

(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



(10) 国际公布号

WO 2019/178787 A1

(43) 国际公布日

2019 年 9 月 26 日 (26.09.2019)

(51) 国际专利分类号:

H04L 9/32 (2006.01)

(21) 国际申请号:

PCT/CN2018/079903

(22) 国际申请日:

2018 年 3 月 21 日 (21.03.2018)

(25) 申请语言:

中文

(26) 公布语言:

中文

(71) 申请人: 深圳市汇顶科技股份有限公司 (SHENZHEN GOODIX TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。

(72) 发明人: 胡丽华 (HU, Lihua); 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。 冯守川 (FENG, Shouchuan); 中国广东省深圳市福田保税区腾飞工业大厦B座

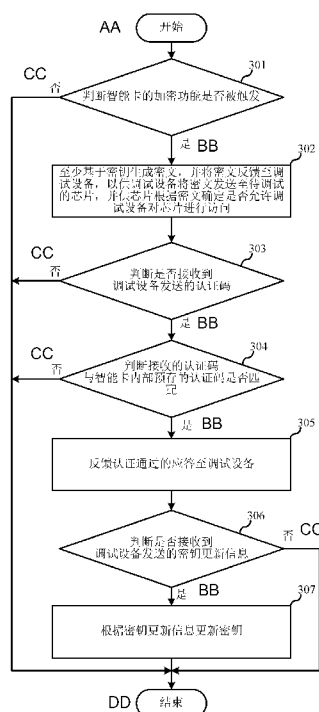
13层, Guangdong 518045 (CN)。 钟成志 (ZHONG, Chengzhi); 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。 朱明 (ZHU, Ming); 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。

(74) 代理人: 上海晨皓知识产权代理事务所 (普通合伙) (SHANGHAI CHENHAO INTELLECTUAL PROPERTY LAW FIRM GENERAL PARTNERSHIP); 中国上海市黄浦区制造局路787号二幢202B室, Shanghai 200011 (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: CHIP ACCESS METHOD, MICROCHIP, SMART CARD, AND DEBUGGING DEVICE

(54) 发明名称: 芯片的访问方法、微芯片、智能卡以及调试设备



- 301 Determine whether an encryption function of a smart card is triggered
302 Generate a ciphertext at least on the basis of a key, and feed back the ciphertext to a debugging device, so that the debugging device transmits the ciphertext to a chip to be debugged, and the chip determines, according to the ciphertext, whether the debugging device is allowed to access the chip
303 Determine whether an authentication code transmitted by the debugging device is received
304 Determine whether the received authentication code matches an authentication code prestored in the smart card
305 Feed back to the debugging device a response indicating that the authentication is passed
306 Determine whether key update information transmitted by the debugging device is received
307 Update the key according to the key update information
AA Start
BB Yes
CC No
DD End

图 4

(57) Abstract: A chip access method, a microchip, a smart card, and a debugging device. The chip access method comprises: determining whether an encryption function of a smart card is triggered (S301); if yes, generating a ciphertext on the basis of at least a key, and feeding back the ciphertext to a debugging device, so that the debugging device transmits the ciphertext to a chip to be debugged, and the chip determines, according to the ciphertext, whether the debugging device is allowed to access the chip (S302). Also provided are a microchip, a smart card, and a debugging device. The present method increases the security of the debugging device

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))。

when accessing the chip.

(57) 摘要: 一种芯片的访问方法、微芯片、智能卡以及调试设备。芯片的访问方法包括: 判断智能卡的加密功能是否被触发(S301); 若加密功能被触发, 则至少基于密钥生成密文, 并将密文反馈至调试设备, 以供调试设备将密文发送至待调试的芯片, 并供芯片根据密文确定是否允许调试设备对芯片进行访问(S302)。还提供了一种微芯片、智能卡以及调试设备。本方法提高了调试设备访问芯片时的安全性。

芯片的访问方法、微芯片、智能卡以及调试设备

技术领域

[0001] 本申请涉及芯片测试技术领域,特别涉及一种芯片的访问方法、微芯片、智能卡以及调试设备。

背景技术

[0002] 目前,在一些对安全性要求较高的使用场景下,例如指纹支付、安全门锁等,所使用的芯片的存储区域不能被随意访问;因此芯片出厂后,其调试功能一般是关闭的,在需要打开芯片的调试功能时需要进行安全认证,从而在一定程度上保证了调试环境的安全性,确保了芯片的存储区域的数据的安全性。

[0003] 当前常用算法认证的方式来打开芯片的调试功能,算法认证具体如下:调试设备内部预存有密钥,调试设备基于预存的该密钥生成密文并将密文发送至待调试的芯片;芯片根据该密文判断该调试设备是否安全。一般而言,调试设备包括主控端和微控制器,微控制器负责生成密钥;即,密钥存储微控制器的存储区,当需要生成密文时,微控制器将密钥从该微控制器的存储区调入该微控制器的加密区。

[0004] 发明人发现现有技术至少存在以下问题:微控制器的存储区和加密区并非是一个封闭的环境,微控制器生成密文时要从存储区域中将密钥调入加密区域中,若在这个过程中受到攻击则会导致密钥泄露。

发明内容

[0005] 本申请部分实施例的目的在于提供一种芯片的访问方法、微芯片、智能卡以及调试设备，提高了调试设备访问芯片时的安全性。

[0006] 本申请实施例提供了一种芯片的访问方法，应用于智能卡且智能卡内预存有密钥，方法包括：判断智能卡的加密功能是否被触发；若加密功能被触发，则至少基于密钥生成密文，并将密文反馈至调试设备，以供调试设备将密文发送至待调试的芯片，并供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0007] 本申请实施例又提供了一种芯片的访问方法，应用于调试设备，调试设备上插设有智能卡且智能卡内预存有密钥，方法包括：触发智能卡的加密功能，以供智能卡至少基于密钥生成密文；接收智能卡反馈的密文，并将密文发送至待调试的芯片，以供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0008] 本申请实施例还提供了一种微芯片，设置于智能卡内，且所述微芯片内预存有密钥；微芯片包括：判断单元，用于判断智能卡的加密功能是否被触发；加密单元，用于在判断单元判定智能卡的加密功能被触发时，至少基于密钥生成密文，并将密文反馈至调试设备，以供调试设备将密文发送至待调试的芯片，并供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0009] 本申请实施例还提供了一种智能卡，包括上述的微芯片。

[0010] 本申请实施例还提供了一种调试设备，包括：调试接口、智能卡插槽、控制模块以及存储器；控制模块连接于智能卡插槽和调试接口；调试接口还用于连接至待调试的芯片；存储器中储存有可被处理器执行的指令，指令被至少一个控制模块执行，当智能卡插槽内插入预存有密钥的智能卡时，指令被处理

器执行，以使处理器能够执行上述的芯片的访问方法。

[0011] 本申请实施例相对于现有技术而言，将密钥存储在智能卡中，由智能卡根据密钥生成芯片外部的密文，并由调试设备将密文发送到芯片，从而芯片可以根据密文确定是否允许调试设备对芯片进行访问；即密钥直接存储在智能卡中，由智能卡独立完成密文的生成，利用了智能卡安全性可靠的优点，提高了调试设备访问芯片时的安全性。

[0012] 另外，判断智能卡的加密功能是否被触发具体为，判断是否接收到调试设备发送过来的随机数；若是，则判定智能卡的加密功能被触发；其中随机数为调试设备从芯片获取的随机数；至少基于密钥生成密文具体为，基于密钥和随机数生成密文。本实施例中，智能卡基于密钥、以及芯片生成的随机数生成密文，进一步提升了芯片访问的安全性。

[0013] 另外，当接收到调试设备发送的密钥更新信息时，根据密钥更新信息更新密钥。本实施例中，由于不同芯片的密钥是可能是不同的，从而可以根据不同的芯片需求对智能卡中的密钥进行更新。

[0014] 另外，在接收到调试设备发送的密钥更新信息之前，还包括：当接收到调试设备发送的认证码时，判断接收的认证码与智能卡内部预存的认证码是否匹配；若判定结果为匹配，则反馈认证通过的应答至调试设备。本实施例中，当需要更新密钥时，进行认证码验证，更加安全。

[0015] 另外，在反馈认证通过的应答至调试设备之后，还包括：当接收到调试设备发送的认证码更新信息时，根据认证码更新信息更新智能卡内部预存的认证码。本实施例中，用户可以自主更换智能卡内部的认证码。

[0016] 另外，智能卡是基于 Java card 的智能卡。本实施例智能卡的一种具体类

型，同时基于 Java card 的智能卡便于实现加密算法。

附图说明

[0017] 一个或多个实施例通过与之对应的附图中的图片进行示例性说明，这些示例性说明并不构成对实施例的限定，附图中具有相同参考数字标号的元件表示为类似的元件，除非有特别申明，附图中的图不构成比例限制。

