



(12) 发明专利

(10) 授权公告号 CN 103246832 B

(45) 授权公告日 2016.01.06

(21) 申请号 201210128403.5

CN 101639887 A, 2010.02.03, 全文.

(22) 申请日 2012.04.27

CN 201556209 U, 2010.08.18, 全文.

(30) 优先权数据

US 5825878 A, 1998.10.20, 全文.

101104635 2012.02.14 TW

审查员 李乐

(73) 专利权人 新唐科技股份有限公司

地址 中国台湾新竹科学工业园区

(72) 发明人 涂结盛

(74) 专利代理机构 北京三友知识产权代理有限公司 11127

代理人 任默闻

(51) Int. Cl.

G06F 21/14(2013.01)

(56) 对比文件

CN 101149768 A, 2008.03.26, 说明书第2,3

页,图1,2.

CN 101149768 A, 2008.03.26,

CN 1677383 A, 2005.10.05, 说明书第3,4

页,图1,2.

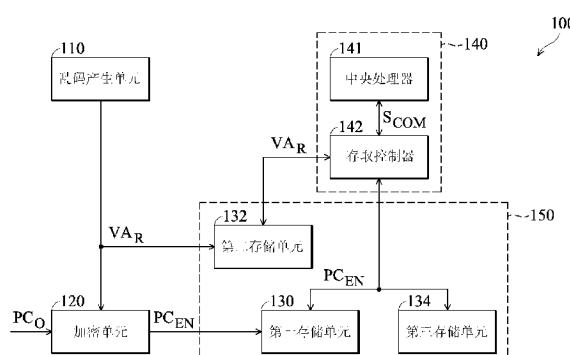
权利要求书2页 说明书5页 附图4页

(54) 发明名称

具有防复制功能的微处理器芯片及其刻录系统

(57) 摘要

本发明的一实施例提供一种具有防复制功能的微处理器芯片及其刻录系统，防复制功能的微处理器芯片包括一乱码产生单元、一加密单元、一存储模块以及一控制单元。乱码产生单元提供一乱码值。加密单元将乱码值与一原始程序码进行加密，用以产生一加密数据。存储模块存储加密数据。控制单元存取存储模块，用以撷取并解密存储模块所存储的加密数据，并根据解密后的结果而动作。



1. 一种具有防复制功能的微处理器芯片,其特征在于,所述具有防复制功能的微处理器芯片包括:

一乱码产生单元,用以提供一第一乱码值;

一加密单元,将所述第一乱码值与一原始程序码进行加密,用以产生一加密数据;

一存储模块,存储所述第一乱码值及所述加密数据;以及

一控制单元,存取所述存储模块,用以撷取并解密所述加密数据,并根据解密后的结果而动作;

所述存储模块包括:

一第一存储单元,用以存储所述加密数据;

一第二存储单元,用以存储所述第一乱码值;以及

一第三存储单元,用以存储一使用者程序;

所述控制单元包括:

一中央处理器,发出一存取命令;以及

一存取控制器,根据所述存取命令,存取所述存储模块所存储的数据,用以比对所述第一存储单元所存储的所述加密数据之中的乱码值是否相同于所述第二存储单元所存储的所述第一乱码值,当所述第一存储单元所存储的所述加密数据之中的乱码值相同于所述第二存储单元所存储的所述第一乱码值时,所述存取控制器撷取并解密所述第一存储单元所存储的所述加密数据,并将解密后的结果提供予所述中央处理器,所述中央处理器执行解密后的结果以及所述使用者程序,其中当所述第一存储单元所存储的所述加密数据之中的乱码值不同于所述第二存储单元所存储的所述第一乱码值时,所述中央处理器对所述第三存储单元所存储的所述使用者程序进行抹除破坏。

2. 如权利要求1所述的具有防复制功能的微处理器芯片,其特征在于,所述乱码产生单元为一计数器。

3. 如权利要求1所述的具有防复制功能的微处理器芯片,其特征在于,所述第一存储单元为一引导程序刻录存储器,所述第二存储单元为一配置存储器,所述第三存储单元为一使用者程序存储器。

4. 如权利要求1所述的具有防复制功能的微处理器芯片,其特征在于,所述第三存储单元更存储一金钥值,所述加密单元更将所述金钥值与所述第一乱码值和所述原始程序码进行加密,用以产生所述加密数据。

5. 一种芯片刻录系统,其特征在于,所述的芯片刻录系统包括:

一第一芯片,包括:

一第一乱码产生单元,用以在刻录工艺时提供一第一乱码值;

一第一加密单元,在刻录工艺时将所述第一乱码值与一第一原始程序码进行加密,用以产生一第一加密数据;

