(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 9 月 7 日 (07.09.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/157724 A1

(51) 国际专利分类号:
H04N 21/418 (2011.01) *H04N 21/266* (2011.01)

(21) 国际申请号: PCT/CN2018/075999

(22) 国际申请日: 2018 年 2 月 9 日 (09.02.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710116619.2 2017年2月28日 (28.02.2017) CN

(71) 申请人: 国家新闻出版广电总局广播科学研究院 (ACADEMY OF BROADCASTING SCIENCE, STATE ADMINISTRATION OF PRESS, PUBLICATION, RADIO, FILM & TELEVISION) [CN/CN]; 中国北京市西城区复兴门外大街 2 号, Beijing 100866 (CN)。

北京永新视博数字电视技术有限公司 (BEIJING NOVEL-SUPER DIGITAL TV TECHNOLOGY CO., LTD) [CN/CN]; 中国北京市海淀区上地东路 5 号京蒙高科大厦 B 座 4 层, Beijing 100085 (CN)。 北京数码视讯科技股份有限公司 (SUMAVISION TECHNOLOGIES CO., LTD) [CN/CN]; 中国北京市海淀区上地信息产业基地开拓路 15 号数码视讯大厦, Beijing 100085 (CN)。 深圳市海思半导体有限公司 (HISILICON TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地, Guangdong 518129 (CN)。

(72) 发明人: 盛志凡 (SHENG, Zhifan); 中国北京市西城区复兴门外大街2号, Beijing 100866 (CN)。 解伟 (XIE, Wei); 中国北京市西城区复兴门外大街2号, Beijing 100866 (CN)。 张晶 (ZHANG, Jing);

(54) **Title:** METHOD FOR PROTECTING ENCRYPTED CONTROL WORD, HARDWARE SECURITY MODULE, MAIN CHIP AND TERMINAL

(54) **发明名称**: 加密控制字的保护方法、硬件安全模块、主芯片和终端

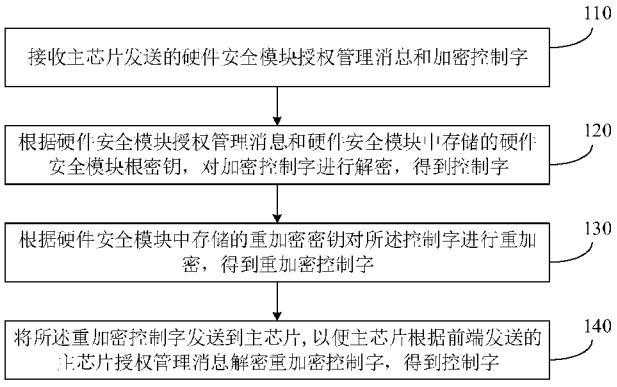

图 1

110 RECEIVE A HARDWARE SECURITY MODULE ENTITLEMENT MANAGEMENT MESSAGE AND AN ENCRYPTED CONTROL WORD SENT BY A MAIN CHIP
120 ACCORDING TO THE HARDWARE SECURITY MODULE ENTITLEMENT MANAGEMENT MESSAGE AND A HARDWARE SECURITY MODULE ROOT KEY STORED IN A HARDWARE SECURITY MODULE, DECRYPT THE ENCRYPTED CONTROL WORD TO OBTAIN A CONTROL WORD
130 ACCORDING TO A RE-ENCRYPTION KEY STORED IN THE HARDWARE SECURITY MODULE, RE-ENCRYPT THE CONTROL WORD TO OBTAIN A RE-ENCRYPTED CONTROL WORD
140 SEND THE RE-ENCRYPTED CONTROL WORD TO THE MAIN CHIP, SO THAT THE MAIN CHIP DECRYPTS, ACCORDING TO A MAIN CHIP ENTITLEMENT MANAGEMENT MESSAGE SENT BY A FRONT END, THE RE-ENCRYPTED CONTROL WORD TO OBTAIN THE CONTROL WORD

(57) **Abstract:** A method for protecting an encrypted control word. The method comprises: receiving a hardware security module entitlement management message and an encrypted control word sent by a main chip, wherein the hardware security module entitlement management message comprises a key for decrypting the encrypted control word; according to the hardware security module entitlement management message and a hardware security module root key stored in a hardware security module, decrypting the encrypted control word to obtain a control word; according to a re-encryption key stored in the hardware security module, re-encrypting the control word

WO 2018/157724 A1

[见续页]

中国北京市海淀区上地东路5号京蒙高科大厦B座4层, Beijing 100085 (CN)。 **田雪冰(TIAN, Xuebing)**; 中国北京市海淀区上地东路5号京蒙高科大厦B座4层, Beijing 100085 (CN)。 **熊彬(XIONG, Bin)**; 中国北京市海淀区上地信息产业基地开拓路15号数码视讯大厦, Beijing 100085 (CN)。 **郑力铮(ZHENG, Lizheng)**; 中国北京市海淀区上地信息产业基地开拓路15号数码视讯大厦, Beijing 100085 (CN)。 **严海峰(YAN, Haifeng)**; 中国广东省深圳市龙岗区坂田华为基地, Guangdong 518129 (CN)。 **方中华(FANG, Zhonghua)**; 中国广东省深圳市龙岗区坂田华为基地, Guangdong 518129 (CN)。 **王强(WANG, Qiang)**; 中国北京市西城区复兴门外大街2号, Beijing 100866 (CN)。 **杨勍(YANG, Qing)**; 中国北京市西城区复兴门外大街2号, Beijing 100866 (CN)。 **陈鹏(CHEN, Peng)**; 中国北京市西城区复兴门外大街2号, Beijing 100866 (CN)。 **靳龙辉(JIN, Longhui)**; 中国北京市海淀区上地东路5号京蒙高科大厦B座4层, Beijing 100085 (CN)。 **刘晶磊(LIU, Jinglei)**; 中国北京市海淀区上地东路5号京蒙高科大厦B座4层, Beijing 100085 (CN)。

(74) **代理人: 北京品源专利代理有限公司(BEYOND ATTORNEYS AT LAW)**; 中国北京市海淀区莲花池东路39号西金大厦6层, Beijing 100036 (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, 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))。

to obtain a re-encrypted control word; and sending the re-encrypted control word to the main chip, so that the main chip decrypts, according to a main chip entitlement management message sent by a front end, the re-encrypted control word to obtain the control word.

(57) **摘要**: 一种加密控制字的保护方法，包括：接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，硬件安全模块授权管理消息中包括用于解密加密控制字的密钥；根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字；根据硬件安全模块中存储的重加密密钥对控制字进行重加密，得到重加密控制字；将重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密重加密控制字，得到控制字。

加密控制字的保护方法、硬件安全模块、主芯片和终端

技术领域

本公开涉及消息安全技术，例如涉及一种加密控制字的保护方法、硬件安全模块、主芯片和终端。

背景技术

条件接收系统（Conditional Access System，CAS）是数字电视加密控制的核心技术保证，为数字电视的运营提供了必要的技术手段，使拥有授权的用户合法的使用特定的一项业务，而未经授权的用户不能使用这一业务。基于条件接收系统，CAS 与机顶盒绑定在一起，制约了行业的发展。为解决此问题，基于软硬件分离的可下载条件接收系统（Downloadable Conditional Access System，DCAS）应运而生。

DCAS 是一套完整的端到端业务保护系统，由前端、终端和安全数据管理平台组成。其中，前端对输入的音视频流进行加扰，通过广播信道或双向通信向终端发送加密控制字等条件接收的授权等消息，其中，控制字（Control Word，CW）用于对音视频流进行解扰，从而完成业务的加密保护传送和合法授权控制管理。

通常，在传统的 CAS 中，智能卡是条件存取操作（Conditional Access ，CA）在机顶盒端的硬件安全核心，用来存储授权密钥并参与控制字的生成。智能卡内部的数据存储和逻辑判断被视为可信消息，向机顶盒的其它组件提供解扰控制字。而与有卡 CAS 相比，DCAS 没有智能卡这样的可信执行环境和安全存储，因此如何保证 DCAS 的安全性，并使终端能够安全地从前端获取授权并解扰音视频流，成为亟待解决的问题。

发明内容

本公开提供一种加密控制字的保护方法、硬件安全模块、主芯片和终端，以保证DCAS的安全性，并使终端能够安全地从前端获取授权并解扰音视频流。

一种加密控制字的保护方法，包括：

接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，所述硬件安全模块授权管理消息中包括用于解密所述加密控制字的密钥；

根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字；

根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；以及

将所述重加密控制字发送到主芯片，以便主芯片根据所述前端发送的主芯片授权管理消息解密所述重加密控制字，得到控制字，其中，所述主芯片授权管理消息中包括用于解密所述重加密控制字的密钥。

