

## (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 6 月 29 日 (29.06.2017)



(10) 国际公布号  
WO 2017/107328 A1

- (51) 国际专利分类号:  
G06F 21/85 (2013.01)
- (21) 国际申请号: PCT/CN2016/077252
- (22) 国际申请日: 2016 年 3 月 24 日 (24.03.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201510981728.1 2015 年 12 月 22 日 (22.12.2015) CN
- (71) 申请人: 广州广电运通金融电子股份有限公司 (GRG BANKING EQUIPMENT CO., LTD.) [CN/CN]; 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。
- (72) 发明人: 熊飞 (XIONG, Fei); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 吴胜楠 (WU, Shengnan); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 陈明宇 (CHEN, Mingyu); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 张雲瑞

(ZHANG, Yunrui); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 梁建明 (LI-ANG, Jianming); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 李柯烨 (LI, Keye); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街 22 号赛特广场 7 层, Beijing 100004 (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。

[见续页]

(54) Title: SECURE COMMUNICATION METHOD AND APPARATUS FOR SELF-SERVICE TERMINAL DEVICE HARDWARE

(54) 发明名称: 一种自助终端设备硬件的安全通信方法和装置

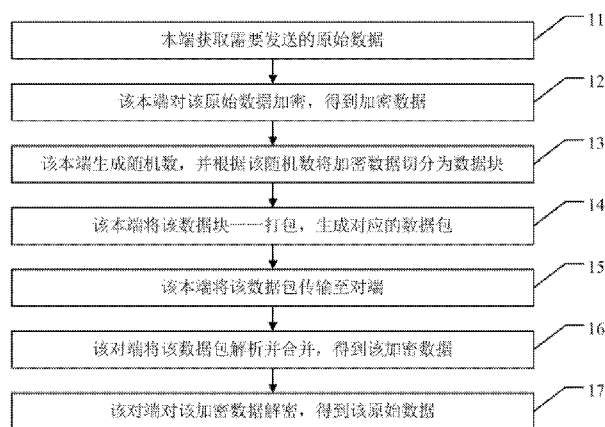


图 1

- 11 A LOCAL END ACQUIRING ORIGINAL DATA NEEDING TO BE SENT  
12 THE LOCAL END ENCRYPTING THE ORIGINAL DATA TO OBTAIN ENCRYPTED DATA  
13 THE LOCAL END GENERATING A RANDOM NUMBER, AND PARTITIONING THE ENCRYPTED DATA INTO A DATA BLOCK ACCORDING TO THE RANDOM NUMBER  
14 THE LOCAL END PACKAGING THE DATA BLOCK ONE BY ONE TO GENERATE A CORRESPONDING DATA PACKET  
15 THE LOCAL END TRANSMITTING THE DATA PACKET TO A PEER END  
16 THE PEER END PARSING AND MERGING THE DATA PACKET TO OBTAIN THE ENCRYPTED DATA  
17 THE PEER END DECRYPTING THE ENCRYPTED DATA TO OBTAIN THE ORIGINAL DATA

(57) Abstract: Disclosed is a secure communication method for self-service terminal device hardware, which is used for solving the problem that a conventional self-service terminal is vulnerable to a financial crime a criminal commits by simulating device hardware through software to communicate with a host. The method comprises: a local end acquiring original data needing to be sent; the local end encrypting the original data to obtain encrypted data; the local end generating a random number, and partitioning the encrypted data into a data block according to the random number; the local end packaging the data block one by one to generate a corresponding data packet; the local end transmitting the data packet to a peer end, such that the peer end parses and merges the data packet to obtain the encrypted data, and then the peer end decrypting the encrypted data to obtain the original data. Also provided is a secure communication apparatus for self-service terminal device hardware.

(57) 摘要: 本发明实施例公开了一种自助终端设备硬件的安全通信方法, 用于解决现有自助终端容易遭到犯罪分子通过软件模拟设备硬件与主机通信进行金融犯罪的问题。本发明实施例方法包括: 本端获取需要发送的原始数据; 所述本端对所述原始数据加密, 得到加密数据; 所述本端生成随机数, 并根据所述随机数将加密数据切分为数据块; 所述本端将所述数据块一一打包, 生成对应的数据包; 所述本端将所述数据包传输至对端, 使得所述对端将所述数据包解析并合并, 得到所述加密数据, 然后所述对端对所述加密数据解密, 得到所述原始数据。本发明实施例还提供一种自助终端设备硬件的安全通信装置。

所述对端对所述加密数据解密, 得到所述原始数据。本发明实施例还提供一种自助终端设备硬件的安全通信装置。



WO 2017/107328 A1



(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))。

## 一种自助终端设备硬件的安全通信方法和装置

本申请要求于 2015 年 12 月 22 日提交中国专利局、申请号为 201510981728.1、发明名称为“一种自助终端设备硬件的安全通信方法和装置”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。

5

### 技术领域

本发明涉及金融设备领域，尤其涉及一种自助终端设备硬件的安全通信方法和装置。

### 10 背景技术

随着金融犯罪的手法不端提高，技术水平不断提升，虽然目前 ATM 机器的保险柜不容易接触到，但是犯罪分子可以通过软件模拟机芯硬件设备，布置在目标 ATM 机器上，达到不断的模拟存款业务，绕过了真实机芯设备，从而导致金融犯罪。犯罪人员通过测试工具，调用 CEN XFS 标准的命令，不需要  
15 打开保险柜门，就能把钞票从保险柜中轻松的拿出来，增加了风险。现有的安全技术是需要联网进行安全验证，会增加因联网验证所产生的未知风险，这样就大大降低 ATMC 软件对主机设备的安全实时检查和追踪，就会被犯罪人员有机可乘。

### 20 发明内容

本发明实施例提供了一种自助终端设备硬件的安全通信方法和装置，能够解决现有自助终端容易遭到犯罪分子通过软件模拟设备硬件与主机通信进行金融犯罪的问题。

本发明实施例提供的一种自助终端设备硬件的安全通信方法，应用于所述  
25 自助终端的主机与设备硬件之间的通信，包括：

本端获取需要发送的原始数据；

所述本端对所述原始数据加密，得到加密数据；

所述本端生成随机数，并根据所述随机数将加密数据切分为数据块；

所述本端将所述数据块一一打包，生成对应的数据包；

-2-

所述本端将所述数据包传输至对端,使得所述对端将所述数据包解析并合并,得到所述加密数据,然后所述对端对所述加密数据解密,得到所述原始数据。

可选地,所述本端生成随机数,并根据所述随机数将加密数据切分为数据

5 块包括:

所述本端生成一个预设范围内的随机数;

所述本端将所述加密数据切分为所述随机数个数据块。

可选地,所述安全通信方法还包括:所述本端预先生成一对非对称密钥,包括公钥和私钥,并将所述公钥预先导入至所述对端;

10 所述私钥用于对所述原始数据加密,所述公钥用于对所述加密数据解密。

可选地,所述本端对所述原始数据加密,得到加密数据包括:

所述本端将所述原始数据和对应的时间信息合并成数据体;

所述本端对所述数据体进行校验运算,得到第一运算结果;

所述本端将所述数据体和所述第一运算结果合并,得到校验数据体;

15 所述本端对所述校验数据体加密,得到加密数据;

所述对端对所述加密数据解密,得到所述原始数据包括:

所述对端对所述加密数据解密,得到待测校验数据体;

所述对端获取所述待测校验数据体中的数据体,并对获取到的数据体进行校验运算,得到第二运算结果;

20 所述对端校验所述第二运算结果与所述待测校验数据体中的第一运算结果是否相符,若相符,则获取所述数据体中的所述原始数据。

可选地,所述对端在得到所述原始数据之后还包括:

所述对端对所述原始数据进行数据合理性检查,若检查通过,则所述对端根据所述原始数据进行操作。

25 本发明实施例提供的一种自助终端设备硬件的安全通信装置,应用于所述自助终端的主机与设备硬件之间的通信,包括本端和对端,所述本端包括:

原始数据获取模块,用于获取需要发送的原始数据;

加密模块,用于对所述原始数据加密,得到加密数据;

随机切分模块,用于生成随机数,并根据所述随机数将加密数据切分为数

据块;

数据包模块, 用于将所述数据块一一打包, 生成对应的数据包;

传输模块, 用于将所述数据包传输至所述对端;

所述对端包括:

5 解析合并模块, 用于将所述数据包解析并合并, 得到所述加密数据;

解密模块, 用于对所述加密数据解密, 得到所述原始数据。

可选地, 所述随机切分模块包括:

随机数生成单元, 用于生成一个预设范围内的随机数;

数据切分单元, 用于将所述加密数据切分为所述随机数个数据块。

10 可选地, 所述安全通信装置还包括:

密钥生成模块, 用于预先生成一对非对称密钥, 包括公钥和私钥;

公钥导入模块, 用于将所述公钥预先导入至所述对端;

所述私钥用于对所述原始数据加密, 所述公钥用于对所述加密数据解密。

可选地, 所述加密模块包括:

15 第一合并单元, 用于将所述原始数据和对应的时间信息合并成数据体;

第一校验运算单元, 用于对所述数据体进行校验运算, 得到第一运算结果;

第二合并单元, 用于将所述数据体和所述第一运算结果合并, 得到校验数据体;

加密单元, 用于对所述校验数据体加密, 得到加密数据;

20 所述解密模块包括:

解密单元, 用于对所述加密数据解密, 得到待测校验数据体;

第二校验运算单元, 用于获取所述待测校验数据体中的数据体, 并对获取到的数据体进行校验运算, 得到第二运算结果;

25 校验单元, 用于校验所述第二运算结果与所述待测校验数据体中的第一运算结果是否相符;

数据获取单元, 用于当所述校验单元的校验结果为是时, 获取所述数据体中的所述原始数据。

可选地, 所述对端还包括:

合理性检查模块, 用于对所述原始数据进行数据合理性检查;

—4—

操作模块，用于当所述合理性检查模块的检查通过时，根据所述原始数据进行操作。

从以上技术方案可以看出，本发明实施例具有以下优点：

本发明实施例中，首先，本端获取需要发送的原始数据；所述本端对所述原始数据加密，得到加密数据；然后，所述本端生成随机数，并根据所述随机数将加密数据切分为数据块；所述本端将所述数据块一一打包，生成对应的数据包；最后，所述本端将所述数据包传输至对端，使得所述对端将所述数据包解析并合并，得到所述加密数据，然后所述对端对所述加密数据解密，得到所述原始数据。在本发明实施例中，该自助终端设备硬件的安全通信方法在自助终端本地主机内实现，无需联网验证，并通过随机分包来提升通信的安全性，防范了犯罪分子通过软件模拟设备硬件与主机通信进行金融犯罪。

## **附图说明**

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

图 1 为本发明实施例中一种自助终端设备硬件的安全通信方法一个实施例流程图；

图 2 为本发明实施例中一种自助终端设备硬件的安全通信方法另一个实施例流程图；

图 3 为本发明实施例中一种自助终端设备硬件的安全通信方法一个应用场景下的自助终端系统结构图；

图 4 为本发明实施例中一种自助终端设备硬件的安全通信方法一个应用场景下的数据加密通信过程中的数据格式结构图；

图 5 为本发明实施例中一种自助终端设备硬件的安全通信装置一个实施例结构图；

图 6 为本发明实施例中一种自助终端设备硬件的安全通信装置另一个实施例结构图。

## **具体实施方式**

—5—

本发明实施例提供了一种自助终端设备硬件的安全通信方法和装置,用于解决现有自助终端容易遭到犯罪分子通过软件模拟设备硬件与主机通信进行金融犯罪的问题。

5 为使得本发明的发明目的、特征、优点能够更加的明显和易懂,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,下面所描述的实施例仅仅是本发明一部分实施例,而非全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

10 请参阅图 1,本发明实施例中一种自助终端设备硬件的安全通信方法一个实施例包括:

11、本端获取需要发送的原始数据;

首先,本端可以获取需要发送的原始数据。需要说明的是,当自助终端的主机向设备硬件进行通信时,该主体为本端,设备硬件为对端;而当自助终端的设备硬件向主机进行通信时,则设备硬件为本端,主机为对端。

15 12、该本端对该原始数据加密,得到加密数据;

在本端获取需要发送的原始数据之后,该本端可以对该原始数据加密,得到加密数据。

13、该本端生成随机数,并根据该随机数将加密数据切分为数据块;

20 在该本端对该原始数据加密,得到加密数据之后,该本端可以生成随机数,并根据该随机数将加密数据切分为数据块。

14、该本端将该数据块一一打包,生成对应的数据包;

在该本端生成随机数,并根据该随机数将加密数据切分为数据块之后,该本端可以将该数据块一一打包,生成对应的数据包。

15、该本端将该数据包传输至对端;

25 在该本端将该数据块一一打包,生成对应的数据包之后,该本端可以将该数据包传输至对端。

16、该对端将该数据包解析并合并,得到该加密数据;

在该本端将该数据包传输至对端之后,该对端可以将该数据包解析并合并,得到该加密数据。

17、该对端对该加密数据解密，得到该原始数据。

在该对端将该数据包解析并合并，得到该加密数据之后，该对端可以对该加密数据解密，得到该原始数据。

5 本实施例中，首先，本端获取需要发送的原始数据；该本端对该原始数据加密，得到加密数据；然后，该本端生成随机数，并根据该随机数将加密数据切分为数据块；该本端将该数据块一一打包，生成对应的数据包；最后，该本端将该数据包传输至对端，使得该对端将该数据包解析并合并，得到该加密数据，然后该对端对该加密数据解密，得到该原始数据。在本实施例中，该自助终端设备硬件的安全通信方法在自助终端本地主机内实现，无需联网验证，并通过  
10 随机分包来提升通信的安全性，防范了犯罪分子通过软件模拟设备硬件与主机通信进行金融犯罪。

为便于理解，下面对本发明实施例中的一种自助终端设备硬件的安全通信方法进行详细描述，请参阅图 2，本发明实施例中一种自助终端设备硬件的安全通信方法另一个实施例包括：

15 21、本端获取需要发送的原始数据；

首先，本端可以获取需要发送的原始数据。需要说明的是，当自助终端的主机向设备硬件进行通信时，该主体为本端，设备硬件为对端；而当自助终端的设备硬件向主机进行通信时，则设备硬件为本端，主机为对端。

22、该本端将该原始数据和对应的时间信息合并成数据体；

20 在本端获取需要发送的原始数据之后，该本端可以将该原始数据和对应的时间信息合并成数据体。可以理解的是，该时间信息与原始数据是对应的，时间信息可以是记录了该原始数据生成的时间，或者是多个原始数据之间的时间顺序。

23、该本端对该数据体进行校验运算，得到第一运算结果；

25 在该本端将该原始数据和对应的时间信息合并成数据体之后，该本端对该数据体进行校验运算，得到第一运算结果。可以理解的是，该校验运算具体可以是 CRC（Cyclic Redundancy Code，循环冗余）校验，从而最后的第一运算结果为 CRC 校验运算结果。

