(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102968392 A
(43)申请公布日 2013.03.13

(21)申请号 201210312832.8

(22)申请日 2012.08.29

(30)优先权数据
1157603 2011.08.29 FR

(71)申请人 英赛瑟库尔公司
地址 法国普罗旺斯地区艾克斯

(72)发明人 B·菲克斯 G·加戈纳罗特

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 杨晓光 于静

(51)Int.Cl.
G06F 12/14(2006.01)

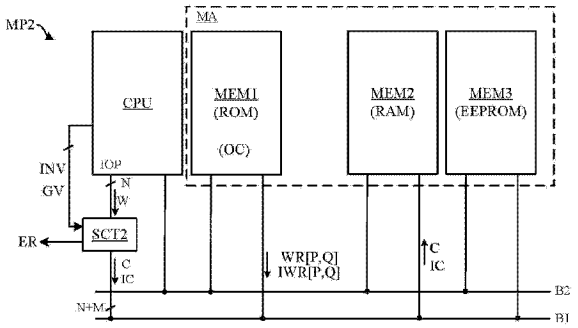
权利要求书 2 页 说明书 7 页 附图 4 页

(54)发明名称

防止存储器转储的微处理器

(57)摘要

微处理器(MP2),包括存储器(MA)和中央处理单元(CPU),该微处理器配置为签名在所述存储器中写入的二进制字(W),以及在所述存储器中的二进制字的读取期间,校验所述二进制字的签名,并且如果所述签名无效,启动所述存储器的保护行为。根据本发明,所述中央处理单元配置为在存储器区域中执行伴随无效签名的二进制字的写入指令,从而由所述中央处理单元对所述存储器区域的稍后的读取启动所述保护行为。



CN 102968392 A

1. 微处理器(MP2),包括存储器(MA,MEM1,MEM2,MEM3)和中央处理单元(CPU,SCT2),所述微处理器配置为:

在所述存储器中的二进制字(W,We)的写入期间,产生签名(S,Se)并在所述存储器中写入伴随所述签名所述二进制字,以及

在所述存储器中的二进制字(W,Wr)的读取期间,伴随所述二进制字校验所述签名(S,Sr),并且如果所述签名无效,启动所述存储器的保护行为(ER),

特征在于,所述中央处理单元配置为在存储器区域中执行伴随无效签名(IS)的二进制字(W,We)的写入指令(IWR[P,Q]),从而由所述中央处理单元对所述存储器区域的稍后的读取启动所述保护行为。

2. 根据权利要求1的微处理器,其中所述存储器是易失性存储器(MEM2)或电可擦除可编程非易失性存储器(MEM3)。

3. 根据权利要求1和2中任一项的微处理器,所述微处理器包括安全电路(SCT2),所述安全电路配置为根据所述中央处理单元的要求产生有效签名(S)或无效签名(IS)。

4. 根据权利要求1至3中任一项的微处理器,其中所述签名包括至少一个奇偶校验位,所述奇偶校验位部分或全部为要签名的所述二进制字的位的函数。

5. 便携式电子设备(CD),包括在半导体芯片(ICT)上的集成电路,其中所述集成电路包括根据权利要求1至4中任一项的微处理器(MP2)。

6. 保护微处理器(MP2)的方法,所述微处理器包括存储器(MA,MEM1,MEM2,MEM3)和中央处理单元(CPU,SCT2),所述方法包括:

在所述存储器中的二进制字(W,We)的写入期间,产生签名(S,Se)并在所述存储器中写入伴随所述签名的所述二进制字,以及

在所述存储器中的二进制字(W,Wr)的读取期间,伴随所述二进制字校验所述签名(S,Sr),并且如果所述签名无效,执行所述存储器的保护行为(ER),

其特征在于,所述方法进一步包括在存储器区域中写入伴随无效签名(IS)的二进制字(W,We),使得由所述中央处理单元对所述存储器区域的稍后的读取启动所述保护行为。

7. 根据权利要求6的方法,其中所述存储器为包含由所述中央处理单元可执行的程序的只读存储器(MEM1),并且所述方法包括在所述存储器的启用之前在所述存储器中预先存储伴随无效签名的所述二进制字。

8. 根据权利要求6的方法,其中所述存储器(MEM2,MEM3)为易失性存储器或电可擦除可编程非易失性存储器,并且所述方法包括使用所述中央处理单元以在所述存储器中写入伴随无效签名的所述二进制字。

9. 根据权利要求8的方法,所述方法包括在由所述中央处理单元执行的程序(OC)中插入至少一个在所述存储器中伴随无效签名的二进制字的写入指令(IWR[P,Q])的预先步骤。

10. 根据权利要求6至9中任一项的方法,其中所述签名包括至少一个奇偶校验位,所述奇偶校验位部分或全部为要签名的所述二进制字的位的函数。

11. 根据权利要求6至10中任一项的方法,其中所述保护行为包括至少一种以下行为:启动中断并执行错误处理程序;重置所述中央处理单元为零;擦除所有或一些所述存储器;暂时或永久地设置所述中央处理单元停止服务;暂时或永久地设置所有或者一些所述存储器停止服务。

12. 配置集成在根据权利要求 1 至 4 中任一项的微处理器中的非易失性存储器程序 (MEM1) 的方法，包括：

－以源代码（SC）的形式设计程序，

－将源代码中的所述程序转换为由微处理器可执行的程序目标代码（OC），

－产生签名（S）并将它们与二进制字关联，以及

－在所述存储器中存储所述已签名的目标代码，

其特征在于，所述方法包括在存储器区域中插入至少一个伴随无效签名的二进制字，从而由所述微处理器的所述中央处理单元的稍后的读取启动所述存储器的保护行为。

13. 根据权利要求 12 的方法，包括：

－在所述源代码中插入至少一个第一类型的指令 (INST1)，并且

－当将所述源代码转换成目标代码时，通过将伴随所述无效签名的所述二进制字插入到所述目标代码来执行所述第一类型的指令。

14. 根据权利要求 12 或 13 中任一项的方法，包括在所述存储器中放置所述目标代码，将至少一个存储器区域留空，产生伴随无效签名的二进制字，并且将伴随无效签名的二进制字放置在所述空的存储器区域中。

