

(12) 发明专利申请

(10) 申请公布号 CN 102324006 A

(43) 申请公布日 2012. 01. 18

(21) 申请号 201110261107. 8

(22) 申请日 2011. 09. 06

(71) 申请人 四川九洲电器集团有限责任公司  
地址 621000 四川省绵阳市绵阳市涪城区跃进路 16 号

(72) 发明人 何敏

(74) 专利代理机构 成都九鼎天元知识产权代理有限公司 51214  
代理人 徐宏 吴彦峰

(51) Int. Cl.  
G06F 21/00 (2006. 01)

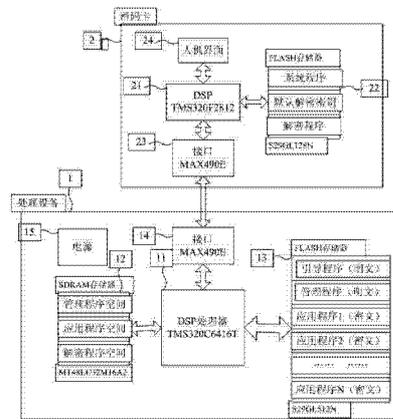
权利要求书 1 页 说明书 5 页 附图 4 页

(54) 发明名称

一种处理器程序安全保护装置及保护方法

(57) 摘要

本发明涉及加密领域,公开了一种处理器程序安全保护装置,包括处理设备、密码卡,所述处理设备和密码卡连接;所述处理设备包括第一处理器、第一存储器、第二存储器、第一接口芯片、电源模块,第一处理器分别与第一存储器、第二存储器、第一接口芯片相连;处理设备和密码卡的各芯片分别连接电源模块;所述第一接口芯片与第二接口芯片通过异步串口连接,所述第一存储器为非易失性存储器,所述第二存储器为易失性存储器。本发明还公开了一种处理器程序安全保护方法。通过使用本发明的装置及方法,对方在未获得解密密钥与解密程序情况下,获得处理器应用程序密文将无任何价值。



1. 一种处理器程序安全保护装置,其特征在于包括处理设备、密码卡,所述处理设备和密码卡连接;所述处理设备包括第一处理器、第一存储器、第二存储器、第一接口芯片、电源模块,第一处理器分别与第一存储器、第二存储器、第一接口芯片相连;处理设备和密码卡的各芯片分别连接电源模块;所述密码卡包括第二处理器、第三存储器、第二接口芯片、人机界面交互器,所述第二处理器分别与第三存储器、第二接口芯片、人机界面交互器相连;所述第一接口芯片与第二接口芯片通过异步串口连接,所述第一存储器为非易失性存储器,所述第二存储器为易失性存储器。

2. 如权利要求1所述的处理器程序安全保护装置,其特征在于所述第一接口芯片与第二接口芯片连接的接口电平为RS422。

3. 如权利要求2所述的处理器程序安全保护装置,其特征在于所述第一处理器为DSP、ARM、FPGA、PowerPC、单片机或PC处理器。

4. 如权利要求3所述的处理器程序安全保护装置,其特征在于所述第一存储器为FLASH、EEPROM、SD卡、CF卡、硬盘、或半导体存储介质。

5. 如权利要求4所述的处理器程序安全保护装置,其特征在于所述第二存储器为RAM或DDR。

6. 一种处理器程序安全保护方法,其具体包含以下步骤:

步骤1 在程序初始化保护过程中,对应用程序明文进行加密,并将加密后的密文保存在第一存储器中,将解密密钥和解密程序保存在第三存储器中;

步骤2 装置上电后,判断第二存储器中的控制字:

若控制字为销毁密码处理,则第一处理器控制擦除第二存储器和第一存储器;同时第二处理器控制擦除第三存储器;

若控制字为应用程序加载,则第一处理器向密码卡申请解密密钥与解密程序,将其放置在第二存储器的指定空间;

步骤3 对应用程序密文进行解密,使用第二存储器中的解密密钥和解密程序对第一存储器中的应用程序密文进行解密,恢复应用程序明文,并运行应用程序。

7. 如权利要求6所述的处理器程序安全保护方法,其特征在于所述步骤2中,完成将解密密钥和解密程序存放在第二存储器后,第一处理器向密码卡发送擦除指令,密码卡接收到指令后擦除第三存储器的解密密钥和解密程序。