一第一存储模块,存储所述第一乱码值及所述第一加密数据;以及

一第一控制单元,存取所述第一存储模块,用以撷取并解密所述第一加密数据,并根据解密后的结果而动作;

所述第一存储模块包括:

一第一存储单元,用以存储所述第一加密数据,所述第一存储单元为一引导程序刻录

存储器；

一第二存储单元，用以存储所述第一乱码值，所述第二存储单元为一配置存储器；以及  
一第三存储单元，用以存储一使用者程序，所述第三存储单元为一使用者程序存储器；

其中，当所述第一存储单元所存储的所述第一加密数据之中的乱码值相同于所述第二存储单元所存储的所述第一乱码值时，所述存取控制器撷取并解密所述第一存储单元所存储的所述第一加密数据，并将解密后的结果提供予所述中央处理器，所述中央处理器执行解密后的结果以及所述使用者程序，其中当所述第一存储单元所存储的所述第一加密数据之中的乱码值不同于所述第二存储单元所存储的所述第一乱码值时，所述中央处理器对所述第三存储单元所存储的所述使用者程序进行抹除破坏。

6. 如权利要求 5 所述的芯片刻录系统，其特征在于，所述第一乱码产生单元为一计数器。

7. 如权利要求 5 所述的芯片刻录系统，其特征在于，所述第一控制单元包括：

一中央处理器，发出一存取命令；以及

一存取控制器，根据所述存取命令，存取所述第一存储模块所存储的数据，用以比对所述第一存储单元所存储的所述第一加密数据之中的第一乱码值是否相同于所述第二存储单元所存储的所述第一乱码值。

8. 如权利要求 5 所述的芯片刻录系统，其特征在于，所述第三存储单元更存储一金钥值。

9. 如权利要求 8 所述的芯片刻录系统，其特征在于，所述的加密单元更将所述金钥值与所述第一乱码值和所述第一原始程序码进行加密，用以产生所述第一加密数据。

10. 如权利要求 9 所述的芯片刻录系统，其特征在于，所述第一控制单元包括：

一中央处理器，发出一存取命令；以及

一存取控制器，根据所述存取命令，存取所述第一存储模块所存储的数据，用以比对所述第一存储单元所存储的所述第一加密数据之中的乱码值及金钥值是否相同于所述第二存储单元所存储的所述第一乱码值及所述第三存储单元所存储的所述金钥值。

11. 如权利要求 5 所述的芯片刻录系统，其特征在于，所述的芯片刻录系统更包括一第二芯片，所述第二芯片包括：

一第二乱码产生单元，用以在刻录工艺时提供一第二乱码值，其中所述第二乱码值不同于所述第一乱码值；

一第二加密单元，在刻录工艺时将所述第二乱码值与一第二原始程序码进行加密，用以产生一第二加密数据；

一第二存储模块，存储所述第二乱码值及所述第二加密数据；以及

一第二控制单元，存取所述第二存储模块，用以撷取并解密所述第二加密数据，并根据解密后的结果而动作。

12. 如权利要求 11 所述的芯片刻录系统，其特征在于，所述第一及第二乱码产生单元具有相同电路结构，所述第一及第二加密单元具有相同电路结构，所述第一及第二存储模块具有相同电路结构，所述第一及第二控制单元具有相同电路结构。

## 具有防复制功能的微处理器芯片及其刻录系统

### 技术领域

[0001] 本发明是有关于一种微处理器芯片，特别是有关于一种具有防复制功能的微处理器芯片及其刻录系统。

### 背景技术

[0002] 电子资讯产品大多数都有微处理器芯片。微处理器芯片具有一中央处理器以及一存储器。芯片制造商或芯片设计商在每一微处理器芯片芯片刻录过程会将一引导程序刻录(loader program)至存储器(ROM)之中，简称LDROM，例如基本输入输出系统(Basic Input Output System, BIOS)，而使用者会将使用者程序(application program)刻录至另一存储器(ROM)之中，简称APROM，在刻录过程之中，为了防止竞争者破解盗拷，大部分会在芯片刻录时在LDROM内刻录一锁码参数(lock bit)，防止破解盗拷，然而单一锁码参数是非常容易被破解的，而且只要破解其中一颗就可以适用全部的相关产品。中央处理器所执行的程序码通常放在存储器中。因此，微处理器芯片内的程序码的防拷是很重要的。