15. 根据权利要求 12 至 14 中任一项的方法，包括：

－在所述源代码中插入至少一个第二类型的指令（INST2），并且

－当将所述源代码转换成目标代码时，在所述存储器中将所述第二类型的指令转换成伴随无效签名的二进制字的可执行的写入指令 (IWR[PQ])。

防止存储器转储的微处理器

技术领域

[0001] 本发明涉及一种包括存储器和中央处理单元的微处理器，该微处理器配置为签名在存储器中写入的二进制字以校验在存储器中读取的字的签名，并且如果签名无效则启动存储器的保护行为。

背景技术

[0002] 如附图 1 所示，常规的微处理器 MP1 通常包括中央处理单元或“CPU”（CPU1）和存储器 MEM。存储器 MEM 可包括机密数据例如加密密钥，安全证书等。微处理器因此容易受到旨在发现这些数据的攻击者的攻击的影响，尤其对于支付应用（银行卡，预付卡，电子钱包等）。

[0003] 已知为“存储器转储（memory dump）”攻击包括通过故障注入或者干扰动态地修改由 CPU 所执行的存储器读取指令，从而 CPU 读取的存储器区域而不是由指令指定的或者是更大的存储器区域。例如假设指令包含读取地址 A1 和指示将在地址 A1 读取二进制字符串的长度的参数 L1。攻击可能以地址 A1、参数 L1 或者两者作为目标。因此可引导 CPU 读取在地址 A2 的长度 L1 的二进制字符串，在地址 A1 的长度 L2 的二进制字符串，或者甚至在地址 A2 的长度 L2 的二进制字符串。攻击者通过监控在总线上传送的数据，可发现在所考虑的存储器区域中存在的数据。另一类型的攻击包含通过恶意程序夺取 CPU 的控制以使其读取包含机密数据的存储器区域。

[0004] 通常提供软件对策以例如在指令执行之前存储指令的参数 A1、L1，并且在执行完指令之后校验执行地址对应于存储的地址 A1 以及读取的字符串的长度对应于所存储的长度 L1。另一已知的对策包含执行两次读取指令并校验同样的数据被读取。然而，该类型的对策不能阻止在参数 A1、L1 存储之前在参数 A1、L1 上执行的攻击。

[0005] 通常也提供资料（material）（硬件）对策。常规硬件对策在附图 1 中示出。CPU 配备有安全电路 SCT1。在存储器 MEM 中的字（word）W 的写入期间，电路 SCT1 产生签名 S 并与字 W 连接以构成保护二进制字符串 C=W,S。在存储器读取期间，电路 SCT1 校验二进制字符串 C 的完整性。为了这个目的，电路 SCT1 重新计算签名 S 并将它与在该二进制字符串中存在的签名进行比较。如果签名无效，电路 SCT1 发出导致存储器的保护行为的错误信号 ER。

[0006] 签名 S 经常仅包括一个或多个奇偶校验位。例如，对于 8 位（bit）微处理器，8 位字 W 可存储在带有构成签名 S 的单个奇偶校验位的存储器中。对于 16 位微处理器，16 位字可存储在带有构成签名 S 的两个奇偶校验位的存储器中，每个奇偶校验位与字的一部分关联。

[0007] 然而，一个奇偶校验位仅允许在字中的奇数位或者与奇偶校验位关联的字的一部分的修改的检测。因此，将检测不到导致相同奇偶性的偶数位的修改。例如，以下字节具有同样的奇偶性 :10000001,0000011,10000111,10011111,...

[0008] 因此期望加强包括奇偶控制机制的微处理器，以及一般使用不提供所签名的数据不改变的完全保证的签名过程的任何微处理器的存储器转储的保护。

发明内容

[0009] 本发明的实施例涉及一种包括存储器和中央处理单元的微处理器，该微处理器配置为：在所述存储器中的二进制字的写入期间，产生签名并在所述存储器中写入伴随所述签名的所述二进制字，以及在所述存储器中的二进制字读取期间，伴随所述二进制字校验所述签名，并且如果所述签名无效，启动所述存储器的保护行为，其中所述中央处理单元配置为在存储器区域中执行伴随无效签名的二进制字的写入指令，从而由所述中央处理单元对所述存储器区域的稍后读取启动所述保护行为。

[0010] 根据一个实施例，所述存储器是易失性存储器或电可擦除可编程非易失性存储器。

[0011] 根据一个实施例，所述微处理器包括安全电路，所述安全电路配置为根据所述中央处理单元的要求产生有效签名或无效签名。

[0012] 根据一个实施例，所述签名包括至少一个奇偶校验位，该奇偶校验位部分或全部为要签名的所述二进制字的位的函数。

[0013] 本发明的实施例也涉及包含在半导体芯片上的集成电路的便携式电子设备，其中所述集成电路包括根据本发明的微处理器。

[0014] 本发明的实施例也涉及保护包括存储器和中央处理单元的微处理器的方法，该方法包括：在存储器中的二进制字写入期间，产生签名并在该存储器中写入伴随所述签名的所述二进制字，以及在所述存储器中的二进制字读取期间，校验伴随所述二进制字的所述签名，以及如果所述签名无效，执行所述存储器的保护行为，其中所述方法进一步包括在存储器区域中写入伴随无效签名的二进制字，从而由所述中央处理单元对所述存储器区域的稍后的读取启动所述保护行为。

[0015] 根据一个实施例，所述存储器是包含由所述中央处理单元可执行的程序的只读存储器，并且所述方法包括在所述存储器的启用(commission)之前在所述存储器中预先存储伴随无效签名的二进制字。

[0016] 根据一个实施例，所述存储器是易失性存储器或电可擦除可编程非易失性存储器，并且所述方法包括使用所述中央处理单元在所述存储器中写入伴随无效签名的二进制字。

[0017] 根据一个实施例，所述方法包括在由所述中央处理单元执行的程序中插入至少一个在所述存储器中伴随无效签名的二进制字的写入指令的预先步骤。

[0018] 根据一个实施例，签名包括至少一个奇偶校验位，该奇偶校验位部分或全部为要签名的所述二进制字的位的函数。

[0019] 根据一个实施例，所述保护行为包括至少一种以下行为：启动中断并执行错误处理程序；重置所述中央处理单元为零；擦除所有或一些所述存储器；暂时或永久地设置所述中央处理单元停止服务；暂时或永久地设置所有或者一些所述存储器停止服务。

[0020] 发明的实施例也涉及配置集成在根据本发明的微处理器中的非易失性存储器程序的方法，所述方法包括：以源代码的形式设计程序，将所述源代码中的程序转换为由微处理器可执行的程序目标代码，产生签名并将他们与二进制字关联，以及在所述存储器中存储所签名的目标代码，其中所述方法进一步包括在存储器区域中插入至少一个伴随无效签

