(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 103679059 A
(43)申请公布日 2014.03.26

(21)申请号 201210313814.1

(22)申请日 2012.08.29

(71)申请人 珠海扬智电子科技有限公司
地址 519080 广东省珠海市唐家湾软件园路1号南方软件园西苑软件生产加工中心B3四层一、三、四单元

(72)发明人 胡德才

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 胡林岭

(51)Int.Cl.
G06F 21/72(2013.01)

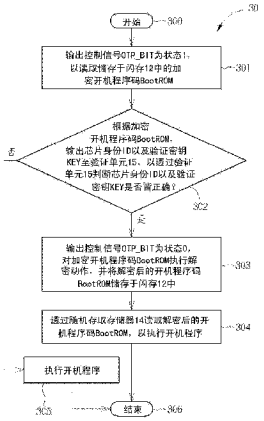
权利要求书2页 说明书4页 附图3页

(54)发明名称

安全开机方法及电脑系统

(57)摘要

用于电脑系统的安全开机方法，包含有藉由一中央处理器设定一第一状态的控制信号并输出至一存储器控制器，以使得一储存有一加密开机程序码的闪存为只读状态；根据该加密开机程序码，该中央处理器输出一芯片身份以及一验证密钥至一验证单元，以透过该验证单元判断该芯片身份以及该验证密钥是否皆正确；若正确，该中央处理器设定一第零状态的控制信号并输出至该存储器控制器，以使得该闪存为可读写状态；以及透过该验证单元对该加密开机程序码执行解密动作，并将该解密后的开机程序码储存于该闪存中。



CN 103679059 A

1. 一种安全开机方法，用于一电脑系统，该安全开机方法包含有：

藉由一中央处理器设定一第一状态的控制信号并输出至一存储器控制器，以使得一储存有一加密开机程序码的闪存为只读状态；

根据该加密开机程序码，该中央处理器输出一芯片身份以及一验证密钥至一验证单元，以透过该验证单元判断该芯片身份以及该验证密钥是否皆正确；

若正确，该中央处理器设定一第零状态的控制信号并并输出至该存储器控制器，以使得该闪存为可读写状态；以及

透过该验证单元对该加密开机程序码执行解密动作，并将该解密后的开机程序码储存于该闪存中。

2. 如权利要求 1 所述的安全开机方法，其中当该验证单元判断该芯片身份以及该验证密钥皆正确时，则该中央处理器透过一随机存取存储器读取解密后的该开机程序码，以执行一开机程序。

3. 如权利要求 1 所述的安全开机方法，其中当该验证单元判断该芯片身份以及该验证密钥中至少一者不正确时，则该中央处理器执行一关机程序。

4. 如权利要求 1 所述的安全开机方法，其中该闪存是一系统级封装串行闪存（System in Package Serial Flash Memory，SiP SFLASH）或是一采用 Hard Macro 工艺的串行闪存。

5. 如权利要求 1 所述的安全开机方法，其中该电脑系统另包含有一只读存储器，用来储存一原始开机程序码。

6. 如权利要求 5 所述的安全开机方法，其中另包含有：

藉由一中央处理器设定一第二状态的控制信号并传输至该存储器控制器，使得一存储有一原始开机程序码的只读存储器可读，并读取该原始开机程序码，执行一原始开机程序。

7. 一种电脑系统，包含有：

一中央处理器；

一闪存，用来储存一加密开机程序码；

一存储器控制器，耦接于该闪存以及该中央处理器，用来根据该中央处理器设定的一第一状态的控制信号，控制该闪存为只读状态，以便该中央处理器读取该加密开机程序码；或根据该中央处理器设定的一第零状态的控制信号，使得该闪存为可读写状态；以便该中央处理器读取该加密开机程序码以及写入一解密开机程序码；以及

一验证单元，耦接于该中央处理器以及该闪存，用来根据该中央处理器输出的一芯片身份及一验证密钥，判断是否由中央处理器对该加密开机程序码执行一解密动作，以产生并储存该解密开机程序码于该闪存。

8. 如权利要求 7 所述的电脑系统，其中当该验证单元判断该芯片身份以及该验证密钥皆正确时，则该中央处理器透过一随机存取存储器读取该闪存储存的该解密开机程序码，以执行一开机程序。