一种加密控制字的保护方法，包括：

接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息；

将所述硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；以及

接收硬件安全模块发送的所述重加密控制字，根据主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到控制字，以便根据所述控制字解扰所述加扰内容。

一种硬件安全模块，配置于可下载条件接收系统，包括：

第一接收单元，设置为接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，所述硬件安全模块授权管理消息中包括设置为解密所述加密控制字的密钥；

安全存储区域，设置为存储硬件安全模块根密钥、重加密密钥和所述硬件安全模块授权管理消息；

第一解密引擎，设置为根据所述硬件安全模块授权管理消息和硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字；

重加密引擎，设置为根据所述重加密密钥对所述控制字进行重加密，得到重加密控制字；

第一发送单元，设置为将所述重加密控制字发送到主芯片，以便主芯片根据所述前端发送的主芯片授权管理消息解密所述重加密控制字，得到控制字，

其中，所述主芯片授权管理消息中包括设置为解密所述重加密控制字的密钥。

一种主芯片，应用于可下载条件接收系统，包括：

第三接收单元，设置为接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息；

第二发送单元，设置为将所述硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；

第四接收单元，设置为接收硬件安全模块发送的所述重加密控制字；

第二解密引擎，设置为根据主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到控制字，以便根据所述控制字解扰所述加扰内容。

一种终端，应用于可下载条件接收系统，包括：如上所述的硬件安全模块和如上所述的主芯片。

一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为上述任一项的方法。

本公开的加密控制字的保护方法，使得外界无法从硬件安全模块中截取到解密的重要信息，从而利用该硬件安全模块增强了 DCAS 的安全性。

附图说明

图 1 是实施例一提供的加密控制字的保护方法的流程图；

图 2 是实施例二提供的加密控制字的保护方法的流程图；

图 3 是实施例三提供的加密控制字的保护方法的流程图；

图 4 是实施例四提供的加密控制字的保护方法的流程图；

图 5 是实施例五提供的加密控制字的保护方法的流程图；

图 6 是实施例六提供的硬件安全模块的结构示意图；

图 7 是实施例七提供的主芯片的结构示意图；

图 8 是实施例八提供的终端的结构示意图；

图 9 是实施例九提供的硬件安全模块结构示意图。

具体实施方式

实施例一

图 1 为实施例一提供的加密控制字的保护方法的流程图，本实施例可应用于可下载条件接收系统 DCAS，其中，DCAS 包括前端和终端，终端包括主芯片和硬件安全模块，该方法可以由该硬件安全模块来执行。本实施例中硬件安全模块 (Hardware Security Module, HSM) 是专为保护加密密钥生命周期而设计的专用加密处理器，硬件安全模块通过在可靠且防篡改的设备中安全地管理、处理和保存加密密钥，保护交易、应用程序和敏感数据中使用的加密密钥的安全。本实施例的方法包括步骤 110-140：

在步骤 110 中，接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，所述硬件安全模块授权管理消息中包括用于解密所述加密控制字的密钥。

本实施例中，控制字用于前端对用户订阅的音视频内容进行加扰，例如数字电视的内容，知道控制字就可以对经加扰的内容解扰，从而观看音视频内容。因此，需要对控制字进行加密，并且只允许经授权的用户才能解密，从而保障系统的正常运行。硬件安全模块授权管理消息中包括用于解密加密控制字的密钥。

在步骤 120 中，根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字。

硬件安全模块根密钥是与该硬件安全模块一一对应的根密钥，即不同的硬件安全模块具有不同的根密钥，根密钥存储在硬件安全模块中，不会被外界获取，而不知道根密钥则无法对加密控制字进行解密。

在一实施例中，所述硬件安全模块授权管理消息包括硬件安全模块二级密钥和硬件安全模块三级密钥；相应的，根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，包括：根据硬件安全模块中存储的硬件安全模块根密钥、硬件安全模块二级密钥和硬件安全模块三级密钥对加密控制字进行层级解密，得到控制字。

在一实施例中，出于安全性的考虑，DCAS 采用层级密钥的机制，即前端对控制字利用三级密钥加密后，再利用二级密钥对三级密钥进行加密，再利用根

密钥对二级密钥进行加密。例如，前端对 CW 利用三级密钥 K1 加密，得到 EK1（CW），再利用二级密钥 K2 对 K1 加密，得到 EK2（K1），再利用硬件安全模块根密钥 Root Key 对二级密钥 K2 加密，得到 Ekroot（K2）。其中的 EK1（CW）、EK2（K1）和 Ekroot（K2）共同构成所述加密控制字。其中，二级密钥和三级密钥可以是前端生成的随机数。

二级密钥和三级密钥以硬件安全模块授权管理消息的方式通过主芯片发送至硬件安全模块，硬件安全模块根据存储的硬件安全模块根密钥、该硬件安全模块授权管理消息中的二级密钥和三级密钥对加密控制字进行层级解密，获得控制字明文。在上述实施例中，硬件安全模块利用存储的根密钥 Root Key 和加密控制字中的 Ekroot（K2）解密得到 K2，再利用 K2 和 EK2（K1）解密得到 K1，再利用 K1 和 EK1（CW）解密得到控制字明文。解密算法可以根据实际需要设置，例如对称分组密码算法（Advanced Encryption Standard ，AES）或 3DES 算法（三重数据加密算法（Triple Data Encryption Algorithm，TDEA）块密码的统称）等。

在步骤 130 中，根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字。

出于安全性的考虑，控制字明文需要进行重加密后再反馈给主芯片。例如，重加密密钥为 CREEK，加密后得到 Ecreek（CW）。

在步骤 140 中，将重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密重加密控制字，得到控制字，其中，所述主芯片授权管理消息中包括用于解密所述重加密控制字的密钥。

可选地，主芯片解密重加密控制字也需要相应的密钥才能实现，该密钥是以主芯片授权管理消息的方式由前端发送给主芯片，实现对主芯片的授权，得到控制字，从而解扰加扰内容进行播放。

在一实施例中，上述硬件安全模块授权管理消息、硬件安全模块根密钥和重加密密钥可以进行更新，以满足安全性需要。更新的频率可以根据实际使用场景的需要进行设置。实现时，可以由前端通过主芯片发来密钥刷新指令，硬件安全模块根据该密钥刷新指令对原有相关密钥进行更新，并存储更新后的密钥。

本实施例通过硬件安全模块根据存储的硬件安全模块根密钥和接收到的硬

件安全模块授权管理消息对加密控制字进行解密，得到控制字，再根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字，之后将所述重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密所述重加密控制字，得到控制字，由于外界无法从硬件安全模块中截取到解密的重要信息，从而利用该硬件安全模块增强了 DCAS 的安全性。

此外，对于如卫星直播广播电视系统而言，其对 CA 的业务需求是无卡单向 DCAS，那么无法通过双向网络通过将数据存储和授权逻辑移至前端来保证 DCAS 的安全性，而本实施例通过硬件安全模块实现授权逻辑，更加适用于这种无卡单向 DCAS，增强了了无卡单向 DCAS 的安全性。

实施例二

图 2 为实施例二提供的方法的流程图，实施例二在实施例一的基础上，对终端激活的操作进行改变。如图 2 所示，本实施例二的方法包括步骤 210-260：

在步骤 210 中，接收主芯片发送的激活消息，所述激活消息中至少包括配对密钥、所述重加密密钥和硬件安全模块根密钥。

此处所述的激活，通常是在终端使用之前进行，激活后就可以正常使用了。本实施例中，是由终端中的主芯片向前端发送激活请求消息，然后前端将激活消息发送至主芯片，再由主芯片发送给硬件安全模块。激活消息中至少包括配对密钥、重加密密钥和硬件安全模块根密钥。

此外，激活也可以由人工协助完成，例如，技术人员通过扫描终端上的二维码获取终端的信息，并通过客户端软件上传至前端实现激活请求消息的发送，然后在通过客户端软件接收激活消息并人工传到终端的主芯片。

在步骤 220 中，存储重加密密钥和硬件安全模块根密钥，并根据配对密钥建立与主芯片的安全认证通道。

保存重加密密钥和硬件安全模块根密钥后，就可以进行如上述实施例所述的解密操作了。本实施例中，可以利用硬件安全模块中的安全存储区域来存储重加密密钥和硬件安全模块根密钥。