名的二进制字，从而由所述微处理器的中央处理单元的稍后的读取启动所述存储器的保护行为。

[0021] 根据一个实施例，所述方法包括：在源代码中插入至少一个第一类型的指令，并且当将所述源代码转换成目标代码时，通过将伴随所述无效签名的二进制字插入到所述目标代码来执行所述第一类型的指令。

[0022] 根据一个实施例，所述方法包括在所述存储器中放置目标代码，将至少一个存储器区域留空，产生伴随无效签名的二进制字，并且将伴随无效签名的二进制字放置在所述空的存储器区域中。

[0023] 根据一个实施例，所述方法包括，在所述源代码中插入至少一个第二类型的指令，并且当将所述源代码转换成所述目标代码时，在所述存储器中将所述第二类型的指令转换成伴随无效签名的二进制字的可执行写入指令。

附图说明

[0024] 本发明的实施例将关于所述附图在下文中以非限制的方式进一步详细地描述，在其中：

[0025] - 先前描述过的图 1 示意性示出常规微处理器，

[0026] - 图 2 示意性示出包括根据本发明的安全电路的微处理器的实施例，

[0027] - 图 3A，3B 分别示出有效二进制字符串和无效二进制字符串，

[0028] - 图 4 示意性示出在微处理器的存储器中的无效二进制字符串的位置，

[0029] - 图 5 示意性示出安全电路的实施例，

[0030] - 图 6 示出安全电路的另一个实施例，

[0031] - 图 7 是描述将无效二进制字符串插入可执行程序中的方法的流程图，

[0032] - 图 8 是图 7 的方法的说明，

[0033] - 图 9 示出包含根据本发明的微处理器的便携式电子设备的一般结构。

具体实施方式

[0034] 图 2 示意性示出根据本发明的微处理器 MP2 的实施例。微处理器 MP2 包括中央处理单元(以下称为“CPU”)，存储器阵列 MA 和安全电路 SCT2。存储器阵列通过数据和指令总线 B1 以及地址总线 B2（在一个实现的变化中，微处理器也可以包括不同的数据和指令总线）的中介连接到 CPU。存储器阵列 MA 在这里包括只读存储器 MEM1（ROM)，随机存取存储器 MEM2(RAM)，和电可擦除可编程存储器 MEM3，例如 EEPROM 型。存储器 MEM1 和 MEM3 是非易失性存储器，而存储器 MEM2 是易失性存储器。

[0035] 存储器 MEM1 包括在存储器中以目标代码形式存储的微处理器可执行程序。该可执行程序包括几个配合的软件层。通常，可区别操作系统的微处理器，控制不同的 CPU 外围设备和引导(pilot)(未示出)的硬件抽象层，以及包括一个或多个应用程序，例如银行交易程序的应用层。除此之外，存储器 MEM1，MEM2，MEM3 可接收机密数据，例如证书，加密密钥，会话密钥，中间加密计算数据，交易数据等等。

[0036] 安全电路 SCT2 配置为从 N 位的二进制字 W 中产生 M 位的签名 S。在存储器阵列 MA 中的字 W 的写入期间，电路 SCT2 将签名 S 与字 W 连接以构成 N+M 位长度的二进制字符串

C=W,S,该二进制字符串在写入存储器中之前施加到总线 B1 上。

[0037] 当 CPU 读取在存储器阵列 MA 中的二进制字符串 C 时,电路 SCT2 校验二进制字符串的完整性。为了这个目的,电路 SCT2 重新计算来自包含在二进制字符串中的字 W 的签名 S,然后将重新计算的签名与在该二进制字符串中存在的签名进行比较。如果在二进制字符串中存在的签名无效,电路 SCT2 发出导致存储器阵列的保护行为的错误信号 ER。

[0038] 例如保护行为包括一个或多个以下行为 :中断的启动以及错误处理程序的由 CPU 的执行,尤其在安全模式中 ;CPU 为零的重置 ;所有或一些存储器 MEM2 和 / 或 MEM3 的擦除 ;CPU 停止服务的暂时或永久设置 ;存储器 MEM1,MEM2,MEM3 中的一个或者每个的所有或一些停止服务的暂时或永久设置。

[0039] 根据本发明,CPU 配置为解码并执行除有效二进制字符串 C 的常规写入指令 WR[P,Q] 外的无效二进制字符串 IC 的写入指令 IWR[P,Q]。如在图 3A 中所示,有效二进制字符串 C 包括连接有效签名 S 的二进制字 W。如图 3B 中所示,无效二进制字符串 IC 包括连接有无效签名 IS 的二进制字 W。

[0040] 在指令 WR 和 IWR 中存在的参数 P,Q 可以为已索引的或未索引的不同类型,取决于微处理器设计者的选择。例如,参数 P 可以是要写入存储器中的字 W 的值或者读取地址,或者甚至是对存储器地址的索引或对包含要写入的字或者在其中可找到要写入的字的地址的 CPU 寄存器的索引。类似地,参数 Q 可以是字的写入地址,或者是对存储器地址或包含字的写入地址的寄存器的索引。

[0041] 安全电路 SCT2 配置为当 CPU 执行特定指令 IWR[P,Q] 时,根据 CPU 的需要产生无效签名 IS。这种情况下,电路 SCT2 将二进制字 W 与无效签名 IS 连接,并提供由 CPU 写入存储器阵列 MA 中的无效二进制字符串 IC=W,IS。

[0042] 在存储器 MEM1 中存在的可执行程序包括至少一个和优选为多个指令 IWR[P,Q]。该程序是想象的使得 CPU 在存储器阵列 MA 中在包含防止由存储器转存所读取的机密数据的存储器区域之后设置无效二进制字符串 IC。

[0043] 优选地,可执行程序的设计者确保在保护的存储器区域之前或之后设置无效二进制字符串。事实上,通过存储器转存读取机密数据的尝试从不优选地集中在包含机密数据的敏感存储器区域上。通常,读取位于敏感存储器区域之前和 / 或之后的临近的存储器区域。如果临近的存储器区域包含无效二进制字符串,转存以敏感存储器区域为目标的存储器的尝试将暗示无效二进制字符串的读取。该读取将导致安全电路 SCT2 发出错误信号 ER 和保护行为的启动,这将中断 CPU 并阻止存储器转存。