[0018] 图 1 是根据本申请第一实施例中的芯片的访问方法的具体流程图；

[0019] 图 2 是根据本申请第二实施例中的芯片的访问方法的具体流程图；

[0020] 图 3 是根据本申请第二实施例中的调试设备、芯片以及智能卡交互过程的示意图；

[0021] 图 4 是根据本申请第三实施例中的芯片的访问方法的具体流程图；

[0022] 图 5 是根据本申请第四实施例中的芯片的访问方法的具体流程图；

[0023] 图 6 是根据本申请第五实施例中的芯片的访问方法的具体流程图；

[0024] 图 7 是根据本申请第六实施例中的芯片的访问方法的具体流程图；

[0025] 图 8 是根据本申请第七实施例中的芯片的访问方法的具体流程图；

[0026] 图 9 是根据本申请第八实施例中的芯片的访问方法的具体流程图；

[0027] 图 10 是根据本申请第九实施例中的微芯片的方框示意图；

[0028] 图 11 是根据本申请第十一实施例中的微芯片的方框示意图；

[0029] 图 12 是根据本申请第十二实施例中的微芯片的方框示意图；

[0030] 图 13 是根据本申请第十三实施例中的调试设备的方框示意图；

[0031] 图 14 是根据本申请第十三实施例中的调试设备的方框示意图，其中控制模块包括主控端与微控制器。

具体实施方式

[0032] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请部分实施例进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0033] 本申请第一实施例涉及一种芯片的访问方法，应用于智能卡；即，本实施例的芯片访问方法，为调试设备对芯片进行访问时，智能卡所做的处理方法。智能卡内预存有密钥以及加密算法，以实现智能卡的加密功能，其中密钥一般放在智能卡的非易失性存储区域中。智能卡可以为基于 Java card 的智能卡，以便于加密算法的实现；基于 Java card 的智能卡包含一个裁剪过的 Java 虚拟机，加密算法作为 Java Applet 运行在基于 Java card 的智能卡的内部。本实施例中选取的加密算法为 Present 算法，其更便于硬件实现，然不限于此，也可以根据需求选取其他的加密算法。

[0034] 本实施例中的待调试的芯片可以安装在嵌入式开发板上，且嵌入式开发板上包括与芯片连接的一个调试接口；调试设备也包括另一个调试接口，且调试设备与芯片通过两个调试接口连接。其中，调试设备可以为 JTAG (Joint Test Action Group, 国际标准测试协议，简称“JTAG”) 设备，此时，调试接口为 JTAG 接口；另外，调试设备上可以设置有卡槽，智能卡通过卡槽插在调试设备中。本实施例中，调试设备可以包括个人电脑 PC 和微控制器，PC 连接于芯片且通过微控制器连接至智能卡。

[0035] 本实施例的芯片的访问方法的具体流程如图 1 所示。

[0036] 步骤 101，判断智能卡的加密功能是否被触发。若是，则进入步骤 102；若否，则直接结束。

[0037] 调试设备可以触发智能卡的加密功能。具体的，当调试设备通过调试接口与芯片连接并检测到芯片后，调试设备控制启动智能卡（包括复位、初始化等操作），随后调试设备发送一个触发指令至智能卡，当智能卡接收到触发指令后，加密功能被触发，进入步骤 102；若智能卡没有接收到触发指令，则智能卡的加密功能没有被触发，直接结束。

[0038] 步骤 102，至少基于密钥生成密文，并将密文反馈至调试设备，以供调试设备将密文发送至待调试的芯片，并供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0039] 在一个例子中，智能卡内部还预存有待加密的预设数值，智能卡可以基于该预设数值与该密钥生成密文，即智能卡运行预设的加密算法，利用该密钥对该预设数值进行加密以生成密文。随后，智能卡将密文反馈至调试设备，且调试设备将密文发送至待调试的芯片。

[0040] 芯片中存有密钥，智能卡中预存的密钥与芯片中的密钥相同，芯片至少基于该密钥生成密文；对应的，芯片内部还预存有上述预设数值（与智能卡中的预设数值相同），芯片基于该预设数值与该密钥生成密文，即芯片运行预设的加密算法（与智能卡中的加密算法相同），利用该密钥对该预设数值进行加密以生成密文。当芯片判定接收到的调试设备发送的密文与自身生成的密文相同时，则芯片确定允许调试设备对芯片进行访问，即，允许调试设备打开芯片的调试功能。

[0041] 需要说明的是，本实施例中，当芯片判定接收到的调试设备发送的密文与自身生成的密文相同时，确定允许调试设备对芯片进行访问，然不限于此，还可以是芯片根据接收到的密文是否和芯片中预存的密文相同，来确定是否允

许调试设备对芯片进行访问；或者，芯片根据密文是否携带芯片的正确型号，来确定是否允许调试设备对芯片进行访问；或者，芯片根据密文是否为某种预设类型的信息，来确定是否允许调试设备对芯片进行访问，其中类型可以为文字、数字、字母、符号或其任意组合。

[0042] 本实施例相对于现有技术而言，将密钥存储在智能卡中，由智能卡根据密钥生成芯片外部的密文，并由调试设备将密文发送到芯片，从而芯片可以根据密文确定是否允许调试设备对芯片进行访问；即密钥直接存储在智能卡中，由智能卡独立完成密文的生成，利用了智能卡安全性可靠的优点，提高了调试设备访问芯片时的安全性。

[0043] 本申请第二实施例涉及一种芯片的访问方法，本实施例是在第一实施例基础上的改进，主要改进之处在于：智能卡基于密钥与随机数生成密文。

[0044] 本实施例的芯片的访问方法的具体流程如图 2 所示。

[0045] 步骤 201，判断是否接收到调试设备发送过来的随机数；若是，则进入步骤 202；若否，则直接结束。

[0046] 步骤 202，基于密钥和随机数生成密文，并将密文反馈至调试设备，以供调试设备将密文发送至待调试的芯片，并供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0047] 请参考图 3，具体而言，芯片生成一个用于安全认证的随机数，PC 从芯片获取该随机数，并通过微控制器将该随机数发送到智能卡，当智能卡接收到微控制器发送过来的随机数时，智能卡的加密功能被触发。

[0048] 智能卡的加密功能被触发后，智能卡基于密钥和随机数生成密文，随后智能卡将密文反馈至调试设备的微控制器，然后调试设备通过 PC 将密文发送

至待调试的芯片。

[0049] 芯片中存有密钥，智能卡中预存的密钥与芯片中的密钥相同，芯片基于密钥与随机数生成密文，当芯片判定接收到的调试设备发送的密文与自身生成的密文相同时，则芯片确定允许调试设备对芯片进行访问，即，允许调试设备打开芯片的调试功能。

[0050] 本实施例中，随机数可以为字符类型和数字类型两种类型的随机数，字符类型可随机生成任意长度的字符串，而数字类型则是生成一定范围内的数字，在生成随机数时，还可以选择允许重复或不允许重复。

[0051] 本实施例相对于第一实施例而言，智能卡基于密钥、以及芯片生成的随机数生成密文，进一步提升了芯片访问的安全性。

[0052] 本申请第三实施例涉及一种芯片访问方法，本实施例是在第一实施例基础上的改进，主要改进之处在于：智能卡中的密钥可以进行更新。

[0053] 本实施例的芯片的访问方法的具体流程如图 4 所示。

[0054] 其中，步骤 301、步骤 302 与步骤 101、步骤 102 大致相同，主要不同之处在于，本实施例中增加了步骤 303 至步骤 307，具体如下：

[0055] 步骤 303，判断是否接收到调试设备发送的认证码。若是，则进入步骤 404；若否，则直接结束。

[0056] 具体而言，芯片出厂时，不同的芯片中烧写的密钥可能是不同的，为了使智能卡中的密钥与待调试的芯片中的密钥保持一致，需要更新智能卡的密钥；在更新智能卡的密钥之前，通过调试设备发送认证码到智能卡；当智能卡接收到调试设备发送的认证码时，则说明用户需要更新智能卡的密钥，进入步骤 304；否则，则说明用户不需要更新智能卡的密钥，直接结束。

[0057] 步骤 304，判断接收的认证码与智能卡内部预存的认证码是否匹配。

[0058] 具体而言，智能卡内部预存有认证码，当智能卡接收到的认证码与其内部预存的认证码匹配时，则说明验证通过，进入步骤 305；否则，则说明验证不通过，直接结束，或者请求调试设备重新发送认证码。

[0059] 步骤 305，反馈认证通过的应答至调试设备。

[0060] 具体而言，智能卡反馈认证通过的应答给调试设备，允许调试设备对智能卡进行密钥更新。

[0061] 步骤 306，判断是否接收到调试设备发送的密钥更新信息。若是，则进入步骤 307；若否，则直接结束。

[0062] 其中，密钥更新信息包含一个新的密钥，该密钥与新的待调试的芯片的密钥相同。在一个例子中，用户可以通过调试设备设定该新的密钥，调试设备根据新的密钥生成密钥更新信息，并将该密钥更新信息发送到智能卡，当智能卡接收到调试设备发送的密钥更新信息时，进入步骤 307；否则，则直接结束。

[0063] 步骤 307，根据密钥更新信息更新密钥。

[0064] 具体而言，智能卡从密钥更新信息中获取新的密钥，并用该新的密钥替换智能卡中原来的密钥，从而使得智能卡中的密钥与芯片中的密钥保持一致。

[0065] 需要说明的是，本实施例中在更新智能卡的密钥时(步骤 306、步骤 307)，对认证码进行验证(步骤 304 至步骤 306)，更加安全；然不限于此，本实施例中也可以不对认证码进行验证，直接更新智能卡的密钥。

[0066] 还需要说明的是，步骤 303 至步骤 307，与步骤 301、步骤 302 并无明显的先后关系，即，本实施例中，只要接收到调试设备发送的密钥更新信息，便可以根据密钥更新信息更新密钥，本实施例只是提供一个例子，在实际应用中

并不以此为限。

[0067] 本实施例相对于第一实施例而言，由于不同芯片的密钥可能是不同的，从而可以根据不同的芯片需求对智能卡中的密钥进行更新。需要说明的是，本实施例也可以作为在第二实施例基础上的改进，可以达到同样的技术效果。

[0068] 本申请第四实施例涉及一种芯片访问方法，本实施例是在第一实施例基础上的改进，主要改进之处在于：用户可以自主更换智能卡内部的认证码。

[0069] 本实施例的芯片的访问方法的具体流程如图 5 所示。

[0070] 其中，步骤 401、步骤 402 与步骤 101、步骤 102 大致相同，主要不同之处在于，本实施例中增加了步骤 403 至步骤 407，具体如下：