此外，还需要在激活后利用配对密钥建立与主芯片的安全认证通道，在使用过程中，硬件安全模块与主芯片之间数据传送都是基于该安全认证通道，从而增强数据的安全性。

在步骤 230 中，通过安全认证通道接收主芯片发送的硬件安全模块授权管

理消息和加密控制字。

在步骤 240 中，根据硬件安全模块中存储的硬件安全模块根密钥、硬件安全模块二级密钥和硬件安全模块三级密钥对加密控制字进行层级解密，得到控制字。

在步骤 250 中，根据硬件安全模块中存储的重加密密钥对控制字进行重加密，得到重加密控制字。

在步骤 260 中，通过所述安全认证通道将重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密重加密控制字，得到控制字，其中，主芯片授权管理消息中包括用于解密重加密控制字的密钥。

本实施例通过激活消息接收并存储重加密密钥和硬件安全模块根密钥，并根据激活消息中的配对密钥与主芯片建立安全认证通道，从而增强数据的安全性。

实施例三

图 3 是实施例三提供的加密控制字的保护方法的流程图，本实施例可应用于可下载条件接收系统 DCAS，其中，DCAS 包括前端和终端，终端包括主芯片和硬件安全模块，该方法可以由主芯片来执行。实施例三的方法包括步骤 310-330：

在步骤 310 中，接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息。

其中，控制字是用于前端对待播放的音视频内容进行加扰的，控制字加密后对终端进行授权，以主芯片授权管理消息和硬件安全模块授权管理消息的方式发送给主芯片，主芯片将硬件安全模块授权管理消息发送给硬件安全模块，以便硬件安全模块对加密控制字进行解密，主芯片也可以利用主芯片授权管理消息对硬件安全模块重加密后的控制字进行解密。

这里，前端例如可以通过广播信道将上述内容发送给各终端，终端根据自己的需要接收。

在步骤 320 中，将硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对控制字进行重加密，得到重加密控制字。

其中，关于硬件安全模块的上述操作，已经在实施例一和实施例二中阐述，这里不再赘述。

在步骤 330 中，接收硬件安全模块发送的重加密控制字，根据主芯片派生的主芯片根密钥和主芯片授权管理消息解密重加密控制字，得到控制字，以便根据控制字解扰加扰内容。

可选的，主芯片根密钥与主芯片相对应，本实施例中是根据主芯片安全密钥和派生标识，并利用主芯片内置的派生算法，派生出主芯片根密钥。其中，主芯片安全密钥可以存储在主芯片内部的一次性写入后不可更改的（One Time Programmable，OTP）区域；派生标识与所选 CA 有关，可以配置在终端运行的软件中，当有解密需求时，由该软件通过指令的方式下发给主芯片，若更改 CA，可以通过更新该软件的方式来更改派生标识。因此，不同的主芯片根据不同的 CA 可以派生出不同的主芯片根密钥，以满足灵活性的需要。

在一实施例中，可以采用层级密钥机制。所述主芯片授权管理消息包括主芯片二级密钥和主芯片三级密钥；相应的，所述根据主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到控制字，包括：根据所述主芯片根密钥、主芯片二级密钥和主芯片三级密钥对所述重加密控制字进行层级解密，得到控制字，其中，所述主芯片三级密钥与所述重加密密钥相对应。例如，可以是主芯片三级密钥与重加密密钥相同，那么前端将控制字 CW 用主芯片二级密钥 K2’对三级密钥 K1’加密，得到 EK2（K1），再用主芯片根密钥 K3 对二级密钥 K2’加密得到 EK3（K2），EK3（K2）和 EK2（K1）作为加密控制字发送给主芯片，主芯片利用 K3 和 EK3（K2）解密得到 K2’，利用 EK2（K1）和 K2’解密得到 K1’，利用硬件安全模块发送给主芯片经重加密后的控制字和 K1’解密得到控制字明文，最终解扰加扰内容进行播放。

本实施例通过主芯片与硬件安全模块完成授权控制，从而利用该硬件安全模块增强了 DCAS 的安全性。并且尤其适用于无卡单向 DCAS。

实施例四

图 4 是实施例四提供的加密控制字的保护方法的流程图，实施例四在上述实施例的基础上进行进一步优化。如图 4 所示，实施例四的方法包括步骤 410-460：

在步骤 410 中，生成激活请求消息，将所述激活请求消息发送至前端，其中，激活请求消息中至少包括主芯片标识、条件接收证书和硬件安全模块的芯

片证书。

在步骤 420 中，接收前端发送的激活消息，并将激活消息发送至硬件安全模块，其中，激活消息中至少包括配对密钥、重加密密钥和硬件安全模块根密钥，并且激活消息中的配对密钥、重加密密钥和硬件安全模块根密钥为前端根据所述激活请求消息派发。

本实施例中，激活请求消息中携带的信息是作为前端派发配对密钥、重加密密钥和硬件安全模块根密钥的依据。前端在校验激活请求消息的合法性之后，根据主芯片标识、条件接收证书和硬件安全模块的芯片证书等信息，为终端中的硬件安全模块派发相对应的重加密密钥和硬件安全模块根密钥，并为终端中的主芯片和硬件安全模块建立他们之间的安全认证通道派发相对应的配对密钥。

在步骤 430 中，根据配对密钥建立与硬件安全模块的安全认证通道。

在步骤 440 中，接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息。

在步骤 450 中，通过安全认证通道将硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字。

在步骤 460 中，通过安全认证通道接收硬件安全模块发送的所述重加密控制字，根据主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到控制字，以便根据所述控制字解扰所述加扰内容。

本实施例通过激活操作获取配对密钥、重加密密钥和硬件安全模块根密钥，利用配对密钥建立与硬件安全模块之间的安全认证通道，并在激活操作之后，根据前端发送的主芯片安全密钥和派生标识派生出主芯片根密钥，用于后续的控制字解密操作，增强了 DCAS 的安全性。

实施例五

图 5 是实施例五提供的方法的加密控制字的保护流程图，实施例五在上述实施例的基础上进行进一步说明。如图 5 所示，实施例五的方法包括：

①主芯片生成激活请求消息，将激活请求消息发送至前端，其中，所述激活请求消息中至少包括主芯片标识、条件接收证书和硬件安全模块的芯片证书。

②前端根据所述激活请求消息生成激活消息，并将该激活消息发送至主芯片，其中，所述激活消息中至少包括配对密钥、所述重加密密钥和硬件安全模块根密钥。

③主芯片将所述激活消息中的配对密钥、重加密密钥和硬件安全模块根密钥发送给硬件安全模块。

④硬件安全模块存储所述重加密密钥和硬件安全模块根密钥，并利用配对密钥与主芯片建立安全认证通道。

⑤前端向主芯片发送加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息。

⑥主芯片通过安全认证通道将硬件安全模块授权管理消息和加密控制字发送至硬件安全模块。

⑦硬件安全模块根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对控制字进行重加密，得到重加密控制字。

⑧硬件安全模块通过安全认证通道将重加密后的控制字通过安全认证通道发送给主芯片。

⑨主芯片根据主芯片派生的主芯片根密钥和主芯片授权管理消息解密重加密控制字，得到控制字，以便根据控制字解扰加扰内容。

本实施例适用于DCAS,尤其适用于无卡单向DCAS,增强了无卡单向DCAS的安全性。

实施例六

图 6 是实施例六提供的硬件安全模块的结构示意图，该硬件安全模块应用于 DCAS，DCAS 包括前端和终端，终端包括主芯片和所述硬件安全模块。如图 6 所示，硬件安全模块 6 包括：

第一接收单元 60，用于接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，所述硬件安全模块授权管理消息中包括用于解密所述加密控制字的密钥。

安全存储区域 61，用于存储硬件安全模块根密钥、重加密密钥和所述硬件安全模块授权管理消息。

第一解密引擎 62，用于根据所述硬件安全模块授权管理消息和硬件安全模

块根密钥，对所述加密控制字进行解密，得到控制字。

重加密引擎 63，用于根据所述重加密密钥对所述控制字进行重加密，得到重加密控制字。

第一发送单元 64，用于将所述重加密控制字发送到主芯片，以便主芯片根据所述前端发送的主芯片授权管理消息解密所述重加密控制字，得到控制字，其中，所述主芯片授权管理消息中包括用于解密所述重加密控制字的密钥。

本实施例中，硬件安全模块 6 还包括：

第二接收单元（图中未示出），用于接收主芯片发送的激活消息，所述激活消息中至少包括配对密钥、所述重加密密钥和硬件安全模块根密钥；

第一配对单元（图中未示出），用于根据所述配对密钥建立与所述主芯片的安全认证通道。

本实施例中，第一接收单元 60 用于：接收主芯片发送的硬件安全模块授权管理消息和加密控制字包括：通过所述安全认证通道接收主芯片发送的硬件安全模块授权管理消息和加密控制字；