[0044] 因此,位于存储器阵列 MA 的每个无效二进制字符串 IC 构成防止存储器转存的一种“屏障”,并且优选地位于包含所要保护的数据的存储器区域之前和之后,并优选地紧随该存储区域的之前或之后。

[0045] 可执行程序的设计者将也可确保 CPU 从不读取在其中放置无效二进制字符串的地址的存储器。因此这些禁止的地址在正常程序执行期间时不允许读取,并且仅在故障注入之后或由于修改读指令的干扰时读取。

[0046] 图 4 是存储器阵列 MA 内容的简化表示。黑色矩形代表无效二进制字符串 IC。白色矩形代表有效二进制字符串 C。有效二进制字符串无需包含由 CPU 写入的数据并且可对应空白位置(还没有接收数据),该空白位置包含由电路 SCT2 缺省认为是有效二进制字符串

的二进制字符串(例如一组 0 的二进制字符串)。可区分出在存储器 MEM2,MEM3 中的无效二进制字符串 IC。这些无效二进制字符串由 CPU 根据指令 IWR 写入。例如,在需要对需要存储在存储器 MEM2 或 MEM3 中的中间机密变量的计算的加密计算的执行期间,设计该可执行程序使得 CPU 紧随中间机密变量的位置之前写入第一无效二进制字符串,并在紧随中间机密变量之后写入第二无效二进制字符串。

[0047] 图 5 示出安全电路 SCT2 的实施例。参考标记“We”指定为由 CPU 的输入 / 输出端口 IOP 发出的二进制字 W,并需要通过由电路 SCT2 产生的签名 Sg 签署。参考标记“Wr”指定为在存储器中由总线 B1 的中介读取的伴随需要由电路 SCT2 校验的签名 Sr 的二进制字 W。

[0048] 电路 SCT2 包括连接到总线 B1 的 N+M 位的输入 / 输出 10,以及连接到 CPU 的端口 IOP 的 N 位的输入 / 输出 11。还包括配置为产生 M 位的有效签名 S 的签名电路 SG1,配置为产生 M 位的无效签名 IS 的签名电路 SG2,带有两个输入和一个输出的多路复用器 MX,带有一个输入和两个输出的多用分离器 DMX,以及签名校验电路 VCT。由信号 INV (“无效”) 控制多路复用器 MX 以及由信号 GV (“产生 / 校验”)控制多路分离器 DMX。这些信号由 CPU 提供。电路 SCT2 的输入和输出 10,11 施加到签名电路 SG1、SG2 的输入上。电路 SG1、SG2 的输出施加到多路复用器 MX 上,多路复用器 MX 的输出施加到多路分离器 DMX 的输入。多路分离器 DMX 的第一输出施加到签名校验电路 VCT 的第一输入,并且多路分离器 DMX 的第二输入连接到电路 SCT2 的输入 / 输出 10,在此它连接到传输接收到的签名 Sr 或产生的签名 Sg 的总线 B1 的 M 条线。签名校验电路 VCT 的第二输入连接到电路 SCT2 的输入 / 输出 10。签名校验电路的输出提供错误信号 ER。

[0049] 电路 SCT2 以下列方式运行(信号 INV,GV,ER 的逻辑值是任意的):

[0050] i) 当 CPU 执行指令 WR[P,Q] 时 :

[0051] — CPU 执行指令的预解码或预执行,直到确定字 We 要写入到存储器阵列 MA 中和它要写入的地址,

[0052] —将字 We 放置在总线 B1 上,并且在分别提供有效签名 S 和无效签名 IS 的电路 SG1,SG2 的输入上发现,

[0053] — CPU 施加信号 INV=1 到多路复用器 MX 以在它的输出上选择有效签名 Sg(Sg = S),

[0054] — CPU 施加信号 DMX=1 到多路分离器 DMX 使得有效签名 Sg 指向它的第二输出,经由输入 / 输出 10 连接到总线 B1,

[0055] —因此有效签名(Sg = S)发现自身在总线 B1 上,与字 We 连接,

[0056] —字 We 和签名 Sg 存储在存储器阵列 MA 中。

[0057] ii) 当 CPU 执行指令 IWR[P,Q] 时 :

[0058] — CPU 执行指令的预解码或预执行,直到知道字 We 要写入存储器阵列 MA 中和它将要写入的地址,

[0059] —将字 We 放置在总线 B1 上,并在分别提供有效签名 S 和无效签名 IS 的电路 SG1,SG2 的输入上发现,

[0060] — CPU 施加信号 INV=0 到多路复用器 MX 以在它的输出上选择无效签名 Sg(Sg = IS),

[0061] — CPU 施加信号 DMX=1 到多路分离器 DMX 使得无效签名指向它的第二输出，经由输入 / 输出 10 连接到总线 B1，

[0062] —从而无效签名 Sg 发现自身在总线 B1 上，与字 We 连接，

[0063] —将字 We 和无效签名 Sg 存储在存储器阵列 MA 中。

[0064] iii）当 CPU 执行存储器阵列 MA 的读取指令时：

[0065] —伴随其签名 Sr 的读取的字 Wr 放置在总线 B1 上。在分别提供有效签名 S 和无效签名 IS 的电路 SG1，SG2 的输入上发现字 Wr。在签名校验电路 VCT 的第二输入发现读取的签名 Sr，

[0066] — CPU 施加信号 INV=1 到多路复用器 MX 以在其输出上选择有效签名 Sg（Sg = S），

[0067] — CPU 施加信号 DMX=0 到多路分离器 DMX 使得签名 Sg 指向其第一输出并施加在签名校验电路 VCT 的第一输入上，

[0068] —如果接收到的签名 Sr 与签名 Sg 不同，校验电路 VCT 设置信号 ER 为 1(活跃值)。

[0069] 应该注意的是安全电路 SCT2 可以集成在 CPU 中，并且可在任何情形下看作为 CPU 的一部分或它的机构(organ)。因此作为连接到端口 IOP 的 CPU 外部的电路的它的表示在这里仅简单地提供作为说明目的。进一步，电路 SCT2 容许具有不同的实施例而不仅仅是硬接线(hard-wire)电路。它还可以微程序控制电路、状态机的形式，以及通常以本领域技术人员的范围内的任何实施方式完成。