8. 如权利要求7所述的处理器程序安全保护方法,其特征在于所述方法还包括应急销毁密码,在应用程序运行时,接收第一处理器系统指令,若系统发出应急销毁密码指令,则擦除第一存储器、第二存储器及第三存储器。

9. 如权利要求8所述的处理器程序安全保护方法,其特征在于所述步骤1的加密过程中,加密密钥为1M字节长度的伪随机序列,加密算法采用明文与加密密钥异或的方式。

## 一种处理器程序安全保护装置及保护方法

### 技术领域

[0001] 本发明涉及加密装置领域,尤其涉及一种处理器程序安全保护装置及方法。

### 背景技术

[0002] 诸如陆、海、空敌我识别、通信导航、电子对抗、导弹跟踪等军用电子系统与商用电子设备中很多功能都是由执行特定应用程序的处理器实现的。典型地,所述处理器可以是数字信号处理器(DSP)、ARM 处理器等微控制器、现场可编程门阵列(FPGA)、PowerPC,或者 PC 等当中采用的通用处理器。

[0003] 通常应用程序放置在外部 FLASH 内,上电时将其加载至处理器内部或外部 RAM 存储器中运行。但是,直接将程序明文存储在 FLASH 内导致任何人可以直接访问应用程序,并通过反向工程窃取程序源代码,若敌方因此解密设备的工作原理与工作参数,则可以研制出与之对抗的电子装备与战术方法,如由于战斗机叛逃而导致某一型敌我识别器失效。特别是在目前的军工电子领域,综合化趋势使得在通用硬件平台下,通过加载不同应用程序可以实现不同功能,多个应用程序以明文形式集中存储更增加系统泄密风险,单个硬件平台泄漏无疑将造成该系统上所有功能的工作原理与工作参数泄密,所造成的损失将无法估量,因此,有必要对处理器应用程序予以安全保护。

### 发明内容

[0004] 本发明的目的是针对现有技术中存在的处理器程序没有进行安全保护导致的系统安全问题,提供一种处理器程序安全保护装置及方法。

[0005] 本发明的目的通过下述技术方案来实现:

一种处理器程序安全保护装置,包括处理设备、密码卡,所述处理设备和密码卡连接;所述处理设备包括第一处理器、第一存储器、第二存储器、第一接口芯片、电源模块,第一处理器分别与第一存储器、第二存储器、第一接口芯片相连;处理设备和密码卡的各芯片分别连接电源模块;所述密码卡包括第二处理器、第三存储器、第二接口芯片、人机界面交互器,所述第二处理器分别与第三存储器、第二接口芯片、人机界面交互器相连;所述第一接口芯片与第二接口芯片通过异步串口连接,所述第一存储器为非易失性存储器,所述第二存储器为易失性存储器。

[0006] 优选地,上述第一接口芯片与第二接口芯片连接的接口电平为 RS422。

[0007] 优选地,上述第一处理器为 DSP、ARM、FPGA、PowerPC、单片机或 PC 处理器。

[0008] 优选地,上述第一存储器为 FLASH、EEPROM、SD 卡、CF 卡、硬盘、或半导体存储介质。

[0009] 优选地,上述第二存储器为 RAM 或 DDR。

[0010] 本发明还公开了一种处理器程序安全保护方法,其具体包含以下步骤:

步骤 1 在程序初始化保护过程中,对应用程序明文进行加密,并将加密后的密文保存在第一存储器中,将解密密钥和解密程序保存在第三存储器中;

步骤 2 装置上电后,判断第二存储器中的控制字:

若控制字为销毁密码处理,则第一处理器控制擦除第二存储器和第一存储器;同时第二处理器控制擦除第三存储器;

若控制字为应用程序加载,则第一处理器向密码卡申请解密密钥与解密程序,将其放置在第二存储器的指定空间;