[0071] 步骤 403，判断是否接收到调试设备发送的认证码。若是，则进入步骤 404；若否，则直接结束。

[0072] 具体而言，智能卡出厂时，其内部会预设有初始的认证码，当需要更新智能卡的认证码时，调试设备发送认证码到智能卡；当智能卡接收到调试设备发送的认证码时，进入步骤 404；否则，直接结束。

[0073] 步骤 404，判断接收的认证码与智能卡内部预存的认证码是否匹配。

[0074] 具体而言，智能卡内部预存有认证码，当智能卡接收到的认证码与其内部预存的认证码匹配时，则说明验证通过，进入步骤 405；否则，则说明验证不通过，直接结束，或者请求调试设备重新发送认证码。

[0075] 步骤 405，反馈认证通过的应答至调试设备。

[0076] 具体而言，智能卡反馈认证通过的应答给调试设备，允许调试设备对智能卡进行认证码更新。

[0077] 步骤 406，判断是否接收到调试设备发送的认证码更新信息。若是，则

进入步骤 407；若否，则直接结束。

[0078] 其中，认证码更新信息中包含新的认证码。在一个例子中，用户可以通过调试设备自定义设定一个新的认证码，调试设备根据新的认证码生成认证码更新信息，并将该认证码更新信息发送到智能卡，当智能卡接收到调试设备发送的认证码更新信息时，进入步骤 407；否则，直接结束。

[0079] 步骤 407，根据认证码更新信息更新智能卡内部预存的认证码。

[0080] 具体而言，智能卡从认证码更新信息中获取新的认证码，并用该新的认证码替换智能卡中原来的认证码。

[0081] 需要说明的是步骤 403 至步骤 407，与步骤 401、步骤 402 并无明显的先后关系，本实施例只是提供一个例子，在实际应用中并不以此为限。

[0082] 本实施例相对于第一实施而言，用户可以自主更换智能卡内部的认证码。需要说明的是，本实施例也可以作为在第二实施例或第三实施例基础上的改进，可以达到同样的技术效果。

[0083] 本申请第五实施例涉及一种芯片的访问方法，应用于调试设备，即，本实施例的芯片访问方法，为调试设备对芯片进行访问时，调试设备所做的处理方法。

[0084] 本申请第五实施例的芯片的访问方法的具体流程如图 6 所示。

[0085] 步骤 501，触发智能卡的加密功能，以供智能卡至少基于密钥生成密文。

[0086] 具体而言，调试设备可以触发智能卡的加密功能，具体的，当调试设备通过调试接口与芯片连接并检测到芯片后，调试设备控制启动智能卡（包括复位、初始化等操作），随后调试设备发送一个触发指令至智能卡，智能卡接收到触发指令后加密功能被触发，至少基于密钥生成密文。

[0087] 在一个例子中，智能卡内部还预存有待加密的预设数值，智能卡可以基于该预设数值与该密钥生成密文，即智能卡运行预设的加密算法，利用该密钥对该预设数值进行加密以生成密文。

[0088] 步骤 502，接收智能卡反馈的密文，并将密文发送至待调试的芯片，以供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0089] 具体而言，智能卡生成密文后，会将密文反馈至调试设备，调试设备将接收的智能卡反馈的密文发送至待调试的芯片；芯片中存有密钥，智能卡中预存的密钥与芯片中的密钥相同，芯片至少基于该密钥生成密文。对应的，芯片内部还预存有上述预设数值（与智能卡中的预设数值相同），芯片基于该预设数值与该密钥生成密文，即芯片运行预设的加密算法（与智能卡中的加密算法相同），利用该密钥对该预设数值进行加密以生成密文。当芯片判定接收到的调试设备发送的密文与自身生成的密文相同时，则芯片确定允许调试设备对芯片进行访问，即，芯片打开自身的调试功能。

[0090] 不难发现，本实施例中的芯片的访问方法应用于调试设备，第一实施例中的芯片的访问方法应用于智能卡，本实施例可以与第一实施例互相配合实施。第一实施例中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第一实施例中。

[0091] 本实施例相对于现有技术而言，将密钥存储在智能卡中，由智能卡根据密钥生成芯片外部的密文，并由调试设备将密文发送到芯片，从而芯片可以根据密文确定是否允许调试设备对芯片进行访问；即密钥直接存储在智能卡中，由智能卡独立完成密文的生成，利用了智能卡安全性可靠的优点，提高了调试

设备访问芯片时的安全性。

[0092] 本申请第六实施例涉及一种芯片的访问方法，本实施例是在第五实施例基础上的改进，主要改进之处在于：智能卡基于密钥与随机数生成密文。

[0093] 本实施例的芯片的访问方法的具体流程如图 7 所示。

[0094] 步骤 601，触发芯片的安全认证功能，并从芯片获取用于安全认证的随机数。

[0095] 步骤 602，将随机数发送至智能卡，以触发智能卡的加密功能，以供智能卡基于智能卡内部预存的密钥和随机数生成密文。

[0096] 步骤 603，接收智能卡反馈的密文，并将密文发送至待调试的芯片，以供芯片根据密文确定是否允许调试设备对芯片进行访问。

[0097] 请参考图 3，具体而言，当调试设备要对芯片进行调试时，需要打开芯片的调试功能时，此时便会触发芯片的安全认证功能，芯片的安全认证功能被触发后，会产生一个用于安全认证的随机数，PC 从芯片获取该随机数。

[0098] PC 通过微控制器将从芯片获取的随机数发送到智能卡，当智能卡接收到微控制器发送过来的随机数时，智能卡的加密功能被触发，此时，智能卡基于智能卡内部预存的密钥和随机数生成密文。

[0099] 智能卡生成密文后，会将密文反馈至调试设备的微控制器，然后调试设备通过 PC 将密文发送至待调试的芯片；芯片中存有密钥，智能卡中预存的密钥与芯片中的密钥相同，芯片基于密钥与随机数生成密文，当芯片判定接收到的调试设备发送的密文与自身生成的密文相同时，则芯片确定允许调试设备对芯片进行访问，即，调试设备打开芯片的调试功能。

[00100] 不难发现，本实施例中的芯片的访问方法应用于调试设备，第二实施例

中的芯片的访问方法应用于智能卡，本实施例可以与第二实施例互相配合实施。第二实施例中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第二实施例中。

[00101] 本实施例相对于第五实施例而言，智能卡基于密钥、以及芯片生成的随机数生成密文，进一步提升了芯片访问的安全性。

[00102] 本申请第七实施例涉及一种芯片访问方法，本实施例是在第五实施例基础上的改进，主要改进之处在于：智能卡中的密钥可以进行更新。

[00103] 本实施例的芯片的访问方法的具体流程如图 8 所示。

[00104] 其中，步骤 701、步骤 702 与步骤 501、步骤 502 大致相同，主要不同之处在于，本实施例中增加了步骤 703 与步骤 704，具体如下：

[00105] 步骤 703，将认证码发送至智能卡，以供智能卡判断接收的认证码与智能卡内部预存的认证码是否匹配，并在判定匹配时反馈认证通过的应答至调试设备。

[00106] 具体而言，芯片出厂时，不同的芯片中烧写的密钥可能是不同的，为了使智能卡中的密钥与待调试的芯片中的密钥保持一致，需要对智能卡中的密钥进行更新。在更新智能卡的密钥之前，通过调试设备发送认证码到智能卡，智能卡内部预存有认证码，当智能卡接收到的认证码与其内部预存的认证码匹配时，则说明验证通过，反馈认证通过的应答给调试设备，允许调试设备对智能卡进行密钥更新。

[00107] 步骤 704，将密钥更新信息发送至智能卡，以供智能卡根据密钥更新信息更新密钥。

[00108] 具体而言，调试设备在接收到认证通过的应答时，将密钥更新信息发送至智能卡，密钥更新信息包含一个新的密钥，该密钥与待调试的芯片的密钥相同；在一个例子中，用户可以通过调试设备设定一个新的密钥，调试设备根据新的密钥生成密钥更新信息，并将该密钥更新信息发送到智能卡，智能卡接收到调试设备发送的密钥更新信息后，从密钥更新信息中获取新的密钥，并用该新的密钥替换智能卡中原来的密钥，从而使得智能卡中的密钥与芯片中的密钥保持一致。

[00109] 需要说明的是，本实施例中在更新智能卡的密钥时（步骤 704），对认证码进行验证（步骤 703），从而更加安全；然不限于此，本实施例中也可以不对认证码进行验证，直接更新智能卡的密钥。

[00110] 还需要说明的是，步骤 703、步骤 704，与步骤 701、步骤 702 并无明显的先后关系，即，本实施例中，只要需要更新密钥时，将密钥更新信息发送至智能卡，以供智能卡根据密钥更新信息更新密钥，本实施例只是提供一个例子，在实际应用中并不以此为限。

[00111] 不难发现，本实施例中的芯片的访问方法应用于调试设备，第三实施例中的芯片的访问方法应用于智能卡，本实施例可以与第三实施例互相配合实施。第三实施例中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第三实施例中。

[00112] 本实施例相对于第五实施例而言，由于不同芯片的密钥是不同的，从而可以根据不同的芯片需求对智能卡中的密钥进行更新。需要说明的是，本实施例也可以作为在第六实施例基础上的改进，可以达到同样的技术效果。