[0070] 在图 6 中示出的电路 SGC2 的一个实施例中，总线 B1 传输字节 W（8 位字）和形成奇偶校验位的 1 位签名。签名电路 SG1 是异或门，其接收 8 位的字节 W 并提供构成签名 S 的奇偶校验位。签名电路 SG2 是非异或门，其接收 8 位的字节 W 并提供构成无效签名 IS 的反向奇偶校验位。签名比较电路 VCR 是包括 2*8 个输入的异或门以两位两位地比较位。在一个未示出的实施例中，例如这 16 输入的异或门包括设置为两位两位地比较签名 Sg 和 Sr 的相同权重的位的每个并行的两个输入的 8 个异或门，以及将 8 个异或门的输出分组以提供错误信号 ER 的或门，如果相同级别(rand)的两位具有不同的值则该错误信号输出 1。

[0071] 再次参考图 4，位于只读存储器 MEM1 中的无效二进制字符串 IC 可在存储器阵列 MA 中进行区分。因为它仅对 CPU 是可只读访问的，这些无效二进制字符串不能由 CPU 放置，而是当可执行程序存储在那里时插入到存储器 MEM1 中。在本发明的一个实施例中，在可执行程序的目标代码从源代码的编译期间，无效二进制字符串 IC 自动插入到可执行程序中。

[0072] 图 7 描述了产生根据本发明的可执行程序以及配置只读存储器 MEM1 的方法的一般步骤。图 8 示意性示出这个过程。

[0073] 该过程包括用低级语言设计程序的步骤 S1，例如用 C 语言。在该程序中提供构成源代码 SC 的第一类型指令 INST1 和第二类型指令 INST2。该低级程序本身可由使用被编译以获得源代码的高级语言编写的程序发布。

[0074] 在步骤 S2 期间，编译源代码 SC 以获得由 CPU 可执行的已签名目标代码 OC。目标代码包括用签名 S 提供的指令和变量，每个指令或变量构成一个或多个有效二进制字符串。在该步骤期间，编译器 CPL 配置为将指令 INST1 转换成在目标代码 OC 中插入的无效二进制字符串 IC，并且转换指令 INST2 为如上所述的可执行指令 IWR[P,Q]，作为目标代码的一部分并因此构成有效二进制字符串。

[0075] 然后提供存储器空间管理的可选择步骤S3。该步骤可由编译器CPL或在编译器后干预的存储器空间管理程序实施。在该步骤期间，目标代码分布遍及存储器MEM1中的空间不同扇区。在图8所示的例子中，源代码SC包括两个不同部分P1，P2，例如一方面为操作系统和硬件抽象层，另一方面为应用程序。将可用存储器空间的扇区ST1分配给部分P1并且存储器空间的扇区ST2分配给部分P2。这样做，可能发生存储器MEM1的扇区ST3没有使用，例如位于在扇区ST1和ST2之间的扇区。

[0076] 在所述方法的一个实施例中，负责存储器空间管理的编译器或程序配置为在扇区ST3中将补充的无效二进制字符串IC插入，而不是将它留空。即使扇区ST3不包含机密数据，在其中存储的无效二进制字符串防止存储器转存尝试通过或集中在空白扇区S3，并因此提供补充的保护。

[0077] 在步骤S4期间，产生ROM掩码(mask)。该掩码为以半导体拓扑图或“布局图(layout)”的形式的目标代码的表示，例如由晶体管以选择的方式互联的字和位线的整体的形式。

[0078] 在步骤S5期间，存储器M1通过掩码配置。

[0079] 在步骤S6期间，启用存储器并且CPU执行其包含的目标代码。该执行包括插入到目标代码中的指令IWR[P,Q]的执行，该执行导致CPU以上面描述的方式在存储器MEM2或MEM3中插入无效二进制字符串IC。

[0080] 显然对本领域技术人员来讲上述描述的方法并不仅仅适用于只读存储器。可执行程序也可以存储在电可编程可擦除类型的程序存储器中，例如FLASH存储器。这种情况下，不执行产生掩码的步骤并且目标代码直接在存储器程序中编程。

[0081] 相似地，上述公开的在存储器MEM2和存储器MEM3中无效二进制字符串的写入过程可应用到不同其他类型的易失性或电可擦除可编程非易失性存储器中。

[0082] 图9示出了根据本发明的微处理器MP2的应用举例。它包括，除CPU和存储器MEM1到MEM3之外，通信接口CINT，存储器管理单元MMU，安全电路SCT3，辅助电路AUXCT（物理参数传感器，信号发生器，振荡器等)，以及连接到总线B1，B2上的外围设备元件。外围设备元件例如包括中断解码器ITD，通用异步接收器/发送器UART，定时器TM，以及随机伪随机数生成器RG。安全电路SCT3例如是CPU用来在交易期间对存储在存储器MEM2、MEM3中的确定数据进行加密和/或在终端验证自身的加密电路。

[0083] 这些元件嵌入在构成集成电路ICT的半导体微芯片中。集成电路安装在配备有通信接口CINT所连接到的触点CP（例如ISO7816触点)的塑料卡CD中。该整体构成对多种应用敏感的芯片卡。通信接口CINT可以是配备有RF天线线圈或UHF天线的非接触类型。