步骤3 对应用程序密文进行解密,使用第二存储器中的解密密钥和解密程序对第一存储器中的应用程序密文进行解密,恢复应用程序明文,并运行应用程序。

[0011] 优选地,上述步骤2中,完成将解密密钥和解密程序存放在第二存储器后,第一处理器向密码卡发送擦除指令,密码卡接收到指令后擦除第三存储器的解密密钥和解密程序。

[0012] 优选地,上述方法还包括应急销毁密码,在应用程序运行时,接收第一处理器系统指令,若系统发出应急销毁密码指令,则擦除第一存储器、第二存储器及第三存储器。

[0013] 优选地,上述步骤1的加密过程中,加密密钥为1M字节长度的伪随机序列,加密算法采用明文与加密密钥异或的方式。

[0014] 本发明的有益效果:将处理器的应用程序通过密码卡进行加密后存储在第一存储器13中,存储在第一存储器13中的应用程序为密文,因此即使得到此密文但不能得到密钥及解密程序时也无法使用此应用程序。本发明的装置在不影响系统功能的情况下对处理器程序实施密码保护、防止应用程序泄密,而且实现简单,便于系统改进与升级。典型地,若电子设备丢失,如战斗机坠毁、导弹被俘获,对方在未获得解密密钥与解密程序情况下,获得处理器应用程序密文将无任何价值,而系统中第二存储器12中的应用程序明文也因为掉电而无法恢复。因此,本发明的安全保护装置可证明是安全有效的。同时本发明的方法还具有人工控制与远程控制销毁密码能力。本发明的方法在使用时,解密密钥与解密程序仅在系统上电时传输一次,保证其安全性,并将其存储在SDRAM存储器12中,在传输完毕之后,处理设备的DSP处理器11向密码卡的DSP处理器21发送擦除指令,DSP处理器21擦除其FLASH存储器22中的所有内容。系统带电复位时,SDRAM存储器12中的解密密钥与解密程序数据不丢失,可重复使用。密码卡使用完以后,其功能自动失效,因此即使设备丢失,也不存在泄密风险。

## 附图说明

[0015] 图1为本发明的处理器程序安全保护装置的结构示意图。

[0016] 图2为本发明的处理器程序安全保护方法的软件功能模块图。

[0017] 图3为执行密码程序加载的流程图。

[0018] 图4为第一处理器完整的执行流程图。

[0019]

## 具体实施方式

[0020] 下面结合具体实施例和附图对本发明作进一步的说明。

[0021] 本发明公开的一种处理器程序安全保护装置,如图1所示,包括处理设备1、密码卡2,所述处理设备和密码卡连接;所述处理设备1包括:第一处理器11、第一存储器13(如FLASH存储器)、第二存储器12(如SDRAM存储器)、第一接口芯片14、电源模块15,第一处理器11分别与第一存储器13、第二存储器12、第一接口芯片14相连;处理设备1和密码

卡 2 的各芯片分别连接电源模块 15,由电源模块 15 提供电源;所述密码卡 2 包括:第二处理器 21、第三存储器 22 (如 FLASH 存储器)、第二接口芯片 23、人机界面交互器 24,所述第二处理器 21 分别与第三存储器 22、第二接口芯片 23、人机界面交互器 24 相连;所述第一接口芯片 14 与第二接口芯片 23 通过异步串口连接,通过异步串口进行数据传输,所述第一存储器 13 为非易失性存储器,所述第二存储器 12 为易失性存储器,第三存储器 22 为非易失性存储器。

[0022] 第一存储器 13 内固化程序包括:引导程序(明文)、管理程序(明文)、应用程序 1 至 N(密文)。上述第一存储器为非易失性存储器,在系统掉电以后数据不丢失,保证系统的稳定。第二存储器在系统使用时存储解密密钥和解密程序,系统带电复位时,第二存储器中的解密密钥和解密程序数据不丢失,可重复使用,所上述第二存储器为易失性存储器,在系统掉电以后,数据不可以恢复,保证程序安全。第三存储器 22 内固化程序包括:系统程序(明文)、解密密钥(明文)、解密程序(明文)。将处理器的应用程序通过密码卡进行加密后存储在所述第一存储器 13 中,存储在所述第一存储器 13 中的应用程序为密文,因此即使得到此密文但不能得到密钥及解密程序时也无法使用此应用程序。本发明的装置在不影响系统功能的情况下对处理器程序实施密码保护、防止应用程序泄密,而且实现简单,便于系统改进与升级。典型地,若电子设备丢失,如战斗机坠毁、导弹被俘获,对方在未获得解密密钥与解密程序情况下,获得处理器应用程序密文将无任何价值,而系统中第二存储器 12 中的应用程序明文也因为掉电而无法恢复。因此,本发明的安全保护装置可证明是安全有效的。