[00113] 本申请第八实施例涉及一种芯片访问方法，本实施例是在第七实施例基础上的改进，主要改进之处在于：用户可以自主更换智能卡内部的认证码。

[00114] 本实施例的芯片的访问方法的具体流程如图 9 所示。

[00115] 其中，步骤 801、步骤 802 与步骤 501、步骤 502 大致相同，主要不同之处在于，本实施例中增加了步骤 803 与步骤 804，具体如下：

[00116] 步骤 803，将认证码发送至智能卡，以供智能卡判断接收的认证码与智能卡内部预存的认证码是否匹配，并在判定匹配时反馈认证通过的应答至调试设备。

[00117] 具体而言，智能卡出厂时，其内部会预设有初始的认证码，当用户需要更新智能卡的认证码时，通过调试设备发送认证码到智能卡，智能卡内部预存有认证码，当智能卡接收到的认证码与其内部预存的认证码匹配时，则说明验证通过，智能卡反馈认证通过的应答给调试设备，允许调试设备对智能卡进行认证码更新。

[00118] 步骤 804，在接收到认证通过的应答时，发送认证码更新信息至智能卡，以供智能卡根据认证码更新信息更新智能卡内部预存的认证码。

[00119] 具体而言，调试设备在接收到智能卡反馈的认证通过的应答时，发送认证码更新信息至智能卡；认证码更新信息中包含新的认证码。在一个例子中，用户可以通过调试设备自定义设定一个新的认证码，调试设备根据新的认证码生成认证码更新信息，并将该认证码更新信息发送到智能卡，当智能卡接收到调试设备发送的认证码更新信息时，从认证码更新信息中获取新的认证码，并用该新的认证码替换智能卡中原来的认证码。

[00120] 需要说明的是步骤 803、步骤 804，与步骤 801、步骤 802 并无明显的

先后关系，本实施例只是提供一个例子，在实际应用中并不以此为限。

[00121] 不难发现，本实施例中的芯片的访问方法应用于调试设备，第四实施例中的芯片的访问方法应用于智能卡，本实施例可以与第四实施例互相配合实施。第四实施例中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第四实施例中。

[00122] 本实施例相对于第五实施例而言，用户可以自主更换智能卡内部的认证码。需要说明的是，本实施例也可以作为在第六至第八实施例中任一项的基础上的改进，可以达到同样的技术效果。

[00123] 本申请第九实施例涉及一种微芯片，设置于智能卡内，且所述微芯片内预存有密钥，智能卡为基于 Java card 的智能卡。请参考图 10，微芯片包括判断单元 1、加密单元 2。

[00124] 判断单元 1 用于判断智能卡的加密功能是否被触发；

[00125] 加密单元 2 用于在判断单元判定智能卡的加密功能被触发时，至少基于密钥生成密文，并将密文反馈至调试设备，以供调试设备将密文发送至待调试的芯片，并供芯片根据密文确定是否允许调试设备对芯片进行访问。

[00126] 不难发现，本实施例与第一实施例相对应，本实施例可以与第一实施例互相配合实施。第一实施例中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第一实施例中。

[00127] 本实施例相对于现有技术而言，将密钥存储在智能卡中，由智能卡根据密钥生成芯片外部的密文，并由调试设备将密文发送到芯片，从而芯片可以根

据密文确定是否允许调试设备对芯片进行访问；即密钥直接存储在智能卡中，由智能卡独立完成密文的生成，利用了智能卡安全性可靠的优点，提高了调试设备访问芯片时的安全性。

[00128] 本申请第十实施例涉及一种微芯片，本实施例是在第十实施例基础上的改进，主要改进之处在于：请参考图 10，加密单元 2 基于密钥与随机数生成密文。

[00129] 判断单元 1 具体用于判断是否接收到调试设备发送过来的随机数；若是，则判定智能卡的加密功能被触发；其中随机数为调试设备从芯片获取的随机数。

[00130] 加密单元 2 具体用于基于密钥和随机数生成密文。

[00131] 不难发现，本实施例与第二实施例相对应，本实施例可以与第二实施例互相配合实施。第二实施例中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第二实施例中。

[00132] 本实施例相对于第十实施例而言，智能卡基于密钥、以及芯片生成的随机数生成密文，进一步提升了芯片访问的安全性。

[00133] 本申请第十一实施例涉及一种微芯片，本实施例是在第十实施例基础上的改进，主要改进之处在于：请参考图 11，微芯片还包括密钥更新单元 3。

[00134] 密钥更新单元 3 用于在接收到调试设备发送的密钥更新信息时，根据密钥更新信息更新密钥。

[00135] 较佳的，微芯片还包括认证单元 4，认证单元 4 用于在接收到调试设备发送的认证码时，判断接收的认证码与智能卡内部预存的认证码是否匹配；若判定结果为匹配，则反馈认证通过的应答至调试设备。

[00136] 密钥更新单元 3 具体用于在认证单元反馈了认证通过的应答后,允许接收密钥更新信息。

[00137] 不难发现,本实施例与第三实施例相对应,本实施例可以与第三实施例互相配合实施。第三实施例中提到的相关技术细节在本实施例中依然有效,为了减少重复,这里不再赘述。相应地,本实施例中提到的相关技术细节也可应用在第三实施例中。

[00138] 本实施例相对于第九实施例而言,由于不同芯片的密钥是不同的,从而可以根据不同的芯片需求对智能卡中的密钥进行更新。需要说明的是,本实施例也可以作为在第十实施例基础上的改进,可以达到同样的技术效果。

[00139] 本申请第十二实施例涉及一种微芯片,本实施例是在第十一实施例基础上的改进,主要改进之处在于:请参考图 12,微芯片还包括认证码更新单元 5。

[00140] 认证码更新单元 5 用于在认证单元 4 反馈了认证通过的应答后,允许接收调试设备发送的认证码更新信息,并在接收到认证码更新信息时,根据认证码更新信息更新智能卡内部预存的认证码。

[00141] 不难发现,本实施例与第四实施例相对应,本实施例可以与第四实施例互相配合实施。第四实施例中提到的相关技术细节在本实施例中依然有效,为了减少重复,这里不再赘述。相应地,本实施例中提到的相关技术细节也可应用在第四实施例中。

[00142] 本实施例相对于第十一实施而言,用户可以自主更换智能卡内部的认证码。需要说明的是,本实施例也可以作为在第十实施例基础上的改进,可以达到同样的技术效果。

[00143] 本申请第十三实施例涉及一种智能卡,包括第九至十二实施例中任一项

的微芯片。其中，智能卡是基于 Java card 的智能卡。

[00144] 本申请第十四实施例涉及一种调试设备，请参考图 13，调试设备包括调试接口 6、智能卡插槽 7、控制模块 8 以及存储器 9。

[00145] 调试设备可以为 JTAG（Joint Test Action Group，国际标准测试协议，简称“JTAG”）设备，此时，调试接口 6 为 JTAG 接口。

[00146] 控制模块 8 连接于智能卡插槽 7 和调试接口 6；调试接口 6 还用于连接至待调试的芯片 10，智能卡插槽 7 用于供预存有密钥的智能卡 11 插入。

[00147] 具体的说，请参考图 14，控制模块 8 包括主控端 81 与微控制器 82，主控端 81 可以为个人电脑 PC，主控端 81 连接到转接板 12，转接板 12 通过调试接口 6 连接到芯片 10，主控端 81 还通过转接板 12 连接于微控制器 82，微控制器 82 连接于智能卡 11；另外，主控端 81 连接于存储器 9。

[00148] 其中，主控端 81、转接板 12 以及微控制器 82 可以为一体机，然不限于此，也可以分开设置。

[00149] 存储器 9 中储存有可被处理器执行的指令，指令被至少一个控制模块执行，当智能卡插槽 7 内插入预存有密钥的智能卡 11 时，指令被控制模块 8 执行，以使控制模块 8 能够第五至第九实施例中任一项的芯片的访问方法。

[00150] 本领域的普通技术人员可以理解，上述各实施例是实现本申请的具体实施例，而在实际应用中，可以在形式上和细节上对其作各种改变，而不偏离本申请的精神和范围。

权利要求书

1、一种芯片的访问方法，其特征在于，应用于智能卡且所述智能卡内预存有密钥，所述方法包括：

判断所述智能卡的加密功能是否被触发；

5 若所述加密功能被触发，则至少基于所述密钥生成密文，并将所述密文反馈至调试设备，以供所述调试设备将所述密文发送至待调试的芯片，并供所述芯片根据所述密文确定是否允许所述调试设备对所述芯片进行访问。

2、如权利要求1所述的芯片的访问方法，其特征在于，所述判断所述智能卡的加密功能是否被触发具体为，判断是否接收到所述调试设备发送过来的随机数；若是，则判定所述智能卡的加密功能被触发；其中所述随机数为所述调试设备从所述芯片获取的随机数；