9. 如权利要求 7 所述的电脑系统，其中当该验证单元判断该芯片身份以及该验证密钥中至少一者不正确时，则该中央处理器执行一关机程序。

10. 如权利要求 7 所述的电脑系统，其中该闪存是一系统级封装串行闪存（System in Package Serial Flash Memory，SiP SFLASH）或是一采用 Hard Macro 工艺的串行闪存。

11. 如权利要求 7 所述的电脑系统，其另包含有一只读存储器，用来储存一原始开机程

序码。

12. 如权利要求 11 所述的电脑系统，其中当该中央处理器设定一第二状态的控制信号时，该中央处理器读取储存于该只读存储器的该原始开机程序码，以执行一原始开机程序。

安全开机方法及电脑系统

技术领域

[0001] 本发明是指一种安全开机方法及电脑系统，尤指一种将加密后的开机程序码储存于闪存中，以提升信息安全以及降低成本的安全开机方法及电脑系统。

背景技术

[0002] 随着电脑系统的功能日益强化，在电脑开机程序中所需要进行的签名验证、硬体初始化等参数的设定也日趋复杂。具体来说，在电脑系统开机后，由基本输入输出系统(Basic Input/Output System)读取开机程序码，执行后续开机步骤，如开机自我测试(Power on Self Test，POST)、随插即用测试(Plug and Play test)、硬体设定(Hardware Configuration)等动作，以进入作业系统。因此，开机程序码几乎无法容许有错误于其中，因为在开机过程中任何的小错误都可能导致电脑系统无法正常开机，陷入停顿或不正常关机的状态。

[0003] 传统上用来储存开机程序码的存储器，常见的有时序/组合逻辑电路(Sequential/combination Logic Cell)、光罩只读存储器(Mask Read-Only Memory，MROM)或超级永久性存储器(eXtra Permanent Memory，XPM)等。逻辑电路是透过半导体工艺，直接将开机程序码编写入逻辑电路中，一旦逻辑电路制造完成，则无法对开机程序码进行修改。因此，在电脑产品生产之前必须完成开机程序码的设计，若在产品生产之后发现错误，则需替换整个逻辑电路，如此即限制了开机程序码的开发周期以及设计弹性。光罩只读存储器为一种可重复编程的存储器，可利用聚集离子束(Focused Ion Beam，FIB)等技术重复编写入数据，因此可具有较高的设计弹性，但相对地其安全性较低，容易遭骇客攻击、窜改其中的内容。超级永久性存储器其价格高昂并存有不稳定的缺陷，因而不常见于市场上。

[0004] 因此，如何将日趋复杂的开机程序码储存于适当的存储器中，同时搭配设计一种具有高设计弹性、高安全性以及低成本的开机方法，实为本领域的重要课题之一。

发明内容

[0005] 因此，本发明的主要目的在于提供一种安全开机方法及电脑系统，将加密后的开机程序码储存于闪存中，以提升信息安全以及降低生产成本。

[0006] 本发明揭露一种安全开机方法，用于一电脑系统，该安全开机方法包含有藉由一中央处理器设定一第一状态的控制信号并输出至一存储器控制器，以使得一储存有一加密开机程序码的闪存为只读状态；根据该加密开机程序码，该中央处理器输出一芯片身份以及一验证密钥至一验证单元，以透过该验证单元判断该芯片身份以及该验证密钥是否皆正确；若正确，该中央处理器设定一第零状态的控制信号并输出至该存储器控制器，以使得该闪存为可读写状态；以及透过该验证单元对该加密开机程序码执行解密动作，并将该解密后的开机程序码储存于该闪存中。

[0007] 本发明另揭露一种电脑系统，包含有一中央处理器；一闪存，用来储存一加密开机程序码；一存储器控制器，耦接于该闪存以及该中央处理器，用来根据该中央处理器设定的