[0003] 然而，现今复制工具的进步与方便，使得花费数月研发的程序码或版权数据，还来不及申请专利，可能就在瞬间被复制并大量制造，使得研发厂商受到相当大的损失。

### 发明内容

[0004] 本发明提供一种具有防复制功能的微处理器芯片，包括一乱码产生单元、一加密单元、一存储单元模块以及一控制单元。乱码产生单元提供一乱码值。加密单元将乱码值与一原始程序码进行加密，用以产生一加密数据。存储模块单元存储加密数据。控制单元存取存储模块单元，用以撷取并解密存储模块单元所存储的加密数据，并根据解密后的结果而动作；所述存储模块包括：一第一存储单元、一第二存储单元以及一第三存储单元。第一存储单元用以存储所述加密数据；第二存储单元用以存储所述第一乱码值；以及第三存储单元用以存储一使用者程序。所述控制单元包括：一中央处理器以及一存取控制器。存取控制器发出一存取命令；以及存取控制器根据所述存取命令，存取所述存储模块所存储的数据，用以比对所述第一存储单元所存储的所述加密数据之中的乱码值是否相同于所述第二存储单元所存储的所述第一乱码值，当所述第一存储单元所存储的所述加密数据之中的乱码值相同于所述第二存储单元所存储的所述第一乱码值时，所述存取控制器撷取并解密所述第一存储单元所存储的所述加密数据，并将解密后的结果提供予所述中央处理器，所述中央处理器执行解密后的结果以及所述使用者程序，其中当所述第一存储单元所存储的所述加密数据之中的乱码值不同于所述第二存储单元所存储的所述第一乱码值时，所述中央处理器对所述第三存储单元所存储的所述使用者程序进行抹除破坏。

[0005] 本发明另提供一种芯片刻录系统，包括一第一芯片，其中第一芯片包括一乱码产生单元，用以在刻录工艺时提供一第一乱码值；一加密单元，在刻录工艺时将第一乱码值与一原始程序码进行加密，用以产生一第一加密数据；一存储模块，存储第一乱码值及该第一加密数据；以及一控制单元，存取存储模块，用以撷取并解密第一加密数据，并根据解密后

的结果而动作。所述第一存储模块包括：一第一存储单元、一第二存储单元及一第三存储单元。第一存储单元用以存储所述第一加密数据，所述第一存储单元为一引导程序刻录存储器；第二存储单元用以存储所述第一乱码值，所述第二存储单元为一配置存储器；以及第三存储单元用以存储一使用者程序，所述第三存储单元为一使用者程序存储器；其中，当所述第一存储单元所存储的所述第一加密数据之中的乱码值不同于所述第二存储单元所存储的所述第一乱码值时，所述存取控制器撷取并解密所述第一存储单元所存储的所述第一加密数据，并将解密后的结果提供予所述中央处理器，所述中央处理器执行解密后的结果以及所述使用者程序，其中当所述第一存储单元所存储的所述第一加密数据之中的乱码值不同于所述第二存储单元所存储的所述第一乱码值时，所述中央处理器对所述第三存储单元所存储的所述使用者程序进行抹除破坏。

[0006] 本发明的有益效果在于，就算有心人士窃取到微处理器芯片内的加密数据，也会因不同的微处理器芯片具有不同的加密数据，而无法得知原始程序码。再者，由于乱码值是随机产生，并无规则性可言，故窃取者无法推得乱码值，进而破解得知原始程序码。因此，可大幅提高程序码的安全性。

[0007] 为让本发明的特征和优点能更明显易懂，下文特举出较佳实施例，并配合所附图式，作详细说明如下：

## 附图说明

[0008] 图 1 为本发明的微处理器芯片的一可能系统架构图。

[0009] 图 2 为本发明的芯片读取数据的流程图。

[0010] 图 3 及图 4 为本发明的微处理器芯片的其它可能系统架构图。

[0011] 附图标号：

[0012] 100、300、400 : 微处理器芯片；

[0013] 110、310、410 : 乱码产生单元；

[0014] 120、320、420 : 加密单元；

[0015] 150、350、450 : 存储模块；

[0016] 130、132、134、330、332、334、430、432、434 : 存储单元；

[0017] 140、340、440 : 控制单元；

[0018] 141、341、441 : 中央处理器；

[0019] 142、342、442 : 存取控制器；

[0020] 500 : 外界电路元件；

[0021] 600 : 电子装置；

[0022] S210 ~ S240 : 步骤；

[0023] VA<sub>R</sub>: 乱码值；

[0024] PC<sub>0</sub>: 原始程序码；

[0025] PC<sub>EN</sub>: 加密数据；

[0026] VA<sub>K</sub>: 金钥值；

[0027] S<sub>COM</sub>: 存取命令；

[0028] PC<sub>ES</sub>: 比对参数；

[0029]  $PC_{Ed}$ :外界数据。

## 具体实施方式

[0030] 本发明在刻录程序码至存储器的过程中，搭配随机所产生的乱码值，对原始程序码进行加密，并将加密后的数据刻录至存储器中。由于乱码值的不同，因此针对同一原始程序码而言，仍可产生不同的加密结果。