所述至少基于所述密钥生成密文具体为，基于所述密钥和所述随机数生成所述密文。

3、如权利要求1所述的芯片的访问方法，其特征在于，所述方法还包括：

15 当接收到所述调试设备发送的密钥更新信息时，根据所述密钥更新信息更新所述密钥。

4、如权利要求3所述的芯片的访问方法，其特征在于，在所述接收到所述调试设备发送的密钥更新信息之前，还包括：

当接收到所述调试设备发送的认证码时，判断接收的所述认证码与所述智能卡内部预存的认证码是否匹配；

若判定结果为匹配，则反馈认证通过的应答至所述调试设备。

5、如权利要求 4 所述的芯片的访问方法，其特征在于，在所述反馈认证通过的应答至所述调试设备之后，还包括：

当接收到所述调试设备发送的认证码更新信息时，根据所述认证码更新信息更新所述智能卡内部预存的认证码。

5 6、如权利要求 1 所述的芯片的访问方法，其特征在于，所述智能卡是基于 Java card 的智能卡。

7、一种芯片的访问方法，其特征在于，应用于调试设备，所述调试设备上插设有智能卡且所述智能卡内预存有密钥，所述方法包括：

触发所述智能卡的加密功能，以供所述智能卡至少基于所述密钥生成密文；

10 接收所述智能卡反馈的所述密文，并将所述密文发送至待调试的芯片，以供所述芯片根据所述密文确定是否允许所述调试设备对所述芯片进行访问。

8、如权利要求 7 所述的芯片的访问方法，其特征在于，在所述触发所述智能卡的加密功能之前，还包括：

触发所述芯片的安全认证功能，并从所述芯片获取用于安全认证的随机数；

15 所述触发所述智能卡的加密功能具体为，将所述随机数发送至所述智能卡，以触发所述智能卡的加密功能；

其中，所述智能卡基于所述智能卡内部预存的所述密钥和所述随机数生成所述密文。

9、如权利要求 7 所述的芯片的访问方法，其特征在于，所述方法还包括：

20 当需要更新密钥时，将密钥更新信息发送至所述智能卡，以供所述智能卡根据所述密钥更新信息更新所述密钥。

10、如权利要求 9 所述的芯片的访问方法，其特征在于，当需要更新密钥时，且在所述将密钥更新信息发送至所述智能卡之前，还包括：

将认证码发送至所述智能卡，以供所述智能卡判断接收的所述认证码与所述智能卡内部预存的认证码是否匹配，并在判定匹配时反馈认证通过的应答至

5 所述调试设备；

所述将密钥更新信息发送至所述智能卡具体为，在接收到所述认证通过的应答时，将密钥更新信息发送至所述智能卡。

11、如权利要求 7 所述的芯片的访问方法，其特征在于，所述方法还包括：

当需要更新认证码时，将认证码发送至所述智能卡，以供所述智能卡判断
10 接收的所述认证码与所述智能卡内部预存的认证码是否匹配，并在判定匹配时反馈认证通过的应答至所述调试设备；

在接收到所述认证通过的应答时，发送认证码更新信息至所述智能卡，以供所述智能卡根据所述认证码更新信息更新所述智能卡内部预存的认证码。

12、一种微芯片，其特征在于，设置于智能卡内，且所述微芯片内预存有
15 密钥，所述微芯片包括：

判断单元，用于判断所述智能卡的加密功能是否被触发；

加密单元，用于在所述判断单元判定所述智能卡的加密功能被触发时，至少基于所述密钥生成密文，并将所述密文反馈至调试设备，以供所述调试设备
20 将所述密文发送至待调试的芯片，并供所述芯片根据所述密文确定是否允许所述调试设备对所述芯片进行访问。

13、如权利要求 12 所述的微芯片，其特征在于，所述判断单元具体用于判断是否接收到所述调试设备发送过来的随机数；若是，则判定所述智能卡的加密功能被触发；其中所述随机数为所述调试设备从所述芯片获取的随机数；

所述加密单元具体用于基于所述密钥和所述随机数生成所述密文。

5 14、如权利要求 12 所述的微芯片，其特征在于，所述微芯片还包括密钥更新单元；

所述密钥更新单元用于在接收到所述调试设备发送的密钥更新信息时，根据所述密钥更新信息更新所述密钥。

15、如权利要求 14 所述的微芯片，其特征在于，所述微芯片还包括认证单元；
10 元；

所述认证单元用于在接收到所述调试设备发送的认证码时，判断接收的所述认证码与所述智能卡内部预存的认证码是否匹配；若判定结果为匹配，则反馈认证通过的应答至所述调试设备；

所述密钥更新单元具体用于在所述认证单元反馈了所述认证通过的应答后，
15 允许接收所述密钥更新信息。

16、如权利要求 15 所述的微芯片，其特征在于，所述微芯片还包括认证码更新单元；

所述认证码更新单元用于在所述认证单元反馈了所述认证通过的应答后，允许接收所述调试设备发送的认证码更新信息，并在接收到所述认证码更新信息时，根据所述认证码更新信息更新所述智能卡内部预存的认证码。
20 息时，根据所述认证码更新信息更新所述智能卡内部预存的认证码。

17、一种智能卡，其特征在于，包括权利要求 12 至 16 中任一项所述的微芯片。

18、如权利要求 17 所述的智能卡,其特征在于,所述智能卡是基于 Java card 的智能卡。

19.一种调试设备,其特征在于,包括: 调试接口、智能卡插槽、控制模块以及存储器;

5 所述控制模块连接于所述智能卡插槽和所述调试接口; 所述调试接口还用于连接至待调试的芯片;

