

(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 1 月 9 日 (09.01.2014)



(10) 国际公布号
WO 2014/005534 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2013/078837
- (22) 国际申请日: 2013 年 7 月 4 日 (04.07.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210232922.6 2012 年 7 月 6 日 (06.07.2012) 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: 万四爽 (WAN, Sishuang); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 刘国宝 (LIU, Guobao); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 何朔 (HE, Shuo); 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 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, 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, 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, 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: METHOD AND SYSTEM FOR TRANSMITTING DATA FROM DATA PROVIDER TO SMART CARD

(54) 发明名称: 一种从数据提供方传输数据到智能卡的方法和系统

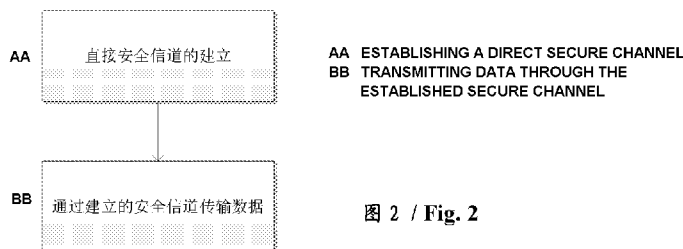


图 2 / Fig. 2

(57) Abstract: Disclosed are a method and system for transmitting data from a data provider to a smart card. The method includes: a smart card generating a key (KEY), encrypting the key (KEY) using a public key PK1 to obtain cipher text PK1 (KEY), and signing the cipher text PK1 (KEY) using an SK2 to obtain signature cipher text SK2 (PK1 (KEY)); a data provider receiving the cipher text PK1 (KEY) and signature cipher text SK2 (PK1 (KEY)) from the smart card, then verifying the signature cipher text SK2 (PK1 (KEY)) using a public key PK2, and decrypting the cipher text PK1 (KEY) using a private key SK1 to obtain the key (KEY); and the data provider encrypting data to be transmitted using the obtained key (KEY) and transmitting same to the smart card.

(57) 摘要: 本发明公开一种从数据提供方传输数据到智能卡的方法和系统。该方法包括, 由智能卡产生密钥 KEY, 然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1 (KEY), 以及利用 SK2 签名该密文 PK1 (KEY) 得到签名密文 SK2 (PK1 (KEY)), 数据提供方从智能卡接收密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY)), 然后利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY)), 以及利用私钥 SK1 解密密文 PK1 (KEY) 得到密钥 KEY; 数据提供方利用得到的密钥 KEY 将要传输的数据加密后传输到智能卡。

WO 2014/005534 A1

一种从数据提供方传输数据到智能卡的方法和系统

优先权要求

本申请要求了 2012 年 7 月 6 日提交的、申请号为 201210232922.6、发明名称为“一种从数据提供方传输数据到智能卡的方法和系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及信息安全领域，尤其涉及一种从数据提供方传输数据到智能卡的方法和系统。

背景技术

随着智能卡多应用的发展，在一张智能卡上加载多个应用变得越来越普遍，应用提供方面面临的一个重要问题就是如何将应用数据（例如，账户信息）安全地传输到由第三方管理的智能卡上。

在现有技术中，从应用提供方将应用数据传输到智能卡包括密钥准备和数据传输两个步骤。如图 1 中的上面部分的示意图所示，在密钥准备的步骤中，首先，应用提供方将主密钥 KMC 设置在第三方个人化系统中；然后第三方个人化系统将主密钥 KMC 分散得到密钥 Kcard，并且将密钥 Kcard 设置在智能卡安全芯片中；最后应用提供方与第三方系统协商传输密钥 KEK。如图 1 中的下面部分的示意图所示，在数据传输的步骤中，首先应用提供方将待传输的数据通过 KEK 加密后传给第三方个人化系统；然后第三方个人化系统接收数据并在加密机中用 KEK 解密，同时在加密机中再用主密钥 KMC 分散得到的密钥 Kcard 加密后传给智能卡；最后智能卡用 Kcard 解密得到应用提供方传输的数据。

上述现有技术存在以下缺陷，一方面，在数据传输过程中，第三方的个人化设备和智能卡在封闭的系统内部（例如，卡厂），这样对于已经发出的智能卡就不方便更新应用数据或者下载新的应用数据。另一方面，虽然有密