[0031] 就算有心人士窃取到微处理器芯片内的加密数据，也会因不同的微处理器芯片具有不同的加密数据，而无法得知原始程序码。再者，由于乱码值是随机产生，并无规则性可言，故窃取者无法推得乱码值，进而破解得知原始程序码。因此，可大幅提高程序码的安全性。

[0032] 另外，本发明的微处理器芯片具有一锁定功能。当有心人士试图解除锁定功能时，微处理器芯片便立即对存储器内的程序码进行抹除或是修改，让有心人士无法读取到正确的程序码。

[0033] 在一可能实施例中，为了提高安全性，可将上述两功能（乱码加密功能及锁定功能）整合于一微处理器芯片中，用以得到一具有防复制功能的微处理器芯片。然而，在其它实施例中，仅具有单一功能（如乱码加密功能或锁定功能）的微处理器芯片仍可达到防复制的功能。

[0034] 第一实施例：

[0035] 图 1 为本发明的微处理器芯片 100 的系统架构图。在本实施例中，微处理器芯片 100 包括，一乱码产生单元 110、一加密单元 120、一存储模块 150 以及一控制单元 140。如图所示，存储模块 150 包括一第一存储单元 130、一第二存储单元 132 以及一第三存储单元 134，其中第一存储单元 130 在本实施例为一引导程序刻录存储器 (LDROM)，第二存储单元 132 在本实施例为一配置存储器 (Configure ROM)，第三存储单元 134 在本实施例为一使用者程序存储器 (APROM)，其中第一存储单元 130、第二存储单元 132 及第三存储单元 134 皆连接至控制单元 140，乱码产生单元 110 也同时连接至加密单元 120 及第二存储单元 132，加密单元 120 连接至第一存储单元 130。控制单元 140 包括一中央处理器 141 以及一存取控制器 142，其中存取控制器 142 具有解码器的功能。

[0036] 在刻录工艺时，乱码产生单元 110 以一随机方式提供一乱码值  $VA_R$  至加密单元 120 与第二存储单元 132 之中，此时，加密单元 120 会将欲刻录的一原始程序码  $PC_0$  与乱码值  $VA_R$  结合进行加密动作，进而产生一加密数据  $PC_{EN}$  至第一存储单元 130 之中。本发明并不限定乱码产生单元 110 的内部架构。在一可能实施例中，乱码产生单元 110 是为一 32 位元计数器，由于计数器可在不同时间产生不同的计数值，因此每一次进行芯片刻录时，每一芯片皆有不同的乱码值  $VA_R$ 。本发明并不限定加密单元 120 的加密方法。只要加密数据  $PC_{EN}$  不等于原始程序码  $PC_0$  的加密方法均可应用于加密单元 120 中。

[0037] 图 2 为本发明的芯片读取数据的流程图，此流程图揭露经由本发明防止盗拷方法所刻录的芯片是如何读取数据及如何进行防拷。请同时参阅图 1，当控制单元 140 要读取加密数据  $PC_{EN}$  时，中央处理器 141 发出一存取命令  $S_{COM}$  至存取控制器 142。存取控制器 142 根据存取命令  $S_{COM}$ ，存取第一存储单元 130 所存储的加密数据  $PC_{EN}$  及第二存储单元 132 所存储的乱码值  $VA_R$  (步骤 S210)，经由存取控制器 142 比对第二存储单元 132 所存储的乱码值  $VA_R$

与加密数据  $PC_{EN}$  之中的乱码值  $VA_R$  是否相同 (步骤 S220), 若比对结果是相同时, 将解密后的结果 (即原始程序码  $PC_0$ ) 提供予中央处理器 141 (步骤 S230)。中央处理器 141 再执行原始程序码  $PC_0$  及执行储在第三存储单元 134 内的一使用者程序 (application software)。若比对结果不相同时, 代表微处理器芯片 100 有被破解的疑虑, 此时中央处理器 141 则会对第三存储单元 134 所存储的一部分或全部数据进行抹除破坏性动作 (步骤 S240), 用以避免有心人士窃取相关程序码及相关设定。并且每一片芯片具有不同的乱码值  $VA_R$ , 因此就算盗拷者破解单一芯片的乱码值  $VA_R$  (此时第三存储单元 134 所存储的一部分或全部数据已经进行抹除破坏), 也无法藉由已得知的乱码值  $VA_R$  对其它芯片的进行破解, 因此可藉由本发明所提供的刻录方法, 在芯片刻录时替客户 (芯片设计商) 做出严密的防盗设计。