[0023] 所述第一接口芯片 14 与第二接口芯片 23 连接的接口电平为 RS422。所述第一处理器 11 为 DSP、ARM、FPGA、PowerPC、单片机或 PC 处理器。所述第一存储器 13 为 FLASH、EEPROM、SD 卡、CF 卡、硬盘、或半导体存储介质。所述第二存储器 12 为 RAM 或 DDR。

[0024] 本发明还公开了一处理器程序安全保护方法,其具体包含以下步骤:

步骤 1 在程序初始化保护过程中,对应用程序明文进行加密,并将加密后的密文保存在第一存储器中,将解密密钥和解密程序保存在第三存储器中;

步骤 2 装置上电后,判断第二存储器中的控制字:

若控制字为销毁密码处理,则第一处理器控制擦除第二存储器和第一存储器;同时第二处理器控制擦除第三存储器;

若控制字为应用程序加载,则第一处理器向密码卡申请解密密钥与解密程序,将其放置在第二存储器的指定空间;

步骤 3 对应用程序密文进行解密,使用第二存储器中的解密密钥和解密程序对第一存储器中的应用程序密文进行解密,恢复应用程序明文,并运行应用程序。

[0025] 首先是对应用程序的初始保护,将应用程序进行加密处理,然后将应用程序密文写入处理设备的第一存储器 FLASH 存储器 13 中,将相应的解密程序和解密密钥写入密码卡的 FLASH 存储器 22 中。这样,处理设备的 FLASH 存储器 13 中就不存在明文形式的应用程序,当处理设备需要运行应用程序时,就要使用解密密钥与解密程序恢复应用程序明文后才能继续运行。

[0026] 优选地,所述步骤 2 中,完成将解密密钥和解密程序存放在第二存储器后,第一处理器向密码卡发送擦除指令,密码卡接收到指令后擦除第三存储器的解密密钥和解密程序;

优选地,所述方法还包括应急销毁密码,在应用程序运行时,可接收第一处理器系统指令,若系统发出应急销毁密码指令,则擦除第一存储器、第二存储器及第三存储器。

[0027] 如图 2 所示的处理器程序安全保护方法的软件功能模块图,每个功能模块分别执行各自的功能,达到加密应用程序及密码销毁的功能,同时因为在应用程序运行的时候可以接收系统指令,还可以跳转至管理程序进行应销毁密码。

[0028] 如图 3 所示的具体的执行密码程序加载的流程图。通过多次加载技术,恢复应用程序明文,让应用程序安全运行。其执行步骤依次为:执行引导程序(步骤 110),执行管理程序(步骤 120),执行解密程序(步骤 140),执行应用程序(160),应用程序执行时,可根据系统指令跳转回管理程序执行(步骤 170)。

[0029] 如图 4 所示的第一处理器完整的执行流程图。处理设备上电运行时,DSP 处理器 11 首先将 FLASH 存储器 13 中的引导程序搬移至处理器内部 RAM 中(步骤 210),然后跳转至其入口地址运行(步骤 220)。引导程序大小为 1K 字节,它主要目的是用于搬移更大的程序至 SDRAM 存储器 12 中执行。

[0030] 引导程序将 FLASH 存储器 13 中的管理程序搬移至 SDRAM 存储器 12 中(步骤 240),然后跳转至管理程序入口地址运行(步骤 250)。管理程序在 SDRAM 存储器 12 中的指定空间运行,本实施例中设计为 0 至 200K,管理程序负责密钥与解密程序的申请、系统管理、销毁密码等。管理程序首先读取 SDRAM 存储器 12 中指定地址 0x201 的控制字(步骤 270),根据控制字判断程序执行流程(步骤 280)。若控制字为销毁密码处理,则 DSP 处理器 11 擦除 SDRAM 存储器 12 中应用程序空间、解密密钥空间、解密程序空间中的内容(步骤 290),擦除 FLASH 存储器 13 中的全部内容(步骤 300),控制密码卡擦除 FLASH 存储器 22 中的全部内容(步骤)。