24、该本端将该数据体和该第一运算结果合并，得到校验数据体；

在该本端对该数据体进行校验运算，得到第一运算结果之后，该本端可以将该数据体和该第一运算结果合并，得到校验数据体。其中，可以预设该校验数据体的数据结构，例如将第一运算结果放在数据结构的前头，数据体放在第一运算结果后面。具体地，该校验数据体的结构可以自定义，本实施例不对此进行限定。

25、该本端采用私钥对该校验数据体加密，得到加密数据；

在该本端将该数据体和该第一运算结果合并，得到校验数据体之后，该本端可以采用私钥对该校验数据体加密，得到加密数据。需要说明的是，该本端预先生成一对非对称密钥，包括公钥和私钥，并将该公钥预先导入至该对端，其中，该私钥用于对该原始数据加密，该公钥用于对该加密数据解密。

26、该本端生成一个预设范围内的随机数；

在切分前，该本端需要生成一个预设范围内的随机数，该随机数对于本端和对端来说都是随机的，从而避免犯罪人员提前获知而破解，提高安全性。其中，为了提高数据传输的效率，该随机数一般不能太大，比如，该加密数据大小为 100 字节，若生成的随机数为 100，则将 100 字节大小的切分为 100 个 1 字节的数据块，这对于后续的数据传输来说是非常不利的。因此，本实施例中，该随机数在预设的数值范围内生成，避免了随机数过大的问题。

27、该本端将该加密数据切分为该随机数个数据块；

在该本端生成一个预设范围内的随机数之后，该本端将该加密数据切分为该随机数个数据块。例如，随机数为 5 时，将该加密数据切分为 5 个数据块。

28、该本端将该数据块一一打包，生成对应的数据包；

在该本端将该加密数据切分为该随机数个数据块之后，该本端可以将该数据块一一打包，生成对应的数据包。例如，当有 5 个数据块时，对每个数据块均进行打包，生成 5 个对应的数据包。具体可以为，在一个数据块的基础上分别增加包头和包尾，从而使一个数据块生成一个数据包。

29、该本端将该数据包传输至对端；

在该本端将该数据块一一打包，生成对应的数据包之后，该本端将该数据包传输至对端。

30、该对端将该数据包解析并合并，得到该加密数据；

该对端接收来自该本端的该数据包后，可以将该数据包解析并合并，得到该加密数据。具体地，也就是将数据包解析成数据块，然后将所有数据块合并成该加密数据。

- 31、该对端采用公钥对该加密数据解密，若解密失败，则执行步骤 37，  
5 若解密成功，则得到待测校验数据体；

在得到该加密数据之后，该对端可以采用公钥对该加密数据解密，若解密失败，则执行步骤 37，若解密成功，则得到待测校验数据体。可以理解的是，用来解密的公钥与加密时所用的私钥是成对的，并且公钥是预先导入至该对端上，避免了犯罪人员通过软件手段获取到对端上的公钥。

- 10 32、该对端获取该待测校验数据体中的数据体，并对获取到的数据体进行校验运算，得到第二运算结果；

在得到待测校验数据体之后，该对端可以获取该待测校验数据体中的数据体，并对获取到的数据体进行校验运算，得到第二运算结果。需要说明的是，步骤 32 的校验运算方法应该与步骤 23 所使用的校验运算方法保持一致。

- 15 33、该对端校验该第二运算结果与该待测校验数据体中的第一运算结果是否相符，若相符，则执行步骤 34，若不符，则执行步骤 37；

- 在得到第二运算结果之后，该对端可以校验该第二运算结果与该待测校验数据体中的第一运算结果是否相符，若相符，则执行步骤 34，若不符，则执行步骤 37。可以理解的是，当第二运算结果与第一运算结果相符时，说明得  
20 到的待测校验数据体中的数据体与本端上的数据体一致，否则，则待测校验数据体存在数据错误，可以做错误数据处理。

34、该对端获取该数据体中的该原始数据；

当第二运算结果与第一运算结果相符时，该对端从该数据体中获取该原始数据。

- 25 35、该对端对该原始数据进行数据合理性检查，若检查通过，则执行步骤 36，若检查不通过，则执行步骤 37；

在该对端获取该数据体中的该原始数据之后，该对端可以对该原始数据进行数据合理性检查，若检查通过，则执行步骤 36，若检查不通过，则执行步骤 37。该数据合理性检查的检查标准可根据实际使用情况进行设定，例如可

以检查该原始数据的命令组合是否合理，或者其对应的时间信息是否合理等。

36、该对端根据该原始数据进行操作；

当该原始数据通过数据合理性检查之后，该对端可以根据该原始数据进行操作。

5 37、该对端作数据丢弃处理。

当加密数据解密失败时，或待测校验数据体校验失败时，或得到的原始数据的数据合理性检查不通过时，该对端对这些数据作数据丢弃处理。

为便于理解，下面以一个实际应用场景对本发明实施例中的一种自助终端设备硬件的安全通信方法进行描述：

10 本应用场景中，该自助终端的主机内置有数据安全处理模块 102，设备硬件中内置有数据安全处理模块 103，该自助终端的系统结构如图 3 所示。自助终端主机安装有 ATMC（一种 ATM 机的系统平台）上层软件，主机通过数据安全处理模块 102 与设备硬件的数据安全处理模块 103 通信，实现主机与设备硬件之间的通信。下面对通信过程中的各个环节进行描述，请参考图 3 和图 4。

15 密钥生成过程：

步骤 1：在设备中的对外通信接口增加硬件的数据安全处理模块 103，也就是将原有的设备连接线缆接入硬件加密模块，然后再由加密模块引出新的通信接口，与主机的通信连接就使用该接口。

20 步骤 2：在 ATMC 上层软件 101 生成一对非对称密钥为：公钥为 A，私钥为 B，同时将公钥 A 导入到硬件设备中；在硬件设备通过硬件的数据安全处理模块 103 生成一对非对称密钥为：公钥为 C，私钥为 D，同时将 C 发送给 ATMC 软件。

数据加密通信过程描述：

25 步骤 1：ATMC 上层软件 101 将二进制命令数据传送给数据安全处理模块 102；

步骤 2：数据安全处理模块 102 首先在二进制命令数据复制到校验数据格式 201 的原始的二进制数据 205 缓存中，数据整理子模块 302 在此基础上按校验数据格式 201 增加时间信息 204，然后将时间信息 204 和原始的二进制数据 205 合并成数据体 202，并且进行 CRC 校验和运算，生成 CRC 校验运算结果

CRC203, 再将 CRC203 和数据体 202 合并生成校验数据格式 201。数据加密子模块 303 用私钥 B 将校验数据格式 201 的数据进行加密生成加密数据格式 206 的加密后的二进制数据 207 (以下简称数据 B'), 然后数据拆分子模块 304 分配一个包编号 212, 并将数据 B' 根据时钟产生一个随机数, 并且保证每个拆

5 分后的二进制数据 210 的字节大小不少于 20 个字节, 然后根据所产生的随机数进行切分数据块, 得到若干块拆分后的二进制数据 210, 在分后的二进制数据 210 的基础上增加分割包头 209 和分割包尾 211 (其中分割包头 209 包括包头标识 0xBF、包编号 212、块数 213 和块序号 214, 分割包尾 211 标识为 0xEF) 生成对应数量的分包数据格式 208 的数据包。然后将所生成的分包数据格式

10 208 的数据包按顺序通过串口或者 USB 传输给数据安全处理模块 103。

步骤 3: 数据安全处理模块 103 接收到传输过来的数据格式为分包数据格式 208 的通信数据, 数据安全处理模块 103 中的合并子模块 307 通过分析传过来的第一个分包数据格式 208 中的块数 213 和块序号 214 (其中块数 213 为分包的块数量, 块序号 214 为分包数据的块位置索引序号) 进行接收后续的同