所述存储器中储存有可被所述控制模块执行的指令,所述指令被所述至少一个控制模块执行,

10 当所述智能卡插槽内插入预存有密钥的智能卡时,所述指令被所述控制模块执行,以使所述控制模块能够执行如权利要求 7 至 11 中任一项所述的芯片的访问方法。

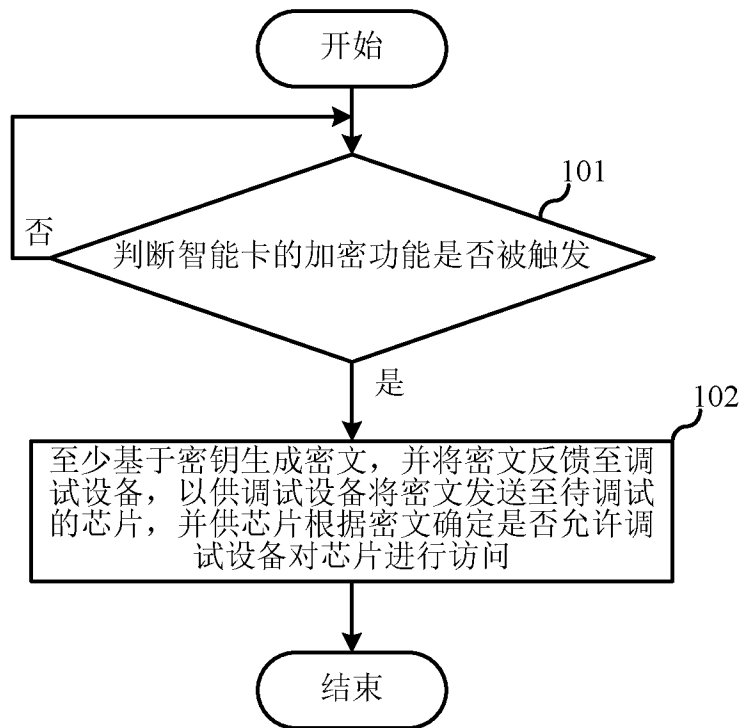


图 1

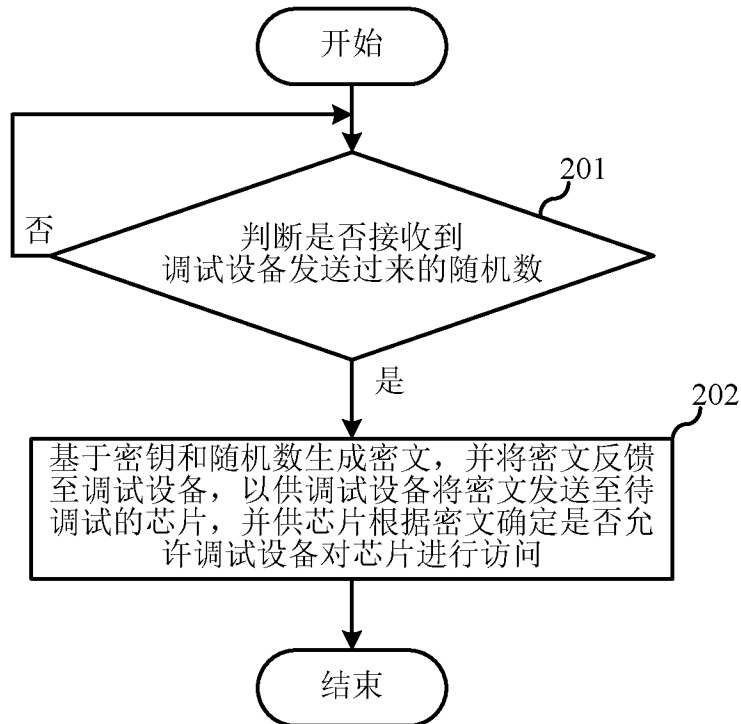


图 2

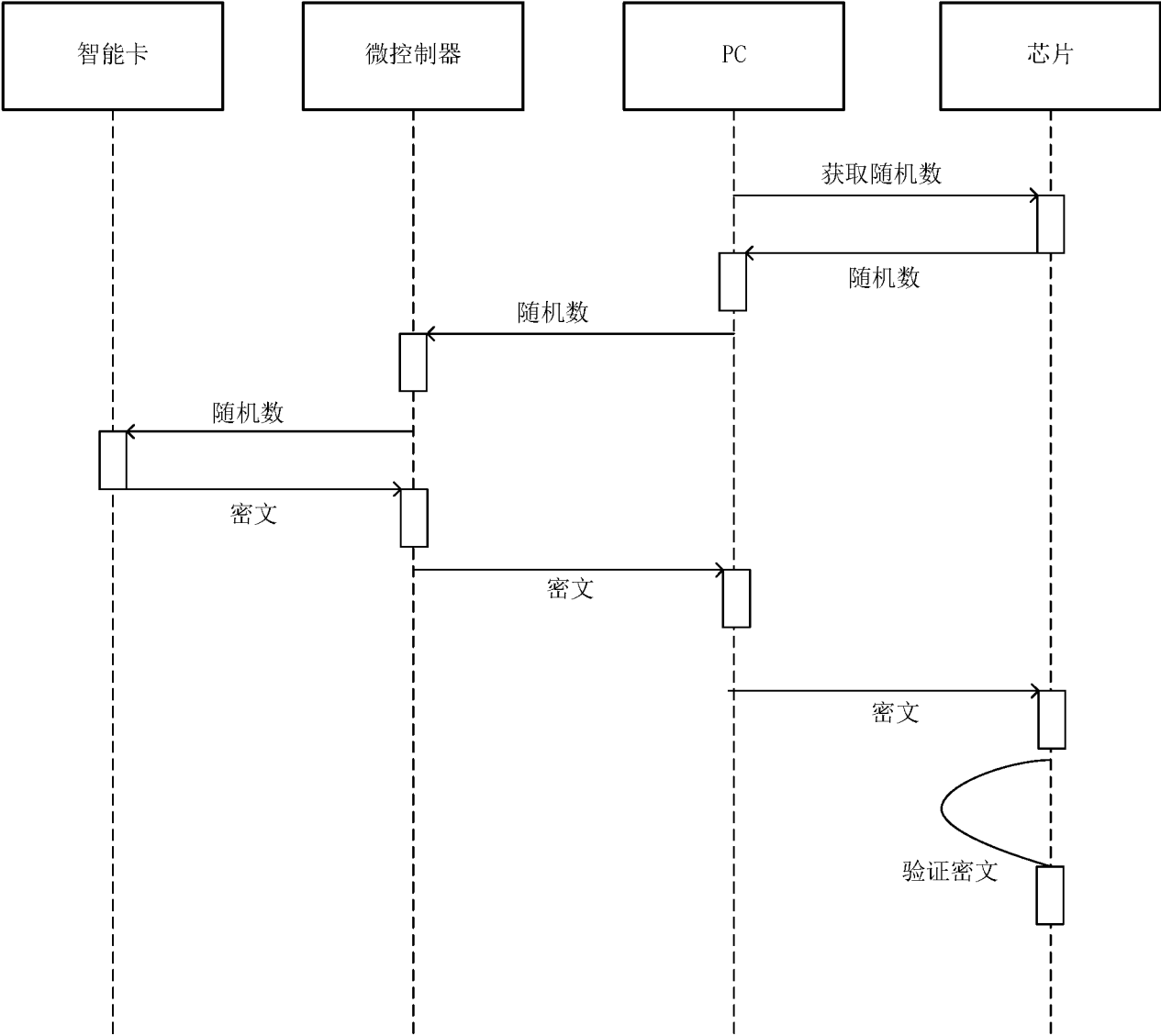


图 3

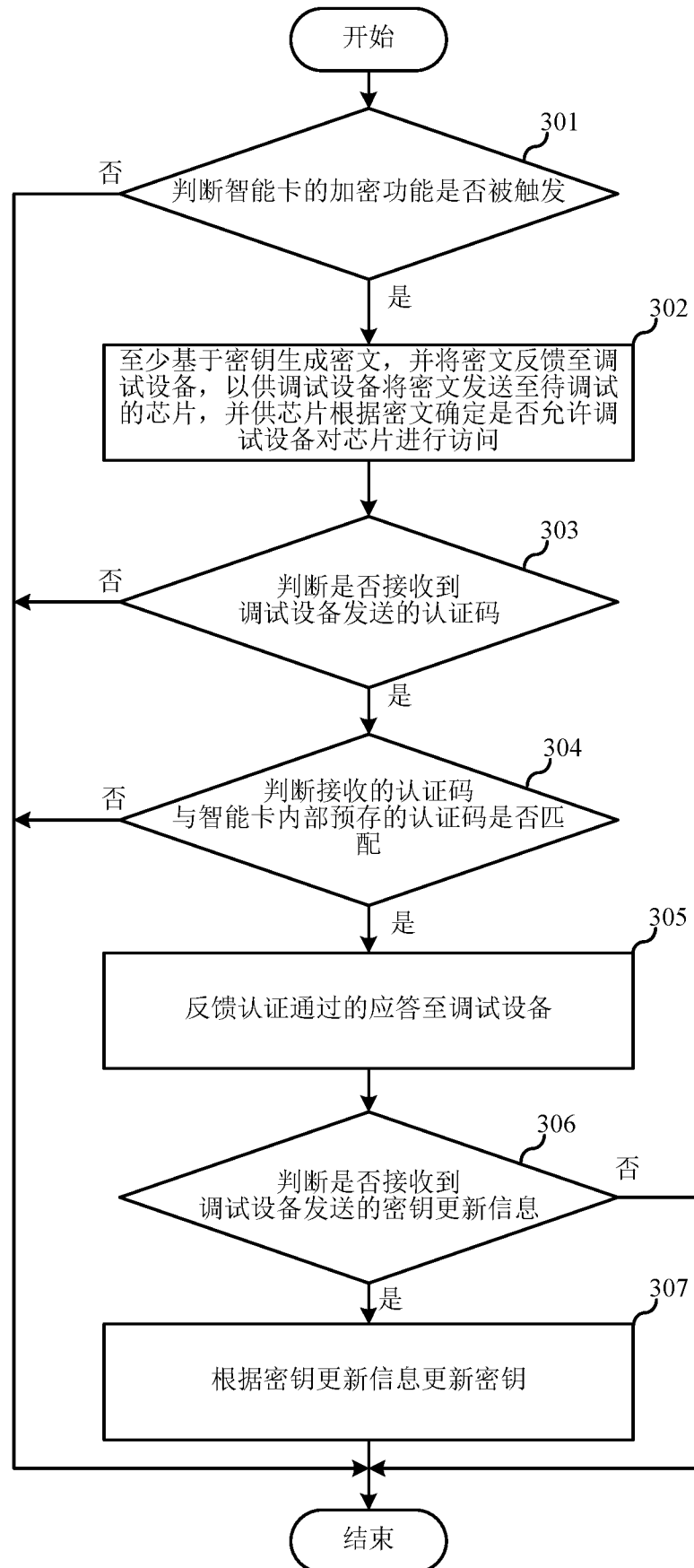


图 4

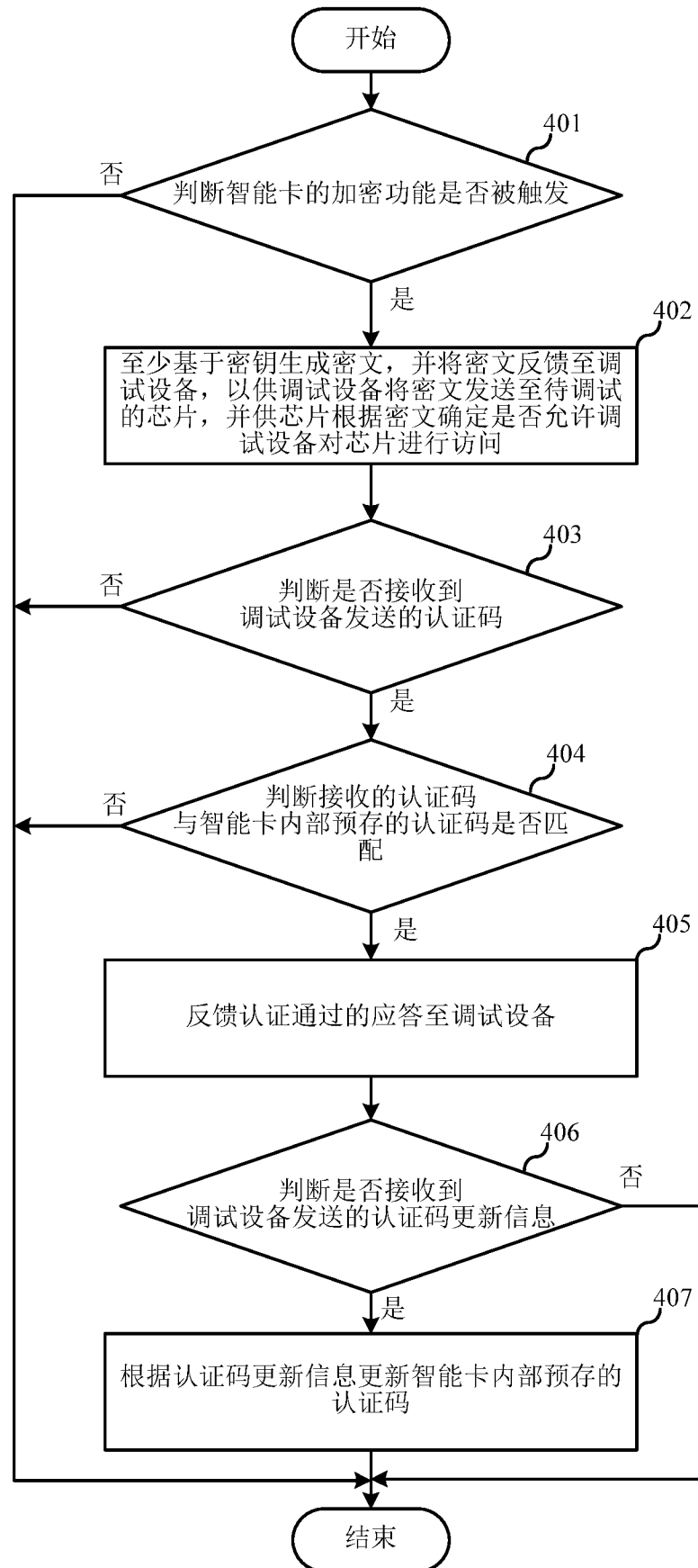


图 5

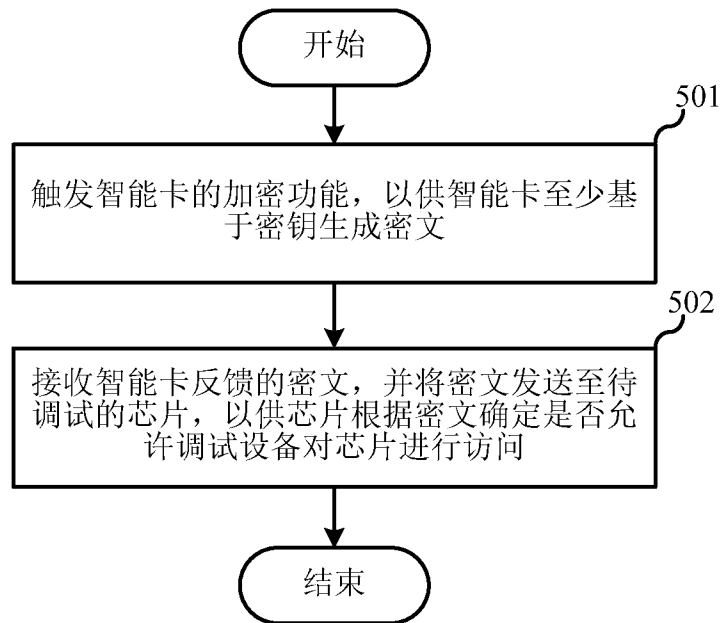


图 6

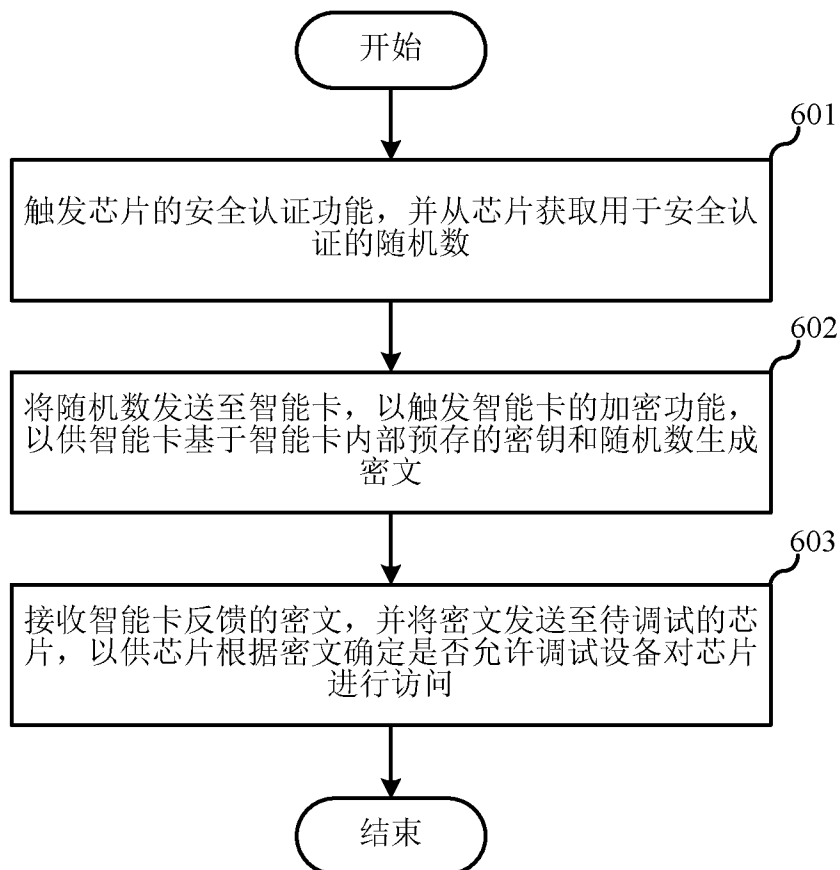


图 7

6/10

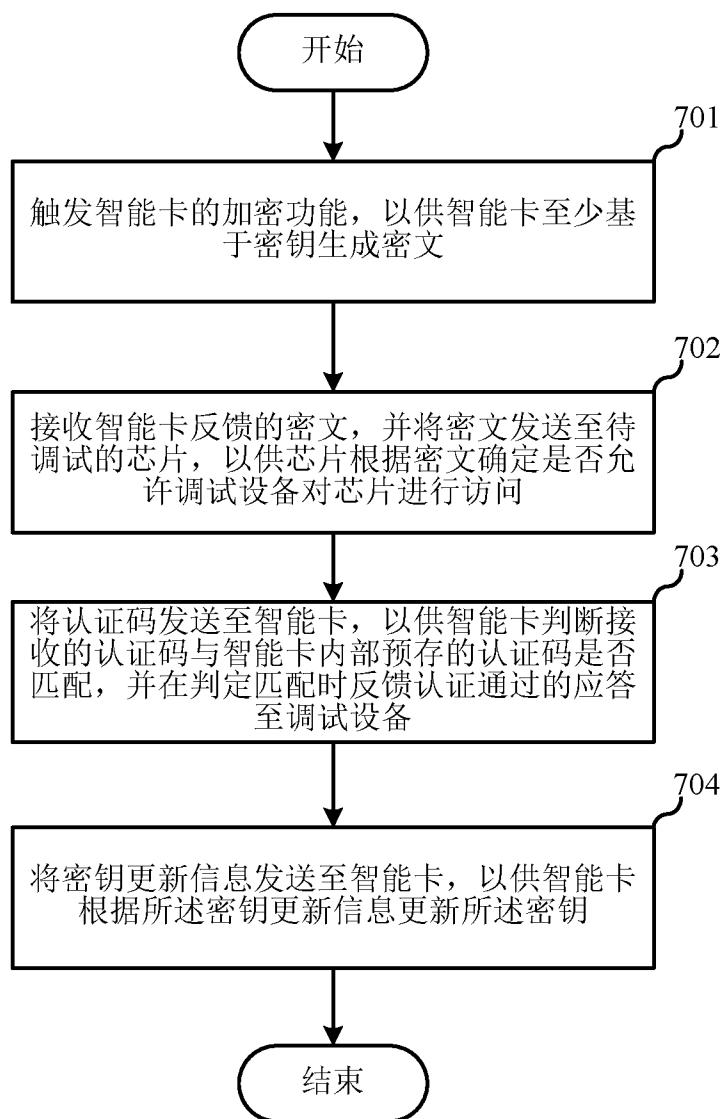


图 8

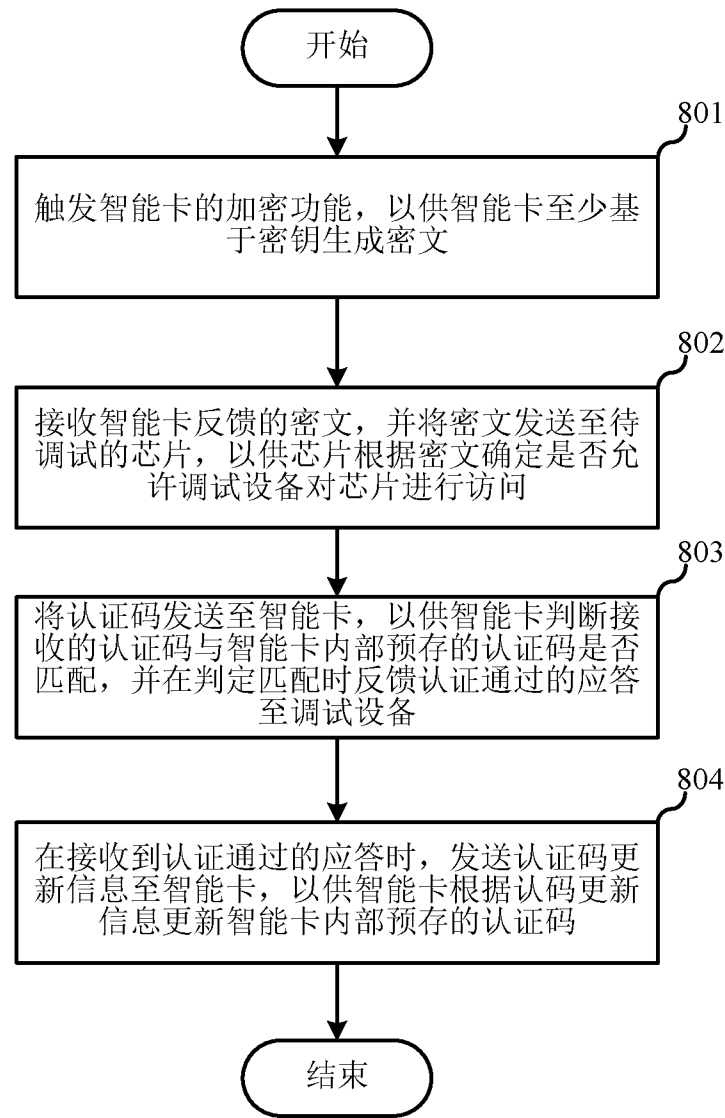


图 9

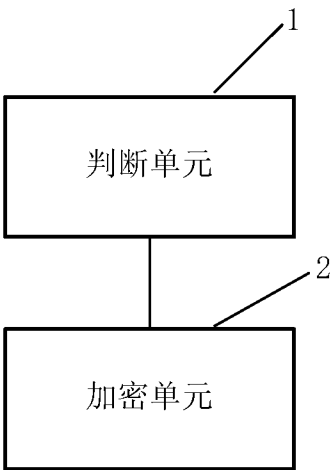


图 10

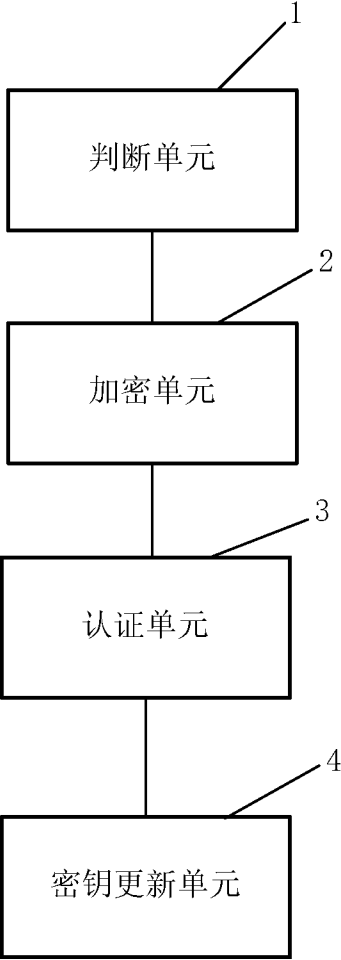


图 11

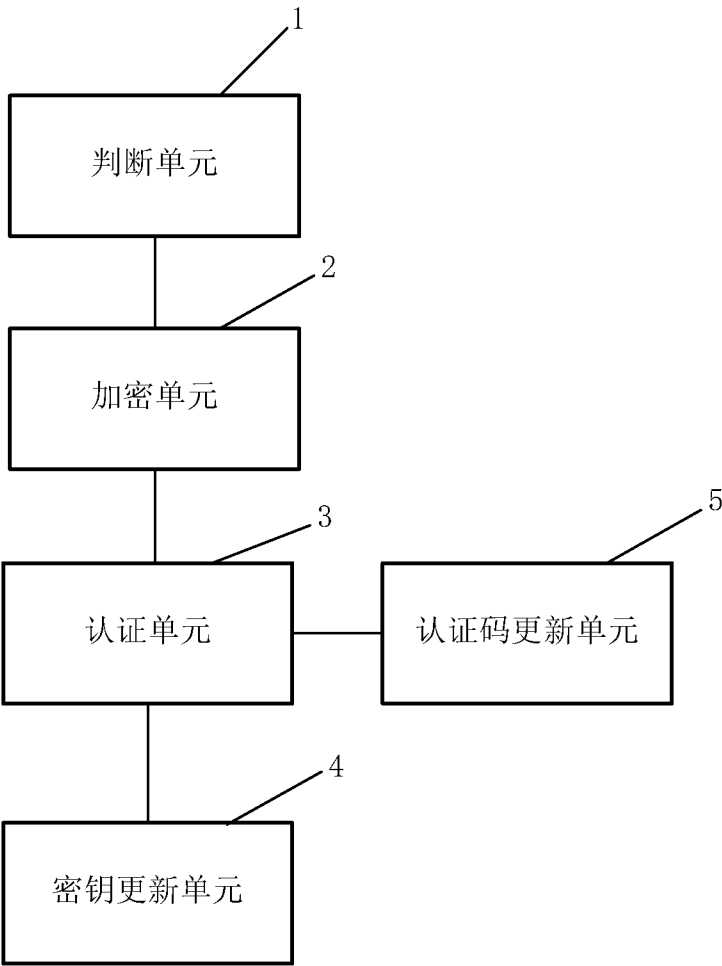


图 12

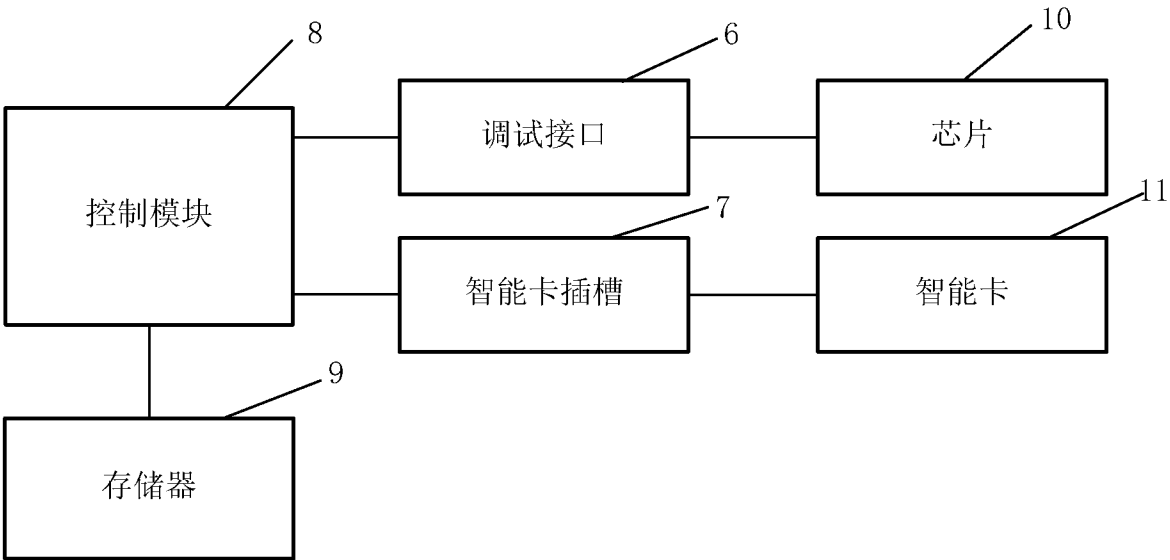


图 13

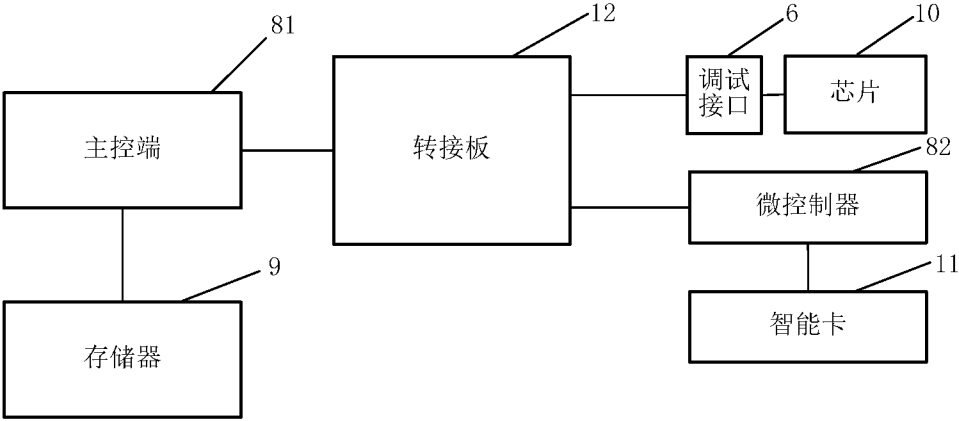


图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/079903

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)

G06F; 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)