钥保护应用提供方准备的数据，但是应用提供方和智能卡卡片不是直接建立的安全信道，而是应用提供方与第三方系统、第三方系统和卡片分别建立安全信道，因此需要在第三方系统内部进行一个数据转换的过程，从而可能存在数据泄露的风险。

5

发明内容

根据本发明的一个目的公开一种从数据提供方传输数据到智能卡的方法，其中数据提供方拥有公钥 PK1 和私钥 SK1，智能卡拥有公钥 PK2 和私钥 SK2，包括以下步骤：

10 由智能卡产生密钥 KEY，然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1 (KEY)，以及利用 SK2 签名该密文 PK1 (KEY) 得到签名密文 SK2 (PK1 (KEY))，
数据提供方从智能卡接收密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY))，
然后利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY))，以及利用私钥 SK1 解密密文 PK1 (KEY) 得到密钥 KEY；

15 数据提供方利用得到的密钥 KEY 将要传输的数据加密后传输到智能卡。

可选地，所述数据提供方是应用提供方，所述数据是应用数据，该应用数据用于将智能卡应用个人化。

可选地，所述数据提供方向智能卡发送密钥生成指令，智能卡在接收到该密钥生成指令后产生密钥 KEY。

20 可选地，密钥 KEY 由智能卡随机产生。

可选地，数据提供方通过第三方与智能卡通信。

可选地，所述要传输的数据包括传输密钥，该传输密钥由关于数据提供方的主密钥分散得到的子密钥，所述方法还包括以下步骤：

智能卡利用密钥 KEY 从数据提供方获取传输密钥，以及

25 应用提供方利用该传输密钥将要传输的另外的数据加密后传输到智能卡。

可选地，所述另外的数据是用于对智能卡进行个人化的数据。

根据本发明的方法和系统，数据提供方通过与智能卡建立端到端的安全

通道，能够将应用数据通过不可信的信道和第三方系统安全地传输到智能卡上。

附图说明

5 在参照附图阅读了本发明的具体实施方式以后，本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是，这些附图仅仅用于配合具体实施方式说明本发明的技术方案，而并非意在对本发明的保护范围构成限制。

图 1 是根据现有技术中从应用提供方将应用数据传输到智能卡的方法示意图。
10

图 2 是根据本发明实施例的从数据提供方将数据传输到智能卡的步骤示意图。

具体实施方式

15 下面参照附图，对本发明的具体实施方式作进一步的详细描述。

图 2 是根据本发明实施例的从数据提供方将数据传输到智能卡的步骤示意图。该方法包括两个步骤，即直接安全信道的建立以及通过建立的安全信道传输数据。

在本发明中，数据提供方拥有公钥 PK1 和私钥 SK1，智能卡拥有公钥 PK2
20 和私钥 SK2。例如，数据提供方和卡厂分别从 CA 申请公私钥对和公钥证书，并且数据提供方和卡厂可以利用公钥 PCA 验证对方公钥证书，并获得对方公钥。在一个实施例中，在数据提供方中设置有 PK1、SK1 和 PK2，在智能卡中设置有 PK1、PCA 和 SK2。在该实施例中，卡厂将 CA 的公钥 PCA 和私钥 SK2 预置到智能卡中；数据提供方可以在获得卡厂的公钥证书后用公钥 PCA
25 验证得到智能卡公钥 PK2；而数据提供方将公钥证书通过网络或者任意第三方传输到智能卡，智能卡通过 CA 的公钥 PCA 验证数据提供方的公钥证书，然后得到数据提供方的公钥 PK1。在上述数据准备过程中，只有公钥证书在网络上传输，而且在获取公钥的时候会根据 CA 公钥 PCA 验证公钥证书，所

以这一步即使信道不可信，整个过程仍然是安全的。

在直接安全信道的建立的步骤中，由智能卡产生密钥 KEY，然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1(KEY)，以及利用 SK2 签名该密文 PK1(KEY) 得到签名密文 SK2 (PK1 (KEY))。智能卡能够通过第三方或者不可信的网络
5 将密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY)) 发送给数据提供方。

接着，数据提供方从智能卡接收密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY))，然后利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY))，以及利用私钥 SK1 解密密文 PK1 (KEY) 得到密钥 KEY。由此，数据提供方和智能卡同时拥有同一密钥 KEY，数据提供方到智能卡的直接安全信道得到建立。