第一发送单元 64 用于：通过所述安全认证通道将所述重加密控制字发送到主芯片。

本实施例中，所述硬件安全模块授权管理消息包括硬件安全模块二级密钥和硬件安全模块三级密钥；

本实施例中，第一解密引擎 62 用于：

根据所述硬件安全模块中存储的硬件安全模块根密钥、硬件安全模块二级密钥和硬件安全模块三级密钥对所述加密控制字进行层级解密，得到控制字。

本实施例中，硬件安全模块 6 还包括：

更新单元（图中未示出），用于接收所述主芯片发送的密钥刷新指令，对所述硬件安全模块授权管理消息、硬件安全模块根密钥和重加密密钥进行更新和存储。

本实施例中，安全存储区域 61 还用于存储更新后的硬件安全模块授权管理消息、硬件安全模块根密钥和重加密密钥。

本实施例通过硬件安全模块根据存储的硬件安全模块根密钥和接收到的硬件安全模块授权管理消息对加密控制字进行解密，得到控制字，再根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字，之

后将所述重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密所述重加密控制字，得到控制字，由于外界无法从硬件安全模块中截取到解密的重要信息，从而利用该硬件安全模块增强了 DCAS 的安全性。此外，尤其适用于无卡单向DCAS，为无卡单向DCAS提供了安全保障。

实施例七

图 7 是实施例七提供的主芯片的结构示意图,该主芯片应用于DCAS,DCAS包括前端和终端，终端包括主芯片和所述硬件安全模块。如图 7 所示，主芯片 7 包括：

第三接收单元 71，用于接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息；

第二发送单元 72，用于将所述硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；

第四接收单元 73，用于接收硬件安全模块发送的所述重加密控制字；

第二解密引擎 74，用于根据主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到控制字，以便根据所述控制字解扰所述加扰内容。

本实施例中，主芯片 7 还包括：

激活请求消息生成单元（图中未示出），用于生成激活请求消息，将所述激活请求消息发送至前端，其中，所述激活请求消息中至少包括主芯片标识、条件接收证书和硬件安全模块的芯片证书；

激活消息接收单元（图中未示出），用于接收前端发送的激活消息，并将所述激活消息发送至硬件安全模块，其中，所述激活消息中至少包括配对密钥、所述重加密密钥和硬件安全模块根密钥，并且所述激活消息中的配对密钥、所述重加密密钥和硬件安全模块根密钥为前端根据所述激活请求消息派发；

第二配对单元（图中未示出），用于根据所述配对密钥建立与所述硬件安全模块的安全认证通道。

本实施例中，第二发送单元 72 用于：通过所述安全认证通道将所述硬件安

全模块授权管理消息和加密控制字发送至硬件安全模块。以及

第四接收单元 73 用于：通过所述安全认证通道接收硬件安全模块发送的所述重加密控制字。

本实施例中，主芯片 7 还包括：

根密钥派生单元（图中未示出），用于根据主芯片安全密钥和派生标识，利用主芯片内置派生算法，派生出所述主芯片根密钥。

本实施例中，所述主芯片授权管理消息包括主芯片二级密钥、主芯片三级密钥；相应的，第二解密引擎 74 用于：

根据所述主芯片根密钥、主芯片二级密钥和主芯片三级密钥对所述重加密控制字进行层级解密，得到控制字，其中，所述主芯片三级密钥与所述重加密密钥相对应。

本实施例通过主芯片与硬件安全模块完成授权控制，从而利用该硬件安全模块增强了 DCAS 的安全性。并且尤其适用于无卡单向 DCAS。

实施例八

图 8 是实施例八提供的终端的结构示意图，该终端应用于 DCAS，DCAS 包括前端和终端。如图 8 所示，终端 8 包括如上述实施例所述的主芯片 81 和硬件安全模块 82，主芯片 81 和硬件安全模块 82 之间通过安全认证通道进行数据的收发，确保重要信息的安全性。

实施例九

图 9 是实施例九提供的硬件安全模块的结构示意图，该硬件安全模块包括：处理器 910 和存储器 920；还可以包括通信接口 930 和总线 940。

其中，处理器 910、存储器 920 和通信接口 930 可以通过总线 940 完成相互间的通信。通信接口 930 可以用于信息传输。处理器 910 可以调用存储器 920 中的逻辑指令，以执行上述实施例的任意一种方法。

存储器 920 可以包括存储程序区和存储数据区，存储程序区可以存储操作系统和至少一个功能所需的应用程序。存储数据区可以存储根据电子设备的使用所创建的数据等。此外，存储器可以包括，例如，随机存取存储器的易失性存储器，还可以包括非易失性存储器。例如闪存器件或者其他非暂态固态存储器件。

本实施例还提供一种计算机可读存储介质，存储有计算机可执行指令，所

述计算机可执行指令设置为上述任一项的方法。

本实施例提供的硬件安全模块、主芯片和终端可执行上述任意实施例提供的加密控制字的保护方法，具备执行方法相应的功能模块和有益效果。

工业实用性

本公开的加密控制字的保护方法，可以保证 DCAS 的安全性，并使终端更安全地解密控制字并解扰音视频流。

权 利 要 求 书

1、一种加密控制字的保护方法，包括：

接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，所述硬件安全模块授权管理消息中包括用于解密所述加密控制字的密钥；

根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字；

根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；以及

将所述重加密控制字发送到所述主芯片，以便所述主芯片根据所述前端发送的主芯片授权管理消息解密所述重加密控制字，得到所述控制字，其中，所述主芯片授权管理消息中包括用于解密所述重加密控制字的密钥。

2、根据权利要求 1 所述的方法，其中，在所述接收主芯片发送的硬件安全模块授权管理消息和加密控制字之前，还包括：

接收所述主芯片发送的激活消息，所述激活消息中至少包括：配对密钥、所述重加密密钥和所述硬件安全模块根密钥；

存储所述重加密密钥和所述硬件安全模块根密钥，并根据所述配对密钥建立与所述主芯片的安全认证通道；

其中，所述接收主芯片发送的硬件安全模块授权管理消息和加密控制字包括：通过所述安全认证通道接收所述主芯片发送的所述硬件安全模块授权管理消息和所述加密控制字；以及

所述将所述重加密控制字发送到主芯片包括：通过所述安全认证通道将所述重加密控制字发送到主芯片。

3、根据权利要求 1 或 2 所述的方法，其中，所述硬件安全模块授权管理消息包括硬件安全模块二级密钥和硬件安全模块三级密钥；

根据所述硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，包括：

根据所述硬件安全模块中存储的所述硬件安全模块根密钥、所述硬件安全模块二级密钥和所述硬件安全模块三级密钥对所述加密控制字进行层级解密，得到所述控制字。

4、根据权利要求 1 所述的方法，还包括：

接收所述主芯片发送的密钥刷新指令，对所述硬件安全模块授权管理消息、

所述硬件安全模块根密钥和所述重加密密钥进行更新和存储。

5、一种加密控制字的保护方法，包括：

接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息；

将所述硬件安全模块授权管理消息和所述加密控制字发送至所述硬件安全模块，以便所述硬件安全模块根据所述硬件安全模块授权管理消息和所述硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，并根据所述硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；以及

接收所述硬件安全模块发送的所述重加密控制字，根据所述主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到所述控制字，以便根据所述控制字解扰所述加扰内容。

6、根据权利要求 5 所述的方法，在所述接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息之前，还包括：

生成激活请求消息，将所述激活请求消息发送至所述前端，其中，所述激活请求消息中至少包括：主芯片标识、条件接收证书和所述硬件安全模块的芯片证书；

接收所述前端发送的激活消息，并将所述激活消息发送至所述硬件安全模块，其中，所述激活消息中至少包括：配对密钥、所述重加密密钥和所述硬件安全模块根密钥，并且所述激活消息中的配对密钥、所述重加密密钥和所述硬件安全模块根密钥为所述前端根据所述激活请求消息派发；

根据所述配对密钥建立与所述硬件安全模块的安全认证通道；

其中，所述将所述硬件安全模块授权管理消息和加密控制字发送至硬件安全模块包括：通过所述安全认证通道将所述硬件安全模块授权管理消息和所述加密控制字发送至所述硬件安全模块；以及

所述接收硬件安全模块发送的所述重加密控制字包括：通过所述安全认证通道接收硬件安全模块发送的所述重加密控制字。

7、根据权利要求 5 所述的方法，其中，在所述解密所述重加密控制字之前，还包括：

根据主芯片安全密钥和派生标识，利用主芯片内置派生算法，派生出所述

主芯片根密钥。

8、根据权利要求 5-7 中任一项所述的方法，其中，所述主芯片授权管理消息包括主芯片二级密钥和主芯片三级密钥；

所述根据主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到控制字，包括：

根据所述主芯片根密钥、所述主芯片二级密钥和所述主芯片三级密钥对所述重加密控制字进行层级解密，得到所述控制字，其中，所述主芯片三级密钥与所述重加密密钥相对应。

9、一种硬件安全模块，配置于可下载条件接收系统，包括：

第一接收单元，设置为接收主芯片发送的硬件安全模块授权管理消息和加密控制字，其中，所述硬件安全模块授权管理消息中包括用于解密所述加密控制字的密钥；

安全存储区域，设置为存储硬件安全模块根密钥、重加密密钥和所述硬件安全模块授权管理消息；

第一解密引擎，设置为根据所述硬件安全模块授权管理消息和所述硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字；

