(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103383668 B
(45)授权公告日 2018.03.20

(21)申请号 201310159666.7

(22)申请日 2013.05.03

(65)同一申请的已公布的文献号
申请公布号 CN 103383668 A

(43)申请公布日 2013.11.06

(30)优先权数据
10-2012-0047743 2012.05.04 KR

(73)专利权人 三星电子株式会社
地址 韩国京畿道

(72)发明人 李宪洙 崔弘默 朴相炫

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 钱大勇

(51)Int.Cl.
G06F 12/14(2006.01)
G06F 21/79(2013.01)
G06F 13/28(2006.01)

(56)对比文件
EP 2161671 A2,2010.03.10,
EP 2226810 A1,2010.09.08,
US 2006090084 A1,2006.04.27,
CN 102346825 A,2012.02.08,
CN 101788958 A,2010.07.28,

审查员 李中兴

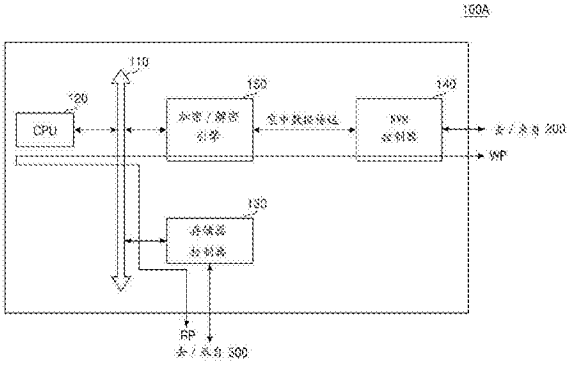
权利要求书1页 说明书9页 附图14页

(54)发明名称

片上系统、操作片上系统的方法和包括片上系统的设备

(57)摘要

提供一种片上系统、操作片上系统的方法和包括片上系统的设备。所述操作片上系统(SoC)的方法包括使用加密密钥将原数据转换为密码数据并且将密码数据直接传送到存储器控制器，所述存储器控制器控制非易失性存储器的操作。加密密钥可以通过一次性可编程(OTP)存储器来输出。



CN 103383668 B

1.一种片上系统SoC,包括:

SoC上的中央处理单元CPU;

易失性存储器控制器,配置为从外部易失性存储器接收原数据;

加密引擎,配置为使用加密密钥将从所述易失性存储器控制器传送的原数据加密为密码数据;

数据总线,连接到CPU和所述易失性存储器控制器;

非易失性存储器控制器,配置为:从所述加密引擎直接接收密码数据而使得密码数据不通过用于传送原数据的数据总线,以及向外部非易失性存储器输出密码数据;以及

存储介质,配置为存储加密密钥,

其中,所述加密引擎直接连接到所述非易失性存储器控制器,使得在所述加密引擎与所述非易失性存储器控制器之间不存在设备,并且其中,阻止CPU存取所述加密密钥。

2.如权利要求1所述的SoC,其中,所述存储介质是一次性可编程OTP存储器。

3.如权利要求1所述的SoC,还包括直接存储器存取DMA单元,用于从所述易失性存储器控制器接收原数据并且将原数据传送到加密引擎。

4.如权利要求3所述的SoC,其中,所述DMA单元连接到加密引擎。

5.一种片上系统SoC,包括:

SoC上的中央处理单元CPU;

易失性存储器控制器,配置为从外部易失性存储器接收原数据;

加密引擎,配置为使用加密密钥将从所述易失性存储器控制器传送的原数据加密为密码数据,所述加密密钥由CPU在安全模式下输入到所述加密引擎;

数据总线,连接到CPU和所述易失性存储器控制器;

非易失性存储器控制器,配置为:从所述加密引擎直接接收密码数据而使得密码数据不通过用于传送原数据的数据总线,以及向外部非易失性存储器输出密码数据;以及

存储介质,配置为存储加密密钥,

其中,所述加密引擎直接连接到所述非易失性存储器控制器,使得在所述加密引擎与所述非易失性存储器控制器之间不存在设备。

6.如权利要求5所述的SoC,其中,所述存储介质是一次性可编程OTP存储器。

7.如权利要求5所述的SoC,还包括直接存储器存取DMA单元,用于从所述易失性存储器控制器接收原数据并且将原数据传送到加密引擎。

8.如权利要求7所述的SoC,其中,所述DMA单元连接到加密引擎。

9.如权利要求8所述的SoC,进一步包括选择电路,所述选择电路具有旁路路径,其中,响应于选择信号,所述原数据经由旁路路径被传送到非易失性存储器控制,以及其中,所述非易失性存储器控制器配置为将所述原数据传送到所述外部非易失性存储器。

10.如权利要求9所述的SoC,其中,所述选择电路进一步包括复用器,所述复用器配置为接收选择信号并且将所述原数据传送到所述旁路路径。

片上系统、操作片上系统的方法和包括片上系统的设备

[0001] 相关申请的交叉引用

[0002] 本申请要求于2012年5月4日向韩国知识产权局提交的韩国专利申请第10-2012-0047743号的优先权，其公开整体地通过引用并入于此。

技术领域

[0003] 本发明构思的示例性实施例涉及片上系统(SoC)、操作SoC的方法和包括SoC的设备。

背景技术

[0004] 主存储器可以从例如非易失性存储设备的单独存储介质接收将由中央处理单元(CPU)执行的程序和CPU所需的数据。主存储器可以将数据传送到例如非易失性存储设备的该单独存储介质，以便存储数据。

[0005] 在主存储器与非易失性存储设备之间交换的数据可被加密以防止未授权用户访问该数据。包括主存储器和非易失性存储设备的系统的性能根据主存储器和非易失性存储设备之间交换数据所使用的路径而不同。

发明内容

[0006] 根据本发明构思的示例性实施例，一种操作片上系统(SoC)的方法包括：通过SoC内的引擎使用加密密钥将原数据(plain data)转换为密码数据；和通过引擎将密码数据直接传送到SoC内的存储器控制器，所述存储器控制器控制非易失性存储器的操作。根据示例性实施例，原数据可以是在中央处理单元(CPU)的控制下经由总线从主存储器读取的数据。例如，在转换之前，所述方法可以包括SoC从主存储器读取原数据。根据示例性实施例，原数据可以是从直接存储器存取(DMA)单元输出的数据。例如，在转换之前，所述方法可以包括SoC内的DMA单元将原数据输出到引擎。

[0007] 所述加密密钥可以从一次性可编程(OTP)存储器输出。例如，在转换之前，所述方法可以包括SoC内的OTP将密钥输出到引擎。所述加密密钥可以仅根据安全程序被输入。例如，在转换之前，所述方法可以包括仅在(例如由SoC内的CPU)正在执行安全程序时将密钥输出到引擎。

[0008] 在所述转换中，可以以块为单位将原数据转换为密码数据。

[0009] 根据本发明构思的示例性实施例，一种操作片上系统(SoC)的方法包括：通过SoC内的引擎从SoC内的存储器控制器直接接收密码数据，所述存储器控制器控制非易失性存储器的操作；和通过引擎使用加密密钥将密码数据转换为原数据。

[0010] 所述方法可以进一步包括将原数据传送到直接存储器存取(DMA)单元。例如，在转换之前，所述方法可以进一步包括SoC内的DMA单元将原数据传送到引擎。在转换中，可以以块为单位将密码数据转换为原数据。

[0011] 根据本发明构思的示例性实施例，一种片上系统(SoC)包括：加密/解密引擎，用于

首先使用加密密钥将第一原数据加密为第一密码数据或者将第二密码数据解密为第二原数据；和存储器控制器，其直接连接到加密/解密引擎，并且将第一密码数据传送到非易失性存储器或者从非易失性存储器接收第二密码数据。

[0012] 所述SoC可以还包括用于存储加密密钥的一次性可编程(OTP)存储器。所述SoC可以还包括直接存储器存取(DMA)单元，用于将从数据源接收的第一原数据传送到加密/解密引擎或者将从加密/解密引擎接收的第二原数据传送到数据源。例如，所述DMA单元可以从SoC外的设备接收第一原数据和将第一原数据传送到引擎或者将从引擎接收的第二原数据传送到设备。

[0013] 所述DMA单元可以直接连接到加密/解密引擎。所述的SoC可以还包括CPU，用于控制第一原数据或第二原数据在数据源与加密/解密引擎之间的传送。例如，所述数据源可以是位于SoC外的设备。

[0014] 根据本发明构思的示例性实施例，一种系统级封装包括SoC和在SoC的控制下与非易失性存储器通信数据的数据源。所述数据源可以是SoC外的设备。根据本发明构思的示例性实施例，一种系统级封装包括SoC、非易失性存储器和在SoC的控制下与非易失性存储器通信数据的数据源。

[0015] 根据本发明构思的示例性实施例，一种片上系统(SoC)包括：存储器控制器，被配置成控制非易失性存储器；和加密/解密引擎，其直接连接到存储器控制器并且被配置成加密或解密数据。所述SoC控制数据在数据源(例如，SoC外的设备)与非易失性存储器之间的传送。所述存储器控制器和引擎对应于用于传送数据的第一数据路径。

[0016] 根据本发明构思的示例性实施例，一种电子设备包括数据源、非易失性存储器和控制数据源与非易失性存储器之间的数据传送的片上系统(SoC)。所述SoC可以包括：控制非易失性存储器的存储器控制器；和加密/解密引擎，其直接连接到存储器控制器并且加密或解密数据。所述加密/解密引擎可以使用存储在一次性可编程(OTP)存储器中的加密密钥来加密或解密数据。

[0017] 根据本发明构思的示例性实施例，一种片上系统(SoC)包括：数据总线；主存储器控制器，被配置成将原数据输出到总线；引擎，被配置成使用密钥将来自总线的原数据加密为密码数据；NVM控制器；第一电路径，用于将总线连接到NVM控制器以便旁路加密引擎；和第二电路径，用于通过加密引擎将总线连接到NVM控制器。在非安全模式中，所述SoC仅激活第一电路径(例如禁用第二电路径)用于将来自总线的原数据发送到NVM控制器。在安全模式中，所述SoC仅激活第二电路径(例如禁用第一电路径)用于将原数据发送到引擎并且将来自引擎的密码数据发送到NVM控制器。

