



(12) 发明专利

(10) 授权公告号 CN 103020552 B

(45) 授权公告日 2015. 05. 13

(21) 申请号 201210572609. 7

《Network and System Security (NSS)》. 2011, 第 2011 卷 (第 5 期), 第 269-273 页.

(22) 申请日 2012. 12. 20

审查员 刘义乐

(73) 专利权人 天津联芯科技有限公司

地址 300384 天津市南开区华苑产业区华天道 2 号 3008 室

(72) 发明人 黄宇

(74) 专利代理机构 天津盛理知识产权代理有限公司 12209

代理人 王利文

(51) Int. Cl.

G06F 21/79(2013. 01)

(56) 对比文件

CN 102387013 A, 2012. 03. 21, 全文.

Bohm 等. A microcontroller SRAM-PUF.

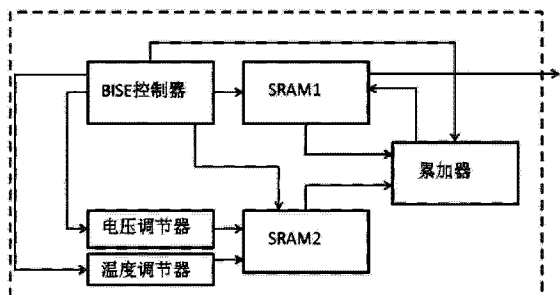
权利要求书1页 说明书5页 附图4页

(54) 发明名称

基于 SRAM 的 PUF 的片上自我注册系统及其实现方法

(57) 摘要

本发明涉及一种基于 SRAM 的 PUF 的片上自我注册系统及其实现方法,其技术特点是:该系统包括 BISE 控制器、电压调节器、温度调节器、累加器、SRAM1 和 SRAM2, BISE 控制器输出端连接到电压调节器和温度调节器,该电压调节器和温度调节器的输出端连接到 SRAM2 上, BISE 控制器分别与 SRAM1、SRAM2 和累加器相连接, SRAM1、SRAM2 分别与累加器的两个输入端相连接,该累加器的输出端连接到 SRAM1 上,该 SRAM1 输出 PUF 单元;该方法包括步骤 1:BISE 控制器由初始态自动进入检测模式 0,进行检测并输出检测模式 0 下的 PUF 单元;步骤 2:BISE 控制器自动进入检测模式 1,进行检测并输出检测模式 1 下的 PUF 单元。本发明可广泛集成在需要保护的芯片内,具有设计合理、可靠性高、使用方便等特点。



1. 一种基于 SRAM 的 PUF 的片上自我注册系统,其特征在于:包括BISE 控制器、电压调节器、温度调节器、累加器、SRAM1 和 SRAM2, BISE 控制器输出端连接到电压调节器和温度调节器,该电压调节器和温度调节器的输出端连接到 SRAM2 上, BISE 控制器分别与 SRAM1、SRAM2 和累加器相连接, SRAM1、SRAM2 分别与累加器的两个输入端相连接,该累加器的输出端连接到 SRAM1 上,该 SRAM1 输出 PUF 单元;

所述 BISE 控制器作为系统的核心,内置有自我注册系统处理软件和包括预设定的一系列的电压和温度的组合的环境参数,通过该处理软件控制电压调节器和温度调节器遍历所有环境参数,从而自动实现稳定可靠的 PUF 单元的功能。

2. 根据权利要求 1 所述的基于 SRAM 的 PUF 的片上自我注册系统,其特征在于:所述的 SRAM1 和 SRAM2 具有同样的大小和地址空间。

3. 根据权利要求 1 所述的基于 SRAM 的 PUF 的片上自我注册系统,其特征在于:所述的电压调节器包括选择电压输出单元和多个分压电阻,工作电压 VDD 通过分压电阻连接到选择电压输出单元上,该选择电压输出单元在 BISE 控制器的控制下向 SRAM2 输出不同的电压。

4. 根据权利要求 1 所述的基于 SRAM 的 PUF 的片上自我注册系统,其特征在于:所述的温度调节器包括计数器,该计数器在 BISE 控制器的控制下,向 SRAM2 循环交替写入“0”和“1”,从而调节 SRAM2 的温度。

5. 一种如权利要求 1 至 4 任一项所述片上自我注册系统的实现方法,其特征在于:包括以下步骤:

步骤 1:BISE 控制器由初始态自动进入检测模式 0,进行检测并输出检测模式 0 下的 PUF 单元;所述检测模式 0 的检测过程为:首先, SRAM1 所有单元被初始化成“0”;然后,在各种环境参数组合下, SRAM2 上电并读取 SRAM2 的每个单元的初始逻辑值,将该逻辑值和 SRAM1 相应单元的逻辑值进行逻辑“或”运算并把结果存入 SRAM1 相应单元,重复以上操作直到所有环境参数全部遍历完毕;最后,将稳定可靠的 SRAM2 “0”的单元地址输出作为 PUF 特征地址,“0”作为这些特征地址的特征值;

步骤 2:BISE 控制器自动进入检测模式 1,进行检测并输出检测模式 1 下的 PUF 单元;所述检测模式 1 的检测过程为:首先, SRAM1 所有单元被初始化成“1”;然后,在各种环境参数组合下, SRAM2 上电并读取 SRAM2 的每个单元的初始逻辑值,将该逻辑值和 SRAM1 相应单元的逻辑值进行逻辑“与”运算并把结果存入 SRAM1 相应单元,重复以上操作直到所有环境参数全部遍历完毕;最后,将稳定可靠的 SRAM2 的“1”的单元地址输出作为 PUF 特征地址,“1”作为这些特征地址的特征值。

6. 根据权利要求 5 所述的基于 SRAM 的 PUF 的片上自我注册系统的实现方法,其特征在于:所述的各种环境参数包括电压调节参数和温度调节参数。

基于 SRAM 的 PUF 的片上自我注册系统及其实现方法

技术领域

[0001] 本发明属于集成电路技术领域,尤其是一种基于 SRAM 的 PUF 的片上自我注册系统及其实现方法。

背景技术

[0002] 传统芯片的防伪依赖于各种加密算法,在系统中(例如在非挥发性存储器中)储存关键秘密/密钥,能够被复制或较容易泄密。另外,由于非挥发性存储器在 90nm 以下工艺很难生产,因此,芯片防伪系统设计需要一个革命。

[0003] 当前芯片设计者和生产技术人员正在努力地消除工艺差别(Process Variation)以保证每一个生产出的芯片与下一个完全一致。但是工艺差别是不可能被完全消除的,我们可以利用这个工艺差别来区分每个芯片。这种工艺差别可以当做是芯片的指纹,也就是说每个芯片有独特的指纹,通过该对特的指纹可以识别芯片。由于,每个芯片都有一些独一无二的物理特性,并且没办法从合法的正版芯片中提取这些物理特性并复制到另一芯片上,因此,它们泛指“物理不可克隆功能”(Physical Unclonable Function,简称为 PUF)。

[0004] 物理不可克隆功能(PUF)不可能是一种完全随机现象,尽管芯片与芯片之间不应有 PUF 相关性,但是同一芯片内 PUF 必定可以可靠地重复。换句话说,两个设备 PUF 应完全不同;同一芯片 PUF 不论在什么情况下必须完全一致。而 PUF 的可靠性恰恰是 PUF 难以广泛使用的关键。

[0005] 现有的芯片 PUF 主要基于两种物理特性:一是芯片的路径延迟,二是静态存储器(SRAM)的上电初始态。无论哪种 PUF,可靠性都是首要问题,因此,各种纠错和统计技术被应用到基于 PUF 的验证系统中。上述方法存在的问题是:(1)纠错技术不是万能的,这是由于所选 PUF 的物理特性对环境变化如温度和电压的敏感性导致 PUF 的不可靠性,纠错技术的成功与否将取决于选择稳定可靠的 PUF 单元;(2)统计技术使得芯片注册非常麻烦,这是由于芯片注册过程就是通过不同环境下的重复实验得到稳定的物理特性,并将之记录在案的过程,这个过程阻碍 PUF 验证的实际应用。

发明内容

[0006] 本发明的目的在于克服现有技术的不足,提供一种设计合理、可靠性高且使用方便的基于 SRAM 的 PUF 的片上自我注册系统及其实现方法。

[0007] 本发明解决其技术问题是采取以下技术方案实现的:

[0008] 一种基于 SRAM 的 PUF 的片上自我注册系统,包括 BISE 控制器、电压调节器、温度调节器、累加器、SRAM1 和 SRAM2,BISE 控制器输出端连接到电压调节器和温度调节器,该电压调节器和温度调节器的输出端连接到 SRAM2 上,BISE 控制器分别与 SRAM1、SRAM2 和累加器相连接,SRAM1、SRAM2 分别与累加器的两个输入端相连接,该累加器的输出端连接到 SRAM1 上,该 SRAM1 输出 PUF 单元。