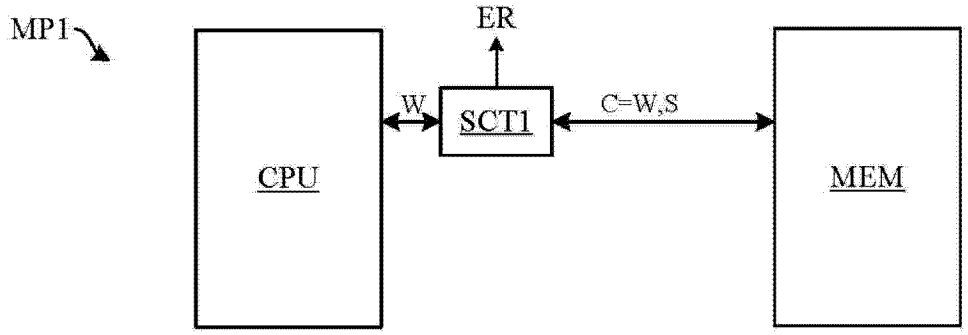


图 1 现有技术

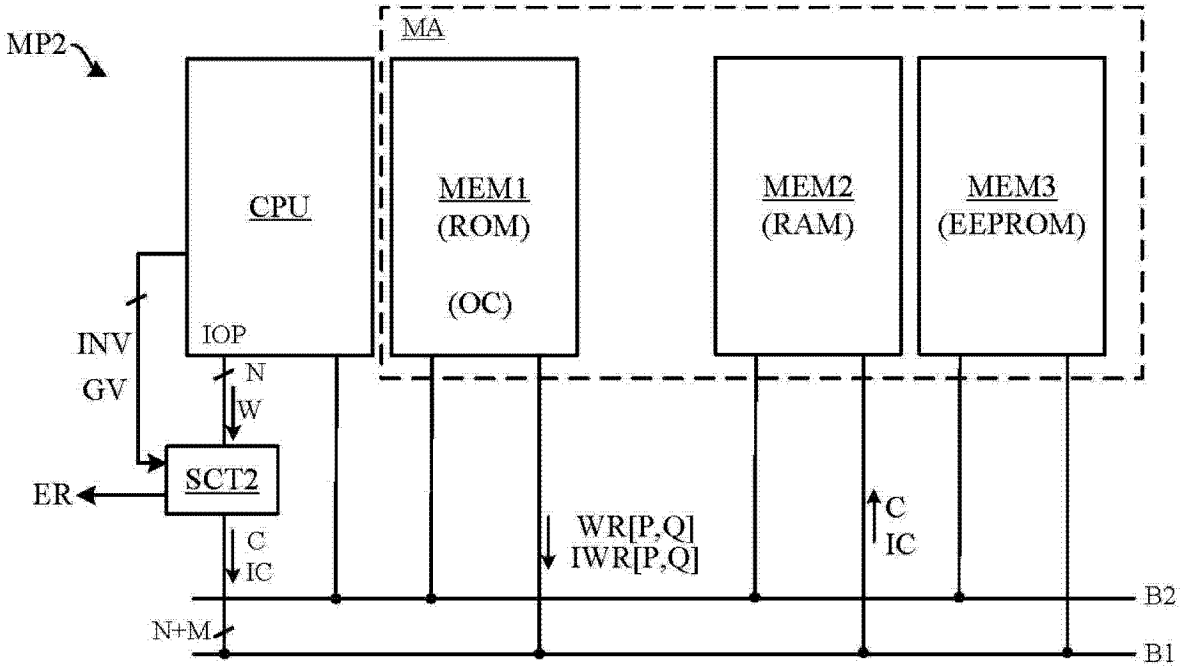


图 2

图 3A 图 3B

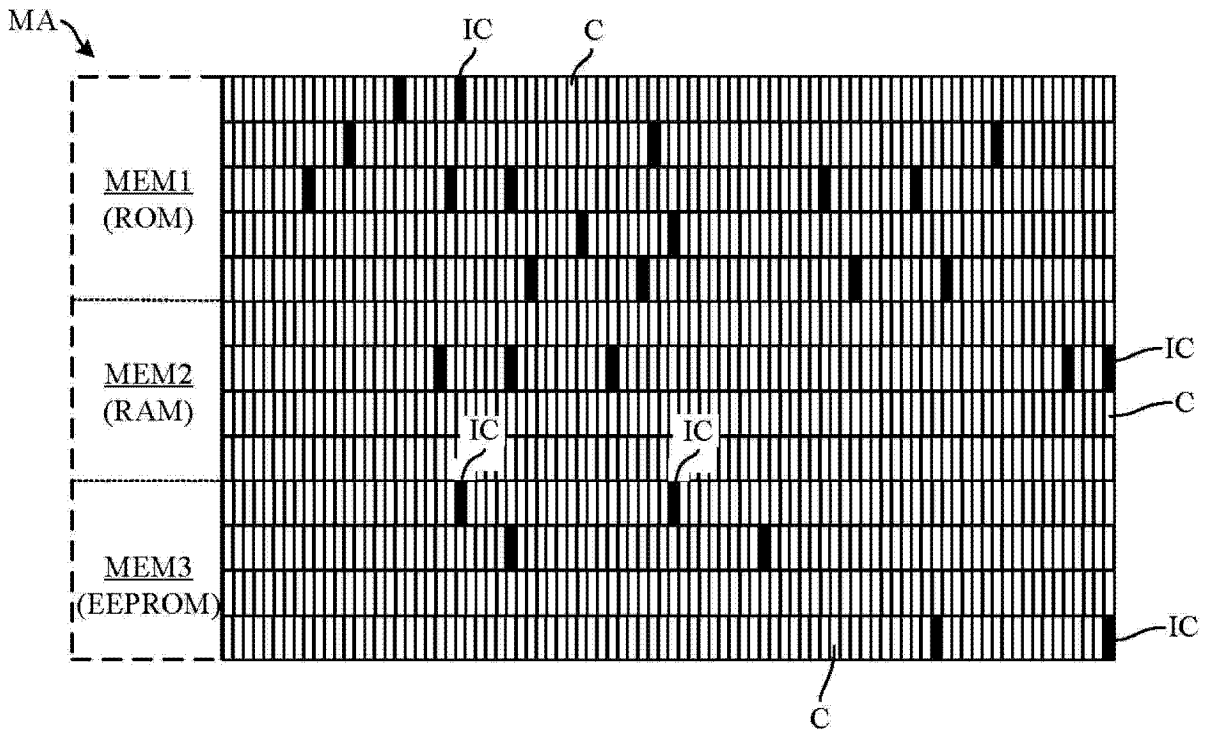

MA
IC
C
MEM1
(ROM)
MEM2
(RAM)
MEM3
(EEPROM)
IC
C
IC
IC
IC
C
IC

图 4

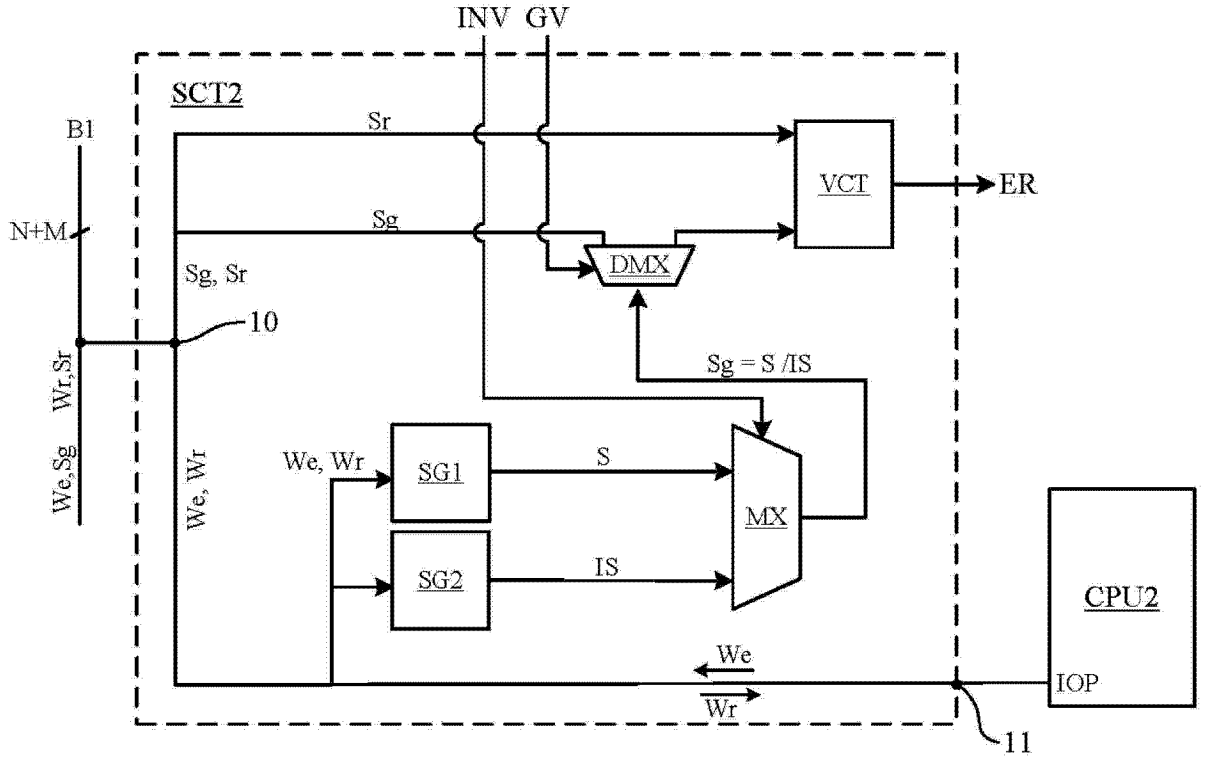

INV GV
SCT2
B1
N+M
Sr
Sg
Sg, Sr
10
VCT
ER
DMX
Sg = S /IS
Wr,Sr
We,Sg
We, Wr
We, Wr
SG1
S
SG2
IS
MX
CPU2
We
Wr
IOP
11

图 5

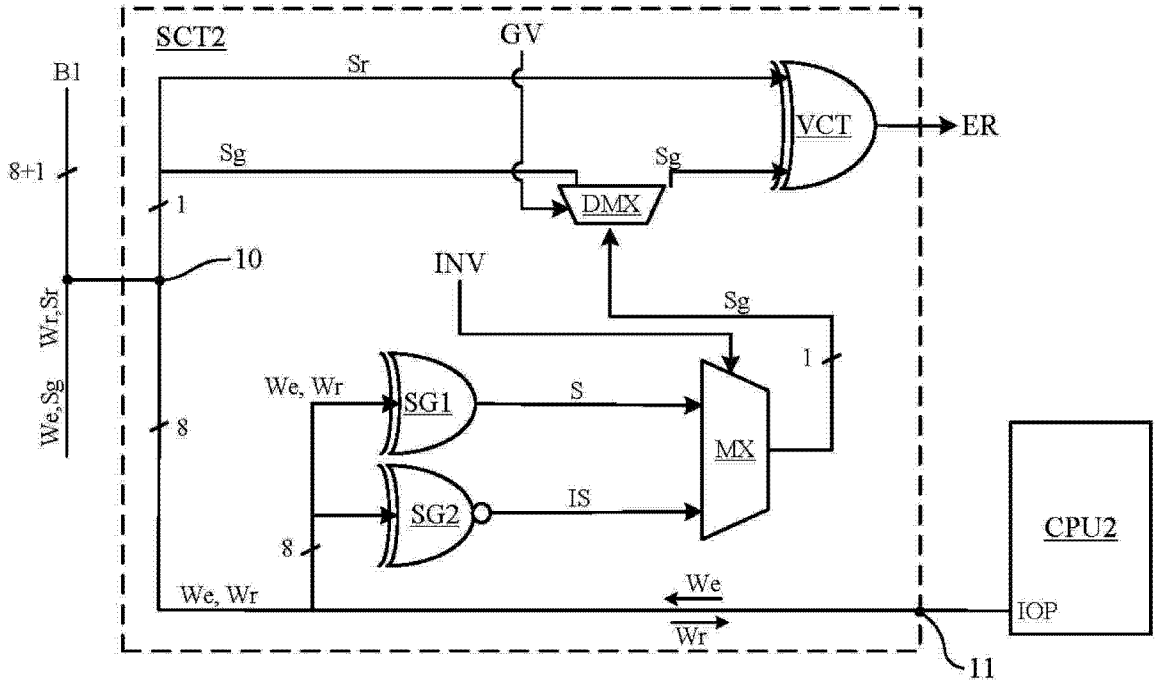

SCT2