重加密引擎，设置为根据所述重加密密钥对所述控制字进行重加密，得到重加密控制字；

第一发送单元，设置为将所述重加密控制字发送到所述主芯片，以便所述主芯片根据所述前端发送的主芯片授权管理消息解密所述重加密控制字，得到所述控制字，其中，所述主芯片授权管理消息中包括用于解密所述重加密控制字的密钥。

10、根据权利要求 9 所述的硬件安全模块，还包括：

第二接收单元，设置为接收所述主芯片发送的激活消息，所述激活消息中至少包括配对密钥、所述重加密密钥和所述硬件安全模块根密钥；

第一配对单元，设置为根据所述配对密钥建立与所述主芯片的安全认证通道；

其中，所述第一接收单元设置为接收主芯片发送的硬件安全模块授权管理消息和加密控制字包括：通过所述安全认证通道接收主芯片发送的硬件安全模块授权管理消息和加密控制字；

所述第一发送单元设置为：通过所述安全认证通道将所述重加密控制字发送到所述主芯片。

11、根据权利要求 9 或 10 所述的硬件安全模块，其中，所述硬件安全模块授权管理消息包括硬件安全模块二级密钥和硬件安全模块三级密钥；

所述第一解密引擎设置为：

根据所述硬件安全模块中存储的所述硬件安全模块根密钥、所述硬件安全模块二级密钥和所述硬件安全模块三级密钥对所述加密控制字进行层级解密，得到所述控制字。

12、根据权利要求 9 所述的硬件安全模块，还包括：

更新单元，设置为接收所述主芯片发送的密钥刷新指令，对所述硬件安全模块授权管理消息、所述硬件安全模块根密钥和所述重加密密钥进行更新和存储；

所述安全存储区域还设置为存储更新后的硬件安全模块授权管理消息、硬件安全模块根密钥和重加密密钥。

13、一种主芯片，应用于可下载条件接收系统，包括：

第三接收单元，设置为接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息；

第二发送单元，设置为将所述硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便所述硬件安全模块根据所述硬件安全模块授权管理消息和所述硬件安全模块中存储的硬件安全模块根密钥，对所述加密控制字进行解密，得到控制字，并根据所述硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字；

第四接收单元，设置为接收硬件安全模块发送的所述重加密控制字；

第二解密引擎，设置为根据所述主芯片派生的主芯片根密钥和所述主芯片授权管理消息解密所述重加密控制字，得到所述控制字，以便根据所述控制字解扰所述加扰内容。

14、根据权利要求 13 所述的主芯片，还包括：

激活请求消息生成单元，设置为生成激活请求消息，将所述激活请求消息发送至所述前端，其中，所述激活请求消息中至少包括主芯片标识、条件接收证书和硬件安全模块的芯片证书；

激活消息接收单元，设置为接收前端发送的激活消息，并将所述激活消息发送至所述硬件安全模块，其中，所述激活消息中至少包括配对密钥、所述重加密密钥和所述硬件安全模块根密钥，并且所述激活消息中的所述配对密钥、所述重加密密钥和所述硬件安全模块根密钥为前端根据所述激活请求消息派发；

第二配对单元，设置为根据所述配对密钥建立与所述硬件安全模块的安全认证通道；

其中，所述第二发送单元设置为通过所述安全认证通道将所述硬件安全模块授权管理消息和所述加密控制字发送至所述硬件安全模块；以及

所述第四接收单元设置为通过所述安全认证通道接收所述硬件安全模块发送的所述重加密控制字。

15、根据权利要求 13 所述的主芯片，还包括：

根密钥派生单元，设置为根据主芯片安全密钥和派生标识，利用主芯片内置派生算法，派生出所述主芯片根密钥。

16、根据权利要求 13-15 中任一项所述的主芯片，其中，所述主芯片授权管理消息包括主芯片二级密钥和主芯片三级密钥；

其中，所述第二解密引擎设置为根据所述主芯片根密钥、所述主芯片二级密钥和所述主芯片三级密钥对所述重加密控制字进行层级解密，得到所述控制字，其中，所述主芯片三级密钥与所述重加密密钥相对应。

17、一种终端，应用于可下载条件接收系统，包括：如权利要求 9-12 中任一项所述的硬件安全模块和如权利要求 13-16 中任一项所述的主芯片。

18、一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为权利要求 1-8 任一项所述的方法。

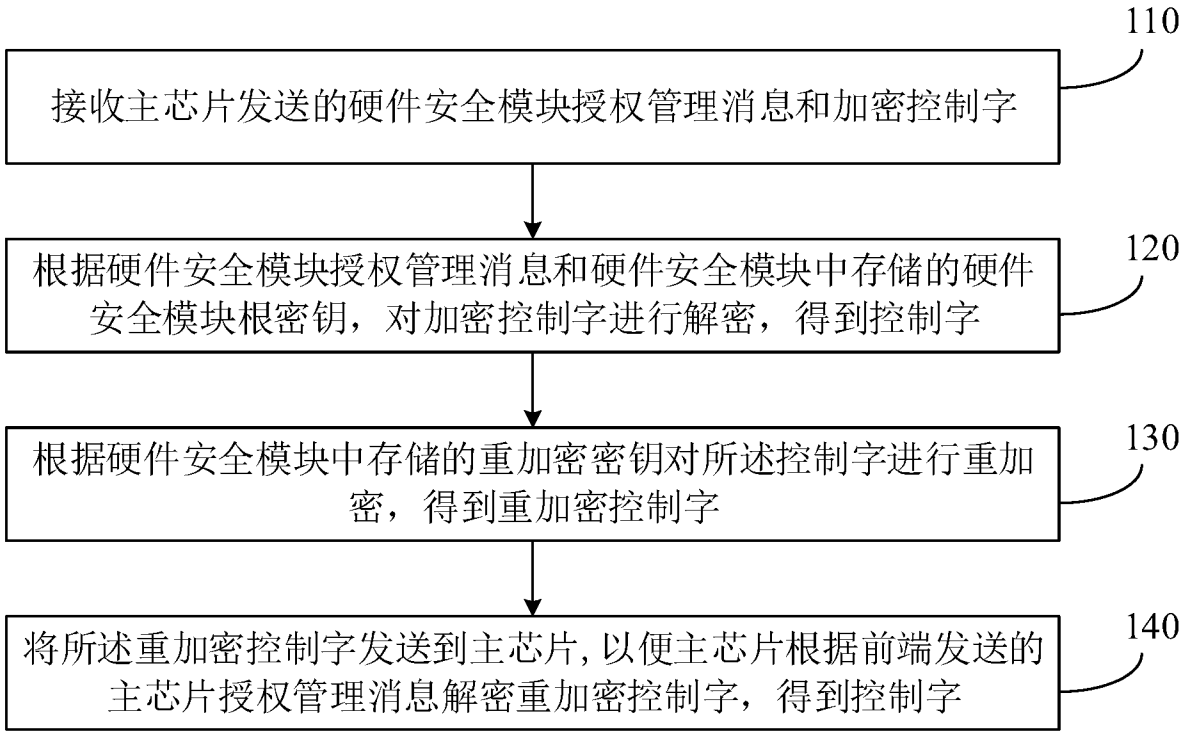
110
接收主芯片发送的硬件安全模块授权管理消息和加密控制字
120
根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字
130
根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字
140
将所述重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密重加密控制字，得到控制字