[0009] 而且,所述的 SRAM1 和 SRAM2 具有同样的大小和地址空间。

[0010] 而且,所述的电压调节器包括选择电压输出单元和多个分压电阻,工作电压 VDD 通过分压电阻连接到选择电压输出单元上,该选择电压输出单元在 BISE 控制器的控制下向 SRAM2 输出不同的电压。

[0011] 而且,所述的温度调节器包括计数器,该计数器在 BISE 控制器的控制下,向 SRAM2 循环交替写入“0”和“1”,从而调节 SRAM2 的温度。

[0012] 一种基于 SRAM 的 PUF 的片上自我注册系统的实现方法,包括以下步骤:

[0013] 步骤 1:BISE 控制器由初始态自动进入检测模式 0,进行检测并输出检测模式 0 下的 PUF 单元。

[0014] 步骤 2:BISE 控制器自动进入检测模式 1,进行检测并输出检测模式 1 下的 PUF 单元。

[0015] 而且,所述检测模式 0 的检测过程为:首先,SRAM1 所有单元被初始化成“0”;然后,在各种环境参数组合下,SRAM2 上电并读取 SRAM2 的每个单元的初始逻辑值,将该逻辑值和 SRAM1 相应单元的逻辑值进行逻辑“或”运算并把结果存入 SRAM1 相应单元,重复以上操作直到所有环境参数全部遍历完毕;最后,将稳定可靠的 SRAM2 “0”的单元地址输出作为 PUF 特征地址,“0”作为这些特征地址的特征值。

[0016] 而且,所述检测模式 1 的检测过程为:首先,SRAM1 所有单元被初始化成“1”;然后,在各种环境参数组合下,SRAM2 上电并读取 SRAM2 的每个单元的初始逻辑值,将该逻辑值和 SRAM1 相应单元的逻辑值进行逻辑“与”运算并把结果存入 SRAM1 相应单元,重复以上操作直到所有环境参数全部遍历完毕;最后,将稳定可靠的 SRAM2 的“1”的单元地址输出作为 PUF 特征地址,“1”作为这些特征地址的特征值。

[0017] 本发明的优点和积极效果是:

[0018] 本发明通过 BISE 控制器、电压调节器和温度调节器能够输出稳定的 PUF 单元,可广泛集成在需要保护的芯片内,具有设计合理、可靠性高、使用方便等特点。

附图说明

[0019] 图 1 为 SRAM 的结构示意图;

[0020] 图 2 为本发明的系统连接示意图;

[0021] 图 3 为电压调节器的结构示意图;

[0022] 图 4 为温度调节器的结构示意图;

[0023] 图 5 为本发明的 BISE 控制器的处理流程图。

具体实施方式

[0024] 以下结合附图对本发明做进一步详述。

[0025] 一种基于 SRAM 的 PUF 的片上自我注册系统,如图 1 所示,是基于 SRAM 的 PUF 并集成在需要保护的芯片内,同样本自我注册系统(Build-In-Self-Enrollment)也可以应用到基于路径延迟的 PUF 验证系统。

[0026] 下面结合图 1 所示,对基于 SRAM 的 PUF 进行介绍。芯片 PUF 利用同一芯片设计在生产中由于工艺差别造成的独立物理特性来特征化每一芯片。由于 SRAM 几乎被每一计算机设备广泛应用,因此,其上电初始态可被用作 PUF。一个互补式金属氧化物半导体(CMOS)

静态随机存取存储器 (SRAM) 的单元是由六个场效应管 (FET) 形成的交叉耦合反相器, 如图 1 所示, 一个反相器驱动 A, 另一个反相器驱动 B。当断电时, $AB=00$, 这是一个非稳态; 一旦来电, 这个非稳态就会变成一个稳态“0” ($AB=01$) 或者“1” ($AB=10$)。究竟会变成“0”还是“1”取决于以下两个条件: (1) 两边 FET 阈值电压差 (V_{th}); (2) 热噪声 (由 L_{eff} , V_{noise} 和 T_{sub} 决定)。如果两边 FET 阈值电压差较大, 那么这个 SRAM 单元的初始态就会稳定地偏向“0”或者偏向“1”而不受热噪声影响。如果两边 FET 阈值电压差较小, 那么这个 SRAM 单元的初始态就会由热噪声决定随机地偏向“0”或者偏向“1”。不同 SRAM 单元会表现随机并彼此独立。因此, 本自我注册系统就是要找到一些初始态为稳定的“0”或“1”的单元, 从而形成这个芯片的特征地址 / 特征值序列; 同时, 不同芯片由于 Process Variation 会形成不同的特征地址 / 特征值序列。