一第一状态的控制信号，控制该闪存为只读状态，以便该中央处理器读取该加密开机程序码；或根据该中央处理器设定的一第零状态的控制信号，使得该闪存为可读写状态；以便该中央处理器读取该加密开机程序码以及写入一解密开机程序码；以及一验证单元，耦接于该中央处理器以及该闪存，用来根据该中央处理器输出的一芯片身份及一验证密钥，判断是否由中央处理器对该加密开机程序码执行一解密动作，以产生并储存该解密开机程序码于该闪存。

附图说明

[0008] 图 1 为本发明实施例一电脑系统的示意图；

[0009] 图 2 为本发明实施例另一电脑系统的示意图；

[0010] 图 3 为本发明实施例一安全开机流程的示意图。

[0011] 主要元件符号说明

[0012]	10、20	电脑系统
[0013]	11	中央处理器
[0014]	12	闪存
[0015]	13	存储器控制器
[0016]	14	随机存取存储器
[0017]	15	验证单元
[0018]	26	只读存储器
[0019]	OTP_BIT	控制信号
[0020]	ID	芯片身份
[0021]	KEY	验证密钥
[0022]	BootROM、BootROM_ori	开机程序码
[0023]	0、1、2	状态
[0024]	30	安全开机流程
[0025]	301、302、303、304、305、306	步骤

具体实施方式

[0026] 请参考图 1，图 1 为本发明实施例一电脑系统 10 的示意图。电脑系统 10 可以是任何需要执行开机程序的电子装置，例如个人电脑、行动电话、个人数位助理、伺服器或数位机上盒等。电脑系统 10 包含有一中央处理器 11、一闪存（Flash Memory）12、一存储器控制器 13、一随机存取存储器（Random Access Memory，RAM）14 以及一验证单元 15。

[0027] 如图 1 所示，闪存 12 较佳地可为一系统级封装串行闪存（System in Package Serial Flash MemoRY，SiP SFLASH）或是采用一 Hard Macro 工艺的串行闪存等。闪存 12 可用来储存一开机程序码 BootROM，以供中央处理器 11 读取来执行开机程序。存储器控制器 13 耦接于闪存 12，并且透过写入以及读取总线耦接于中央处理器 11，用来根据中央处理器 11 输出的控制信号 OTP_BIT，控制中央处理器 11 读取或写入闪存 12 的权限。举例来说，当控制信号 OTP_BIT 预设为状态 0（第零状态）时，中央处理器 11 可自由读取或将数据写入闪存 12 中。当控制信号 OTP_BIT 设定为状态 1（第一状态）时，中央处理器 11 只能读取

闪存 12 的内容，而限制其写入动作。验证单元 15 耦接于中央处理器 11、闪存 12 以及随机存取存储器 14，用来根据中央处理器 11 输出的芯片身份 ID 以及验证密钥 KEY，对开机程序码 BootROM 执行解密动作，并将解密后的开机程序码 BootROM 储存于闪存 12。中央处理器 11 透过随机存取存储器 14 读取解密后的开机程序码 BootROM，以执行开机程序。

[0028] 具体来说，当电脑系统 10 开启电源准备执行开机程序之前，中央处理器 11 设定控制信号 OTP_BIT 为 1，使得存储器控制器 13 限制写入闪存 12 的动作并进入只读状态。中央处理器 11 读取储存于闪存 12 中的加密开机程序码 BootROM，据以输出芯片身份 ID 以及验证密钥 KEY 至验证单元 15。若验证单元 15 判断芯片身份 ID 以及验证密钥 KEY 皆正确无误，则对加密的开机程序码 BootROM 执行解密动作，并将解密后的开机程序码 BootROM 储存于闪存 12 中。需要指出的是，在电脑系统中，任何指令操作归根结底是由中央处理器执行，因此上述对开机程序码 BootROM 进行解密的动作也需要由中央处理器 11 透过验证单元 15 完成；具体的，中央处理器 11 首先设定控制信号 OTP_BIT 为 0，使得闪存 12 进入可读写状态，然后依照验证单元 15 的解密指令，藉助随机存取存储器 14，从闪存 12 中提取加密的开机程序码 BootROM，执行解密操作，并将完成解密的开机程序码 BootROM 再写回闪存 12 中。当验证单元 15 完成上述开机程序码 BootROM 的解密动作，中央处理器 11 则透过随机存取存储器 14 读取解密后的开机程序码 BootROM，以执行开机程序。