15 分包数据格式 208 的数据包, 将相同包编号 212 的拆包数据格式 208 中的拆分后的二进制数据 210 合并数据, 得到加密数据格式 206 的数据 (以下简称数据 B'), 数据解密子模块 308 使用公钥 A 解密数据 B', 得到校验数据格式 201 的数据 B, 数据校验子模块 309 将数据 B 中的数据体 202 进行 CRC 校验和运算, 再与校验数据格式 201 中的 CRC203 进行校验, 如果结果不相符时就主动

20 拒绝将校验数据格式 201 中的原始的二进制数据 205 往硬件命令主控 104 发送, 如果校验的结果符合时, 校对数据合理性 (参考安全检查操作步骤), 如果不可理也会拒绝将校验数据格式 201 中的原始的二进制数据 204 往硬件命令主控 104 发送, 如果合理则将校验数据格式 201 中的原始的二进制数据 205 发送给硬件命令主控 104。

25 步骤 4: 硬件命令主控 104 接收到二进制数据后进行命令处理。硬件命令主控 104 处理完成命令后将结果数据返回给数据安全处理模块 103。

步骤 5: 数据安全处理模块 103 接收到返回的数据后, 将返回的数据复制到校验数据格式 215 的原始的二进制数据 219 缓存中, 然后数据整理子模块 302 在此基础上按校验数据格式 215 增加时间信息 218, 然后将时间信息 218

和原始的二进制数据 219 合并成数据体 216, 并且进行 CRC 校验和运算, 生成 CRC 校验运算结果 CRC217, 再将 CRC217 和数据体 216 合并生成校验数据格式 215。数据加密子模块 303 使用私钥 D, 将校验数据格式 215 的数据加密成加密数据格式 220 的加密后的二进制数据 221 (以下简称数据 D'), 然后

5 数据拆分子模块 304 分配一个包编号 226, 并将数据 D' 根据时钟产生一个随机数, 并且保证每个拆分后的二进制数据 224 的字节大小不少于 20 个字节, 然后根据所产生的随机数进行切分数据块, 得到若干块拆分后的二进制数据 224, 在分后的二进制数据 224 的基础上增加分割包头 223 和分割包尾 225 (其中分割包头 223 包括包头标识 0xBF、包编号 226、块数 227 和块序号 228, 分割包尾 225 标识为 0xEF) 生成对应数量的分包数据格式 222 的数据包。然后

10 将所生成的分包数据格式 222 的分割数据包按顺序通过串口或者 USB 传输给数据安全处理模块 102。

步骤 6: 数据安全处理模块 102 接收到传输过来的数据格式为分包数据格式 222 的通信数据, 数据安全处理模块 103 中的合并子模块 307 通过分析传过来的第一个分包数据格式 222 中的块数 227 和块序号 228 (其中块数 227 为分包的块数量, 块序号 228 为分包数据的块位置索引序号) 进行接收后续的相同

15 分包数据格式 222 的数据包, 将相同包编号 226 的拆包数据格式 222 中的拆分后的二进制数据 224 合并数据, 得到加密数据格式 220 的数据 (以下简称数据 D'), 数据解密子模块 308 使用公钥 C 解密数据 D', 得到校验数据格式 215

20 的数据 D, 数据校验子模块 309 将数据 D 中的数据体 216 进行 CRC 校验和运算, 再与校验数据格式 215 中的 CRC217 进行校验, 如果结果不相符时就主动拒绝将校验数据格式 215 中的原始的二进制数据 219 往 ATMC 上层软件 101 发送, 如果校验的结果符合时, 校对数据合理性 (参考安全检查操作步骤), 如果不可理也会拒绝将校验数据格式 215 中的原始的二进制数据 219 往 ATMC

25 上层软件 101 发送, 如果合理则将校验数据格式 215 中的原始的二进制数据 219 发送给 ATMC 上层软件 101。

步骤 7: ATMC 上层软件 101 收到二进制数据 D 后, 就可以得到由硬件设备返回的数据。此过程为一次完成的传输过程。

安全检查操作步骤:

-12-

步骤 1: 根据密钥生成过程的步骤生成数据安全处理模块 103 的密钥。

步骤 2: 将数据安全处理模块 103 主控程序烧入模块中。

步骤 3: 数据安全处理模块 103 在首次通电后, 数据安全处理模块 103 进入数据采样模式, 此时会自动记录该模块的命令组合和命令组合所对应的时间。

步骤 4: 采样完成后断开数据安全处理模块 103 的电源, 再次上电时就会进入正常工作模式。在此模式中, 首先会对来往的命令数据进行校验, 然后就是校验命令组合的合理性以及时间的合理性(其中时间的命令组合不应该超过 20% 毫秒的误差)。

步骤 5: 如果发生合理性异常, 数据安全处理模块 103 就会终止服务, 并记录其行为时间和数据内容, 以备后查。

上面主要描述了一种自助终端设备硬件的安全通信方法, 下面将对一种自助终端设备硬件的安全通信装置进行详细描述, 请参阅图 5, 本发明实施例中一种自助终端设备硬件的安全通信装置一个实施例包括:

本端 A5 和对端 B5;

该本端 A5 包括:

原始数据获取模块 501, 用于获取需要发送的原始数据;

加密模块 502, 用于对该原始数据加密, 得到加密数据;

随机切分模块 503, 用于生成随机数, 并根据该随机数将加密数据切分为

数据块;

数据包模块 504, 用于将该数据块一一打包, 生成对应的数据包;

传输模块 505, 用于将该数据包传输至该对端 B5;

该对端 B5 包括:

解析合并模块 506, 用于将该数据包解析并合并, 得到该加密数据;

解密模块 507, 用于对该加密数据解密, 得到该原始数据。

本实施例中, 首先, 原始数据获取模块 501 获取需要发送的原始数据; 加密模块 502 对该原始数据加密, 得到加密数据; 然后, 随机切分模块 503 生成随机数, 并根据该随机数将加密数据切分为数据块; 数据包模块 504 将该数据块一一打包, 生成对应的数据包; 接着, 传输模块 505 将该数据包传输至该对

-13-

端 B5; 对端 B5 接收到该数据包后, 解析合并模块 506 将该数据包解析并合并, 得到该加密数据; 最后, 解密模块 507 对该加密数据解密, 得到该原始数据。在本实施例中, 该自助终端设备硬件的安全通信装置在自助终端本地主机内实现, 无需联网验证, 并通过随机分包来提升通信的安全性, 防范了犯罪分子通过软件模拟设备硬件与主机通信进行金融犯罪。

为便于理解, 下面对本发明实施例中的一种自助终端设备硬件的安全通信装置进行详细描述, 请参阅图 6, 本发明实施例中一种自助终端设备硬件的安全通信装置另一个实施例包括:

本端 A6 和对端 B6;

10 该本端 A6 包括:

原始数据获取模块 601, 用于获取需要发送的原始数据;

加密模块 602, 用于对该原始数据加密, 得到加密数据;

随机切分模块 603, 用于生成随机数, 并根据该随机数将加密数据切分为数据块;

15 数据包模块 604, 用于将该数据块一一打包, 生成对应的数据包;

传输模块 605, 用于将该数据包传输至该对端 B6;

该对端 B6 包括:

解析合并模块 606, 用于将该数据包解析并合并, 得到该加密数据;

解密模块 607, 用于对该加密数据解密, 得到该原始数据。

20 本实施例中该随机切分模块 603 可以包括:

随机数生成单元 6031, 用于生成一个预设范围内的随机数;

数据切分单元 6032, 用于将该加密数据切分为该随机数个数据块。

本实施例中该安全通信装置还可以包括:

密钥生成模块 608, 用于预先生成一对非对称密钥, 包括公钥和私钥;

25 公钥导入模块 609, 用于将该公钥预先导入至该对端 B6;

该私钥用于对该原始数据加密, 该公钥用于对该加密数据解密。

本实施例中该加密模块 602 可以包括:

第一合并单元 6021, 用于将该原始数据和对应的时间信息合并成数据体;

第一校验运算单元 6022, 用于对该数据体进行校验运算, 得到第一运算

结果;

第二合并单元 6023, 用于将该数据体和该第一运算结果合并, 得到校验数据体;

加密单元 6024, 用于对该校验数据体加密, 得到加密数据;

5 该解密模块 607 包括:

解密单元 6071, 用于对该加密数据解密, 得到待测校验数据体;

第二校验运算单元 6072, 用于获取该待测校验数据体中的数据体, 并对获取到的数据体进行校验运算, 得到第二运算结果;

10 校验单元 6073, 用于校验该第二运算结果与该待测校验数据体中的第一运算结果是否相符;

数据获取单元 6074, 用于当该校验单元 6073 的校验结果为是时, 获取该数据体中的该原始数据。

本实施例中该对端 B6 还包括:

合理性检查模块 610, 用于对该原始数据进行数据合理性检查;

15 操作模块 611, 用于当该合理性检查模块 610 的检查通过时, 根据该原始数据进行操作。

所属领域的技术人员可以清楚地了解到, 为描述的方便和简洁, 上述描述的系统, 装置和单元的具体工作过程, 可以参考前述方法实施例中的对应过程, 在此不再赘述。

20 在本申请所提供的几个实施例中, 应该理解到, 所揭露的系统, 装置和方法, 可以通过其它的方式实现。例如, 以上所描述的装置实施例仅仅是示意性的, 例如, 所述单元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个系统, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直  
25 接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性, 机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是或者也可以不是物理单元, 即可以位于一个地方, 或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部

单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

## 权 利 要 求

1、一种自助终端设备硬件的安全通信方法，应用于所述自助终端的主机与设备硬件之间的通信，其特征在于，包括：

本端获取需要发送的原始数据；

5 所述本端对所述原始数据加密，得到加密数据；

所述本端生成随机数，并根据所述随机数将加密数据切分为数据块；

所述本端将所述数据块一一打包，生成对应的数据包；

所述本端将所述数据包传输至对端，使得所述对端将所述数据包解析并合并，得到所述加密数据，然后所述对端对所述加密数据解密，得到所述原始数据。

2、根据权利要求1所述的安全通信方法，其特征在于，所述本端生成随机数，并根据所述随机数将加密数据切分为数据块包括：

所述本端生成一个预设范围内的随机数；

所述本端将所述加密数据切分为所述随机数个数据块。

15 3、根据权利要求1所述的安全通信方法，其特征在于，所述安全通信方法还包括：所述本端预先生成一对非对称密钥，包括公钥和私钥，并将所述公钥预先导入至所述对端；

所述私钥用于对所述原始数据加密，所述公钥用于对所述加密数据解密。

20 4、根据权利要求1所述的安全通信方法，其特征在于，所述本端对所述原始数据加密，得到加密数据，具体包括：

所述本端将所述原始数据和对应的时间信息合并成数据体；

所述本端对所述数据体进行校验运算，得到第一运算结果；

所述本端将所述数据体和所述第一运算结果合并，得到校验数据体；

所述本端对所述校验数据体加密，得到加密数据；

25 所述对端对所述加密数据解密，得到所述原始数据，具体包括：

所述对端对所述加密数据解密，得到待测校验数据体；

所述对端获取所述待测校验数据体中的数据体，并对获取到的数据体进行校验运算，得到第二运算结果；

所述对端校验所述第二运算结果与所述待测校验数据体中的第一运算结

-17-

果是否相符，若相符，则获取所述数据体中的所述原始数据。

5、根据权利要求 4 所述的安全通信方法，其特征在于，所述对端在得到所述原始数据之后还包括：

所述对端对所述原始数据进行数据合理性检查，若检查通过，则所述对端

5 根据所述原始数据进行操作。

6、一种自助终端设备硬件的安全通信装置，应用于所述自助终端的主机与设备硬件之间的通信，其特征在于，包括本端和对端，所述本端包括：

原始数据获取模块，用于获取需要发送的原始数据；

加密模块，用于对所述原始数据加密，得到加密数据；

10 随机切分模块，用于生成随机数，并根据所述随机数将加密数据切分为数据块；

数据包模块，用于将所述数据块一一打包，生成对应的数据包；

传输模块，用于将所述数据包传输至所述对端；

所述对端包括：

15 解析合并模块，用于将所述数据包解析并合并，得到所述加密数据；

解密模块，用于对所述加密数据解密，得到所述原始数据。

7、根据权利要求 6 所述的安全通信装置，其特征在于，所述随机切分模块包括：

随机数生成单元，用于生成一个预设范围内的随机数；

20 数据切分单元，用于将所述加密数据切分为所述随机数个数据块。

8、根据权利要求 6 所述的安全通信装置，其特征在于，所述安全通信装置还包括：

密钥生成模块，用于预先生成一对非对称密钥，包括公钥和私钥；

公钥导入模块，用于将所述公钥预先导入至所述对端；

25 所述私钥用于对所述原始数据加密，所述公钥用于对所述加密数据解密。

9、根据权利要求 6 所述的安全通信装置，其特征在于，所述加密模块包括：

第一合并单元，用于将所述原始数据和对应的时间信息合并成数据体；

第一校验运算单元，用于对所述数据体进行校验运算，得到第一运算结果；

-18-

第二合并单元,用于将所述数据体和所述第一运算结果合并,得到校验数据体;

加密单元,用于对所述校验数据体加密,得到加密数据;

所述解密模块包括:

5 解密单元,用于对所述加密数据解密,得到待测校验数据体;

第二校验运算单元,用于获取所述待测校验数据体中的数据体,并对获取到的数据体进行校验运算,得到第二运算结果;

校验单元,用于校验所述第二运算结果与所述待测校验数据体中的第一运算结果是否相符;

10 数据获取单元,用于当所述校验单元的校验结果为是时,获取所述数据体中的所述原始数据。

10、根据权利要求9所述的安全通信装置,其特征在于,所述对端还包括:合理性检查模块,用于对所述原始数据进行数据合理性检查;

