一个安全性信息交互计数值（例如应用交易计数器 ATC 的值）绑定（即多个限制密钥中的每个与多个安全性信息交互计数值中的每个具有一一对应关系），即所述安全性信息交互应用在发起基于当前安全性信息交互计数值的安全性信息交互时使用与该当前安全性信息交互计数值相绑定的一个限制密钥。

[0029] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，所述安全性信息交互应用在每次完成相关联的一组安全性信息交互过程（例如完成一次交易过程）后将其维护的安全性信息交互计数值加 1。

[0030] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，所述一个或多个限制密钥中的每个在被使用一次后均失效。

[0031] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，所述密钥管理及数据处理服务器基于每个安全性信息交互计数值生成与其相对应的限制密钥，并且所述安全性信息交互应用在发起基于当前安全性信息交互计数值的安全性信息交互时使用与该当前安全性信息交互计数值相绑定的一个限制密钥生成所述应用密文，以确保每个应用密文的唯一性。

[0032] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，所述步骤（A1）进一步包括：以如下方式生成所述一个或多个限制密钥：（1）使用与所述安全性信息交互应用相关联的应用密文密钥对预定字符串（例如

“CCCCYYMMDDHHNN80”，其中，“CCCC”是参数更新计数器，其每批次被设置为 UDK 加 1，“YY”是年份，其范围为 00-99，“MM”是月份，其范围为 01-12，“DD”是日期，其范围为 01-31，“HH”是小时，其范围为 00-23，“NN”是当前小时内每次密钥更新加 1，当前值为一小时内参数更新的次数，其范围是 0x00-0xFF，“80”是固定填充位）执行预定的运算操作（例如对称加密算法）以获得中间密钥（LUK-A1）；（2）使用所述中间密钥对特定范围（例如每批针对连续的 10 个安全性信息交互计数值）的安全性信息交互计数值（例如应用交易计数器 ATC 的值）中的每个及其取反后的值执行预定的运算操作（例如采用与常规的方案中生成过程密钥 SK 的算法相同的算法），以得到与所述特定范围的安全性信息交互计数值中的每个分别对应的限制密钥。

[0033] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，所述步骤（A2）进一步包括：为所述一个或多个限制密钥中的每个设定有效期，并且如果某个限制密钥超过有效期未被使用，则该限制密钥失效。

[0034] 优选地，在本发明所公开的用于 HCE 模式的数据加密方法中，用户能够对所述安全性信息交互应用存储的所述一个或多个限制密钥增加基于生物识别和/或解锁口令的附加的加密操作。

[0035] 由上可见，本发明所公开的用于 HCE 模式的数据加密方法具有下列优点：由于限制密钥仅能够使用一次，故其可以被存储在移动终端所提供的可信执行环境或白盒数据库中，而无需独立的硬件安全单元，故成本较低，并且能够避免或者减轻密钥被恶意盗用的风险，故具有高的安全性。

[0036] 尽管本发明是通过上述的优选实施方式进行描述的，但是其实现形式并不局限于上述的实施方式。应该认识到：在不脱离本发明主旨和范围的情况下，本领域技术人员可以对本发明做出不同的变化和修改。

权利要求书

1. 一种用于 HCE 模式的数据加密方法，所述用于 HCE 模式的数据加密方法包括下列步骤：

(A1) 密钥管理及数据处理服务器针对驻留并运行于特定的移动终端上的安全性信息交互应用生成一个或多个限制密钥，并将所生成的一个或多个限制密钥发送至所述安全性信息交互应用；

(A2) 在根据用户指令进行针对一个安全性信息交互计数值的数据交互时，所述安全性信息交互应用基于所述一个或多个限制密钥中的一个加密安全性信息交互数据以生成应用密文，并将所述应用密文发送至所述密钥管理及数据处理服务器；

(A3) 在接收到所述应用密文后，所述密钥管理及数据处理服务器校验所述应用密文的有效性和合法性，并在验证成功后执行后续的与所述安全性信息交互数据相关联的处理操作。