图 1

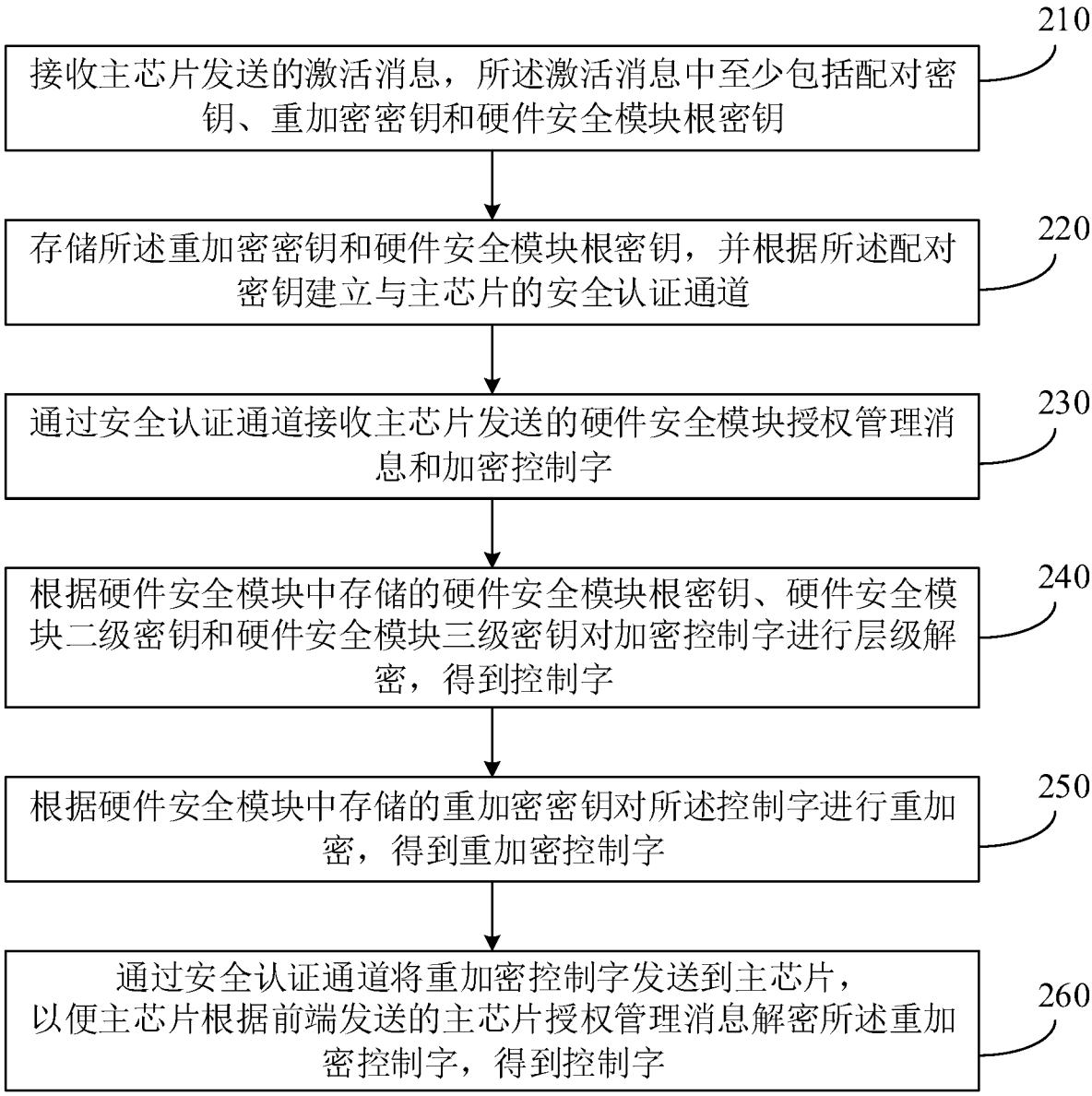
210
接收主芯片发送的激活消息，所述激活消息中至少包括配对密钥、重加密密钥和硬件安全模块根密钥
220
存储所述重加密密钥和硬件安全模块根密钥，并根据所述配对密钥建立与主芯片的安全认证通道
230
通过安全认证通道接收主芯片发送的硬件安全模块授权管理消息和加密控制字
240
根据硬件安全模块中存储的硬件安全模块根密钥、硬件安全模块二级密钥和硬件安全模块三级密钥对加密控制字进行层级解密，得到控制字
250
根据硬件安全模块中存储的重加密密钥对所述控制字进行重加密，得到重加密控制字
260
通过安全认证通道将重加密控制字发送到主芯片，以便主芯片根据前端发送的主芯片授权管理消息解密所述重加密控制字，得到控制字

图 2

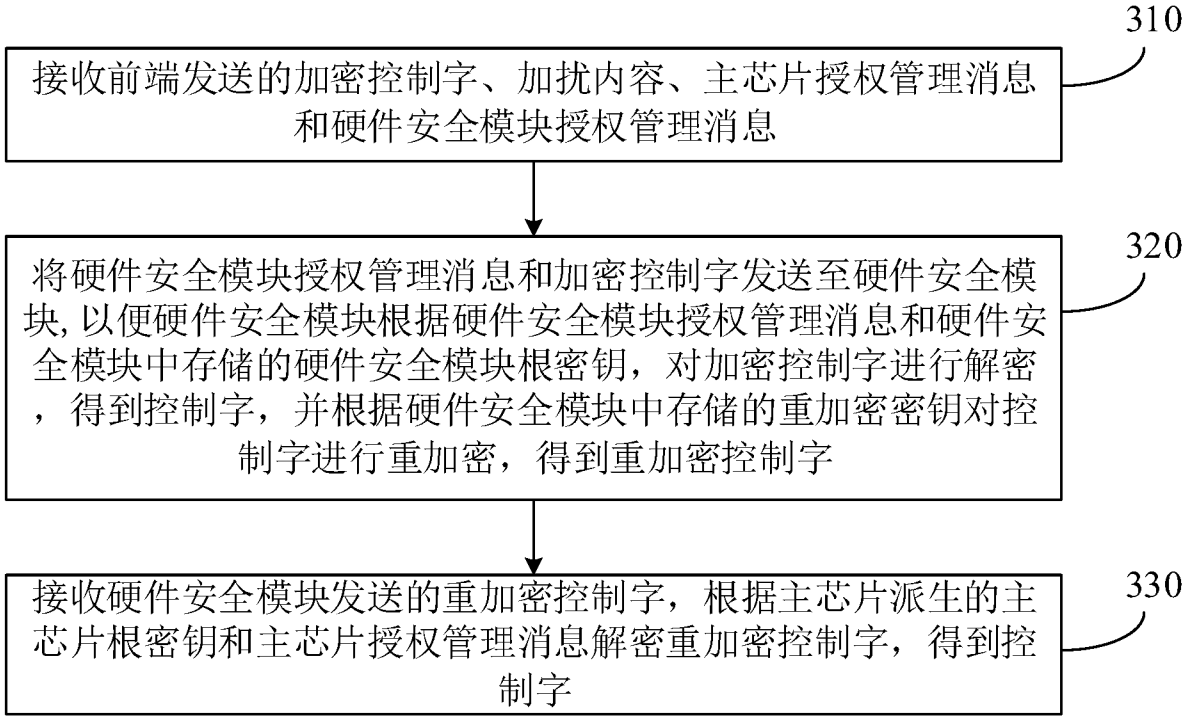
310
接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息
320
将硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对控制字进行重加密，得到重加密控制字
330
接收硬件安全模块发送的重加密控制字，根据主芯片派生的主芯片根密钥和主芯片授权管理消息解密重加密控制字，得到控制字