15 操作模块,用于当所述合理性检查模块的检查通过时,根据所述原始数据进行操作。

— 1/6 —

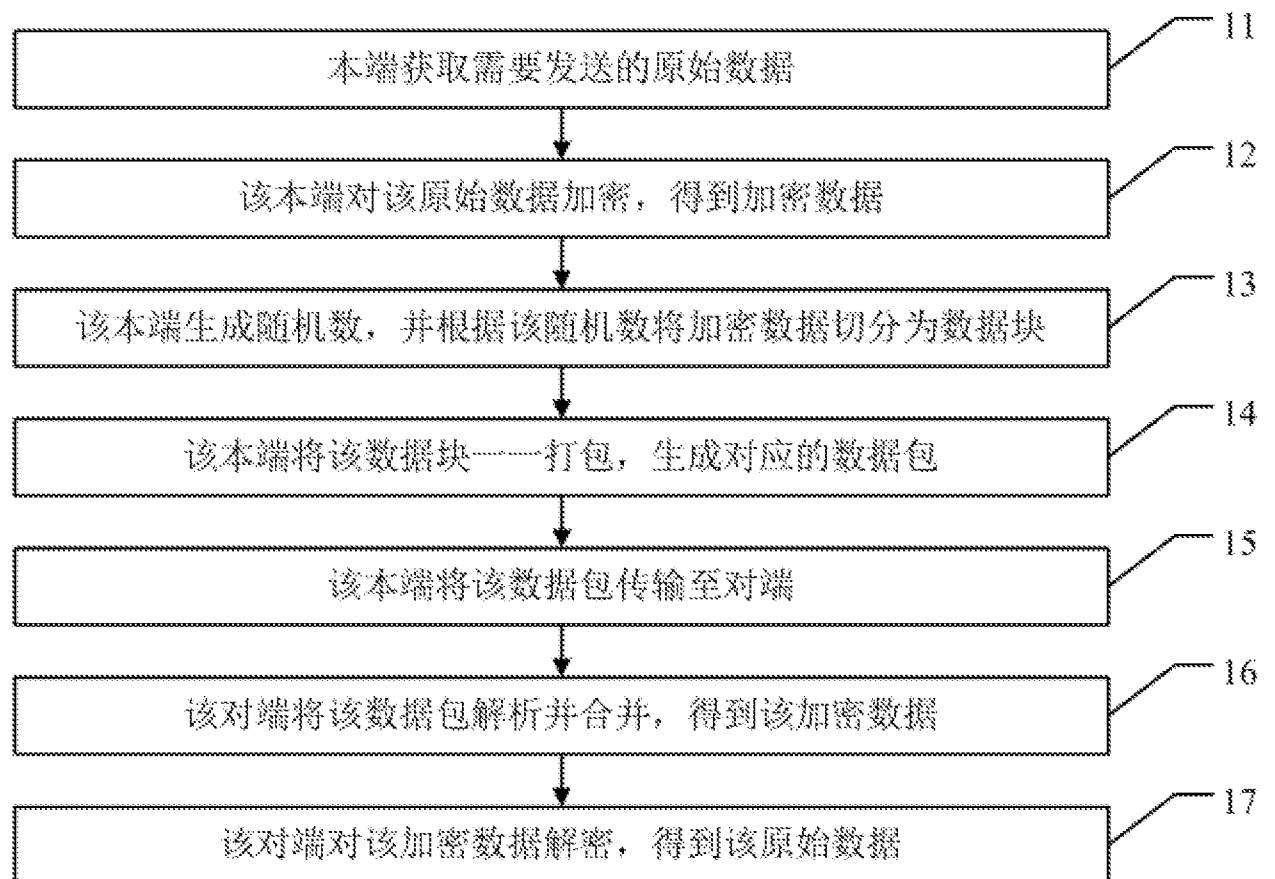


图 1

-2/6-

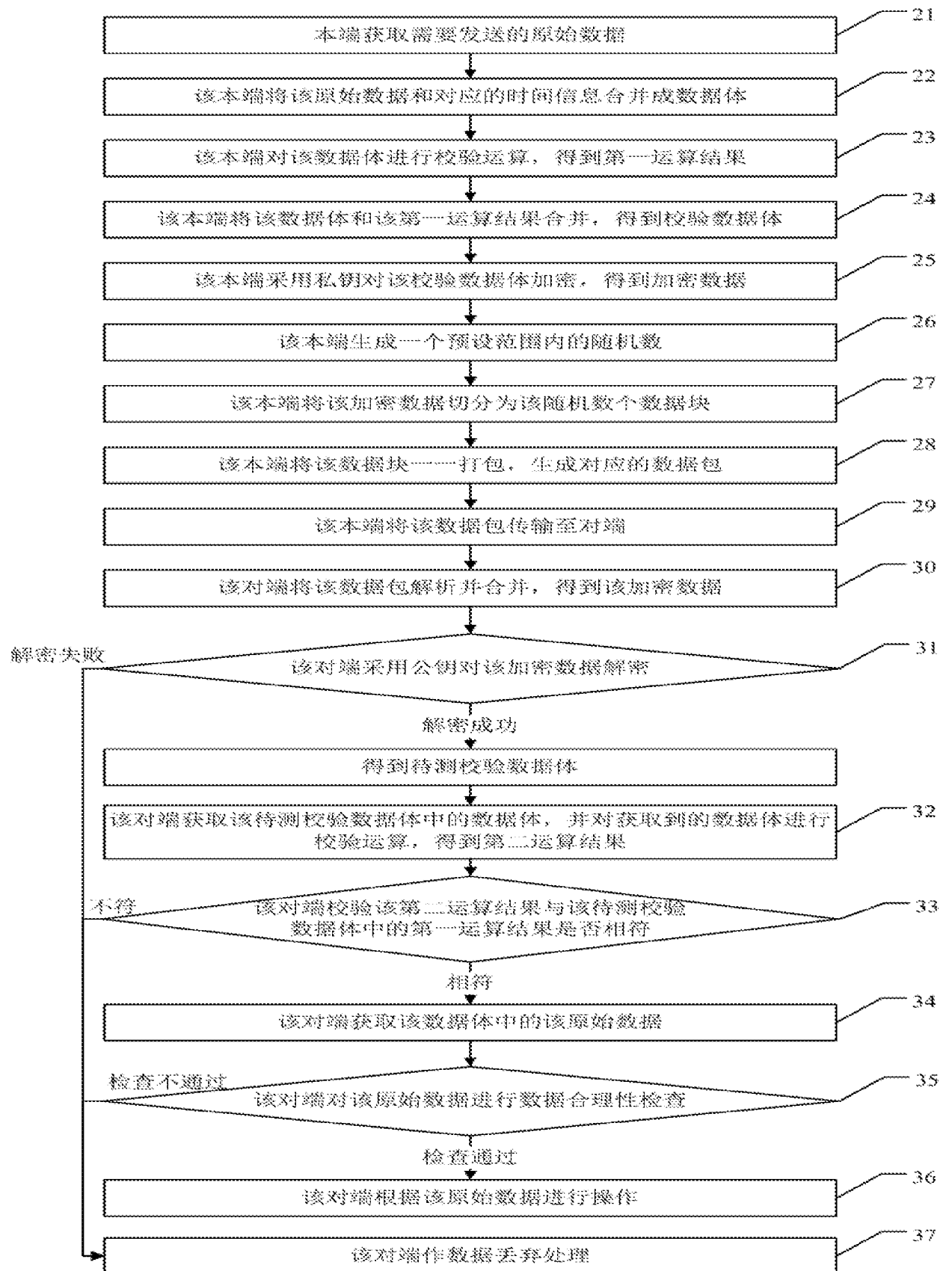


图 2

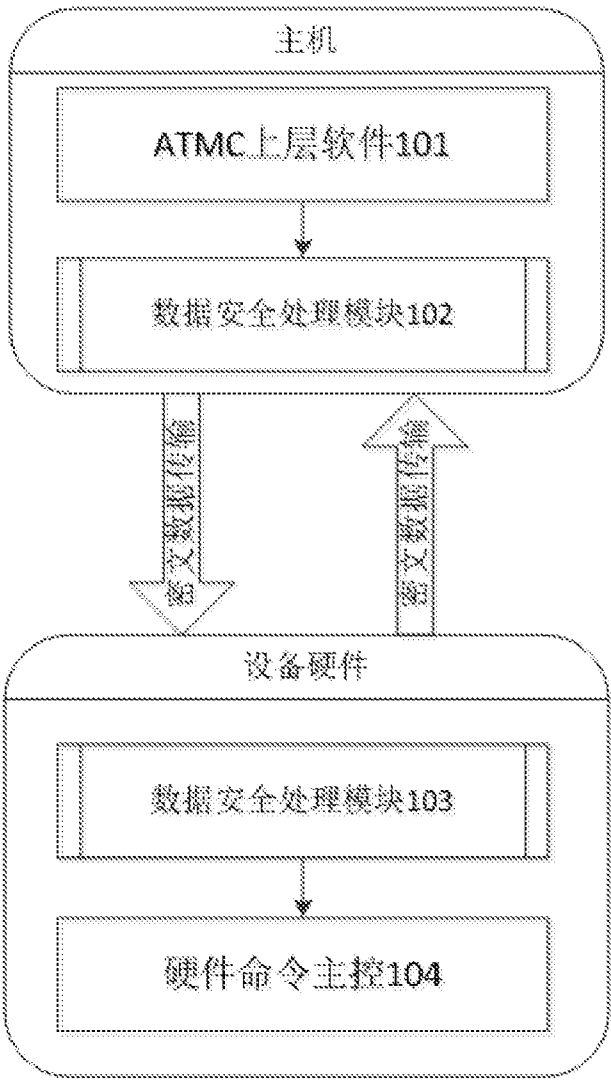


图 3

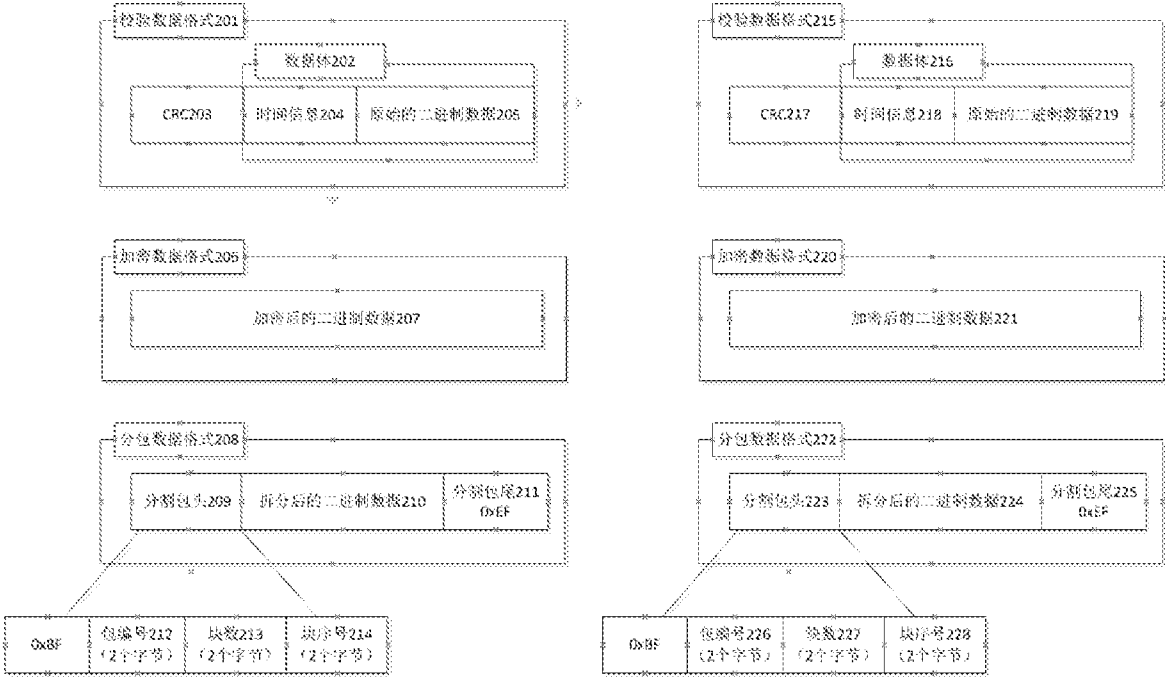


图 4

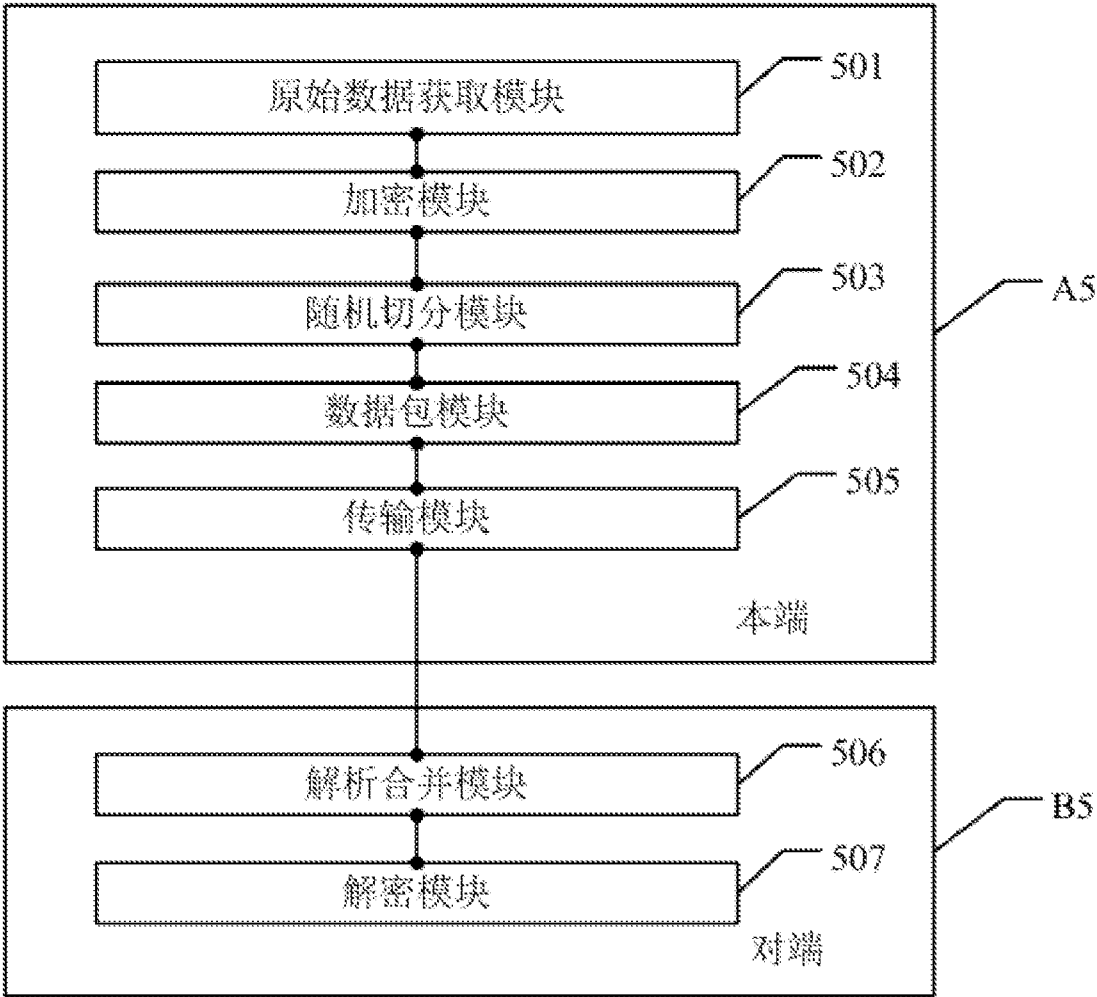


图 5

—6/6—

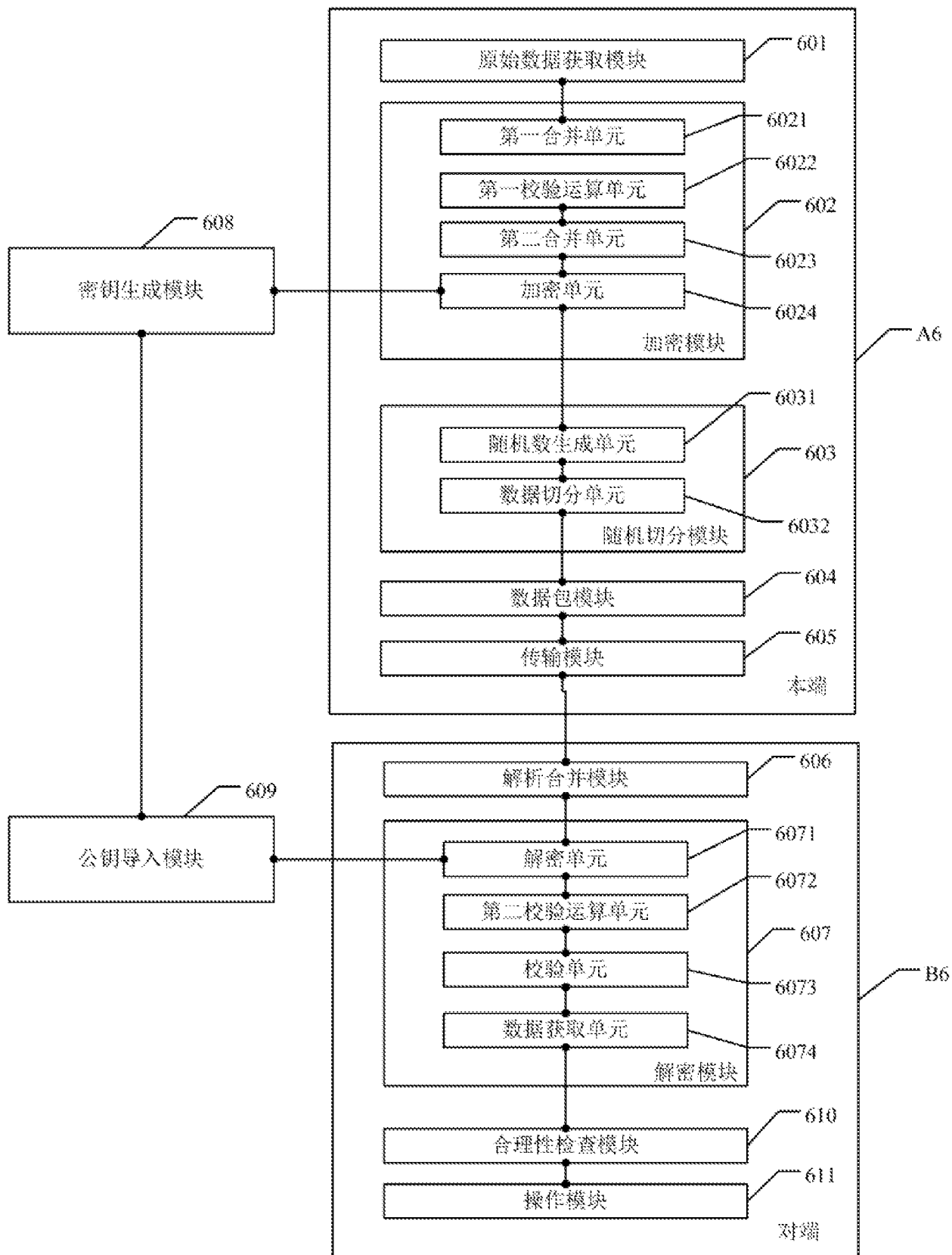


图 6

# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2016/077252**

## A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/85 (2013.01) 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)

CNPAT; CNKI; EPODOC; WPI; IEEE: automatic teller machine, self-help terminal, encryption, random number, cut, public key, asymmetric encryption, ATM, key, public, cryptograph, decode, random, divide, dissymmetrical, encapsulation, send

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                    | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | CN 104408834 A (HUNAN GREATWALL INFORMATION FINANCIAL EQUIPMENT CO., LTD. et al.), 11 March 2015 (11.03.2015), description, paragraphs [0008]-[0041], and figures 3-5 | 1-10                  |
| A         | CN 102135944 A (SHENZHEN HUAXIN ANCHUANG TECHNOLOGY CO., LTD.), 27 July 2011 (27.07.2011), the whole document                                                         | 1-10                  |
| A         | US 2012036355 A1 (KOREA ELECTRIC POWER CORPORATION), 09 February 2012 (09.02.2012), the whole document                                                                | 1-10                  |
| A         | CN 102932349 A (CHENGDU LEAD SOFTWARE TECHNOLOGY CO., LTD.), 13 February 2013 (13.02.2013), the whole document                                                        | 1-10                  |
| A         | CN 102332981 A (SHENZHEN VODATONE INDUSTRY CO., LTD.), 25 January 2012 (25.01.2012), 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<br>13 July 2016 (13.07.2016)                                                                                                                             | Date of mailing of the international search report<br><b>28 July 2016 (28.07.2016)</b> |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br><b>ZHANG, Cuiling</b><br>Telephone No.: (86-10) <b>62413373</b>  |