GV
B1
Sr
Sg
8+1
1
Sg
VCT
ER
DMX
10
INV
Sg
Wr,Sr
We,Sg
1
We, Wr
SG1
S
8
MX
SG2
IS
8
CPU2
We, Wr
We
Wr
IOP
11

图 6

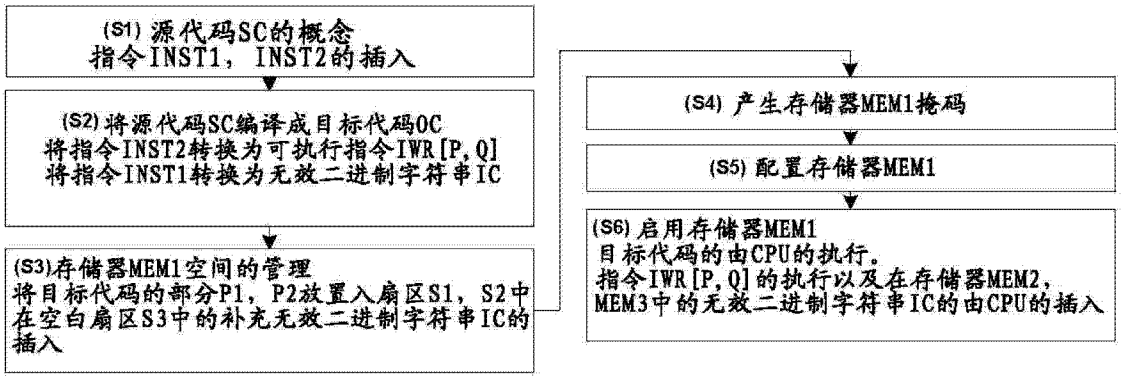

(S1) 源代码SC的概念
指令INST1，INST2的插入
(S2) 将源代码SC编译成目标代码OC
将指令INST2转换为可执行指令IWR[P,Q]
将指令INST1转换为无效二进制字符串IC
(S3)存储器MEM1空间的管理
将目标代码的部分P1，P2放置入扇区S1，S2中
在空白扇区S3中的补充无效二进制字符串IC的
插入
(S4) 产生存储器MEM1掩码
(S5) 配置存储器MEM1
(S6) 启用存储器MEM1
目标代码的由CPU的执行。
指令IWR[P,Q]的执行以及在存储器MEM2，
MEM3中的无效二进制字符串IC的由CPU的插入