[0018] 所述第一电路径可以包括原数据(plain text)通过复用器和信号分离器到NVM控制器的路径。所述第二电路径可以包括原数据通过复用器到引擎的路径和密码数据通过信号分离器到NVM控制器的路径。所述SoC可以进一步包括OTP存储器，其被配置成将相同选择信号提供给复用器和信号分离器用以激活第一和第二电路径之一。所述引擎可被配置成解密穿过第二电路径从NVM控制器接收的密码数据。

附图说明

[0019] 图1是根据本发明构思的示例性实施例的包括片上系统(SoC)的系统的方框图；

[0020] 图2是根据本发明构思的示例性实施例的图1中图示的SoC的方框图；

[0021] 图3是用于描述安全模式的概念图，在所述安全模式中加密密钥可被输入到图2中图示的加密/解密引擎；

[0022] 图4是根据本发明构思的示例性实施例的图1中图示的SoC的方框图；

[0023] 图5是根据本发明构思的示例性实施例的图1中图示的SoC的方框图；

[0024] 图6是根据本发明构思的示例性实施例的图1中图示的SoC的方框图；

[0025] 图7是根据本发明构思的示例性实施例的图1中图示的SoC的方框图；

[0026] 图8是根据本发明构思的示例性实施例的图7中图示的选择电路和加密/解密引擎的方框图；

[0027] 图9是根据本发明构思的示例性实施例的图1中图示的SoC的方框图；

[0028] 图10是根据本发明构思的示例性实施例的操作SoC的方法的流程图；

[0029] 图11是根据本发明构思的示例性实施例的操作SoC的方法的流程图；

[0030] 图12是根据本发明构思的示例性实施例的操作SoC的方法的流程图；

[0031] 图13是根据本发明构思的示例性实施例的操作SoC的方法的流程图；

[0032] 图14是根据本发明构思的示例性实施例的包括图1的系统的数据处理设备的方框图；

[0033] 图15是根据本发明构思的示例性实施例的包括图1的系统的数据处理设备的方框图；

[0034] 图16是根据本发明构思的示例性实施例的包括图1的系统的数据处理设备的方框图；

[0035] 图17是根据本发明构思的示例性实施例的包括图1中图示的SoC和图1中图示的非易失性存储器设备的系统级封装的方框图；和

[0036] 图18是根据本发明构思的示例性实施例的包括图1中图示的SoC的系统级封装的方框图。

具体实施方式

[0037] 此处，当一个设备被描述为将数据传送到另一个设备时，所述数据或者是从一个设备直接传送或者间接传送到另一个设备。在一个设备直接传送数据的示例性实施例中，除了电线外不通过另一个设备将数据从一个设备传送到另一个设备。在一个设备间接传送数据的示例性实施例中，不使用另外的设备通过复用器或信号分离器将数据从一个设备传送到另一个设备。

[0038] 此处，当一个设备被描述为连接到另一个设备时，这些设备可以直接连接或者间接连接到另一个设备。在两个设备彼此直接连接的实施例中，除了电线外两个设备之间不存在其他设备。在两个设备彼此间接连接的实施例中，除了复用器或信号分离器以外两个设备之间不存在其他设备。

[0039] 将会理解，此处描述的装置和方法能够以各种形式的硬件、软件、固件、特殊用途处理器或者它们的组合来实现。具体地，本发明构思的一部分可被实现为包括程序指令的应用程序，所述程序指令具体体现在一个或多个程序存储设备或者计算机可读媒体(例如，硬盘、磁软盘、RAM、ROM、CD ROM等)上并且可由包括合适结构的任何设备或机器(例如具有

处理器、存储器和输入/输出接口的通用数字计算机)执行。将进一步理解,因为附图中描绘的一些组成装置组件和处理步骤可以以软件来实现,装置模块(或者方法步骤的逻辑流程)之间的连接可以根据本发明构思被编程的方式而不同。

[0040] 图1是根据本发明构思的示例性实施例的包括片上系统(SoC)100的系统10的方框图。参考图1,系统10包括SoC100、非易失性存储器设备200和主存储器300。

[0041] 系统10可以使用个人电脑(PC)、数据服务器或者便携式设备来实现。例如,便携式设备可以使用膝上型电脑、移动电话、智能电话、平板PC、个人数字助理(PDA)、企业数字助理(EDA)、数码相机、数码摄像机、便携式多媒体播放器(PMP)、个人(或便携式)导航设备(PND)、手持式游戏控制台或者电子书来实现。

[0042] SoC100可以控制非易失性存储器设备200与主存储器300之间的数据传送和接收。后面将参考图2和4到9来详细描述SoC100的结构和操作。

[0043] 非易失性存储器设备200可以存储各种程序和数据。非易失性存储器设备200可以使用电可擦除可编程只读存储器(EEPROM)、快闪存储器、磁性随机存取存储器(MRAM)、自旋转移力矩MRAM、传导桥RAM(CBRAM)、铁电RAM(FeRAM)、相变RAM(PRAM)RAM、电阻RAM(RRAM)、纳米管RRAM、聚合体RAM(PoRAM)、纳米浮栅存储器(NFGM)、全息存储器、分子电子存储器设备(molecular electronics memory device)、绝缘电阻变化存储器等来实现。

[0044] 主存储器300可以经由SoC100从非易失性存储器设备200接收将在SoC100中执行的程序以及SoC100所需的数据。主存储器300可以经由SoC100把将要存储的数据传送到非易失性存储器设备200。主存储器300可以使用例如动态RAM(DRAM)或者静态RAM(SRAM)的RAM(这是易失性存储器)来实现。然而,主存储器300不限于RAM、DRAM或SRAM,而是可以使用不同类型的存储器。

[0045] 图2是作为图1的SoC100实施例的SoC100A的方框图。参考图2,SoC100A包括总线110、中央处理单元(CPU)120、存储器控制器130、非易失性存储器控制器140和加密/解密引擎150。

[0046] CPU120可以连接到总线110并且可以控制SoC100A的整体操作。存储器控制器130可以控制主存储器300的操作,例如读或写操作。存储器控制器130可以连接到总线110。

[0047] 非易失性存储器控制器140可以控制非易失性存储器设备200的数据读取操作,例如写操作、读操作、编程操作或擦除操作。

[0048] 加密/解密引擎150可以将经由存储器控制器130和总线110从主存储器300接收的原数据转换(即加密)为密码数据(例如,加密的数据)。加密/解密引擎150可以将密码数据直接(例如在空中(on-the-fly))传送到非易失性存储器控制器140,而不通过总线110。

[0049] 在示例性实施例中,加密/解密引擎150不通过总线110从非易失性存储器控制器140直接(例如在空中)接收密码数据。加密/解密引擎150可以将密码数据转换(例如解密)为原数据(例如未加密的数据)。

[0050] 在加密/解密引擎150的加密或解密中可以使用加密密钥。在示例性实施例中,加密/解密引擎150包括用于存储加密密钥的存储介质(未示出)。例如,该存储介质可以是寄存器、锁存器、闪存等。根据示例性实施例,加密密钥仅在安全模式中被输入到存储介质。后面将参考图3来描述该安全模式。

[0051] 加密/解密引擎150可以以预定大小(例如64位、128位或256位)的块为单位来加密

或解密数据。

[0052] 当加密/解密引擎150以块为单位加密或解密时，可以将在加密或解密中使用的加密密钥和算法应用于每个块。例如，所述算法可以是数据加密标准(DES)算法或高级加密标准(AES)算法。然而，所述算法不限于此，而是可以使用其他加密或解密算法。

[0053] 所述安全模式可以确定加密/解密引擎150用来转换数据(例如以块为单位加密或解密数据)的方法。安全模式的示例包括电子源码书(electronic code book,ECB)模式、密码块链(cipher block chaining,CBC)模式、传播密码块链(propagating cipher block chaining,PCBC)模式或者密码反馈(cipher feed back,CFB)模式。在ECB中，每个块被独立地加密。在CBC中，每块原数据(例如未加密的数据)在被加密之前与先前的密码文本块(例如加密的数据)异或。PCBC是CBC的一种变型并且被设计成延伸或传播密码文本中的单个位错误，以便使得传送中的错误被捕获以及使得到的原数据将被拒绝。在CFB中，数据可以以比块大小要小的单位被加密。然而，安全模式不限于被设定为上述模式中的一种。

[0054] 在数据被写入到非易失性存储器设备200时的写数据路径WP中，从主存储器300输出的原数据(例如未加密的数据)经由存储器控制器130和总线110被传送到CPU120，并且随后经由总线110被从CPU120传送到加密/解密引擎150。换句话说，在CPU120的控制下，原数据被传送到加密/解密引擎150。

[0055] 加密/解密引擎150可以使用加密密钥将原数据转换为密码数据。该密码数据可经由非易失性存储器控制器140被传送到非易失性存储器设备200。在当从非易失性存储器设备200读取数据时的读数据路径RP中，从非易失性存储器设备200输出的密码数据经由非易失性存储器控制器140被传送到加密/解密引擎150。

[0056] 加密/解密引擎150可以使用解密密钥将密码数据转换为原数据。解密密钥可以与加密密钥相同或可以与加密密钥不同。原数据可以经由总线110传送到CPU120并且随后经由总线110和存储器控制器130从CPU120传送到主存储器300。换句话说，在CPU120的控制下，原数据可以经由总线110和存储器控制器130被传送到主存储器300。

[0057] 图3是用于描述安全模式的概念图，在所述安全模式中加密密钥或解密密钥可被输入到图2中图示的加密/解密引擎150。参考图2和图3，一般操作系统(OS)可以管理硬件并且可以安装在硬件中用来执行应用程序。

[0058] 安全OS也可独立于一般操作系统(OS)被安装在硬件中用来执行需要安全性的安全应用程序。安全OS可以使用实时操作系统(RTOS)来实现。例如，RTOS可被用来执行必须在预定的时间段内完成的应用程序，例如安全应用程序。安全OS可以是受信任的操作系统，其提供了多级安全性的充分支持以及满足政府机构特定需求的正确性的证据。