International application No.  
**PCT/CN2016/077252**

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

| <b>A. 主题的分类</b><br>G06F 21/85 (2013.01) i<br><br>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>B. 检索领域</b><br>检索的最低限度文献 (标明分类系统和分类号)<br>H04L; G06F<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>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))<br>CNPAT; CNKI; EPODOC; WPI; IEEE: 自动柜员机, 自助柜员机, 自助终端, 取款机, 密钥, 加密, 密文, 随机数, 分成, 切割, 分割, 划分, 公钥, 非对称加密, ATM, key, public, cryptograph, decode, random, divide, dissymmetrical, encapsulation, send                                                            |                                                                                                |                                              |
| <b>C. 相关文件</b>                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                |                                              |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                              | 引用文件, 必要时, 指明相关段落                                                                              | 相关的权利要求                                      |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 104408834 A (湖南长城信息金融设备有限责任公司 等) 2015年 3月 11日 (2015 - 03 - 11)<br>说明书第[0008]-[0041]段, 附图3-5 | 1-10                                         |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 102135944 A (深圳市华信安创科技有限公司) 2011年 7月 27日 (2011 - 07 - 27)<br>全文                             | 1-10                                         |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | US 2012036355 A1 (KOREA ELECTRIC POWER CORPORATION) 2012年 2月 9日 (2012 - 02 - 09)<br>全文         | 1-10                                         |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 102932349 A (成都主导软件技术有限公司) 2013年 2月 13日 (2013 - 02 - 13)<br>全文                              | 1-10                                         |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 102332981 A (深圳市沃达通实业有限公司) 2012年 1月 25日 (2012 - 01 - 25)<br>全文                              | 1-10                                         |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                              |                                                                                                |                                              |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“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)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“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<br>“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<br>“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<br>“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<br>“&” 同族专利的文件 |                                                                                                |                                              |
| 国际检索实际完成的日期<br><br>2016年 7月 13日                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                | 国际检索报告邮寄日期<br><br>2016年 7月 28日               |
| ISA/CN的名称和邮寄地址<br><br>中华人民共和国国家知识产权局 (ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10) 62019451                                                                                                                                                                                                                                                                                                 |                                                                                                | 授权官员<br><br>张翠玲<br><br>电话号码 (86-10) 62413373 |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2016/077252

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利            | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|-----------------|----------------|
| CN          | 104408834  | A  | 2015年 3月 11日   | 无               |                |
| CN          | 102135944  | A  | 2011年 7月 27日   | 无               |                |
| US          | 2012036355 | A1 | 2012年 2月 9日    | KR 101055843 B1 | 2011年 8月 9日    |
| CN          | 102932349  | A  | 2013年 2月 13日   | 无               |                |
| CN          | 102332981  | A  | 2012年 1月 25日   | 无               |                |