图 7

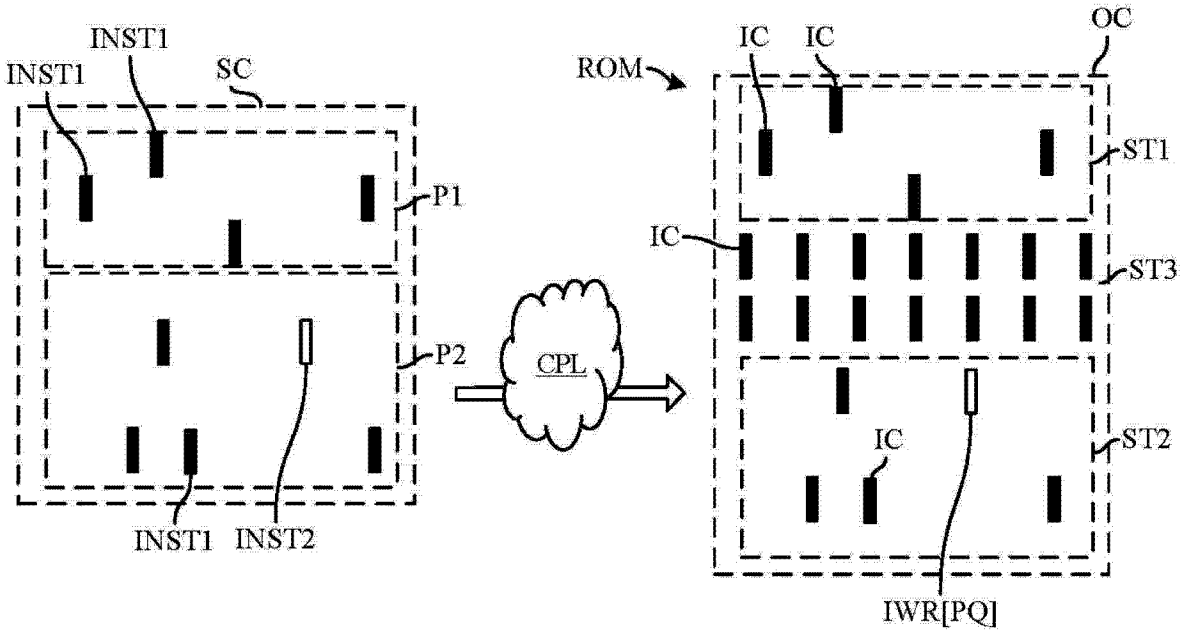

INST1
INST1
SC
P1
P2
INST1
INST2
CPL
ROM
IC
IC
OC
ST1
IC
ST3
IC
ST2
IWR[PQ]

图 8

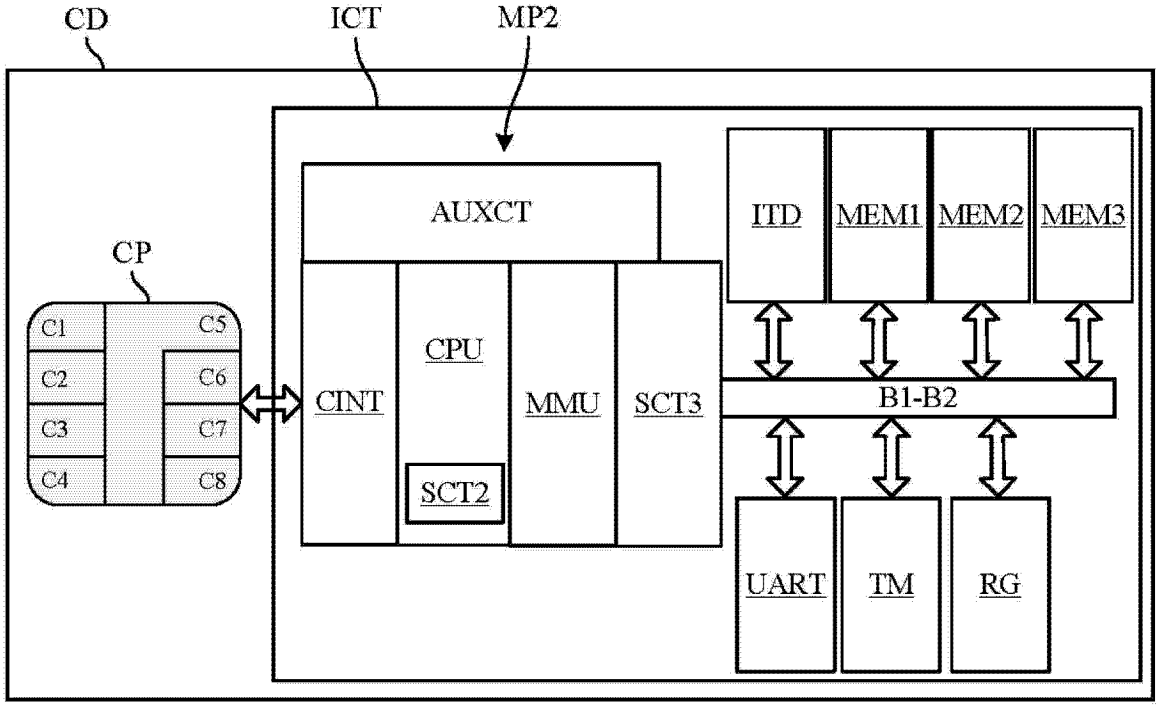

CD
ICT
MP2
AUXCT
ITD
MEM1
MEM2
MEM3
CP
C1
C2
C3
C4
C5
C6
C7
C8
CINT
CPU
SCT2
MMU
SCT3
B1-B2
UART
TM
RG

图 9