WPI, EPODOC, CNPAT, CNKI: 加密, 随机数, 芯片, 智能卡, 密钥, 设备, 认证, 调试, 智能密钥, 密文, encrypt, chip, smart card, debug, key, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106330455 A (BEIJING HUADA INFOSEC TECHNOLOGY CO., LTD.) 11 January 2017 (2017-01-11) description, paragraphs [0074]-[0105]	1-19
A	CN 106506479 A (BEIJING MINGHUA UNION TECHNOLOGY CO., LTD.) 15 March 2017 (2017-03-15) entire document	1-19
A	CN 103679062 A (SHANGHAI BELLING CO., LTD.) 26 March 2014 (2014-03-26) entire document	1-19
A	CN 106855924 A (SOUTHERN WALLGREAT INFORMATION SAFETY TECHNOLOGY CO., LTD.) 16 June 2017 (2017-06-16) entire document	1-19
A	CN 105743654 A (DYNAMICODE COMPANY LIMITED) 06 July 2016 (2016-07-06) entire document	1-19

☐ 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

03 December 2018

Date of mailing of the international search report

25 December 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/079903

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	106330455	A	11 January 2017	None	
CN	106506479	A	15 March 2017	None	
CN	103679062	A	26 March 2014	None	
CN	106855924	A	16 June 2017	None	
CN	105743654	A	06 July 2016	None	

国际检索报告

国际申请号

PCT/CN2018/079903

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)