[0027] 下面结合图 2 给出的自我注册系统体系结构对本发明进行说明。

[0028] 一种基于 SRAM 的 PUF 的片上自我注册系统, 包括 BISE 控制器、电压调节器、温度调节器、累加器、SRAM1 和 SRAM2, BISE 控制器输出端连接到电压调节器和温度调节器相连接控制电压调节和温度调节, BISE 控制器分别与 SRAM1、SRAM2 和累加器相连接, 电压调节器和温度调节器的输出端连接到 SRAM2 上, SRAM1、SRAM2 分别与累加器的两个输入端相连接, 该累加器的输出端连接到 SRAM1 上, 该 SRAM1 输出可靠的 PUF 单元。所述的 SRAM1 和 SRAM2 有同样的大小和地址空间。下面对系统中的各个部分分别进行说明:

[0029] BISE 控制器作为系统的核心, 内置有自我注册系统处理软件和包括预设定的一系列的电压和温度的组合的环境参数, 通过该处理软件控制电压调节器和温度调节器遍历所有环境参数, 从而自动实现稳定可靠的 PUF 单元的功能。

[0030] 电压调节器, 如图 3 所示, 包括选择电压输出单元和多个分压电阻, 工作电压 VDD 通过分压电阻连接到选择电压输出单元上, 该选择电压输出单元在 BISE 控制器的控制下, 向 SRAM2 输出不同的电压。当 BISE 控制器输出“0000”到电压调节器, 它将输出 0 电压到 SRAM2。其他 4-bit 组合在正常电压的 A%-B% (例如 80%-120%) 之间线性选择一个电压作为 SRAM2 的 VDD。电压调节器可以模拟各种电压在有效范围内波动的情况, 并在此环境参数基础上选择稳定可靠的 PUF 单元。

[0031] 温度调节器, 如图 4 所示, 包括计数器, 该计数器在 BISE 控制器的控制下, 向 SRAM2 循环交替写入“0”和“1”, 从而调节 SRAM2 的温度。半导体器件的功率是由晶体管的翻转频率直接决定的。我们用重复交替写入“0”和“1”来增加 SRAM2 的功率, 从而间接调控 SRAM2 的温度。以前的做法是调控环境温度, 继而调控基片噪声。由于同一 SRAM 单元的两个反相器有相同的基片噪声, 它们将互相抵消。因此用重复交替写入 SRAM 来模拟温度波动比已往的方法更加有效。当 BISE 控制器输出“1111”到温度调节器, 它将产生 16 次交替的“0”, “1”写入直到计数器递减为“0000”。温度调节器可以输入更多位元来模拟更大范围内的温度波动的情况, 并在此环境参数基础上选择稳定可靠的 PUF 单元。

[0032] 一种基于 SRAM 的 PUF 的片上自我注册方法, 包括以下步骤:

[0033] 步骤 1: BISE 控制器由初始态自动进入检测模式 0, 检测后输出检测模式 0 下的可靠的 PUF 单元。具体检测过程如下:

[0034] 首先, SRAM1 所有单元被初始化成“0”。

[0035] 然后, 在各种环境参数 (电压 / 温度) 组合下, SRAM2 上电, 并读取 SRAM2 的每个单

元的初始逻辑值。我们把这个逻辑值和 SRAM1 相应单元的逻辑值进行逻辑“或”运算,并把结果存入 SRAM1 相应单元。我们重复以上操作直到所有环境参数全部遍历完毕。这时只有在不同环境参数下一直得到稳定初始“0”的 SRAM2 的单元,它对应的 SRAM1 单元才能得到“0”。如果在某一环境参数下,SRAM2 的某单元得到初始“1”,由于逻辑“或”运算,它对应的 SRAM1 单元将一直得到“1”。

[0036] 最后,当遍历完所有环境参数,我们将稳定可靠的 SRAM2 “0”的单元地址输出作为 PUF 特征地址,“0”作为这些特征地址的特征值。

[0037] 步骤 2 :BISE 控制器自动进入检测模式 1,检测后输出检测模式 1 下的可靠的 PUF 单元。具体检测过程如下:

[0038] 首先 SRAM1 所有单元被初始化成“1”。

[0039] 然后在各种环境参数(电压 / 温度)组合下,SRAM2 上电,并读取 SRAM2 的每个单元的初始逻辑值。我们把这个逻辑值和 SRAM1 相应单元的逻辑值进行逻辑“与”运算,并把结果存入 SRAM1 相应单元。我们重复以上操作直到所有环境参数全部遍历完毕。这时只有在不同环境参数下一直得到稳定初始“1”的 SRAM2 的单元,它对应的 SRAM1 单元才能得到“1”。如果在某一环境参数下,SRAM2 的某单元得到初始“0”,由于逻辑“与”运算,它对应的 SRAM1 单元将一直得到“0”。

[0040] 最后,当遍历完所有环境参数,我们将稳定可靠的 SRAM2 “1”的单元地址输出作为 PUF 特征地址,“1”作为这些特征地址的特征值,然后系统自动退出注册模式。

[0041] 下面通过激励 - 响应认证技术对本发明的应用进行说明。

[0042] 认证由一对随时间变化的激励 / 响应完成,这一激励通常由认证器选择一个随机 SRAM PUF 的特征地址,使用者的响应依据激励查询 SRAM PUF 的特征值。

[0043] 当一设备 / 芯片第一次被使用(也可能发生在生产后,出厂前)必须“注册”。这个过程记录正常使用时 SRAM 中稳定可靠的单元作为 PUF。一系列激励和相应的 PUF 响应存储于安全数据库,这个过程叫注册。

[0044] 以往的注册过程相当麻烦,所以大大影响了 PUF 的实用性。如果使用本自我注册系统(BISE),从用户角度,一切流程变得非常简单。

[0045] 正常使用过程中,SRAM PUF 的特征地址 / 特征值提供一个不需储存,不能被读取,且不可能复制的密钥。每个这样的芯片都带有唯一的密钥,只有通过正常注册过程的芯片,它的密钥才能被使用。

[0046] 对这些 PUF 认证过程,可以使用普通的基于激励响应的模式。验证系统给出一个激励(SRAM PUF 的特征地址),你就可以从 PUF 中得到对于设备独特的响应(SRAM PUF 的特征值)。如果响应符合注册结果,你所用的即是合法 / 正版芯片。假如生产完毕后,用此机制可防止过份生产,因只有合法设备将被注册。任何没有注册的响应被标识为非法。

[0047] 激励和响应可简单看作一个握手协议,但那样能被轻易窥探。因此更典型的做法是记录许多对激励和响应。这些激励和响应被存储于一个数据库(按照终端应用,这些可以放在读取器中或云中)。传统的做法,每对激励 / 响应仅用一次而后被扔掉。这需要根据应用变化提前存储大量激励 / 响应,并且如果用光,比较难产生新的激励 / 响应。如果使用本专利的自我注册系统(BISE),这个问题也可以得到解决。如果 1K RAM 中有 256 个单元可以提供稳定的 PUF 特征地址,我们可以随机挑选 128 个单元地址,并以随机顺序发送激励。

[0048] 随半导体工艺发展,Process Variation 变大。SRAM PUF 特征地址增多,这就意味着使用 SRAM PUF 加密的优越性增加。

[0049] 需要强调的是,本发明所述的实施例是说明性的,而不是限定性的,因此本发明包括并不限于具体实施方式中所述的实施例,凡是由本领域技术人员根据本发明的技术方案得出的其他实施方式,同样属于本发明保护的范围。