2. 根据权利要求 1 所述的用于 HCE 模式的数据加密方法，其特征在于，所述步骤 (A1) 进一步包括：所述密钥管理及数据处理服务器基于所述安全性信息交互应用的请求或者周期性地根据安全性信息交互计数值的预设范围生成所述一个或多个限制密钥。

3. 根据权利要求 2 所述的用于 HCE 模式的数据加密方法，其特征在于，所述步骤 (A2) 进一步包括：所述安全性信息交互应用经由近场通信信道将所述应用密文发送至所述密钥管理及数据处理服务器。

4. 根据权利要求 3 所述的用于 HCE 模式的数据加密方法，其特征在于，所述步骤 (A1) 进一步包括：所述密钥管理及数据处理服务器存储与所述安全性信息交互应用相关联的应用密文密钥，并基于该应用密文密钥生成所述一个或多个限制密钥。

5. 根据权利要求 4 所述的用于 HCE 模式的数据加密方法，其特征在于，所述安全性信息交互应用在所述移动终端提供的可信执行环境或白盒加密库中存储所

述一个或多个限制密钥。

6. 根据权利要求 5 所述的用于 HCE 模式的数据加密方法，其特征在于，所述一个或多个限制密钥中的每个与一个安全性信息交互计数值绑定，即所述安全性信息交互应用在发起基于当前安全性信息交互计数值的安全性信息交互时使用与该当前安全性信息交互计数值相绑定的一个限制密钥。

7. 根据权利要求 6 所述的用于 HCE 模式的数据加密方法，其特征在于，所述安全性信息交互应用在每次完成相关联的一组安全性信息交互过程后将其维护的安全性信息交互计数值加 1。

8. 根据权利要求 7 所述的用于 HCE 模式的数据加密方法，其特征在于，所述一个或多个限制密钥中的每个在被使用一次后均失效。

9. 根据权利要求 8 所述的用于 HCE 模式的数据加密方法，其特征在于，所述密钥管理及数据处理服务器基于每个安全性信息交互计数值生成与其相对应的限制密钥，并且所述安全性信息交互应用在发起基于当前安全性信息交互计数值的安全性信息交互时使用与该当前安全性信息交互计数值相绑定的一个限制密钥生成所述应用密文，以确保每个应用密文的唯一性。

10. 根据权利要求 9 所述的用于 HCE 模式的数据加密方法，其特征在于，所述步骤（A1）进一步包括：以如下方式生成所述一个或多个限制密钥：（1）使用与所述安全性信息交互应用相关联的应用密文密钥对预定字符串执行预定的运算操作以获得中间密钥；（2）使用所述中间密钥对特定范围的安全性信息交互计数值中的每个及其取反后的值执行预定的运算操作，以得到与所述特定范围的安全性信息交互计数值中的每个分别对应的限制密钥。

11. 根据权利要求 10 所述的用于 HCE 模式的数据加密方法，其特征在于，所述步骤（A2）进一步包括：为所述一个或多个限制密钥中的每个设定有效期，并且如果某个限制密钥超过有效期未被使用，则该限制密钥失效。

12. 根据权利要求 11 所述的用于 HCE 模式的数据加密方法，其特征在于，用户能够对所述安全性信息交互应用存储的所述一个或多个限制密钥增加基于生物识别和/或解锁口令的附加的加密操作。