[0029] 简言之，由于闪存 12 的单位储存容量的价格低廉以及具有易更新的特点，本发明主要系将开机程序码 BootROM 储存于闪存 12 中，以达到节省成本以及高设计弹性的目的。并且，为了提高开机程序码 BootROM 的安全性，本发明搭配了开机程序码 BootROM 的验证步骤，以防止开机程序码 BootROM 遭受骇客攻击，达到信息保护的目的。

[0030] 除此之外，图 1 描述的开机方法可与现有的开机方法近一步地结合，以作为备用的开机方案。请参考图 2，图 2 为本发明实施例一电脑系统 20 的示意图。图 2 与图 1 的差异在于，当中央处理器 11 输出的控制信号 OTP_BIT 为状态 2（第二状态）时，可直接读取另一只读存储器 26 储存的开机程序码 BootROM_ori，进行开机程序。其中只读存储器 26 可为任意形式的只读存储器，例如一次性可编程（One Time Programmable，OTP）只读存储器、电子抹除式可复写只读存储器（Electrically Erasable Programmable ROM，EEPROM）等。若在电脑系统 20 量产的过程中或是量产之后，发现开机程序码 BootROM_ori 存有错误，则设计者可将除错完成的开机程序码 BootROM 储存入闪存 12 中，并设定中央处理器 11 在执行开机程序前输出的控制信号 OTP_BIT 为状态 1，以启动备用的开机方案。如此可使电脑系统 20 在生产之后具有可维修性，不需为了修改开机程序码 BootROM_ori 而替换只读存储器 26。

[0031] 关于上述电脑系统 10、20 的运作方式可归纳为一安全开机流程 30，如图 3 所示，安全开机流程 30 包含有以下步骤：

[0032] 步骤 300：开始。

[0033] 步骤 301：输出控制信号 OTP_BIT 为状态 1，以读取储存于闪存 12 中的加密开机程序码 BootROM。

[0034] 步骤 302：根据加密开机程序码 BootROM，输出芯片身份 ID 以及验证密钥 KEY 至验证单元 15，以透过验证单元 15 判断芯片身份 ID 以及验证密钥 KEY 是否皆正确，若是，则进行步骤 303；若否，则进行步骤 305。

[0035] 步骤 303 :输出控制信号 OTP_BIT 为状态 0,对加密开机程序码 BootROM 执行解密动作,并将解密后的开机程序码 BootROM 储存于闪存 12 中。

[0036] 步骤 304 :透过随机存取存储器 14 读取解密后的开机程序码 BootROM,以执行开机程序。

[0037] 步骤 305 :执行关机程序。

[0038] 步骤 306 :结束。

[0039] 关于安全开机流程 30 的详细实施方式可参考前述,于此不赘述。

[0040] 综上所述,由于电脑系统可支援的功能日益强大,因此电脑系统开机过程中所需的开机程序码也日趋复杂。本发明主要根据闪存的单位储存容量的价格低廉以及具有易更新的特点,将开机程序码储存于闪存中,以达到节省成本以及高设计弹性的目的。并且,为了提高开机程序码的安全性,本发明搭配了开机程序码的验证步骤,以防止开机程序码遭受骇客攻击,达到信息保护的目的。因此,本发明不仅可提供设计者更多的开发时间、实现客制化功能,甚至可以在电脑系统量产过程中随时更新开机程序码,达到设计灵活性佳、高信息安全性以及低成本的功效。