[0059] 非安全模式可以表示其中应用程序由一般OS执行的示例，而安全模式可以表示其中安全应用程序由安全OS执行的示例。

[0060] 在示例性实施例中，当安全应用程序以安全模式执行时，CPU120将加密密钥或解密密钥输入到加密/解密引擎150。在示例性实施例中，加密/解密引擎15可以访问存储在其自身内部或者加密/解密引擎150外部的加密密钥或解密密钥。在示例性实施例中，当安全应用程序以安全模式执行时，加密密钥或解密密钥可以改变或者重新设置。例如，当密钥改变时，出现的下一次加密/解密使用更新后的密钥。

[0061] 图4是作为图1的SoC100的示例性实施例的SoC100B的方框图。参考图1至4，

SoC100B包括总线110、CPU120、存储器控制器130、非易失性存储器控制器140、加密/解密引擎150和一次性可编程(OTP)存储器160。在示例性实施例中，OTP存储器160存储由加密/解密引擎150在加密或解密中使用的加密密钥或解密密钥。

[0062] 在示例性实施例中，OTP存储器160使用熔丝、反熔丝(anti-fuse)或电子熔丝(e-fuse)来实现。在示例性实施例中，反熔丝是对熔丝执行相反功能的电子设备。例如，尽管熔丝以低阻抗启动且被设计成永久地断开导电路径(例如，当通过路径的电流超过预定界限时)，但是反熔丝以高阻抗启动且被设计成永久地形成导电路径(例如，当反熔丝两端的电压超过预定电平时)。在示例性实施例中，电子熔丝允许计算机芯片的动态实时再编程。

[0063] 与图2的SoC100A相反，在图4的SoC100B中，CPU120可被实现为使得它被阻止访问存储在OTP存储器160中的加密密钥或解密密钥，即使安全应用程序以安全模式执行。例如，CPU120可被实现为使得它被阻止读、写或擦除所存储的密钥。图4的SoC100B的写数据路径WP和读数据路径RP基本分别与图2的SoC100A的那些路径相同，除了在数据的加密或解密中可以使用的加密密钥或解密密钥被OTP存储器160提供到加密/解密引擎150。

[0064] 图5是作为图1示出的SoC100的示例性实施例的SoC100C的方框图。参考图1和5，SoC100C包括总线110、CPU120、存储器控制器130、非易失性存储器控制器140、加密/解密引擎150、OTP存储器160和直接存储器存取(DMA)单元170。

[0065] DMA单元170可以经由组件(例如存储器控制器130、非易失性存储器控制器140或加密/解密引擎150)而不通过CPU120传递数据来访问主存储器300或非易失性存储器设备200。在该示例中，DMA单元170可以连接到总线110。

[0066] 在当数据被写入非易失性存储器设备200时的写数据路径WP中，从主存储器300输出的原数据经由存储器控制器130和总线110被传送到DMA单元170。原数据经由总线110被从DMA单元170传送到加密/解密引擎150。

[0067] 加密/解密引擎150将原数据转换为密码数据。从加密/解密引擎150输出的密码数据可被直接传送到非易失性存储器控制器140并且随后被传送到非易失性存储器设备200。换句话说，加密/解密引擎150可以将密码数据直接(例如在空中)传送到非易失性存储器控制器140。

[0068] 在当从非易失性存储器设备200读数据时的读数据路径RP中，从非易失性存储器设备200输出的密码数据经由非易失性存储器控制器140被传送到加密/解密引擎150。换句话说，加密/解密引擎150可以从非易失性存储器控制器140直接(例如在空中)接收密码数据。

[0069] 加密/解密引擎150将密码数据转换为原数据。原数据经由总线110被传送到DMA单元170。原数据可以经由总线110和存储器控制器130从DMA单元170被传送到主存储器300。

[0070] 图6是作为图1的SoC100的示例性实施例的SoC100D的方框图。参考图1和6，SoC100D包括总线110、CPU120、存储器控制器130、非易失性存储器控制器140、加密/解密引擎150、OTP存储器160和DMA单元170。

[0071] DMA单元170可以连接在总线110与加密/解密引擎150之间。数据可以在DMA单元170与加密/解密引擎150之间在空中传送。

[0072] 在当数据被写入非易失性存储器设备200时的写数据路径WP中，从主存储器300输出的原数据经由存储器控制器130、总线110和DMA单元170被传送到加密/解密引擎150。

[0073] 加密/解密引擎150可以将原数据转换(例如加密)为密码数据。密码数据可以经由非易失性存储器控制器140被传送到非易失性存储器设备200。在这个示例中,加密/解密引擎150可以将密码数据直接(例如在空中)传送到非易失性存储器控制器140。

[0074] 在当从非易失性存储器设备200读数据时的读数据路径RP中,从非易失性存储器设备200输出的密码数据经由非易失性存储器控制器140被传送到加密/解密引擎150。在这个示例中,加密/解密引擎150可以从非易失性存储器控制器140直接(例如在空中)接收密码数据。

[0075] 加密/解密引擎150可以将密码数据转换(例如解密)为原数据。原数据可以经由DMA单元170、总线110和存储器控制器130被传送到主存储器300。

[0076] 图7是作为图1的SoC100的示例性实施例的SoC100E的方框图。参考图1、3和7,SoC100E包括总线110、CPU120、存储器控制器130、非易失性存储器控制器140、加密/解密引擎150、OTP存储器160、DMA单元170、寄存器180和选择电路190。

[0077] 寄存器180可以连接到总线110。寄存器180可以操作为用于生成选择信号SEL的选择信号生成器。寄存器180可以基于CPU120是否执行安全应用程序、即基于指示安全模式的指示信号来改变选择信号SEL。指示信号可以通过CPU120来输出。例如,指示信号在安全模式中可以为逻辑高,而指示信号在非安全模式中可以为逻辑低。

[0078] 选择电路190可以根据寄存器180输出的选择信号SEL来选择数据路径。现在参考图8来描述选择电路190的示例性结构和操作。

[0079] 图8是根据本发明构思的示例性实施例的图7中图示的选择电路190和加密/解密引擎150的方框图。参考图3、7和8,选择电路190包括第一选择器192和第二选择器194。第一选择器192可以使用信号分离器来实现,而第二选择器194可以使用复用器来实现。

[0080] 例如,当选择信号SEL为逻辑高时,选择电路190选择包括加密/解密引擎150的数据路径。当CPU120执行安全应用程序时,即,在安全模式中,选择电路190选择包括加密/解密引擎150的数据路径。在示例性实施例中,当选择信号SEL为逻辑低时,选择电路190选择排除加密/解密引擎150的数据路径,即,旁路路径。例如,当CPU120执行一般应用程序时,即,在非安全模式中,选择电路190可以选择排除加密/解密引擎150的数据路径,即,旁路路径。

[0081] 图9是作为图1中图示的SoC100的示例性实施例的SoC100F的方框图。参考图1、8和9,SoC100F包括总线110、CPU120、存储器控制器130、非易失性存储器控制器140、加密/解密引擎150、OTP存储器160、DMA单元170、第二OTP存储器182和选择电路190。

[0082] 在示例性实施例中,第二OTP存储器182操作为用于生成选择信号SEL的选择信号生成器。在示例性实施例中,OTP存储器182被编成用来生成具有一个逻辑电平(例如逻辑高电平)的选择信号SEL。在这个实施例中,选择电路190仅选择包括加密/解密引擎150的数据路径。

[0083] 图10是根据本发明构思的示例性实施例的操作SoC的方法的流程图。参考图2、4到7、9和10,加密/解密引擎150使用加密密钥将原数据转换(例如加密)为密码数据(S10)。加密/解密引擎150可以将密码数据直接(例如在空中)传送到非易失性存储器控制器140(S12)。由于加密密钥存在于SoC100中而不是输出在SoC100外部,因此SoC与其他存储器设备(例如200和300)之间的通信的探索将不会发现密钥。

[0084] 图11是根据本发明构思的示例性实施例的操作SoC的方法的流程图。参考图5到7、9和10，加密/解密引擎150从DMA单元170接收原数据(S20)。在示例性实施例中，加密/解密引擎150从DMA单元170直接(例如在空中)接收原数据。然后类似于图10，加密/解密引擎150将原数据加密为密码数据(S10)并且将密码数据直接传送到非易失性存储器控制器(S12)。

[0085] 图12是根据本发明构思的示例性实施例的操作SoC的方法的流程图。参考图2、4到7、9和10，加密/解密引擎150从非易失性存储器控制器140直接(例如在空中)接收密码数据(S30)。加密/解密引擎150将密码数据解密为原数据(S32)。

[0086] 图13是根据本发明构思的示例性实施例的操作SoC的方法的流程图。类似于图12，加密/解密引擎150从非易失性存储器控制器直接接收密码数据(S30)并且将密码数据解密为原数据(S32)。参考图5到7、9和13，加密/解密引擎150将原数据传送到DMA单元170(S34)。在示例性实施例中，加密/解密引擎150将原数据直接(例如在空中)传送到DMA单元170。

[0087] 图14是根据本发明构思的示例性实施例的包括图1的系统10的数据处理设备400的方框图。参考图1和14，数据处理设备400可以使用个人电脑(PC)或数据服务器来实现。

[0088] 数据处理设备400包括处理器100、存储设备200、存储器300、电源410、输入/输出(I/O)端口420、扩展卡430、网络设备440和显示器450。数据处理设备400可以进一步包括相机模块460。在示例性实施例中，可以忽略处理设备400的一个或多个元件。

[0089] 处理器100可以对应于图1的SoC100。处理器100可以是多核处理器。在示例性实施例中，处理器100包括图1的SoC100。处理器100可以控制元件200、300和410-460的至少一个的操作。

