(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104658601 B
(45)授权公告日 2017.12.29

(21)申请号 201510031305.3

(22)申请日 2015.01.22

(65)同一申请的已公布的文献号
申请公布号 CN 104658601 A

(43)申请公布日 2015.05.27

(73)专利权人 北京大学
地址 100871 北京市海淀区颐和园路5号

(72)发明人 孙广宇 张宪

(74)专利代理机构 北京万象新悦知识产权代理事务所(普通合伙) 11360
代理人 苏爱华

(51)Int.Cl.
G11C 16/02(2006.01)
G11C 16/06(2006.01)

(56)对比文件
WO 2009/024913 A2,2009.02.26,
US 2011/0234241 A1,2011.09.29,
US 2012/0066571 A1,2012.03.15,
US 2014/0268994 A1,2014.09.18,
CN 102656588 A,2012.09.05,
US 2012/0106235 A1,2012.05.03,

审查员 李元

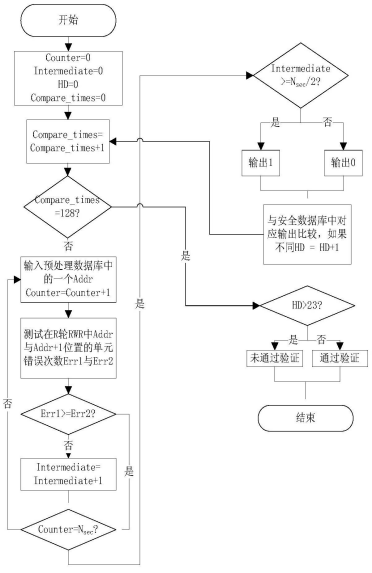
权利要求书2页 说明书5页 附图3页

(54)发明名称

基于STT-RAM存储单元错误率分布的PUF认证方法

(57)摘要

本发明公布了一种利用自旋矩传输随机读写器(STT-RAM)存储单元错误率分布的物理不可克隆认证方法,包括预处理阶段、注册阶段和验证阶段,包括步骤:首先在预处理阶段记录STT-RAM阵列中所有EDP的位置,然后在注册阶段输入若干EDP位置,芯片电路利用这些EDP内两个单元错误率相对大小来输出参考输出,在验证阶段再次重现注册阶段,最后根据验证阶段和注册阶段的输出验证给定设备与注册阶段的设备是否相同,从而认证芯片真假。本发明提供方法在很小的硬件代价以及时间代价下,解决设备认证的问题,提高认证的可靠性。



CN 104658601 B

1.一种基于STT-RAM存储单元错误率分布的物理不可克隆认证方法,依次包括如下步骤:

1)在预处理阶段执行如下操作,得到多个错误率差分对单元的地址,所述错误率差分对记为EDP:

1.1分别在Error-Least-State与Error-Most-State环境下,对于每个奇地址单元,设定该单元的地址为Addr,通过N轮读写读测试判断单元地址为Addr与Addr+1的两个单元是否构成EDP;所述Error-Least-State是STT-RAM单元错误率最低的工作环境;所述Error-Most-State是STT-RAM单元错误率最高的环境;所述读写读测试记为RWR测试;

1.2如果上述两个单元构成EDP,则得到该EDP的地址EDP_Addr和EDP_Addr+1;

1.3将EDP_Addr输出保存到数据库;

2)在注册阶段执行如下操作,得到参考输出:

2.1从步骤1.3所述数据库中取得N_{sec}个在预处理阶段得到的EDP,将计数器置为0;所述N_{sec}为大于等于128的偶数;

2.2对于步骤2.1中的每个EDP,判断EDP_Addr与EDP_Addr+1地址的两个单元在R轮RWR测试中,哪个单元发生错误的次数更多;如果EDP_Addr+1比EDP_Addr发生错误的次数多,步骤2.1中的计数器加1;

2.3当遍历N_{sec}个EDP后,将计数器中的数与N_{sec}的一半比大小,计数器中的数大于等于N_{sec}的一半时输出1,否则输出0;

2.4将2.3输出结果作为参考输出,存到一个安全的数据库中;