[0041] 以上所述仅为本发明的较佳实施例,凡依本发明申请专利范围所做的均等变化与修饰,皆应属本发明的涵盖范围。

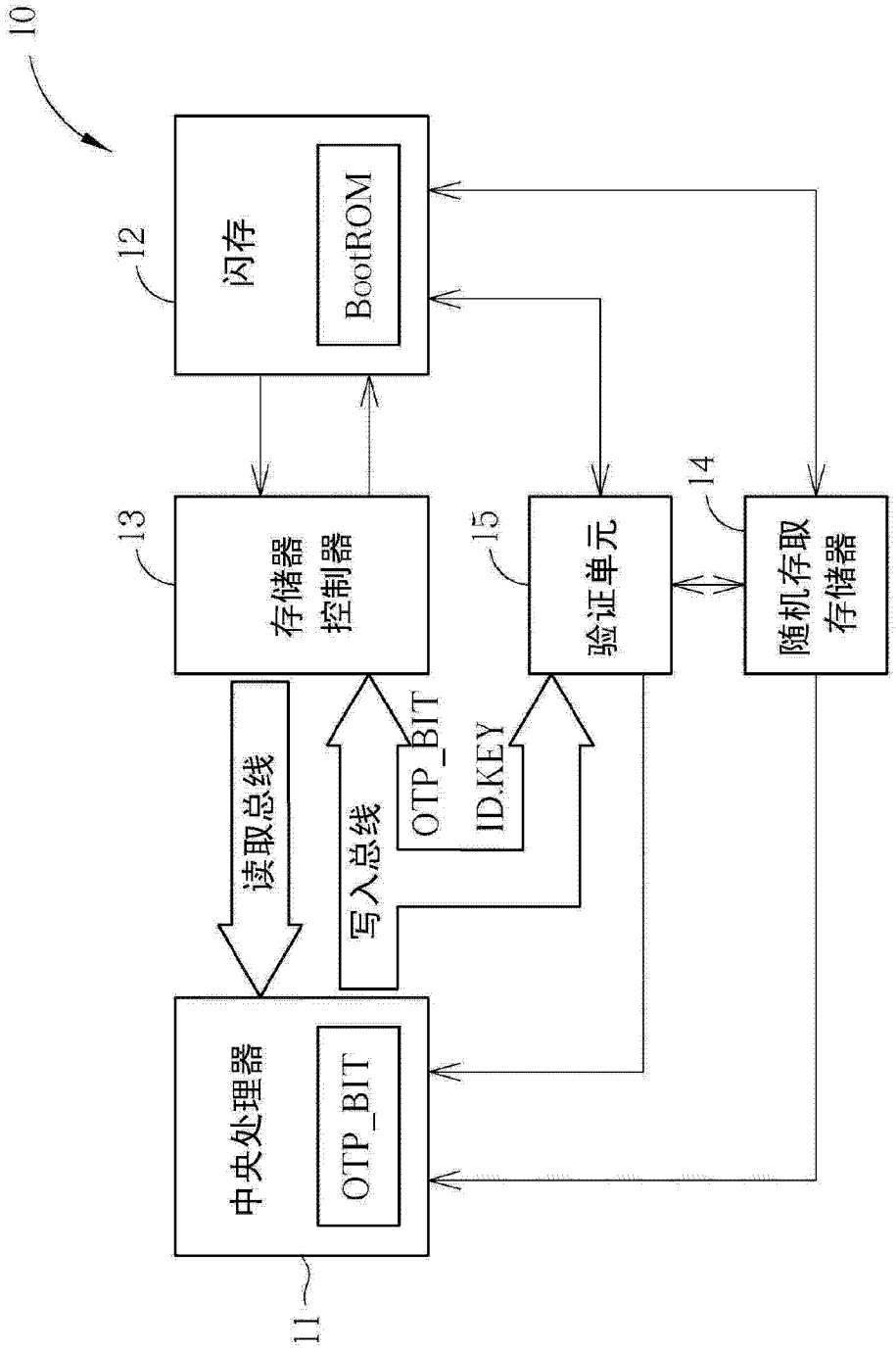

10
12
闪存
BootROM
13
存储器
控制器
15
验证单元
14
随机存取
存储器
读取总线
写入总线
OTP_BIT
ID.KEY
中央处理器
OTP_BIT
11