[0090] 存储设备200可以对应于图1的非易失性存储器设备200。存储设备200可以使用硬盘驱动器或者固态驱动器(SSD)来实现。

[0091] 存储器300可以对应于图1的主存储器300。存储器300可以使用易失性存储器或非易失性存储器来实现。在示例性实施例中，图2的存储器控制器140能够针对存储器300控制数据存取操作，例如，读操作、写操作(或者编程操作)、或擦除操作。存储器300可被集成到或者被嵌入在处理器100中。

[0092] 电源410可以将操作电压提供给元件100、200、300和420-460中的至少一个。I/O端口420可以能够将数据传送到存储设备200或者将从存储设备200输出的数据传送到外部设备。例如，I/O端口420可以是用于将诸如计算机鼠标的定点设备连接到数据处理设备400的端口、用于将打印机连接到数据处理设备400的端口、或者用于将通用串行总线(USB)驱动器连接到数据处理设备400的端口。

[0093] 扩展卡430可以使用安全数字(SD)卡或多媒体卡(MMC)来实现。在示例性实施例中，扩展卡430是用户识别模块(SIM)卡或通用用户身份模块(USIM)卡。

[0094] 网络设备440可以对应于能够将存储设备200连接到有线或无线网络的设备。显示器450可以显示从存储设备200、存储器300、I/O端口420、扩展卡430或网络设备440输出的数据。

[0095] 相机模块460可以能够将光学图像转换为电图像。因此，从相机模块460输出的电图像可被存储在存储设备200、存储器300或扩展卡430中。从相机模块460输出的电图像可以在显示器450上显示。

[0096] 图15是根据本发明构思的示例性实施例的包括图1的系统10的数据处理设备500

的方框图。例如，数据处理设备500可以使用膝上型电脑来实现。

[0097] 类似于图14的数据处理设备400，图15的数据处理设备500包括处理器100、存储设备200、存储器300、电源510、输入/输出(I/O)端口520、扩展卡530、网络设备540和显示器550。数据处理设备500可以进一步包括相机模块560。在示例性实施例中，可以忽略处理设备500的一个或多个元件。

[0098] 图16是根据本发明构思的示例性实施例的包括图1的系统10的数据处理设备600的方框图。参考图1和16，数据处理设备600可以使用便携式设备来实现。

[0099] 便携式设备可以使用移动电话、智能电话、平板PC、个人数字助理(PDA)、企业数字助理(EDA)、数码相机、数码摄像机、便携式多媒体播放器(PMP)、个人(或便携式)导航设备(PND)、手持式游戏控制台或者电子书来实现。

[0100] 类似于图14的数据处理设备400，图16的数据处理设备600包括处理器100、存储设备200、存储器300、电源610、输入/输出(I/O)端口620、扩展卡630、网络设备640和显示器650。数据处理设备600可以进一步包括相机模块660。在示例性实施例中，可以忽略处理设备600的一个或多个元件。

[0101] 图17是根据本发明构思的示例性实施例的包括图1的SoC100和图1的非易失性存储器设备200的系统级封装(SiP)700的方框图。图18是根据本发明构思的示例性实施例的包括图1的SoC100的SiP700'的方框图。在示例性实施例中，SIP可以称作芯片堆栈MCM(多芯片模块)。SiP可以包括在单个模块或封装中包含的许多集成电路。

[0102] 参考图1和17，SoC100和主存储器300被封装到SiP700。因此，非易失性存储器200位于SiP700外部并且可以连接到SiP700的管脚。参考图1和18，SoC100、非易失性存储器设备200和主存储器300都被封装到SiP700'。

[0103] 根据本发明构思的示例性实施例的SoC在SoC内加密数据，因此可以阻止SoC与其他设备之间的通信的探索对未加密数据的访问。而且，根据示例性实施例的SoC在自身内存储用于加密的加密密钥而不将密钥输出自身外部，因此阻止了加密密钥暴露。

[0104] 在本发明构思的示例性实施例中，SoC的软件不能访问用于加密的加密密钥，这可以防止加密密钥由于黑客行为造成的泄露。由于SoC的软件不参与加密，因此软件的负担降低。在示例性实施例中，SoC包括直接连接的加密/解密引擎和存储器控制器，从而在SoC内数据传送路径变短。因此，SoC可提高性能。

[0105] 尽管已经示出并描述了本发明构思的示例性实施例，但是本领域的普通技术人员将会理解，在不背离本发明构思的精神和范畴的情况下可以在这些实施例中进行各种变化。

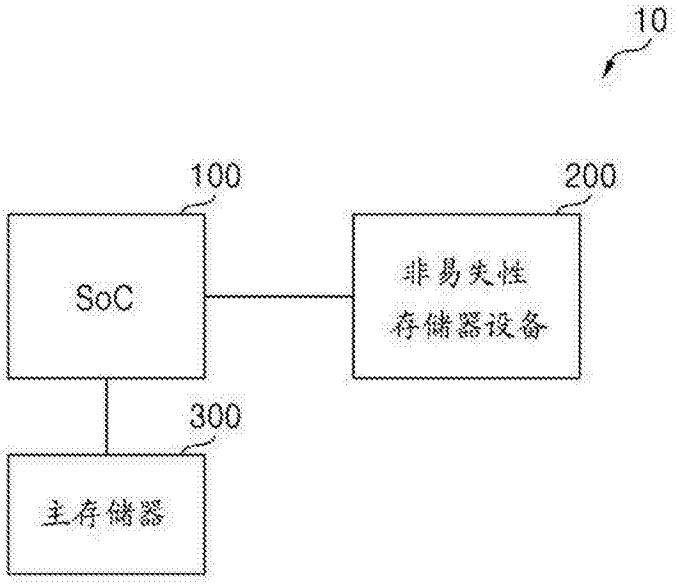


图1

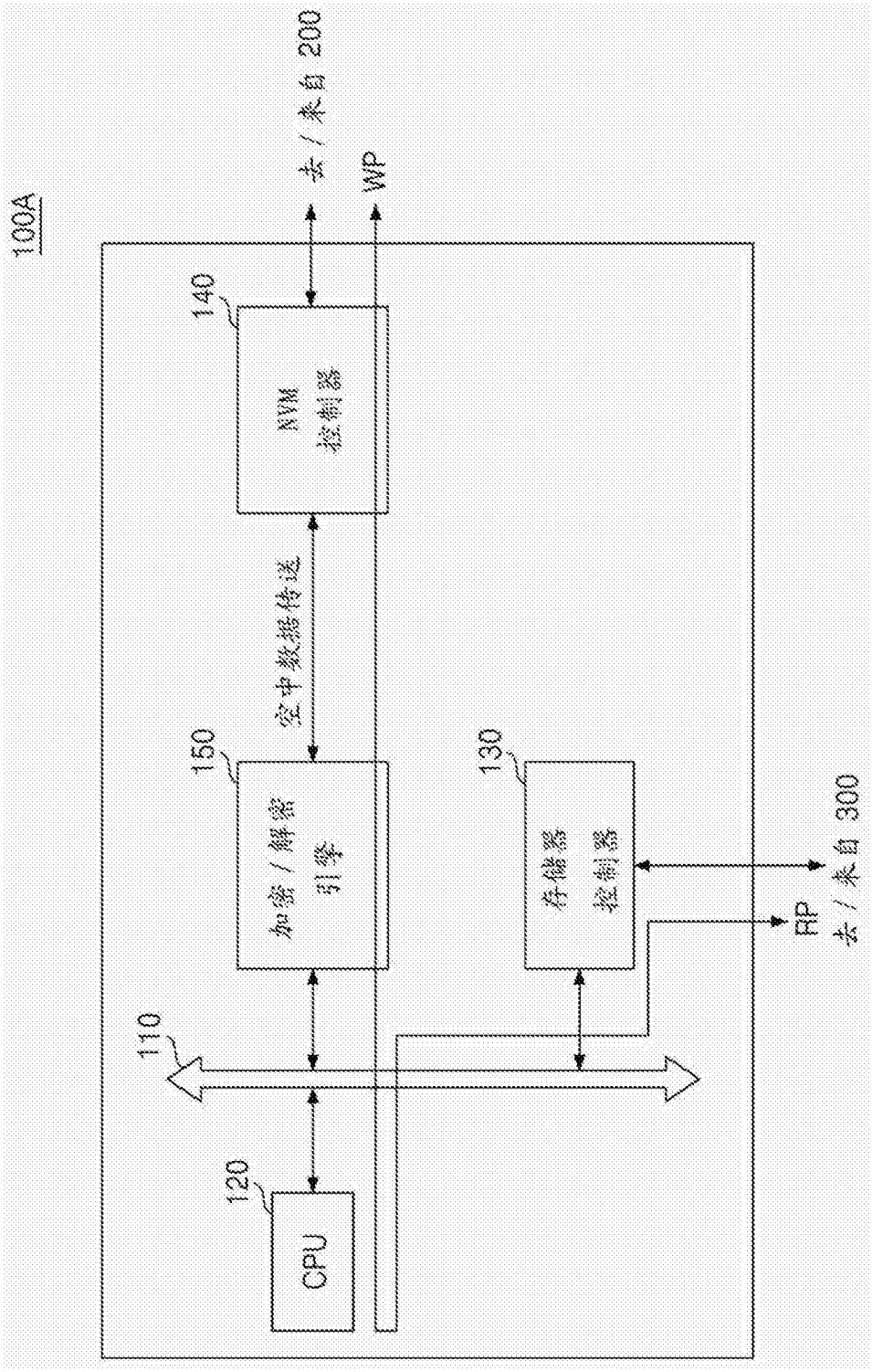

100A
去 / 来自 200
WP
140
NVM
控制器
空中数据传送
150
加密 / 解密
引擎
130
存储器
控制器
RP
去 / 来自 300
110
120
CPU