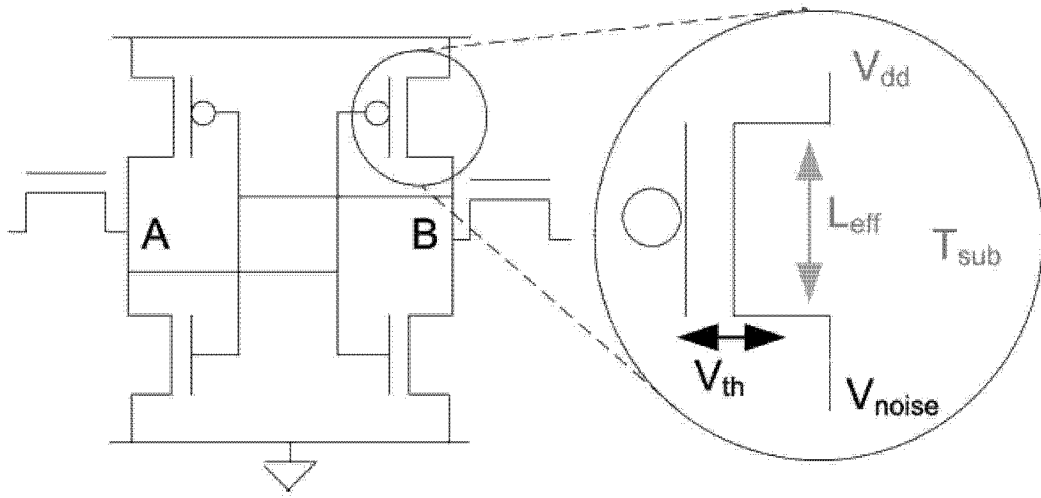


图 1

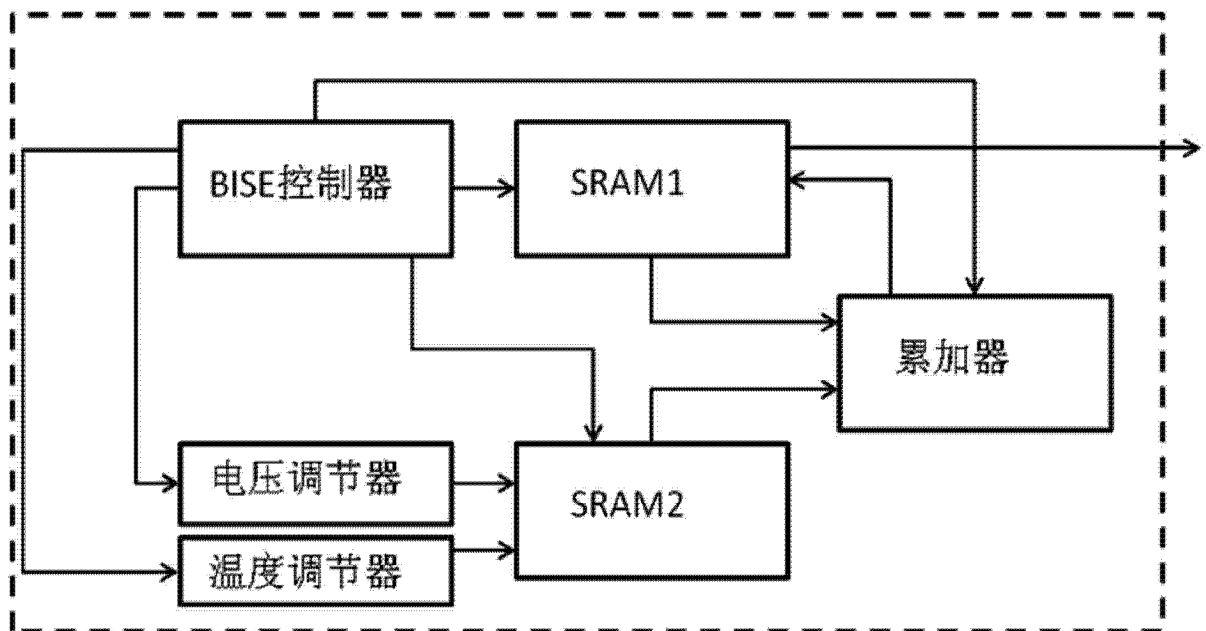