[0031] 若控制字判断为应用程序加载,则向密码卡 2 申请解密密钥(步骤 310)与解密程序(步骤 320),将其放置在 SDRAM 存储器 12 中的指定空间,然后向密码卡 2 发送擦除指令(步骤 330),密码卡 2 接收到指令后擦除卡中 FLASH 存储器 22 中的解密密钥与解密程序,管理程序最后跳转至解密程序入口地址运行(步骤 340)。密码卡与处理设备通过异步串口芯片 14 与 23 连接,采用 RS422 电平进行数据传输,设计速率为 2.5Mbps,解密密钥与解密程序的传输时间约为 3.2 秒。

[0032] 在解密程序过程中,首先根据系统指令在 FLASH 存储器 13 中读取需要执行的应用程序密文(步骤 360),使用解密算法和解密密钥将 FLASH 存储器 13 中的应用程序密文恢复成明文,并放置在 SDRAM 存储器 12 的应用程序空间(步骤 370),解密程序跳转至应用程序入口地址运行(步骤 380)。

[0033] DSP 处理器运行 SDRAM 存储器中的应用程序,完成系统所需要的功能(步骤 400)。应用程序正常工作时通过中断实时接收外部的控制指令,判断是否进行应急销毁密码处理(步骤 410),若为应急销毁密码,则向 SDRAM 存储器中指定地址 0x201 写控制字(步骤 420),跳转至 SDRAM 存储器中管理程序的入口地址运行(步骤 430),在管理程序中销毁存储器中的所有涉密信息,因此本实施例具有人工控制与远程控制销毁密码能力。

[0034] 如图 5 所示的应用程序加密与密码卡烧写的流程图。在应用程序初始保护过程中,PC 机首先读取处理器应用程序明文(步骤 510),然后随机选择一种加/解密算法(步骤 520),利用加密算法与加密密钥加密应用程序明文(步骤 530),将加密后的应用程序密文烧

写至 FLASH 存储器 13 中(步骤 540),将解密密钥与解密程序烧写至密码卡 2 的 FLASH 存储器 22 中(步骤 550)。

[0035] 优选地,所述步骤 1 的加密过程中,加密密钥为 1M 字节长度的伪随机序列,加密算法采用明文与加密密钥异或的方式。如果加密密钥与待加密的明文长度相近,则在未获得解密密钥情况下要恢复明文几乎是不可能的。因此,本实施例选取的加密算法简单有效,可达到理想的安全效果。

[0036] 在本实施例中,引导程序为 1K 字节,管理程序为 200K 字节,解密程序为 5K 字节,解密密钥为 1M 字节,DSP 主频为 1GHz,每秒可执行 8000M 条指令,DSP 与 SDRAM 的传输速率为 40MHz,通过对程序长度与时间复杂度的分析,引导程序、管理程序、解密程序的加载与执行时间不超过 100 毫秒。因此,初始上电时整个明文恢复时间不超过 3.3 秒。而在系统带电复位情况下,由于不需要重新传输解密密钥与解密程序,因此明文恢复时间不超过 100 毫秒,对处理设备的功能毫无影响。

[0037] 解密密钥与解密程序管理非常关键,可以说,该处理器应用程序保护系统的安全与否就体现在密钥管理上。因此,密码卡 2 作为处理器程序安全保护系统中至关重要的设备,需要有效的管理与使用,以确保其安全性。处理设备 1 运行前,应首先获得烧有相应解密密钥与解密程序的密码卡 2。