[0038] 第二实施例 :

[0039] 请参阅图 3 所示, 另外为了提高芯片在刻录时的加密程度, 芯片制造商要求客户提供一金钥值  $VA_K$ 。金钥值  $VA_K$  可存储在第三存储单元 334 中或其它存储单元之中, 当微处理器芯片 300 进行刻录时, 此加密单元 320 会将欲刻录的一原始程序码  $PC_0$  与乱码值  $VA_R$  及金钥值  $VA_K$  结合进行加密动作, 进而产生加密等级更为复杂一加密数据  $PC_{EN}$  至第一存储单元 330 之中。

[0040] 当控制单元 340 要读取此加密数据  $PC_{EN}$  时, 中央处理器 341 发出一存取命令  $S_{COM}$  至存取控制器 342。存取控制器 342 根据存取命令  $S_{COM}$ , 存取第一存储单元 330 所存储的加密数据  $PC_{EN}$ 、第二存储单元 332 所存储的乱码值  $VA_R$  及第三存储单元 334 所存储的金钥值  $VA_K$ , 经由存取控制器 342 比对第二存储单元 332 所存储的乱码值  $VA_R$  及金钥值  $VA_K$  与加密数据  $PC_{EN}$  之中的乱码值  $VA_R$  及金钥值  $VA_K$  是否相同, 若比对结果是相同时, 将解密后的结果 (即原始程序码  $PC_0$ ) 提供予中央处理器 341。中央处理器 341 再执行原始程序码  $PC_0$  及执行储在第三存储单元 334 内的一使用者程序。若比对结果不相同时, 代表微处理器芯片 300 有被破解的疑虑, 此时中央处理器 341 则会对第三存储单元 334 所存储的一部分或全部数据进行抹除破坏性动作, 用以避免有心人士窃取相关程序码及相关设定。如此除了提高竞争者破解的难度, 芯片制造商更是以客制化的方式服务客户。

[0041] 第三实施例 :

[0042] 请参阅图 4 所示, 当微处理器芯片 400 进行刻录时, 预先在第二存储单元 432 存储一特定比对参数  $PC_{ES}$ , 除了原有第一实施例及第二实施例的比对方式外, 当此微处理器芯片 400 安装在一电子装置 600 时, 当此电子装置 600 运作时, 此微处理器芯片 400 会接收至少一外界电路元件 500 输入至微处理器芯片 400 的一外界数据  $PC_{Ed}$ , 控制单元 440 比对外界数据  $PC_{Ed}$  内的参数与第二存储单元 432 存储的特定比对参数  $PC_{Es}$  是否相同, 若比对结果是相同时, 将解密后的结果 (即原始程序码  $PC_0$ ) 提供予中央处理器 441。中央处理器 441 再执行原始程序码  $PC_0$  及执行储在第三存储单元 434 内的一使用者程序。若比对结果不相同时, 代表微处理器芯片 400 有被拔除并安装至其它电子装置之中的疑虑, 同时也代表此微处理器芯片 400 有破解的疑虑, 此时中央处理器 441 则会对第三存储单元 434 所存储的一部分或全部数据进行抹除破坏性动作。

[0043] 另外, 在不同时间下的刻录工艺中, 微处理器芯片 400 内的乱码产生单元所产生的乱码值  $VA_R$  并不相同。举例而言, 假设欲对两微处理器芯片进行刻录工艺。在刻录第一微处理器芯片时, 第一微处理器芯片内的乱码产生单元产生一第一乱码值, 而在刻录第二微处理器芯片时, 第二微处理器芯片内的乱码产生单元产生一第二乱码值。

片时，第二微处理芯片内的乱码产生单元产生一第二乱码值。在本实施例中，第一乱码值不同于第二乱码值。

[0044] 由于第一及第二微处理芯片具有不同的乱码值，因此，针对同一原始程序码而言，可产生两不同的加密数据。此两不同的加密数据可存储于相对应的存储单元中，并可由相对应的控制单元所存取。因此，就算有心人士破解了第一微处理芯片，也无法利用相同的乱码值，窃取第二微处理芯片内的程序码，因而提高了竞争者破解的难度。

[0045] 再者，本发明并不限定第一及第二微处理芯片的内部架构。在一可能实施例中，第一及第二微处理芯片内的各单元具有相同或不同的电路架构。举例而言，第一微处理芯片内的乱码产生单元的电路架构可相同或不同于第二微处理芯片内的乱码产生单元的电路架构。同样地，第一微处理芯片内的加密单元、存储模块及控制单元的电路架构亦可相同或不同于第二微处理芯片内的加密单元、存储模块及控制单元的电路架构。