10 由于密钥 KEY 是被数据提供方的公钥 PK1 加密的，而只有数据提供方具有对应的解密私钥 SK1，所以密钥 KEY 不可能被窃取。另外，由于密钥 KEY 每次都可以由智能卡随机产生，所以第三方不可能截取密文 PK1(KEY)和签名密文 SK2(PK1(KEY))进行重放攻击。另一方面，由于只有智能卡具有私钥 SK2，并且利用该私钥 SK2 对加密的密钥签名，所以数据提供方根据公钥 PK2 验签
15 能够避免签名密文 SK2(PK1(KEY))被冒充和篡改。

在通过建立的安全信道传输数据的步骤中，数据提供方利用得到的密钥 KEY 将要传输的数据加密后传输到智能卡。

可选地，所述数据提供方是应用提供方，所述数据是应用数据，该应用数据用于将智能卡应用个人化。

20 可选地，所述数据提供方向智能卡发送密钥生成指令，智能卡在接收到该密钥生成指令后产生密钥 KEY。

在一个实施例中，应用提供方和智能卡之间通过下述步骤完成直接安全信道的建立以及数据传输：

在步骤 1 中，由应用提供方向智能卡发送生成密钥指令 GENERATE KEY；

25 在步骤 2 中，智能卡向应用提供方返回 GENERATE KEY 指令响应，在该步骤中，当智能卡接收到生成密钥指令 GENERATE KEY 之后，由智能卡产生密钥 KEY，然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1 (KEY)，以及利用 SK2 签名该密文 PK1 (KEY) 得到签名密文 SK2 (PK1 (KEY))，智能卡向应

用提供方返回 GENERATE KEY 指令响应, 其中 GENERATE KEY 指令响应包括密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY)) ;

在步骤 3 中, 由应用提供方向智能卡发送 PUT KEY 指令, 在该步骤中, 应用提供方接收包括密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY)) 的 GENERATE KEY 指令响应之后, 判断 GENERATE KEY 指令是否执行成功, 如果执行成功则以及利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY)), 以及利用私钥 SK1 解密密文 PK1 (KEY) 得到密钥 KEY, 将得到的密钥 KEY 作为后续操作的临时会话密钥, 然后由应用提供方向智能卡发送 PUT KEY 指令, 该 PUT KEY 指令包括传输密钥, 并且根据上述的临时会话密钥被加密;

10 在步骤 4 中, 智能卡向应用提供方返回 PUT KEY 指令响应, 在该步骤中, 智能卡利用上述临时会话密钥解密 PUT KEY 指令并且获取传输密钥, 并将该传输密钥存储在智能卡中, 以及向应用提供方返回 PUT KEY 指令响应指示获取并存储传输密钥是否成功。在一个实施例中, 传输密钥是由关于应用提供方的主密钥分散得到的子密钥, 由此, 应用提供方和智能卡都具有传输密钥。
15 作为子密钥的传输密钥被用于加密后续的应用提供方和智能卡之间的数据的传输;

在步骤 5 中, 由应用提供方向智能卡发送个人化 STORE DATA 指令, 该 STORE DATA 指令利用传输密钥加密并且用于向智能卡写入数据以对智能卡进行个人化;

20 在步骤 6 中, 智能卡向应用提供方返回 STORE DATA 指令响应, 指示数据写入是否成功。

本领域的技术人员可以理解的是, 上述描述的 6 个步骤可以分别独立地与本发明的其它实施例组合, 或者该 6 个步骤可以互相结合而得到用于实现本发明的目的其它技术方案。

25 本发明还公开从数据提供方传输数据到智能卡的系统, 该系统包括数据提供方和智能卡, 其中数据提供方拥有公钥 PK1 和私钥 SK1, 智能卡拥有公钥 PK2 和私钥 SK2, 其中, 智能卡被配置成产生密钥 KEY, 然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1 (KEY), 以及利用 SK2 签名该密文 PK1 (KEY)

得到签名密文 SK2 (PK1 (KEY))，数据提供方被配置成从智能卡接收密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY))，然后利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY))，以及利用私钥 SK1 解密密文 PK1 (KEY) 得到密钥 KEY；以及数据提供方被进一步配置成利用得到的密钥 KEY 将要传输的数据加密后传输到智能卡。