3)设结果不同次数为0,在验证阶段执行如下操作,得到结果不同的总次数,用于验证给定设备与注册阶段的设备是否相同:

3.1取得N_{sec}个预处理阶段得到的数据库中的EDP,将计数器置为0;所述N_{sec}个EDP作为一次整体的输入在注册阶段被使用过;所述N_{sec}的取值与步骤2.1中的N_{sec}相同;

3.2对于步骤3.1中的每个EDP,判断EDP_Addr与EDP_Addr+1地址的两个单元在R轮RWR测试中,哪个单元发生错误的次数更多;如果EDP_Addr+1比EDP_Addr发生错误的次数多,步骤3.1中的计数器加1;

3.3当遍历所述N_{sec}个EDP_Addr后,将计数器中的数与N_{sec}的一半比大小,计数器中的数大于等于N_{sec}的一半时输出1,否则输出0;

3.4将3.3的输出结果与注册阶段步骤2.4的参考输出结果作比较,如果二者结果不同则结果不同次数加1;

3.5多次重复步骤3.1到3.4,得到结果不同的总次数;

3.6判断步骤3.5中结果不同的总次数是否大于设定阈值,如大于则判断设备没通过认证,否则设备通过认证。

2.如权利要求1所述物理不可克隆认证方法,其特征是,步骤1.1所述Error-Most-State表示最低工作电压为0.9V,最高工作温度为325K的环境;所述Error-Least-State表示最高工作电压为1.1V,最低工作温度为275K的环境。

3.如权利要求1所述物理不可克隆认证方法,其特征是,步骤1.1所述是否构成EDP具体是通过所述单元地址为Addr与Addr+1的两个单元发生错误的次数之差是否大于等于N_{th}来判断,N_{th}与步骤1.1所述N相等,取值为大于等于3。

4.如权利要求3所述物理不可克隆认证方法，其特征是，步骤1.1所述N取值为3。

5.如权利要求1所述物理不可克隆认证方法，其特征是，步骤2.1和步骤3.1中的N_{sec}取值均为128。

6.如权利要求1所述物理不可克隆认证方法，其特征是，步骤2.2和步骤3.2所述R的取值均为4。

7.如权利要求1所述物理不可克隆认证方法，其特征是，步骤3.5所述多次为128次。

8.如权利要求1所述物理不可克隆认证方法，其特征是，步骤3.6所述阈值为23。

基于STT-RAM存储单元错误率分布的PUF认证方法

技术领域

[0001] 本发明属于信息安全领域,涉及一种物理不可克隆(PUF)认证方法,尤其涉及一种基于STT-RAM存储单元错误率分布的物理不可克隆认证方法。

背景技术

[0002] 自旋矩传输随机读写器(STT-RAM)是一种新型非易失(Non-volatile)存储器。STT-RAM被认为是未来SRAM的替代品之一,拥有高密度,低静态功耗,低访存时间等优点。与此同时,物理不可克隆技术(PUF)正被广泛建议应用于设备认证,而其他非易失性存储已经被提出用于制作PUF,但是普遍存在硬件开销大或者延迟高等问题。

[0003] 2011年,美国的Prabhu等人提出利用NAND Flash来进行设备认证。他们首先提取Flash中每个比特对干扰错误(disturb error)的敏感程度,编程延迟等等,然后计算相关系数的办法来区分和认证芯片。这种办法延迟长(15s),且环境影响下可能会失效。

[0004] 2012年,美国的Rajendran等人提出利用忆阻器(Memristor)来进行设备认证。他们首先用感应器(sensor)采集每个单元节点的电压,然后利用电压信息进行认证芯片。这种办法由于需要使用感应器采集每个节点电压,额外电路开销较大,并且环境变化也会影响稳定性。

发明内容

[0005] 为了克服上述现有技术的不足,本发明提供一种利用自旋矩传输随机读写器(STT-RAM)存储单元错误率分布的物理不可克隆认证方法,在很小的硬件代价以及时间代价下,解决设备认证的问题,提高认证的可靠性。

[0006] 本文定义如下术语:

[0007] (1)Error-Least-State:表示本发明工作环境中,STT-RAM单元错误率最低的环境。例如,在工作电压0.9V-1.1V、工作温度275K-325K的环境下,Error-Least-State表示最高工作电压、最低工作温度的环境,即(1.1V,275K)的环境。

[0008] (2)Error-Most-State:表示本发明工作环境中,STT-RAM单元错误率最高的环境。例如,在工作电压0.9V-1.1V、工作温度275K-325K环境下,Error-Most-State表示最低工作电压、最高工作温度的环境,即(0.9V,325K)的环境。

[0009] (3)RWR测试:即读写读测试,是一种检测单元错误率的方法。该方法首先读取单元数据,反转数据后写回,再读出数据检测数据是否成功改变来检测读写错误。

[0010] (4)EDP:即错误率差分对(Error-rate Differential Pair),表示STT-RAM阵列中满足下列关系的两个相邻单元:在N轮RWR测试中,两个单元发生错误的次数之差大于等于一给定次数N_{th}。通过对1MB大小1T1J的STT-RAM存储阵列进行仿真实验,证明N和N_{th}的取值应该满足$N=N_{th}>=3$,本发明实施例中$N=N_{th}=3$。

[0011] 本发明的原理是,本发明基于STT-RAM存储单元错误率分布的物理不可克隆认证方法包括三个阶段:预处理阶段、注册阶段和验证阶段。首先在预处理阶段(Pre-process)

记录STT-RAM阵列中所有EDP的位置，然后在注册阶段(Enrollment Phase)输入多个EDP位置，芯片电路利用这些EDP内两个单元错误率相对大小来输出参考输出(Reference Response)，在验证阶段(Evaluation Phase)再次重现注册阶段，最后根据验证阶段和注册阶段的输出判断芯片的真假。

[0012] 本发明提供的技术方案是：

[0013] 一种基于STT-RAM存储单元错误率分布的物理不可克隆认证方法，依次包括如下步骤：

[0014] 1)在预处理阶段执行如下操作，得到多个EDP单元的地址：

[0015] 1.1分别在Error-Least-State与Error-Most-State环境下，对于每个奇地址单元，设定该单元的地址为Addr，通过N轮RWR测试判断地址为Addr与Addr+1两个单元是否构成EDP；

[0016] 1.2如果上述两个单元构成EDP，则得到该EDP的地址EDP_Addr和EDP_Addr+1；

[0017] 1.3将EDP_Addr输出保存到数据库；

[0018] 2)在注册阶段执行如下操作，得到参考输出：

[0019] 2.1取得N_{sec}个在预处理阶段得到的数据库中的EDP，计数器置为0；其中，N_{sec}为偶数；N_{sec}的取值应大于等于128，本发明中实施例中N_{sec}取值为128；

[0020] 2.2对于每个EDP，判断EDP_Addr与EDP_Addr+1地址的两个单元在R轮RWR测试中，哪个单元发生错误的次数更多；如果EDP_Addr+1比EDP_Addr发生错误的次数多，计数器加1；通过对1MB大小1T1J的STT-RAM存储阵列进行仿真实验，证明R的取值应该满足R>＝4，本发明实施例中R＝4。

[0021] 2.3当遍历N_{sec}个EDP后，将计数器中的数与N_{sec}的一半比大小，大于等于时输出1否则输出0；

[0022] 2.4将2.3输出结果作为参考输出，存到一个安全的数据库中；

[0023] 3)设结果不同次数为0，在验证阶段执行如下操作，得到结果不同的总次数，用于验证给定设备与注册阶段的设备是否相同：

[0024] 3.1取得N_{sec}个在预处理阶段得到的数据库中的EDP，将计数器置为0；确保这N_{sec}个EDP作为一次整体的输入在注册阶段被使用过；该N_{sec}取值与步骤2.1中的N_{sec}取值相同，本发明实施例中取值为128；

[0025] 3.2对于每个EDP，判断EDP_Addr与EDP_Addr+1地址的两个单元在R轮RWR测试中，哪个单元发生错误的次数更多；如果EDP_Addr+1比EDP_Addr发生错误的次数多，计数器加1；该R取值与步骤2.2中的R取值相同，本发明实施例中取值为4；