图2

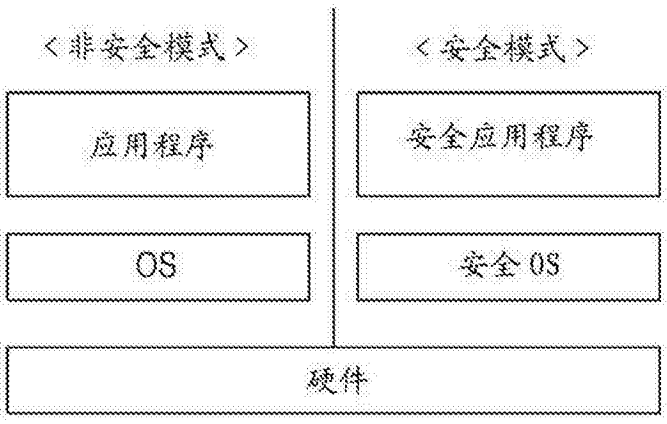


图3

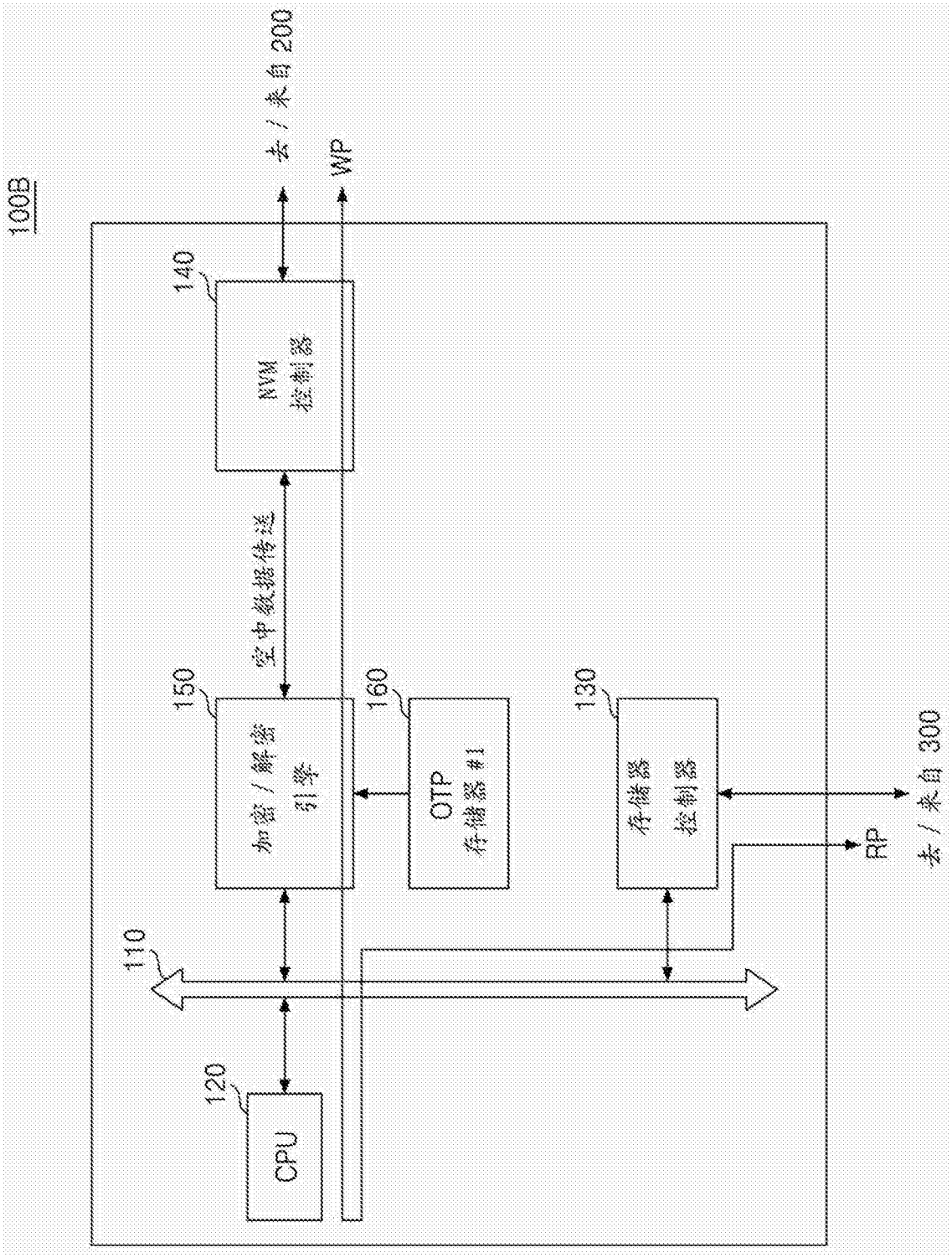

100B
去 / 来自 200
WP
140
NVM
控制器
空中数据传送
150
加密 / 解密
引擎
160
OTP
存储器 #1
130
存储器
控制器
RP
去 / 来自 300
110
120
CPU

图4

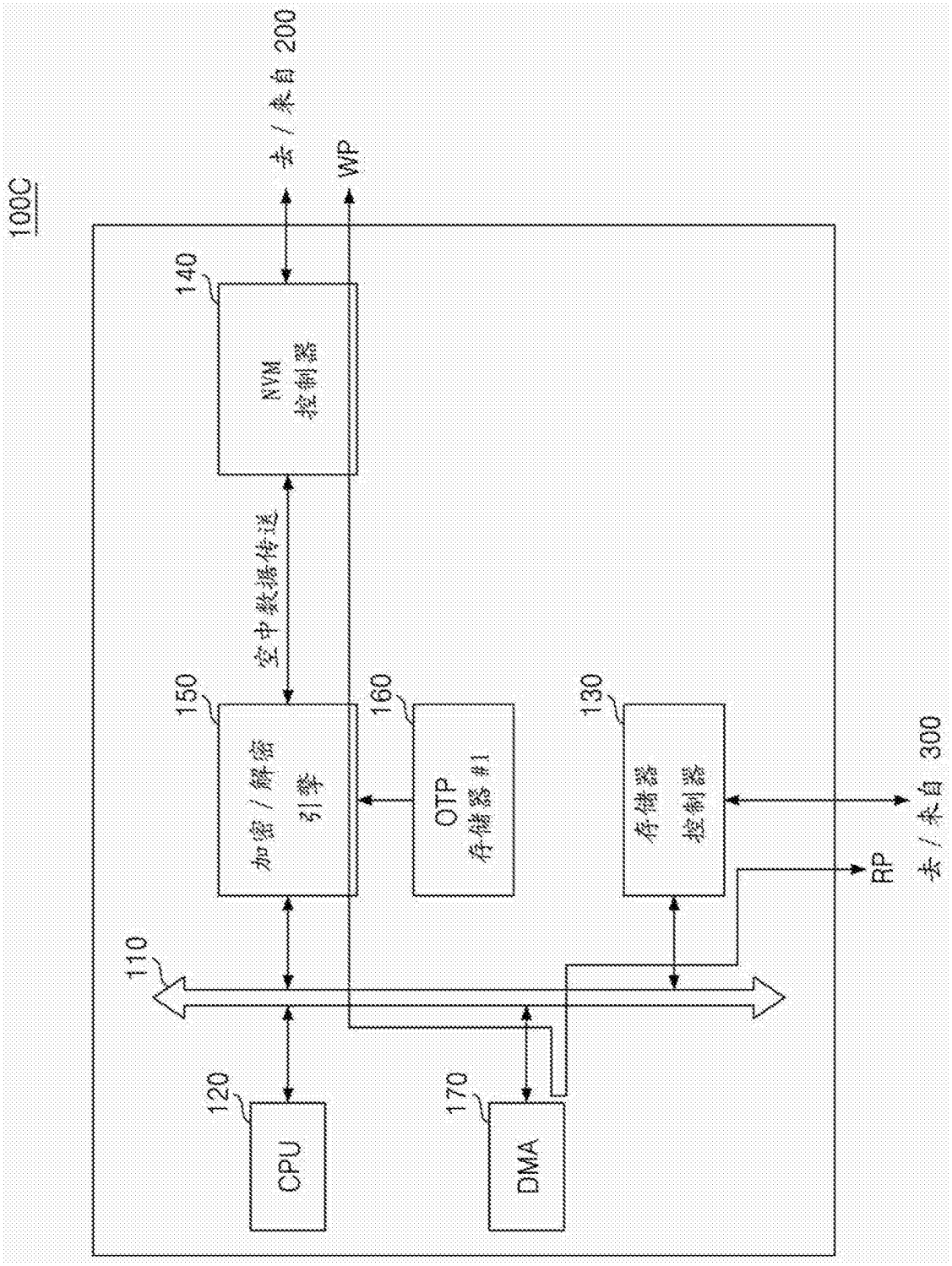

100C
去 / 来自 200
WP
140
NVM 控制器
空中数据传送
150
加密 / 解密 引擎
160
OTP 存储器 #1
130
存储器 控制器
RP
去 / 来自 300
110
120
CPU
170
DMA