可选地，数据提供方被配置成向智能卡发送密钥生成指令，智能卡被配置成在接收到该密钥生成指令后产生密钥 KEY，数据提供方通过第三方与智能卡通信。

可选地，所述要传输的数据包括传输密钥，该传输密钥由关于数据提供方的主密钥分散得到的子密钥，其中：智能卡还被配置成利用密钥 KEY 从数据提供方获取传输密钥，以及应用提供方被配置成利用该传输密钥将要传输的另外的数据加密后传输到智能卡。

通过以上实施方式的描述，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

20

25

30

权 利 要 求

1. 一种从数据提供方传输数据到智能卡的方法,其中数据提供方拥有公钥 PK1 和私钥 SK1, 智能卡拥有公钥 PK2 和私钥 SK2, 其特征在于, 包括以

5 下步骤:

由智能卡产生密钥 KEY, 然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1 (KEY), 以及利用 SK2 签名该密文 PK1 (KEY) 得到签名密文 SK2 (PK1 (KEY)),

数据提供方从智能卡接收密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY)), 然后利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY)), 以及利用私钥 SK1 解

10 密密文 PK1 (KEY) 得到密钥 KEY;

数据提供方利用得到的密钥 KEY 将要传输的数据加密后传输到智能卡。

2. 如权利要求 1 所述的方法, 其特征在于,

15 所述数据提供方向智能卡发送密钥生成指令, 智能卡在接收到该密钥生成指令后产生密钥 KEY。

3. 如权利要求 2 所述的方法, 其特征在于, 密钥 KEY 由智能卡随机产生。

4. 如权利要求 1 所述的方法, 其特征在于, 所述要传输的数据包括传输
20 密钥, 该传输密钥由关于数据提供方的主密钥分散得到的子密钥, 所述方法还包括以下步骤:

智能卡利用密钥 KEY 从数据提供方获取传输密钥, 以及

应用提供方利用该传输密钥将要传输的另外的数据加密后传输到智能卡。

25

5. 如权利要求 4 所述的方法, 其特征在于, 所述另外的数据是用于对智能卡进行个人化的数据。

6. 一种从数据提供方传输数据到智能卡的系统,该系统包括数据提供方和智能卡,其中数据提供方拥有公钥 PK1 和私钥 SK1,智能卡拥有公钥 PK2 和私钥 SK2,其特征在于,

智能卡被配置成产生密钥 KEY,然后利用公钥 PK1 加密密钥 KEY 得到密文 PK1 (KEY),以及利用 SK2 签名该密文 PK1 (KEY) 得到签名密文 SK2 (PK1 (KEY)),

数据提供方被配置成从智能卡接收密文 PK1 (KEY) 和签名密文 SK2 (PK1 (KEY)),然后利用公钥 PK2 验证签名密文 SK2 (PK1 (KEY)),以及利用私钥 SK1 解密密文 PK1 (KEY) 得到密钥 KEY; 以及

10 数据提供方被进一步配置成利用得到的密钥 KEY 将要传输的数据加密后传输到智能卡。

7. 如权利要求 6 所述的系统,其特征在于,

数据提供方被配置成向智能卡发送密钥生成指令,

15 智能卡被配置成在接收到该密钥生成指令后产生密钥 KEY。

8. 如权利要求 7 所述的系统,其特征在于,密钥 KEY 由智能卡随机产生。

9. 如权利要求 6 所述的系统,其特征在于,所述要传输的数据包括传输
20 密钥,该传输密钥由关于数据提供方的主密钥分散得到的子密钥,其中:

智能卡还被配置成利用密钥 KEY 从数据提供方获取传输密钥,以及

应用提供方被配置成利用该传输密钥将要传输的另外的数据加密后传输到智能卡。

25 10. 如权利要求 9 所述的系统,其特征在于,所述另外的数据是用于对智能卡进行个人化的数据。

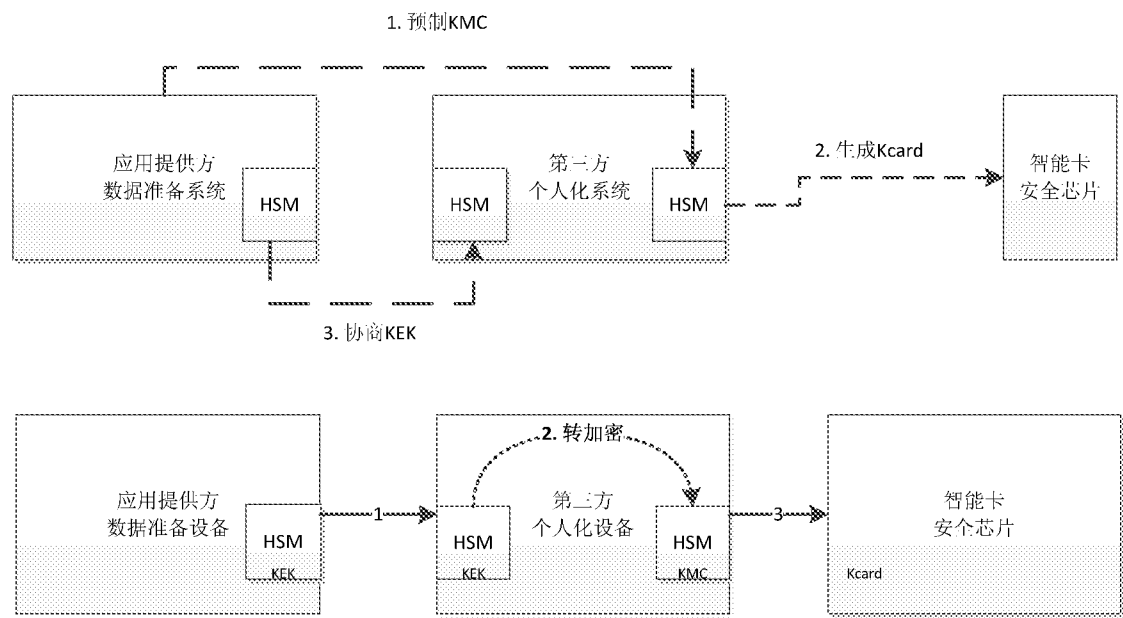


图 1

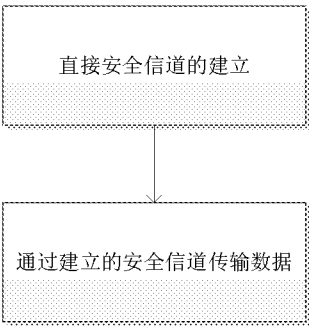


图 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/078837

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (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)

IPC: 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, CNTXT, DWPI, USTXT, IEEE: smartcard, public key, private key, data, transmit, signature, validate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102394749 A (EXCELSECU DATA TECHNOLOGY INC.), 28 March 2012 (28.03.2012), see description, paragraphs 0061-0076 and 0109-0110, and figures 2 and 8	1-10
A	CN 102075802 A (GUANGDONG IKER DIGITAL TECHNOLOGY CO., LTD.), 25 May 2011 (25.05.2011), the whole document	1-10
A	CN 101894235 A (THE THIRD INSTITUTE OF MINISTRY OF PUBLIC SECURITY), 24 November 2010 (24.11.2010), the whole document	1-10

☐ 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
17 September 2013 (17.09.2013)

Date of mailing of the international search report
10 October 2013 (10.10.2013)

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
NIE, Peng
Telephone No.: (86-10) **62413689**

International application No.
PCT/CN2013/078837

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

A. 主题的分类

H04L 9/32 (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)

IPC: 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, CNTXT, DWPI, USTXT, IEEE: 智能卡, 公钥, 私钥, 数据, 传输, 签名, 验证, smartcard, public key, private key, data, transmit, signature, validate

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 102394749 A (深圳市文鼎创数据科技有限公司) 28.3 月 2012 (28.03.2012) 参见说明书第 0061-0076 段, 0109-0110 段以及附图 2 和 8	1-10
A	CN 102075802 A (广东爱科数字科技有限公司) 25.5 月 2011 (25.05.2011) 全文	1-10
A	CN 101894235 A (公安部第三研究所) 24.11 月 2010 (24.11.2010) 全文	1-10

☐ 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

17.9 月 2013 (17.09.2013)

国际检索报告邮寄日期

10.10 月 2013 (10.10.2013)

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

受权官员

聂鹏

电话号码: (86-10) 62413689

关于同族专利的信息

PCT/CN2013/078837

PCT/ISA/210 表(同族专利附件) (2009 年 7 月)