图 3

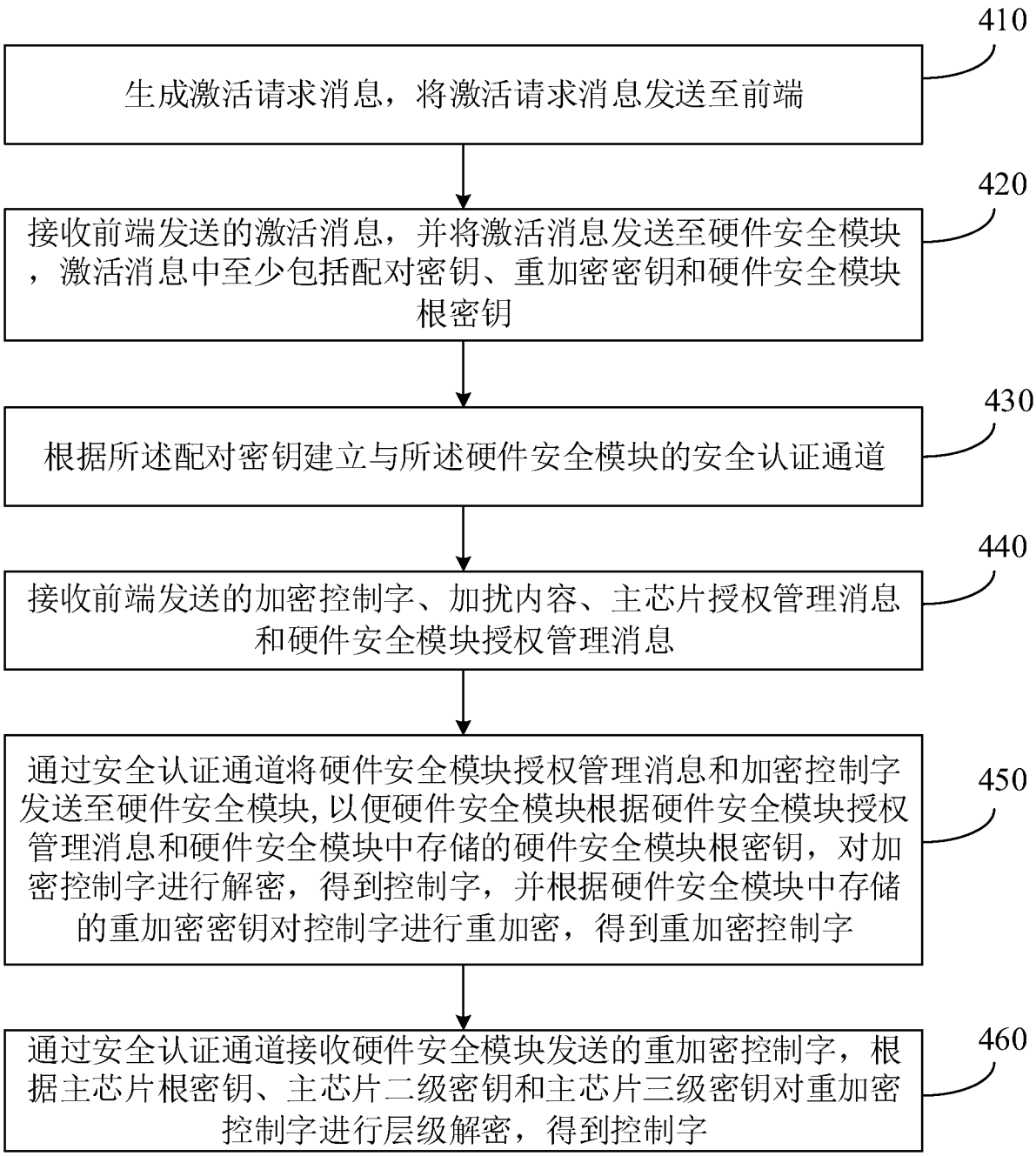
410
生成激活请求消息，将激活请求消息发送至前端
420
接收前端发送的激活消息，并将激活消息发送至硬件安全模块，激活消息中至少包括配对密钥、重加密密钥和硬件安全模块根密钥
430
根据所述配对密钥建立与所述硬件安全模块的安全认证通道
440
接收前端发送的加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息
450
通过安全认证通道将硬件安全模块授权管理消息和加密控制字发送至硬件安全模块，以便硬件安全模块根据硬件安全模块授权管理消息和硬件安全模块中存储的硬件安全模块根密钥，对加密控制字进行解密，得到控制字，并根据硬件安全模块中存储的重加密密钥对控制字进行重加密，得到重加密控制字
460
通过安全认证通道接收硬件安全模块发送的重加密控制字，根据主芯片根密钥、主芯片二级密钥和主芯片三级密钥对重加密控制字进行层级解密，得到控制字

图 4

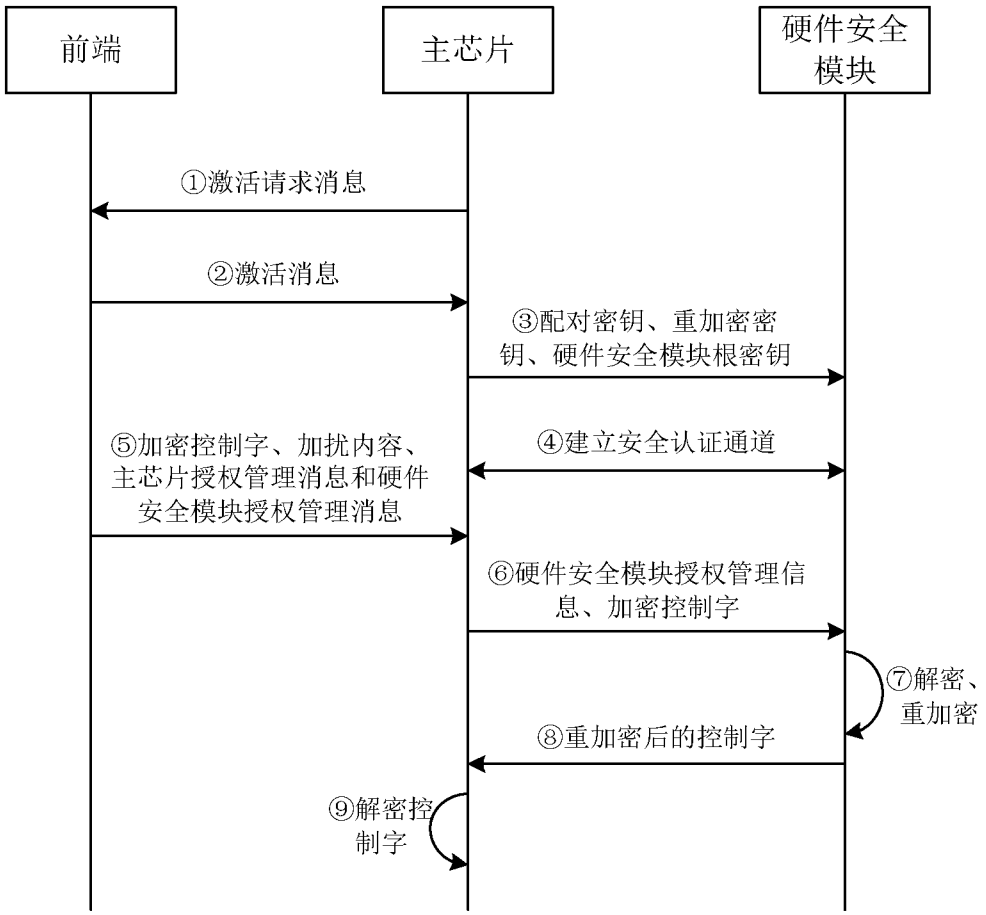
前端
主芯片
硬件安全模块
①激活请求消息
②激活消息
③配对密钥、重加密密钥、硬件安全模块根密钥
④建立安全认证通道
⑤加密控制字、加扰内容、主芯片授权管理消息和硬件安全模块授权管理消息
⑥硬件安全模块授权管理信息、加密控制字
⑦解密、重加密
⑧重加密后的控制字
⑨解密控制字

图 5

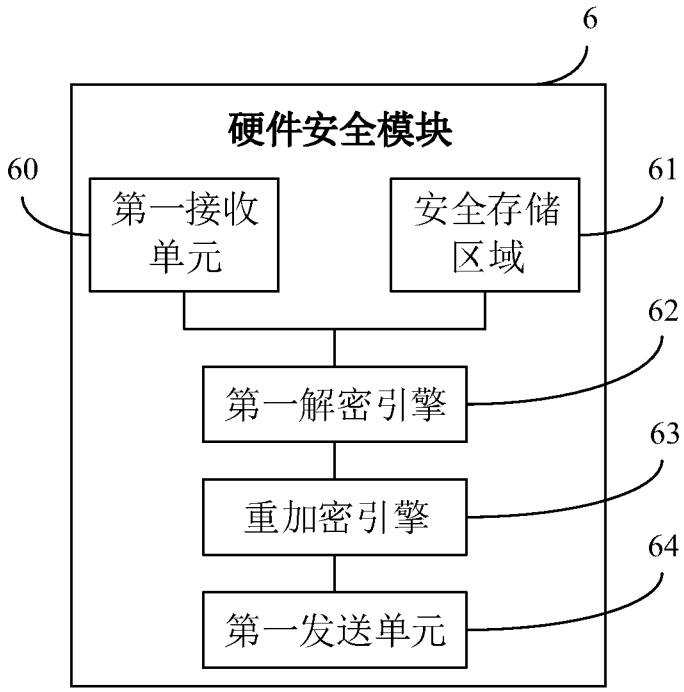
6
硬件安全模块
60
第一接收单元
61
安全存储区域
62
第一解密引擎
63
重加密引擎
64
第一发送单元

图 6

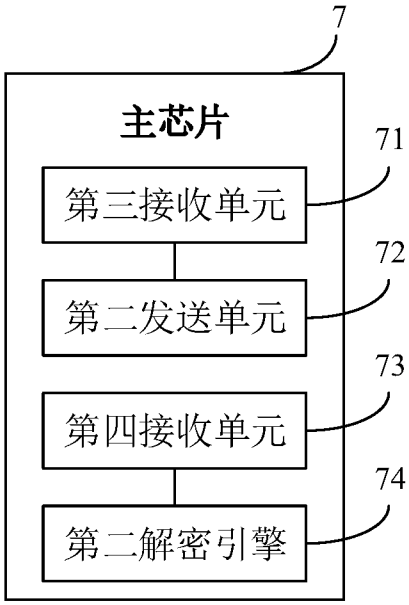
7
主芯片
71
第三接收单元
72
第二发送单元
73
第四接收单元
74
第二解密引擎