G06F; 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))

WPI, EPODOC, CNPAT, CNKI: 加密, 随机数, 芯片, 智能卡, 密钥, 设备, 认证, 调试, 智能密钥, 密文, encrypt, chip, smart card, debug, key, authentication

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 106330455 A (北京华大信安科技有限公司) 2017年 1月 11日 (2017 - 01 - 11) 说明书第[0074]-[0105]段	1-19
A	CN 106506479 A (北京明华联盟科技有限公司) 2017年 3月 15日 (2017 - 03 - 15) 全文	1-19
A	CN 103679062 A (上海贝岭股份有限公司) 2014年 3月 26日 (2014 - 03 - 26) 全文	1-19
A	CN 106855924 A (南方城墙信息科技有限公司) 2017年 6月 16日 (2017 - 06 - 16) 全文	1-19
A	CN 105743654 A (上海动联信息技术股份有限公司) 2016年 7月 6日 (2016 - 07 - 06) 全文	1-19

☐ 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

2018年 12月 3日

国际检索报告邮寄日期

2018年 12月 25日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

丁文勃

传真号 (86-10) 62019451

电话号码 86-(10)-53961330

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/079903

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	106330455	A	2017年 1月 11日	无	
CN	106506479	A	2017年 3月 15日	无	
CN	103679062	A	2014年 3月 26日	无	
CN	106855924	A	2017年 6月 16日	无	
CN	105743654	A	2016年 7月 6日	无	

表 PCT/ISA/210 (同族专利附件) (2015年1月)