[0026] 3.3当遍历N_{sec}个EDP_Addr后，将计数器中的数与N_{sec}的一半比大小，大于等于时输出1否则输出0；

[0027] 3.4将3.3的输出结果与注册阶段步骤2.4的参考输出结果作比较，如果二者结果不同则结果不同次数加1；

[0028] 3.5多次重复步骤3.1到3.4，得到结果不同的总次数；

[0029] 3.6判断步骤3.5中结果不同的总次数是否大于设定阈值，如大于则判断设备没通过认证，否则设备通过认证。

[0030] 在本发明实施例中，上述基于STT-RAM存储单元错误率分布的物理不可克隆认证

方法是在工作电压0.9V-1.1V、工作温度275K-325K环境下进行的，其中，步骤1.1中的Error-Most-State表示最低工作电压、最高工作温度的环境，即(0.9V，325K)的环境；Error-Least-State表示最高工作电压、最低工作温度的环境，即(1.1V，275K)的环境。

[0031] 上述基于STT-RAM存储单元错误率分布的物理不可克隆认证方法中，经过仿真实验，步骤1.1是通过两个单元发生错误的次数之差是否大于等于N_{th}来判断两个位置的单元是否构成EDP；步骤1.1中的N和N_{th}的取值应该满足$N=N_{th}>=3$，本发明实施例中$N=N_{th}=3$；步骤2.2中的R取值应该满足$R>=4$，本发明实施例中$R=4$；步骤3.2中的R取值与步骤2.2相同；步骤3.5中的多次为128次，步骤3.6中的阈值为23。在本发明实施例中，步骤2.1和步骤3.1中的N_{sec}取值为128。

[0032] 与现有技术相比，本发明的有益效果是：

[0033] 通过本发明所提供的基于STT-RAM存储单元错误率分布的物理不可克隆认证方法，利用验证阶段和注册阶段输出的EDP内两个单元错误率相对大小对硬件设备进行认证，提高了认证的可靠性，加快了认证速度，节省了硬件开销。

附图说明

[0034] 图1是本发明实施例中预处理阶段的流程框图。

[0035] 图2是本发明实施例中注册阶段的流程框图。

[0036] 图3是本发明实施例中验证阶段的流程框图。

具体实施方式

[0037] 下面结合附图，通过实施例进一步描述本发明，但不以任何方式限制本发明的范围。

[0038] 本实施例针对1个1MB大小1T1J的STT-RAM进行认证，指定其工作环境为电压范围0.9V-1.1V，温度范围275K到325K。利用本发明提供的基于STT-RAM存储单元错误率分布的物理不可克隆认证方法，本实施例的认证工作分为三个阶段——预处理阶段、注册阶段，验证阶段。

[0039] A.在预处理阶段，执行如下操作：

[0040] A1.分别在Error-Least-State与Error-Most-State下，对于每个奇地址Addr，判断Addr与Addr+1两个位置的单元是否构成EDP。判断EDP的方法是，在N轮RWR测试中，两个单元发生错误的次数之差大于等于N_{th}，本实施例中，N和N_{th}均取值为3；

[0041] A2.如果构成EDP输出Addr的值，否则继续检测下个奇地址对应的两个单元是否构成EDP。；

[0042] A3.将输出的EDP保存以供稍后使用；

[0043] B.在注册阶段，执行如下操作：

[0044] B1.输入128个预处理阶段得到的EDP_Addr；

[0045] B2.对于每个EDP_Addr，判断EDP_Addr与EDP_Addr+1地址的两个单元在4轮RWR测试中，哪个单元发生错误次数多，如果后者多，计数器加1，否则不加；

[0046] B3.当遍历128个EDP_Addr后，将计数器中的数与64比大小，大于等于时输出1否则0；

[0047] B4.将输出结果存到一个安全的数据库中作为稍后认证阶段的参考输出；

[0048] C.在验证阶段，执行如下操作：

[0049] C1.输入128个EDP_Addr，确保在注册阶段这128个EDP_Addr作为一次整体的输入被使用过；

[0050] C2.对于每个EDP_Addr，判断EDP_Addr与EDP_Addr+1地址的两个单元在R轮RWR测试中，哪个单元发生错误次数多，如果后者多，计数器加1，否则不加；