图5

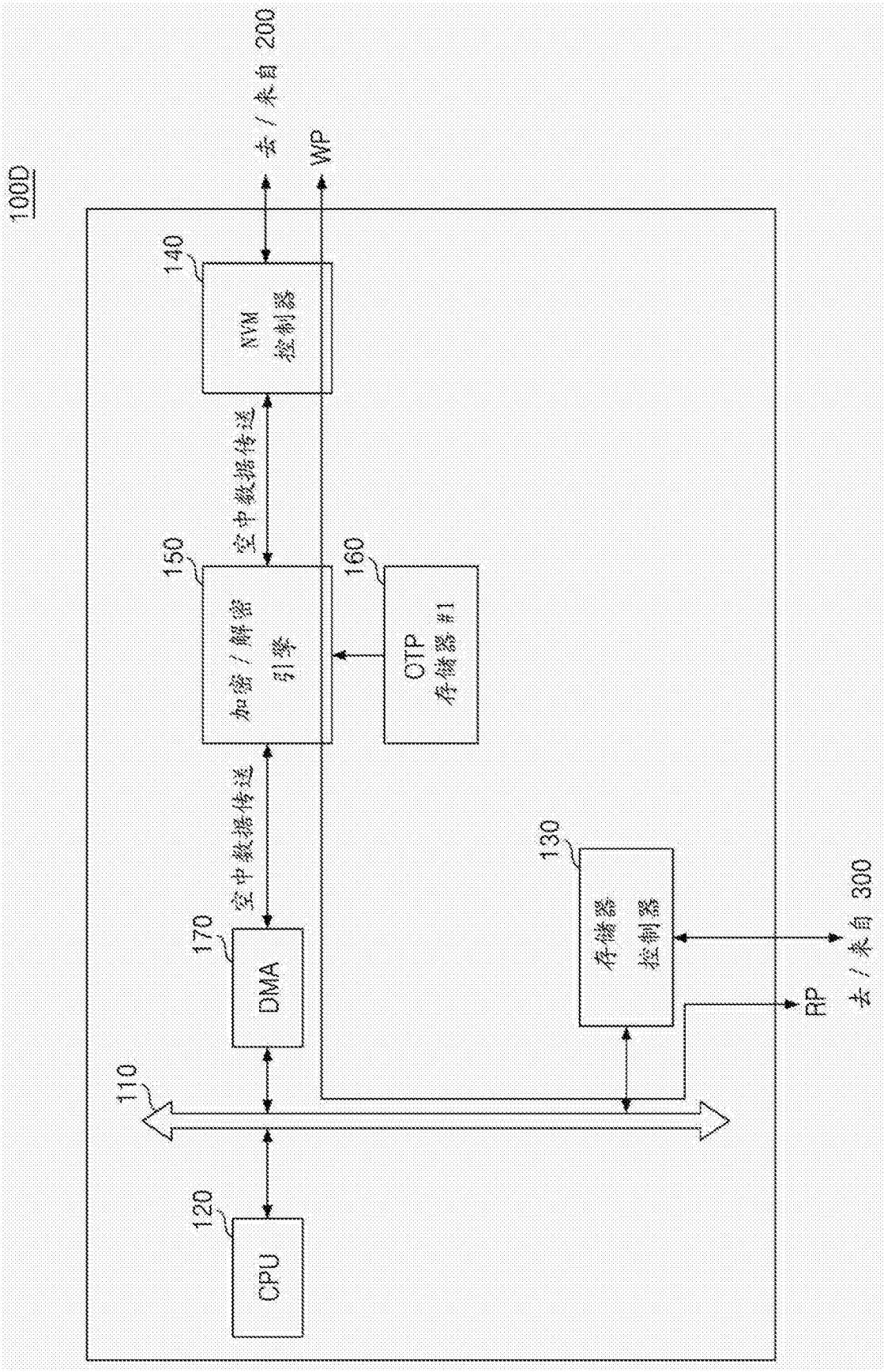

100D
去 / 来自 200
WP
140
NVM 控制器
空中数据传送
150
加密 / 解密 引擎
160
OTP 存储器 #1
空中数据传送
170
DMA
130
存储器 控制器
去 / 来自 300
RP
110
120
CPU

图6

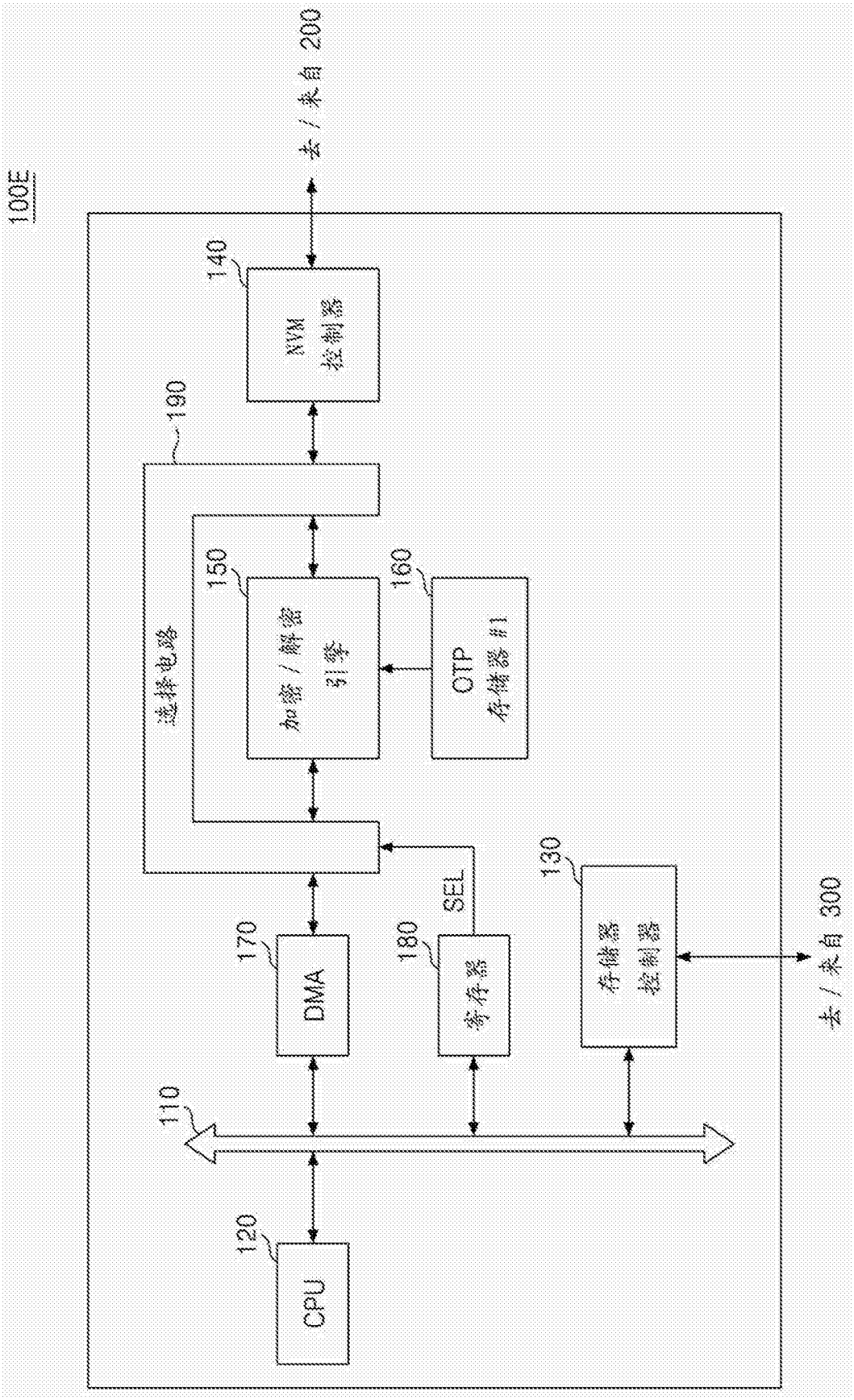

100E
去 / 来自 200
140
NVM
控制器
190
选择电路
150
加密 / 解密
引擎
160
OTP
存储器 #1
SEL
170
DMA
180
寄存器
130
存储器
控制器
去 / 来自 300
110
120
CPU