图 2

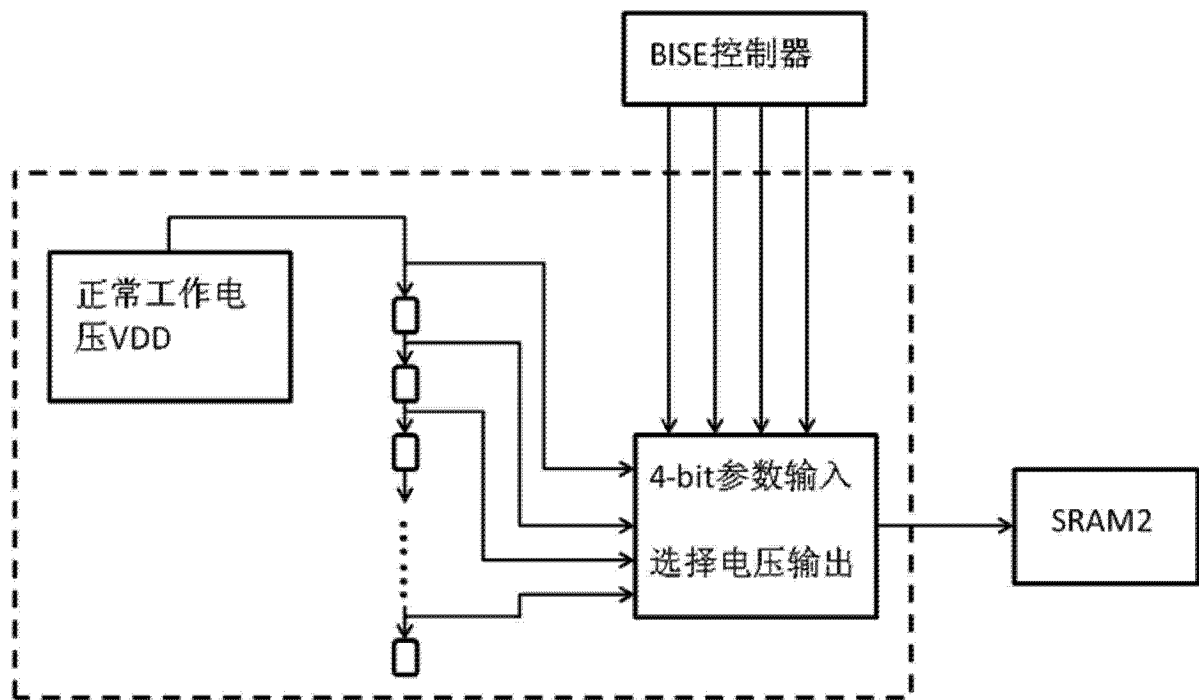


图 3