[0051] C3.当遍历128个EDP_Addr后，将计数器中的数与64比大小，大于等于时输出1否则0；

[0052] C4.将输出结果与注册阶段的结果作比较；

[0053] C5.重复C1到C4步骤一定次数，看最终有多少次输出不一样，如果不一样的次数大于23，则判断芯片没通过认证，否则通过认证。

[0054] 图1是本发明实施例中预处理阶段的流程框图。参考附图1，在预处理阶段，STT-RAM的工作环境首先被置为Error-Most-State，即(0.9V，325K)的环境；然后逐个验证奇地址Addr与Addr+1位置的单元在3轮RWR测试中，奇地址Addr与Addr+1位置发生错误的次数Err1与Err2之差是否大于等于N_{th}，N_{th}取值为3，如果是则将Addr存入数据库。例如经过3轮RWR测试发现1与2位置的单元分别错误了3次与0次，那么1将被存入数据库。紧接着，STT-RAM的工作环境被置为Error-Least-State，即(1.1V，275K)的环境，然后测试上述数据库中的Addr在这种环境下是否依旧满足Addr与Addr+1位置的单元在3轮RWR测试中的错误次数Err1与Err2之差大于等于N_{th}，N_{th}取值为3，如果满足则保留Addr，如果不满足则从数据库中剔除Addr。例如在Error-Least-State下发现地址1与地址2的单元在3轮RWR测试中的错误次数之差小于3，那么1将从数据库中剔除。

[0055] 图2是本发明实施例中注册阶段的流程框图。参考附图2，在注册阶段，首先将计数器Intermediate置为0，然后输入128个在预处理阶段得到的、数据库中的Addr。对于每个Addr，比较Addr与Addr+1位置单元在R(R取值为4)轮RWR测试下的错误次数，如果Addr的错误次数大于Addr+1，那么计数器Intermediate加1。再遍历了128个Addr后，即Counter＝128时，比较计数器Intermediate的值与64(128的一半)的大小，如果大于，输出1，否则输出0。最后将输出存入一个安全的数据库。例如对于128个Addr，假设其中有67个Addr都满足Addr比Addr+1位置单元在4轮RWR测试下的错误次数多，那么最后计数器的数值为67。由于67>64，因此输出1到安全数据库中。

[0056] 图3是本发明实施例中验证阶段的流程框图。参考附图3，在验证阶段，首先将计数器Intermediate置为0，然后输入曾经在注册阶段作为一组输入的128个Addr。对于每个Addr，比较Addr与Addr+1位置单元在4轮RWR测试下的错误次数，如果Addr的错误次数大于Addr+1，那么计数器Intermediate加1。再遍历了128个Addr后，即Counter＝128时，比较计数器与64的大小，如果大于，输出1，否则输出0。最后将输出与安全数据库中对应数据进行比较，如果不同则记录下不同的次数HD。反复进行上述步骤128次，即Compare_times＝128时，将不同的次数HD与阈值23相比较，如果大于23则判断验证失败否则成功。例如对于被测试的STT-RAM芯片，若通过测试发现在验证阶段其输出共有25次与安全数据库中对应输出不同，那么其认证结果为验证失败，即可以认为这块芯片不是注册阶段的芯片。

[0057] 需要注意的是，公布实施例的目的在于帮助进一步理解本发明，但是本领域的技

术人员可以理解:在不脱离本发明及所附权利要求的精神和范围内,各种替换和修改都是可能的。因此,本发明不应局限于实施例所公开的内容,本发明要求保护的范围以权利要求书界定的范围为准。