图7

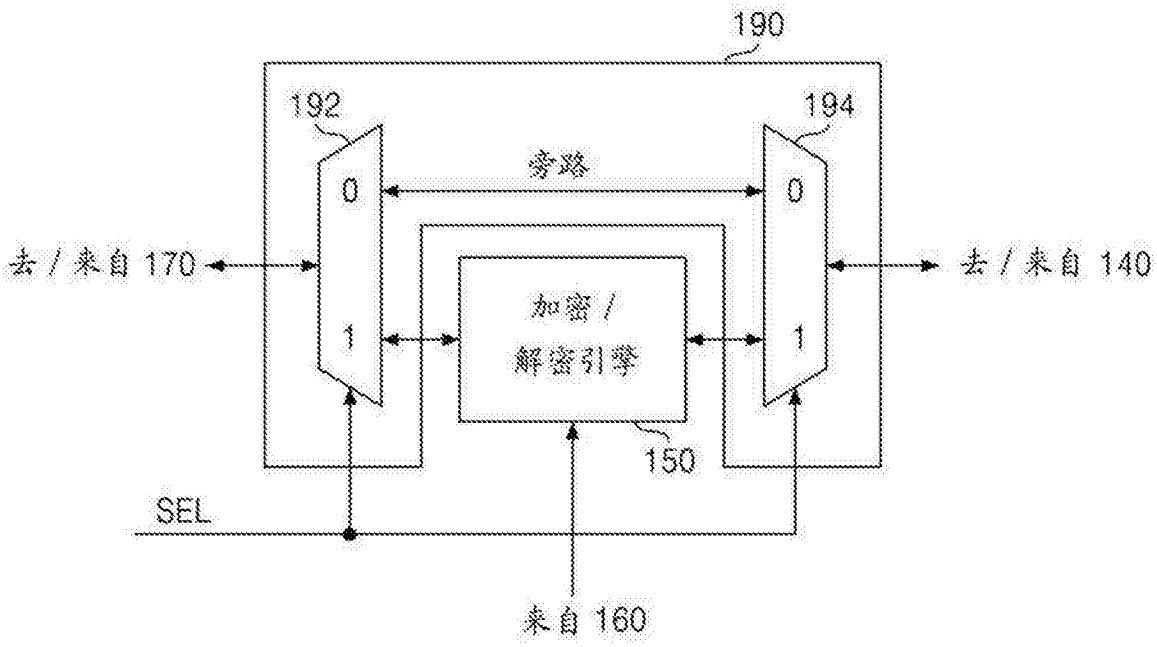


图8

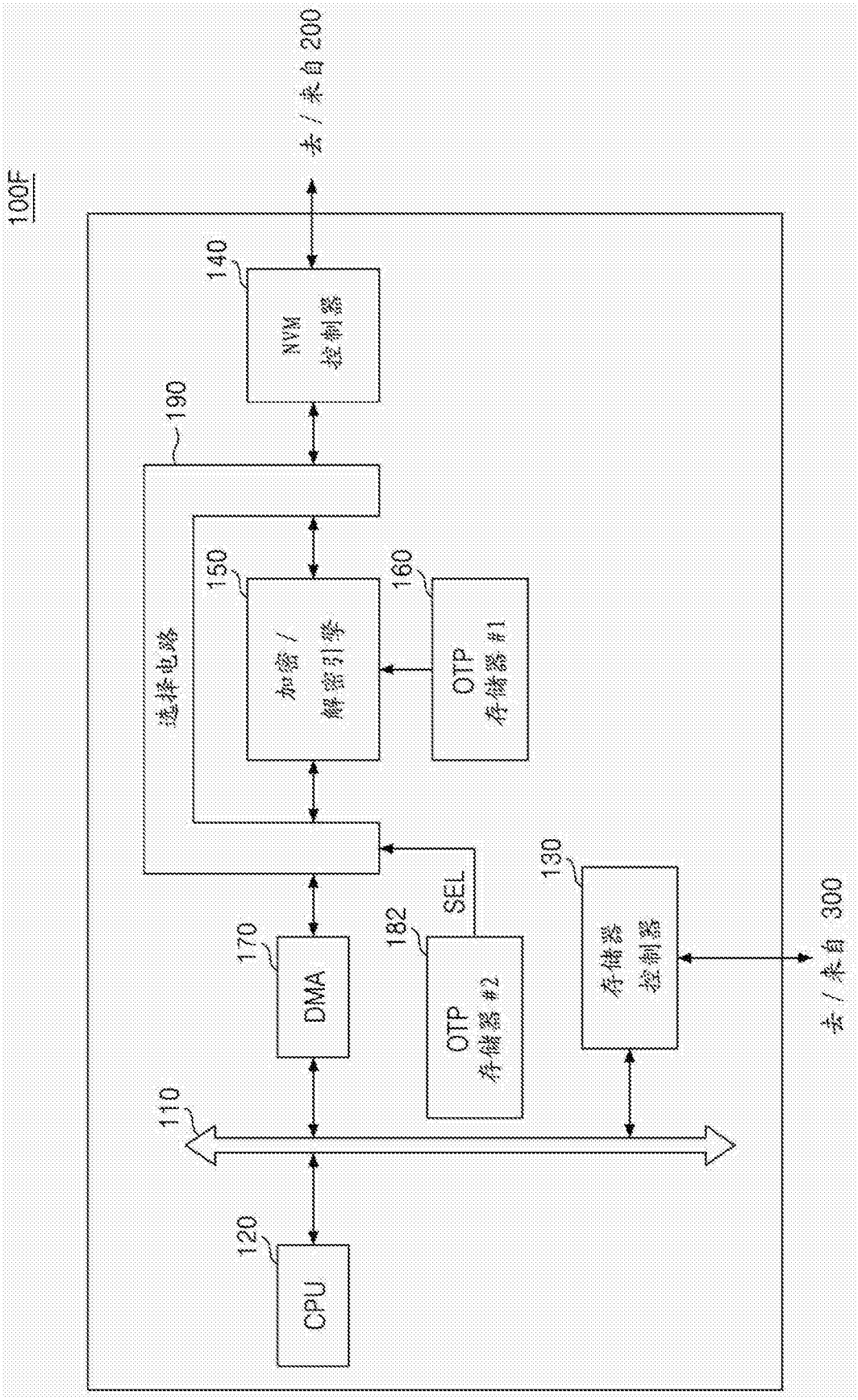

100F
去 / 来自 200
140
NVM 控制器
190
选择电路
150
加密 / 解密引擎
160
OTP 存储器 #1
SEL
182
OTP 存储器 #2
130
存储器控制器
去 / 来自 300
170
DMA
110
120
CPU

图9

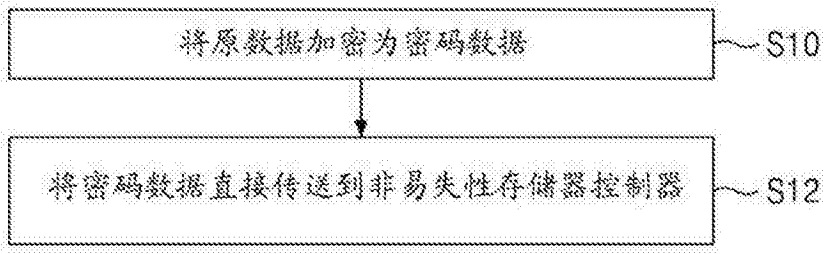


图10

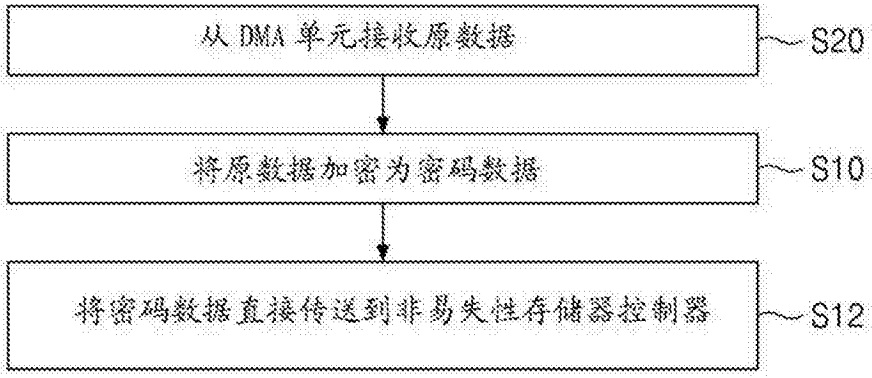


图11

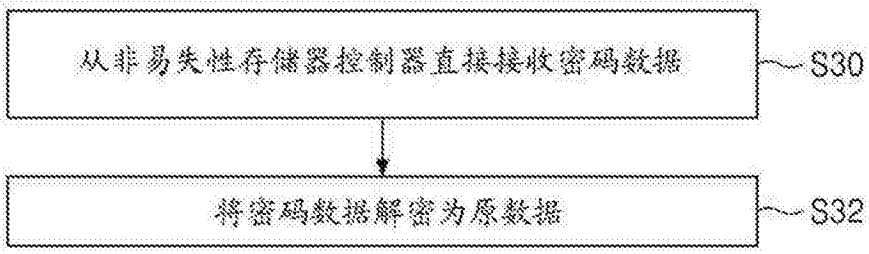


图12

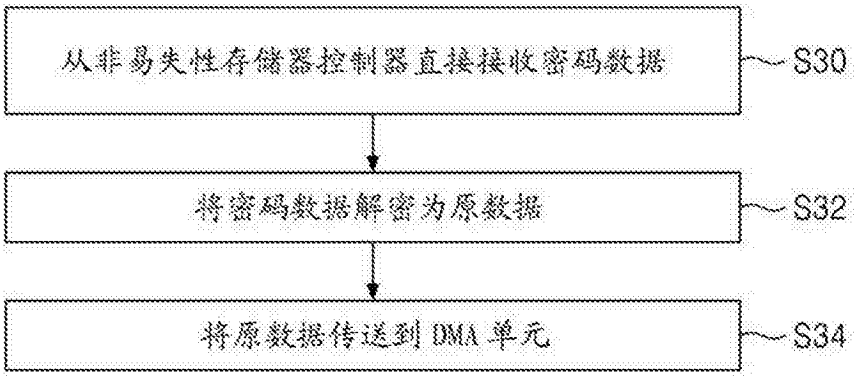


图13

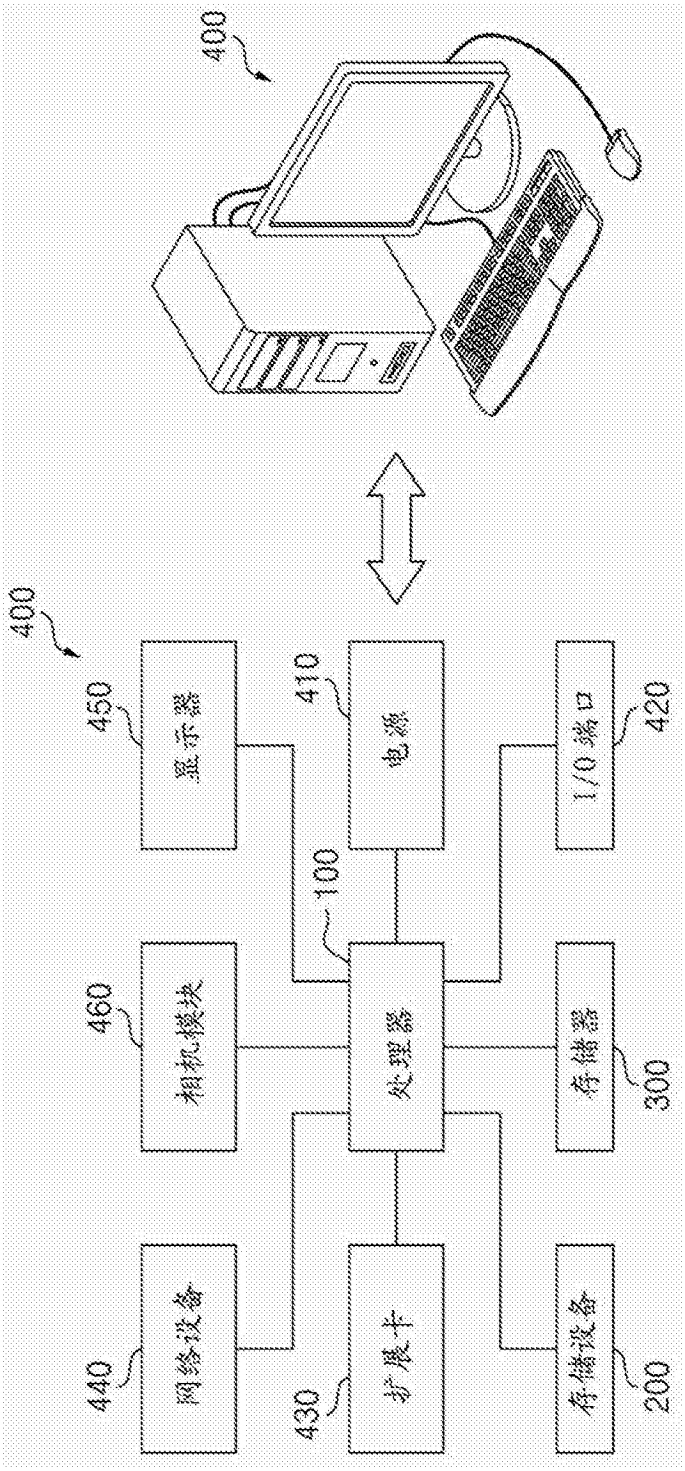

400
400
450
显示器
410
电源
420
I/O 端口
100
460
相机模块
处理器
300
存储器
440
网络设备
430
扩展卡
200
存储设备