[0046] 除非另作定义，在此所有词汇（包含技术与科学词汇）均属本发明所属技术领域中技术人员的一般理解。此外，除非明白表示，词汇于一般字典中的定义应解释为与其相关技术领域的文章中意义一致，而不应解释为理想状态或过分正式的语态。

[0047] 虽然本发明已以较佳实施例揭露如上，然其并非用以限定本发明，任何所属技术领域中技术人员，在不脱离本发明的精神和范围内，当可作些许的更动与润饰，因此本发明的保护范围当以权利要求所界定的为准。

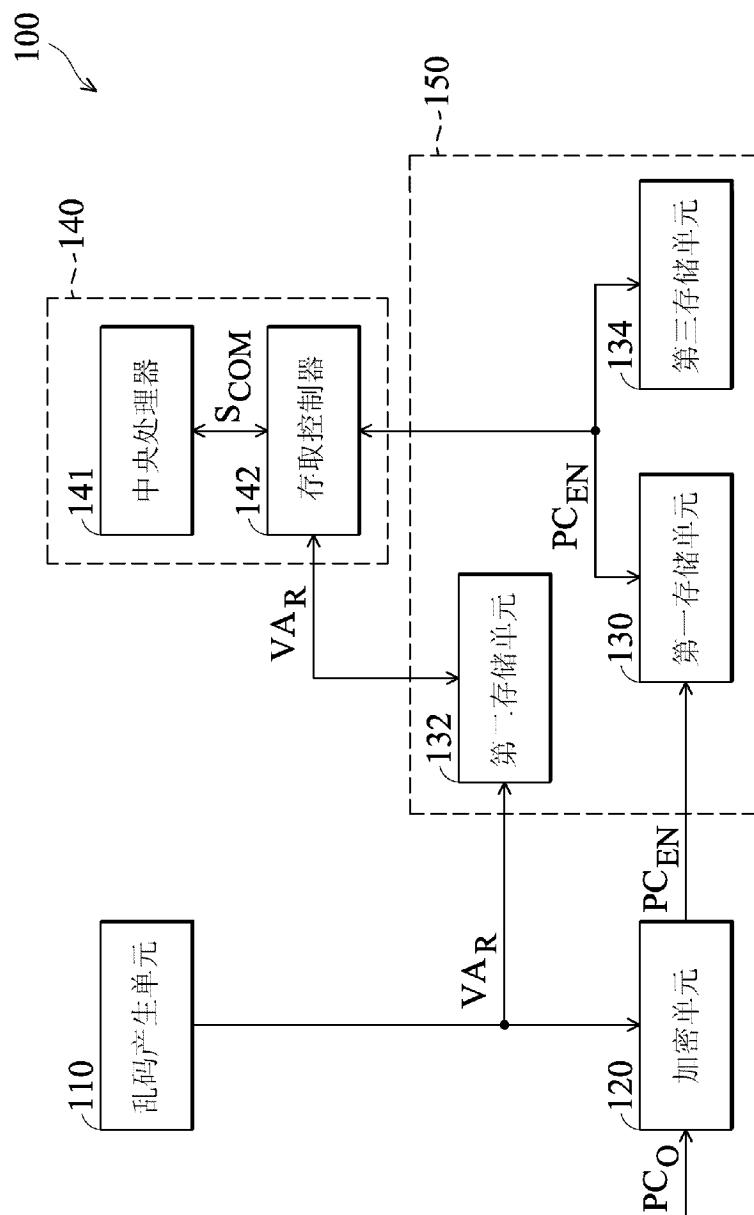


图 1