[0038] 解密密钥与解密程序由管理部门统一管理,且各处理设备之间的解密密钥与解密程序各不相同,因此需要由管理部门烧写指定的解密密钥与解密程序到密码卡 2 的 FLASH 存储器 22 内。使用时,解密密钥与解密程序仅在系统上电时传输一次,将其存储在 SDRAM 存储器 12 中,在传输完毕之后,处理设备的 DSP 处理器 11 向密码卡的 DSP 处理器 21 发送擦除指令,DSP 处理器 21 擦除其 FLASH 存储器 22 中的所有内容。系统带电复位时,SDRAM 存储器 12 中的解密密钥与解密程序数据不丢失,可重复使用。密码卡使用完以后,其功能自动失效,因此即使设备丢失,也不存在泄密风险。

[0039] 以上上述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

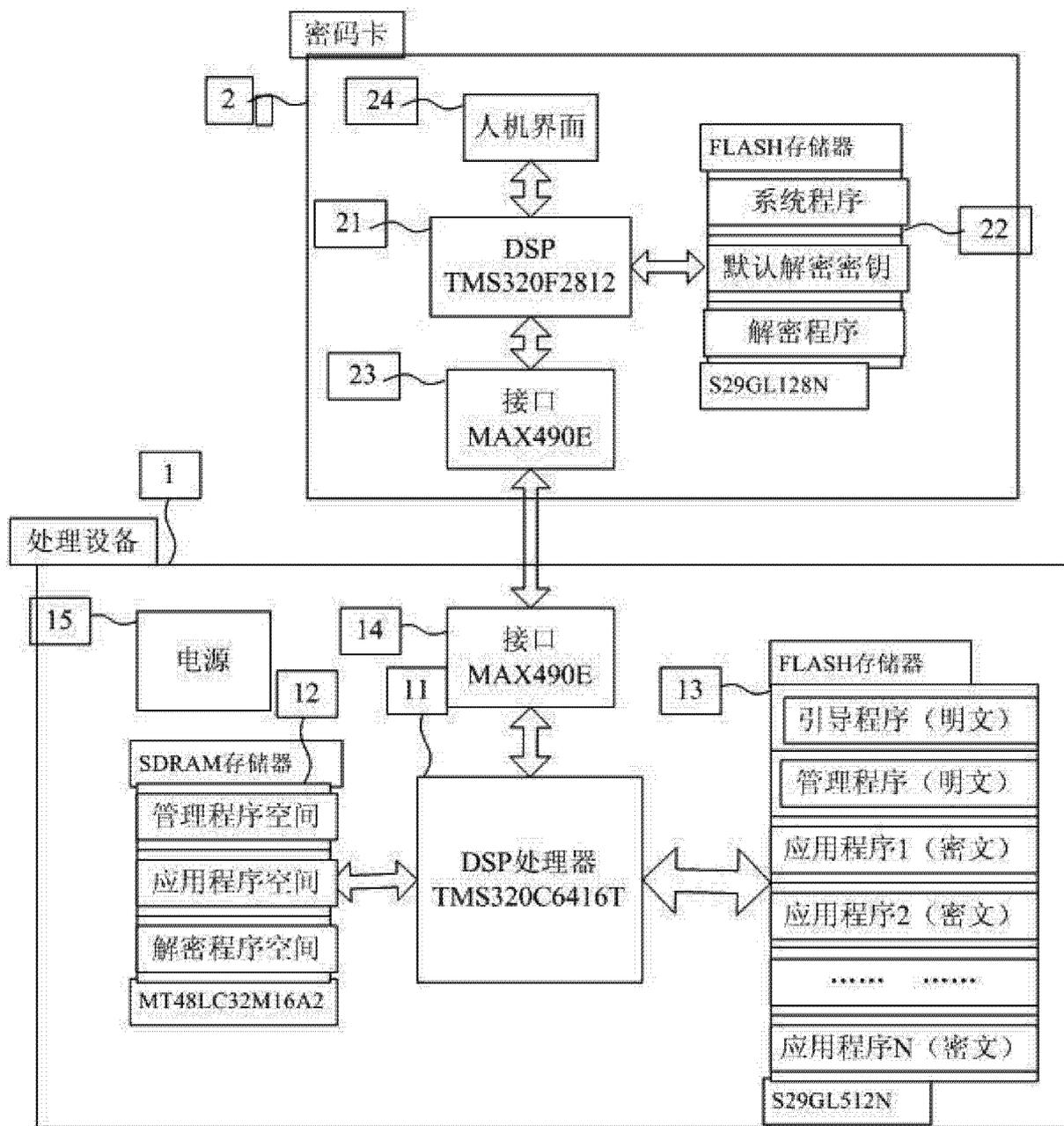


图 1

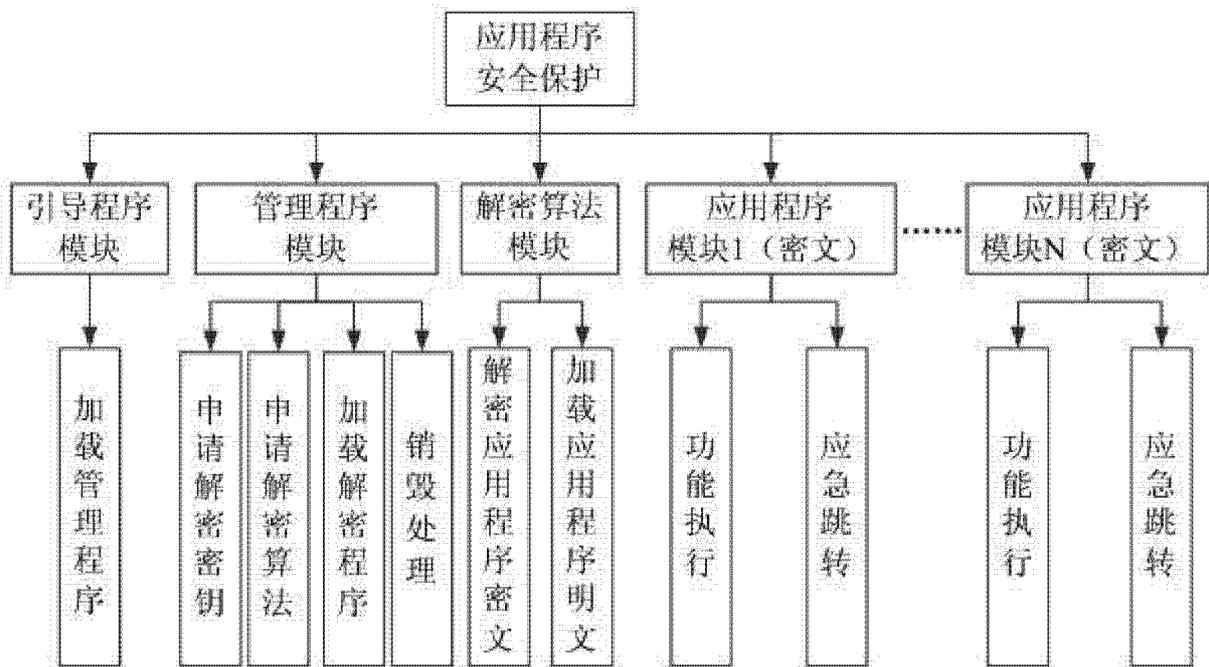


图 2

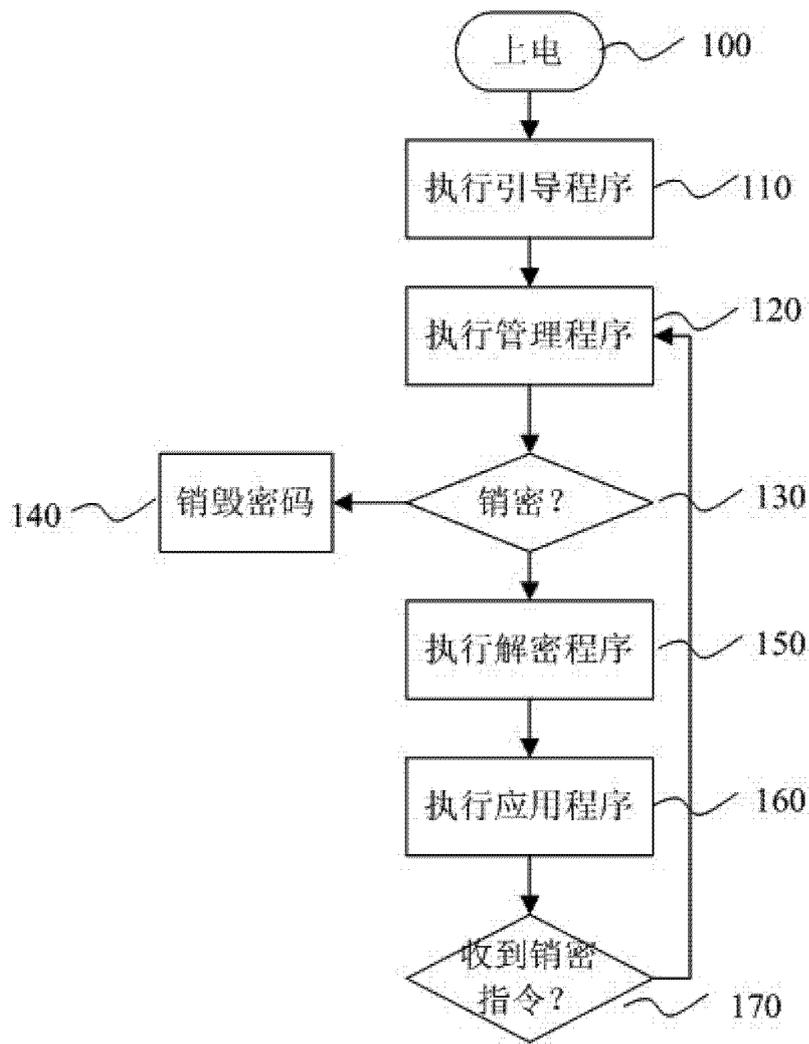


图 3

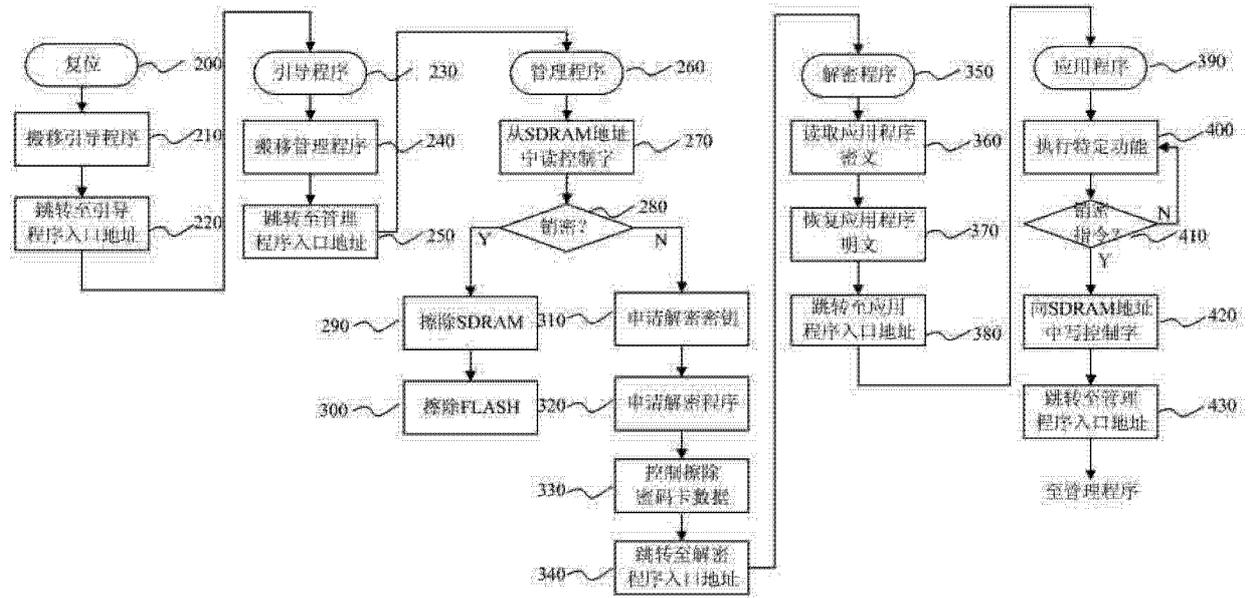


图 4