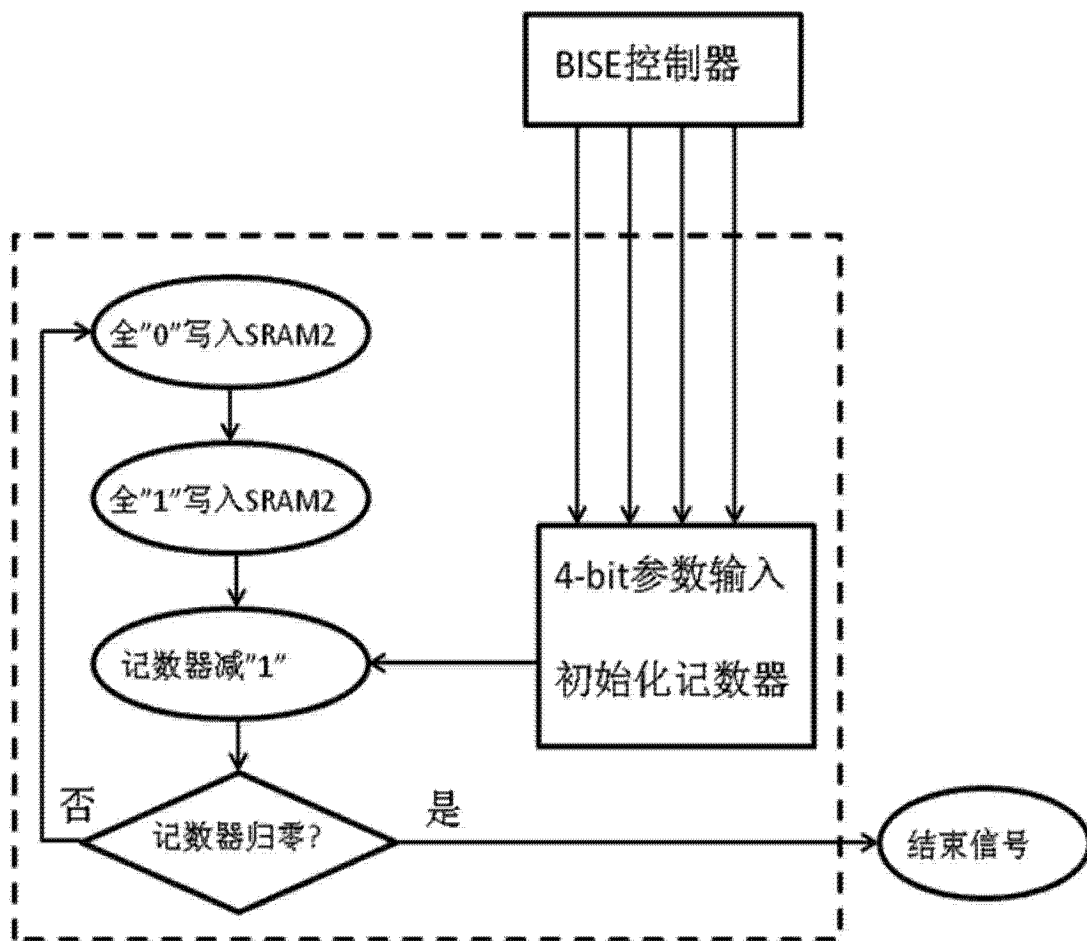


图 4

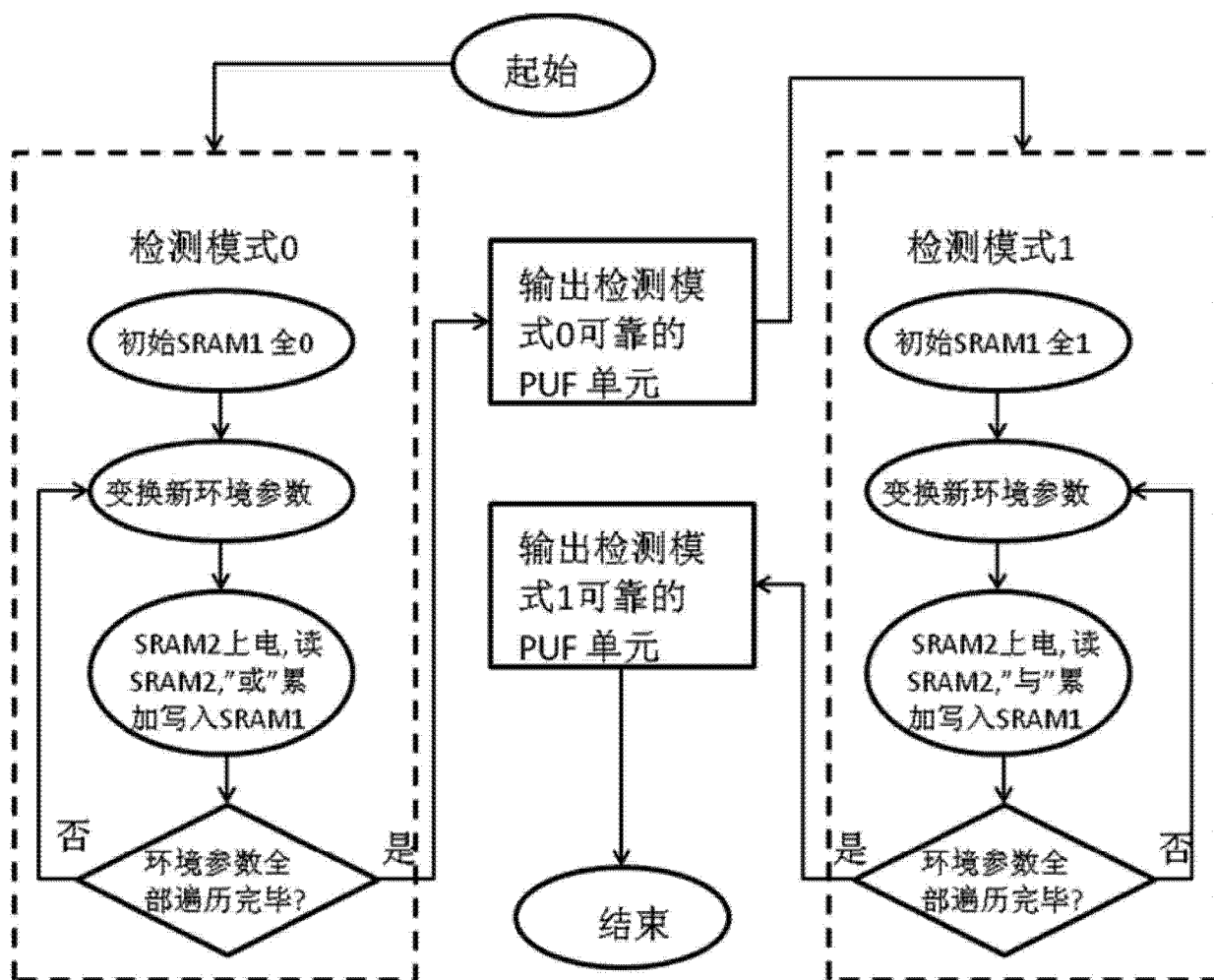


图 5