图14

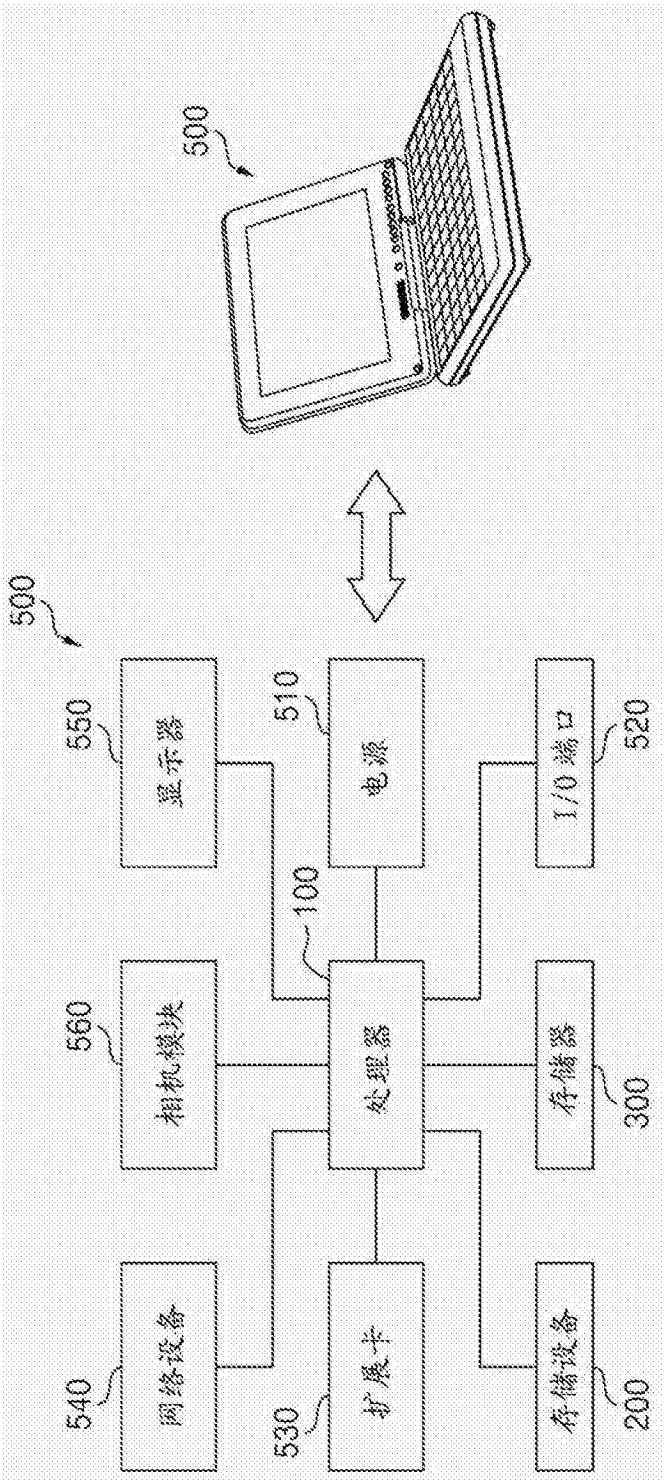

500
500
550
显示器
510
电源
520
I/O 端口
100
560
相机模块
处理器
存储器
300
540
网络设备
530
扩展卡
存储设备
200

图15

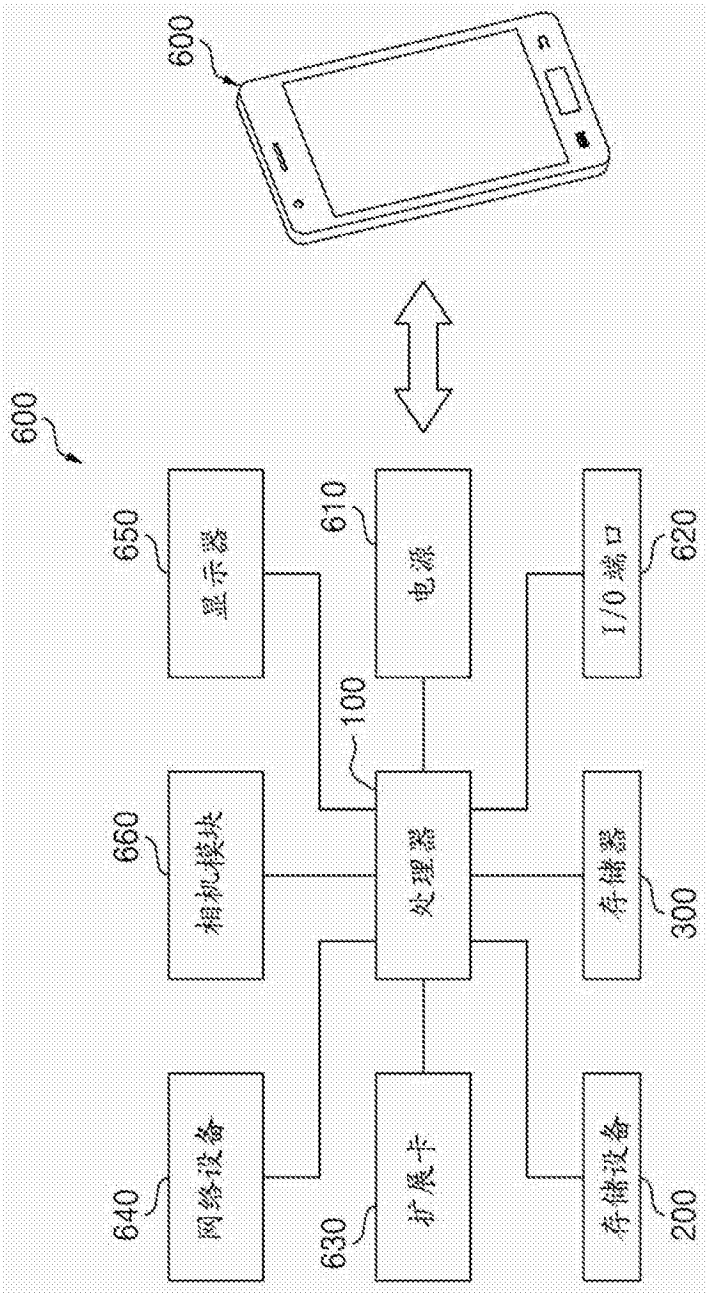

600
600
650
显示器
610
电源
620
I/O 端口
100
660
相机模块
处理器
存储器
300
640
网络设备
630
扩展卡
存储设备
200

图16

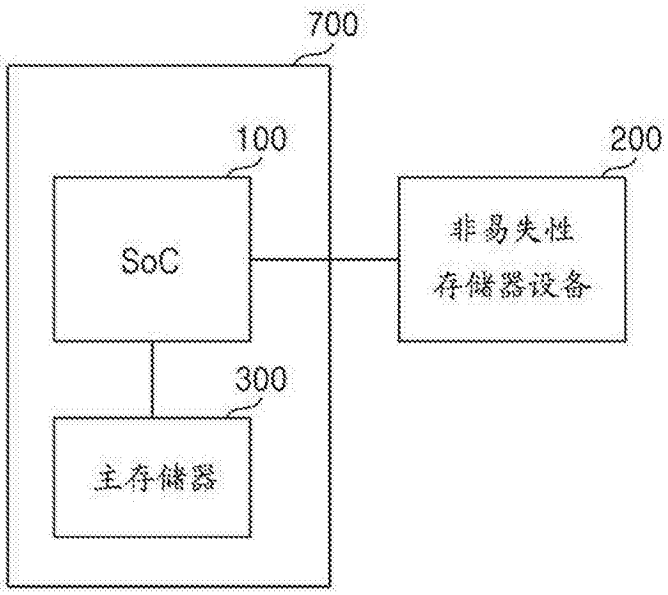

700
100
200
SoC
非易失性
存储器设备
300
主存储器

图17

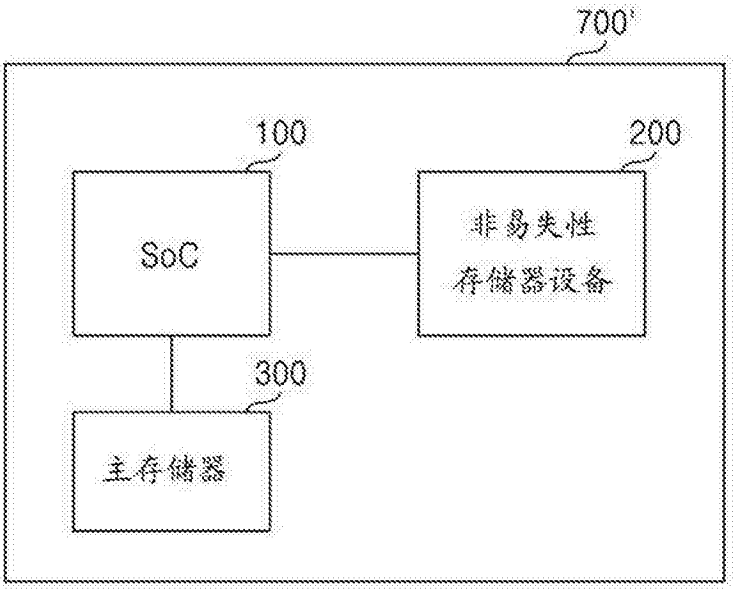

700'
100
200
SoC
非易失性
存储器设备
300
主存储器

图18