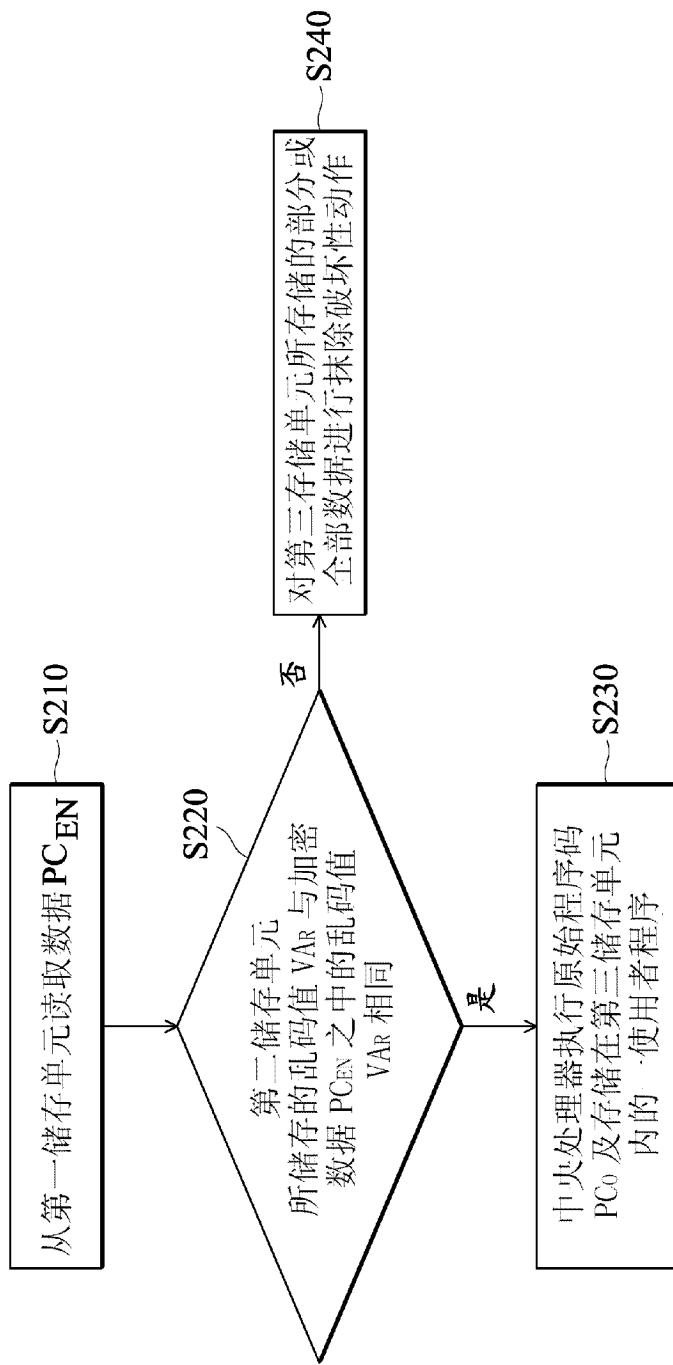


图 2

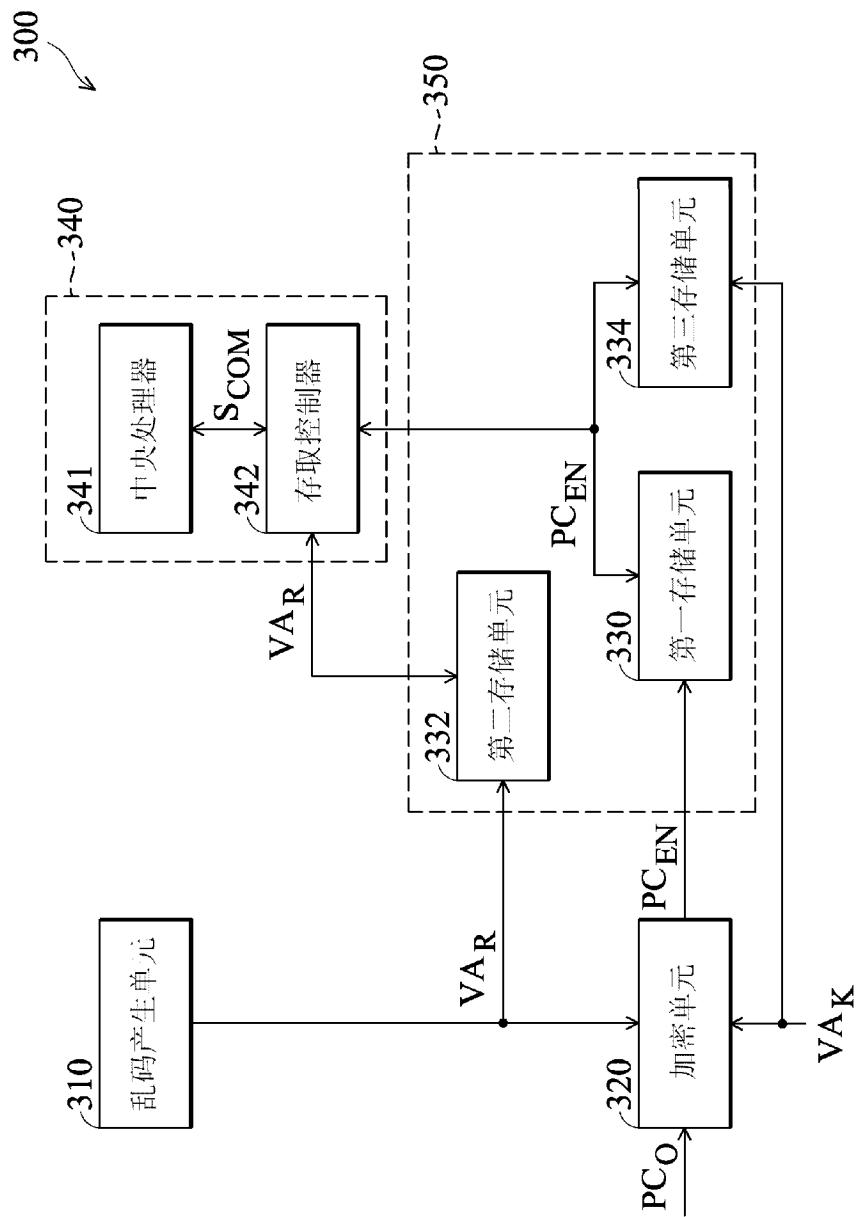


图 3

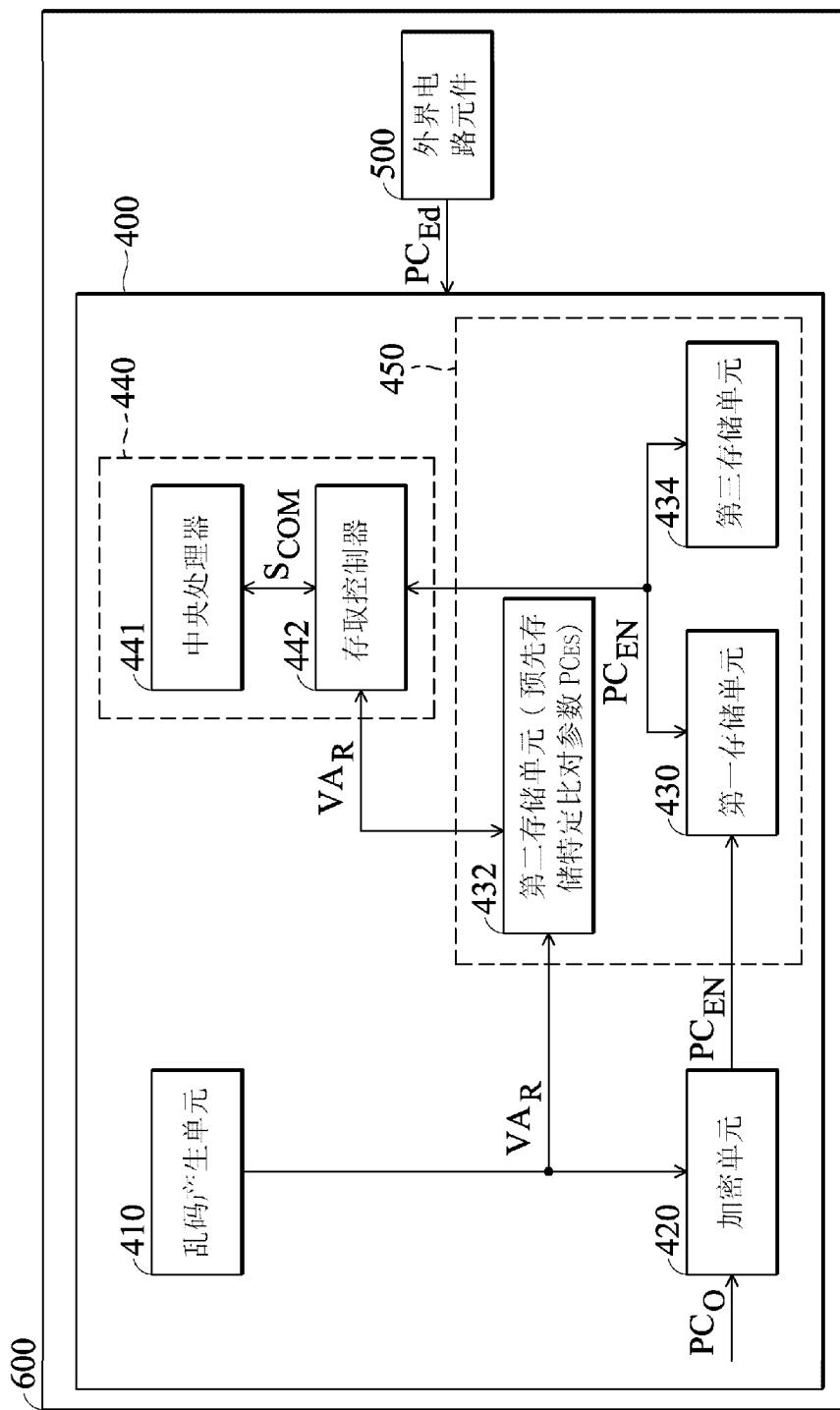


图 4