图 7

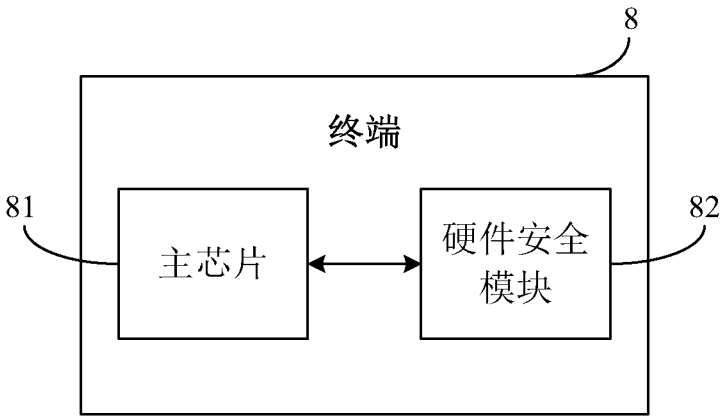
8
终端
81
主芯片
硬件安全模块
82

图 8

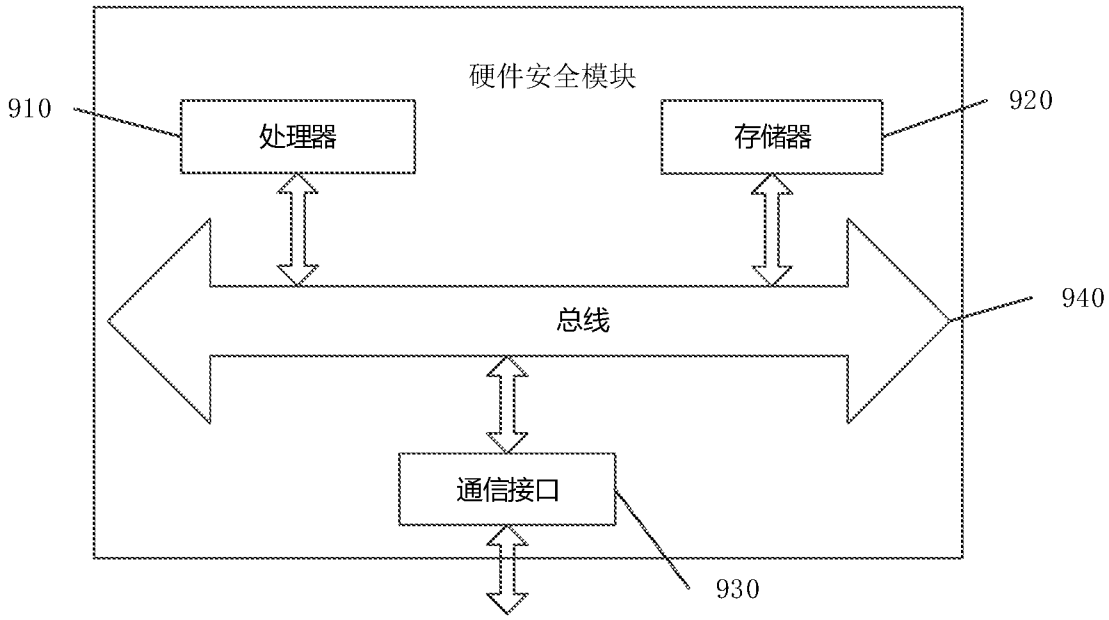

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/075999

A. CLASSIFICATION OF SUBJECT MATTER

H04N 21/418 (2011.01) i; H04N 21/266 (2011.01) 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)

H04N

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, CNKI, VEN: 控制字, 加密, 解密, 密钥, 硬件安全模块, 条件接收系统, 条件接入系统, control word, CW, encrypt, decrypt, key, hardware security module, HSM, DCAS, conditional access system, CAS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106803980 A (ACADEMY OF BROADCASTING SCIENCE, SAPPRFT et al.), 06 June 2017 (06.06.2017), description, paragraphs 37-137	1-18
Y	CN 102082971 A (WUHAN TIANYU INFORMATION INDUSTRY CO., LTD.), 01 June 2011 (01.06.2011), description, paragraphs 30-35	1, 3-5, 7-9, 11-13, 15-18
Y	CN 101924907 A (BEIJING NOVEL-SUPERTV DIGITAL TV TECHNOLOGY CO., LTD.), 22 December 2010 (22.12.2010), description, paragraphs 36-42	1, 3-5, 7-9, 11-13, 15-18
A	CN 102164320 A (UNITEND TECHNOLOGIES INC.), 24 August 2011 (24.08.2011), entire document	1-18
A	CN 101437145 A (BEIJING NOVEL-SUPERTV DIGITAL TV TECHNOLOGY CO., LTD.), 20 May 2009 (20.05.2009), entire document	1-18
A	WO 2008157522 A1 (GENERAL INSTRUMENT CORPORATION), 24 December 2008 (24.12.2008), entire document	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 April 2018	27 April 2018
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 WANG, Bo Telephone No. 86-010-62089145

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/075999

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106803980 A	06 June 2017	None	
CN 102082971 A	01 June 2011	CN 102082971 B	01 May 2013
CN 101924907 A	22 December 2010	CN 101924907 B	28 August 2013
CN 102164320 A	24 August 2011	US 9479825 B2	25 October 2016
		RU 2013150043 A	20 May 2015
		WO 2012139481 A1	18 October 2012
		US 2014082658 A1	20 March 2014
		EP 2699014 A4	22 April 2015
		EP 2699014 A1	19 February 2014
		CN 102164320 B	22 June 2016
CN 101437145 A	20 May 2009	CN 101437145 B	05 January 2011
WO 2008157522 A1	24 December 2008	CA 2688581 C	18 March 2014
		US 2008313463 A1	18 December 2008
		GB 2461474 B	04 July 2012
		US 8837723 B2	16 September 2014
		GB 2461474 A	06 January 2010

国际检索报告

国际申请号
PCT/CN2018/075999

A. 主题的分类

H04N 21/418(2011.01)i; H04N 21/266(2011.01)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)

H04N

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,CNKI,VEN:控制字，加密，解密，密钥，硬件安全模块，条件接收系统，条件接入系统，control word,CW,encrypt,decrypt,key,hardware security module,HSM,DCAS,conditional access system,CAS

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 106803980 A (国家新闻出版广电总局广播科学研究院等) 2017年 6月 6日 (2017-06-06) 说明书第37-137段	1-18
Y	CN 102082971 A (武汉天喻信息产业股份有限公司) 2011年 6月 1日 (2011-06-01) 说明书第30-35段	1，3-5，7-9，11-13，15-18
Y	CN 101924907 A (北京视博数字电视科技有限公司) 2010年 12月 22日 (2010-12-22) 说明书第36-42段	1，3-5，7-9，11-13，15-18
A	CN 102164320 A (北京数字太和科技有限责任公司) 2011年 8月 24日 (2011-08-24) 全文	1-18
A	CN 101437145 A (北京永新视博数字电视技术有限公司) 2009年 5月 20日 (2009-05-20) 全文	1-18
A	WO 2008157522 A1 (GENERAL INSTRUMENT CORPORATION) 2008年 12月 24日 (2008-12-24) 全文	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 4月 23日	2018年 4月 27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 王博 电话号码 86-010-62089145

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/075999

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	106803980	A	2017年 6月 6日	无			
CN	102082971	A	2011年 6月 1日	CN	102082971	B	2013年 5月 1日
CN	101924907	A	2010年 12月 22日	CN	101924907	B	2013年 8月 28日
CN	102164320	A	2011年 8月 24日	US	9479825	B2	2016年 10月 25日
				RU	2013150043	A	2015年 5月 20日
				WO	2012139481	A1	2012年 10月 18日
				US	2014082658	A1	2014年 3月 20日
				EP	2699014	A4	2015年 4月 22日
				EP	2699014	A1	2014年 2月 19日
				CN	102164320	B	2016年 6月 22日
CN	101437145	A	2009年 5月 20日	CN	101437145	B	2011年 1月 5日
WO	2008157522	A1	2008年 12月 24日	CA	2688581	C	2014年 3月 18日
				US	2008313463	A1	2008年 12月 18日
				GB	2461474	B	2012年 7月 4日
				US	8837723	B2	2014年 9月 16日
				GB	2461474	A	2010年 1月 6日