图 1

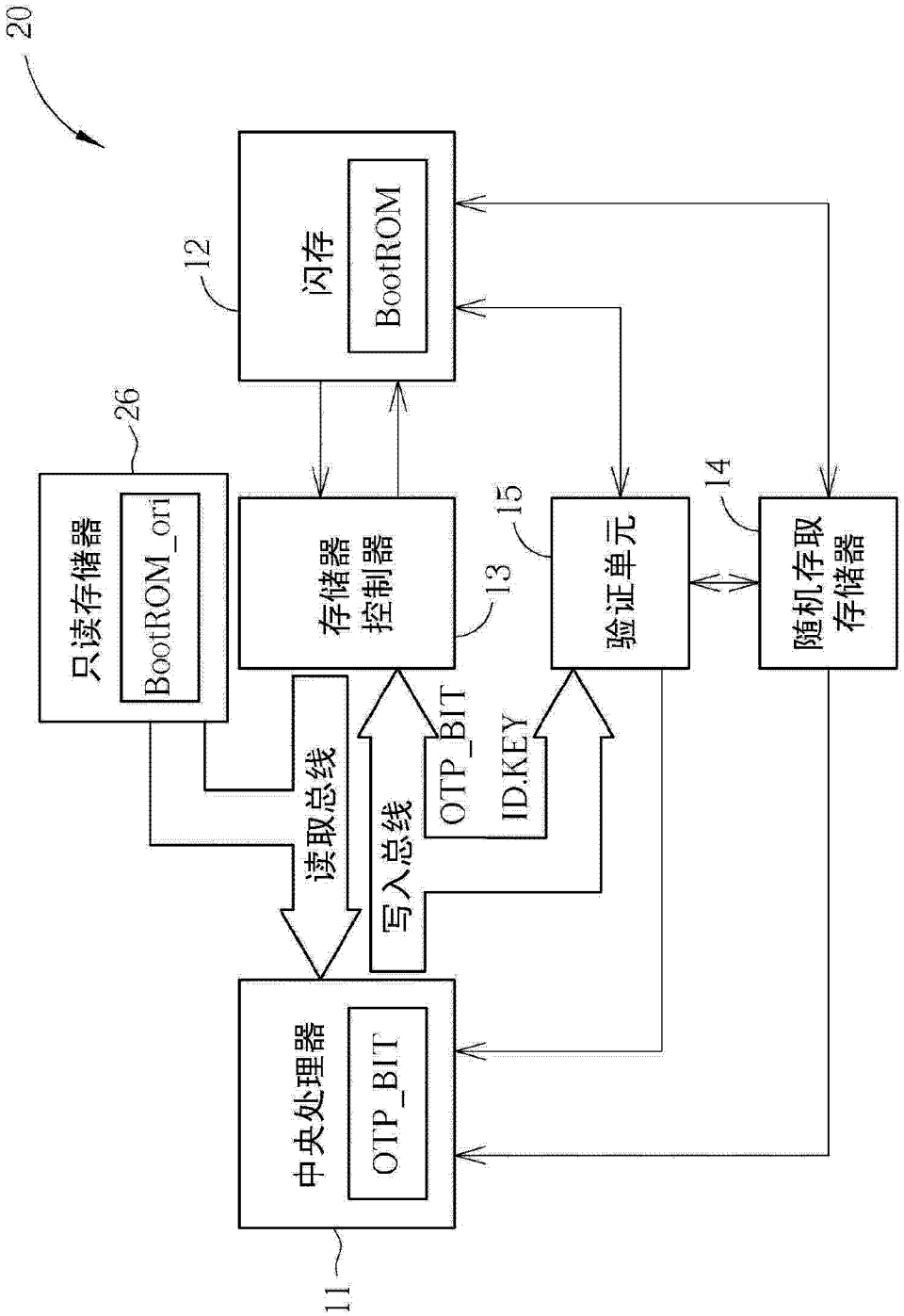

20
闪存
BootROM
12
只读存储器
BootROM_ori
26
存储器
控制器
13
验证单元
15
随机存取
存储器
14
读取总线
写入总线
OTP_BIT
ID.KEY
中央处理器
OTP_BIT
11