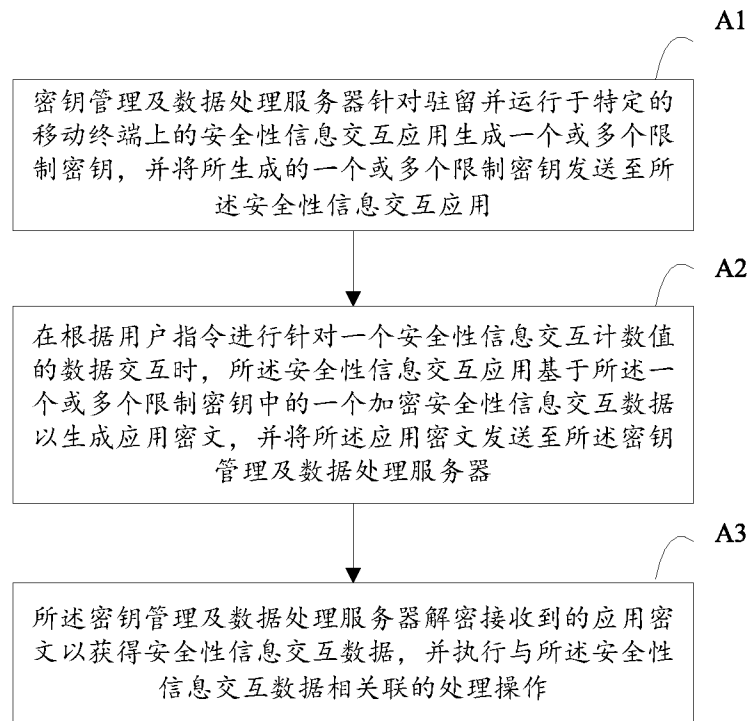


图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/102076

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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; H04W; H04Q

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)

WPI, EPODOC, CNPAT, CNKI, 3GPP: 加密 限制 密钥 支付 应用 密文 主机卡 近场 通信 HCE NFC UDK LUK host card emulation encrypt key security limit pay application cryptogram cipher

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106357663 A (CHINA UNIONPAY CO., LTD.), 25 January 2017 (25.01.2017), claims 1-12	1-12
X	CN 105678543 A (SHENZHEN QIANHAI WEIZHONG BANK CO., LTD.), 15 June 2016 (15.06.2016), description, paragraphs [0055]-[0122], and figures 1-6	1-12
A	CN 105631655 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 01 June 2016 (01.06.2016), entire document	1-12
A	CN 105635168 A (HENGBAO CO., LTD.), 01 June 2016 (01.06.2016), entire document	1-12
A	US 9432087 B2 (GOTRUST TECHNOLOGY INC.), 30 August 2016 (30.08.2016), entire document	1-12

☐ 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 08 November 2017	Date of mailing of the international search report 01 December 2017
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 LI, Tingting Telephone No. (86-10) 62413868

International application No.
PCT/CN2017/102076

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2017/102076

A. 主题的分类 H04L 29/06 (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; H04W; H04Q 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)) WPI, EPDOC, CNPAT, CNKI, 3GPP: 加密 限制 密钥 支付 应用 密文 主机卡 近场通信 HCE NFC UDK LUK host card emulation encrypt key security limit pay application cryptogram cipher		
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 106357663 A (中国银联股份有限公司) 2017年 1月 25日 (2017 - 01 - 25) 权利要求1-12	1-12
X	CN 105678543 A (深圳前海微众银行股份有限公司) 2016年 6月 15日 (2016 - 06 - 15) 说明书第[0055]-[0122]段, 附图1-6	1-12
A	CN 105631655 A (宇龙计算机通信科技深圳有限公司) 2016年 6月 1日 (2016 - 06 - 01) 全文	1-12
A	CN 105635168 A (恒宝股份有限公司) 2016年 6月 1日 (2016 - 06 - 01) 全文	1-12
A	US 9432087 B2 (GOTRUST TECHNOLOGY INC.) 2016年 8月 30日 (2016 - 08 - 30) 全文	1-12
☐ 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 2017年 11月 8日		国际检索报告邮寄日期 2017年 12月 1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 李婷婷 电话号码 (86-10) 62413868

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/102076

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	106357663	A	2017年 1月 25日	无			
CN	105678543	A	2016年 6月 15日	无			
CN	105631655	A	2016年 6月 1日	WO	2017012176	A1	2017年 1月 26日
CN	105635168	A	2016年 6月 1日	无			
US	9432087	B2	2016年 8月 30日	TW	201614967	A	2016年 4月 16日
				CN	106033983	A	2016年 10月 19日