图 2

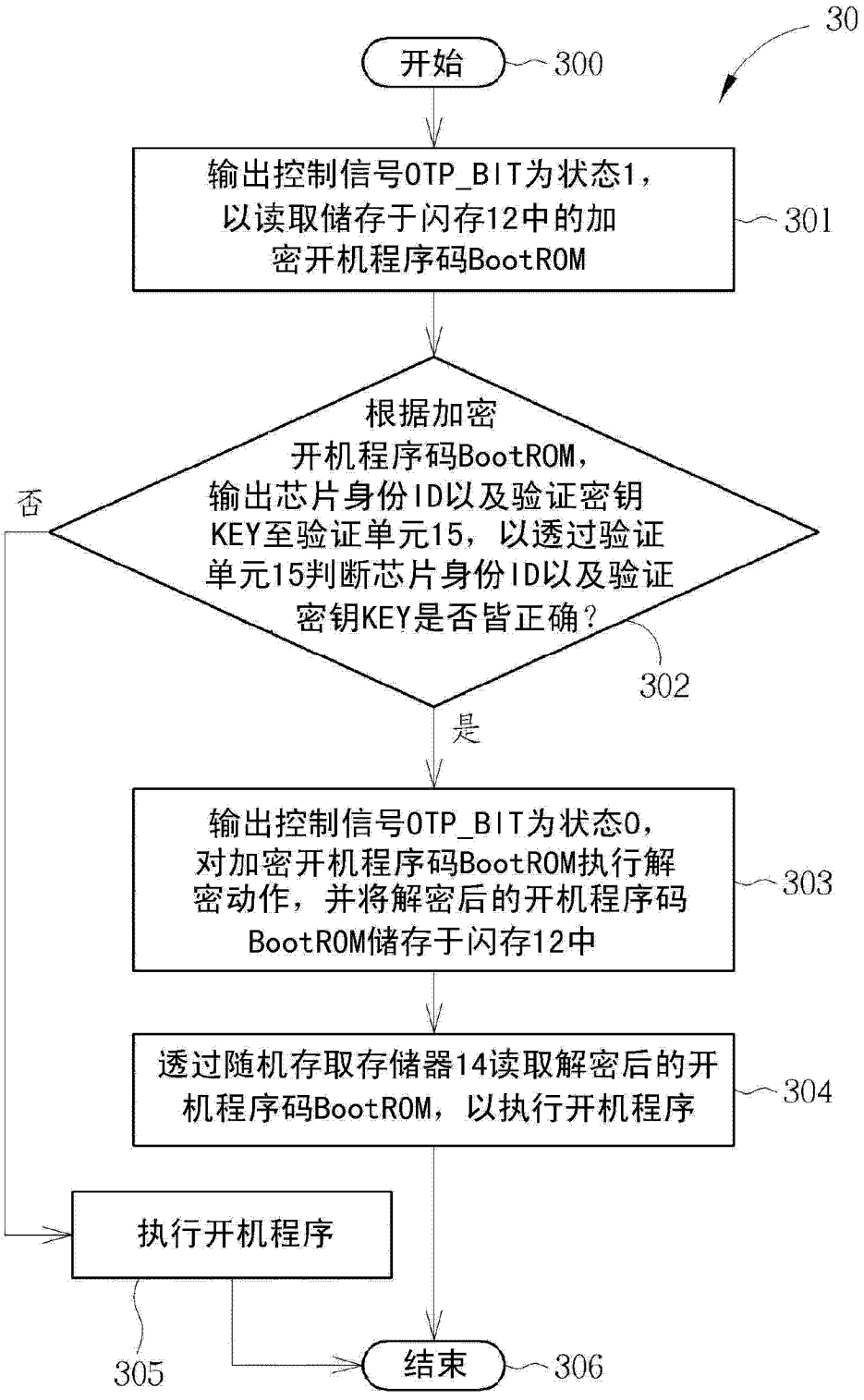

30
开始
300
输出控制信号OTP_BIT为状态1，以读取储存于闪存12中的加密开机程序码BootROM
301
根据加密开机程序码BootROM，输出芯片身份ID以及验证密钥KEY至验证单元15，以透过验证单元15判断芯片身份ID以及验证密钥KEY是否皆正确？
302
否
是
输出控制信号OTP_BIT为状态0，对加密开机程序码BootROM执行解密动作，并将解密后的开机程序码BootROM储存于闪存12中
303
透过随机存取存储器14读取解密后的开机程序码BootROM，以执行开机程序
304
执行开机程序
305
结束
306

图 3