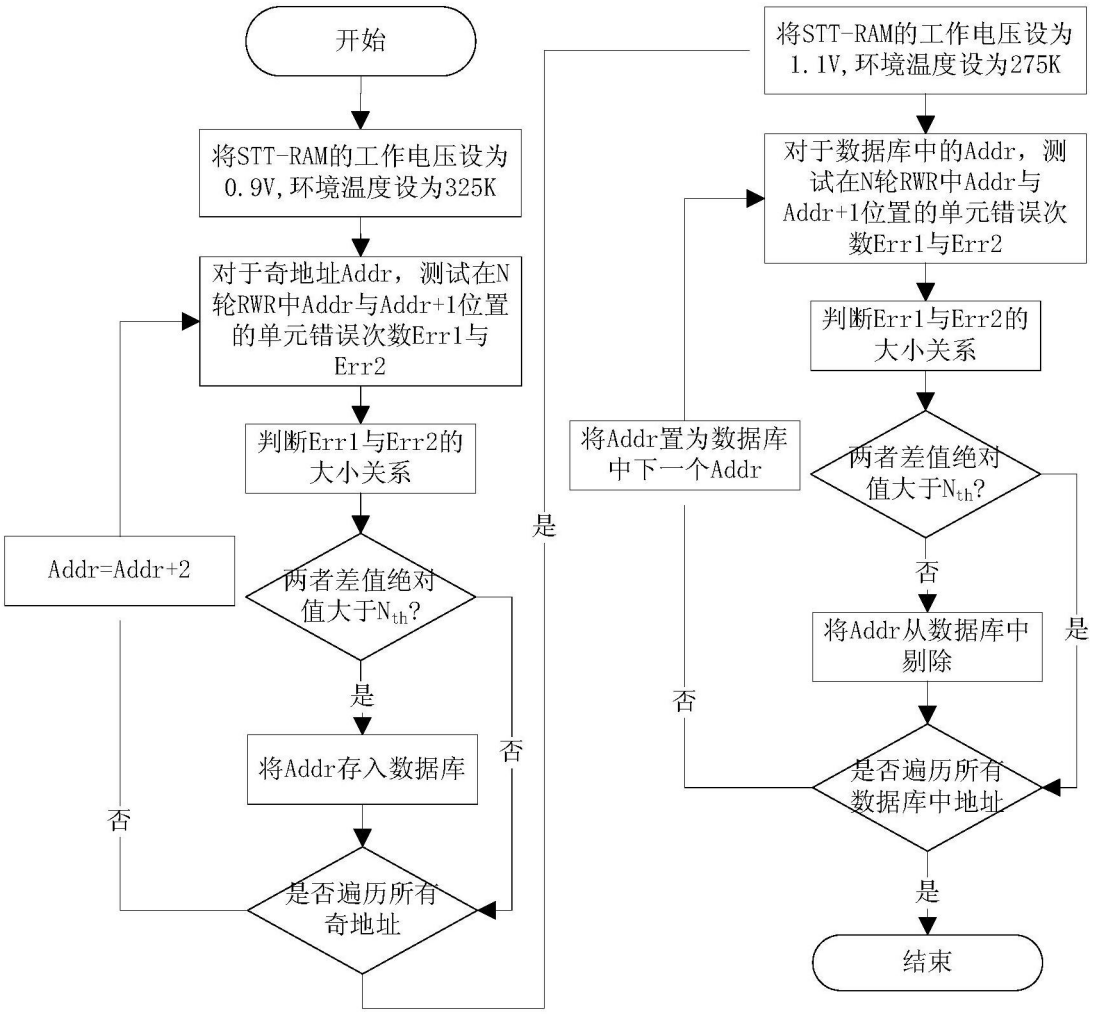

开始
将STT-RAM的工作电压设为0.9V,环境温度设为325K
对于奇地址Addr，测试在N轮RWR中Addr与Addr+1位置的单元错误次数Err1与Err2
判断Err1与Err2的大小关系
两者差值绝对值大于N_{th}?
是
否
将Addr存入数据库
是否遍历所有奇地址
否
是
Addr=Addr+2
将STT-RAM的工作电压设为1.1V,环境温度设为275K
对于数据库中的Addr，测试在N轮RWR中Addr与Addr+1位置的单元错误次数Err1与Err2
判断Err1与Err2的大小关系
两者差值绝对值大于N_{th}?
否
是
将Addr从数据库中剔除
是否遍历所有数据库中地址
否
是
将Addr置为数据库中下一个Addr
结束

图1

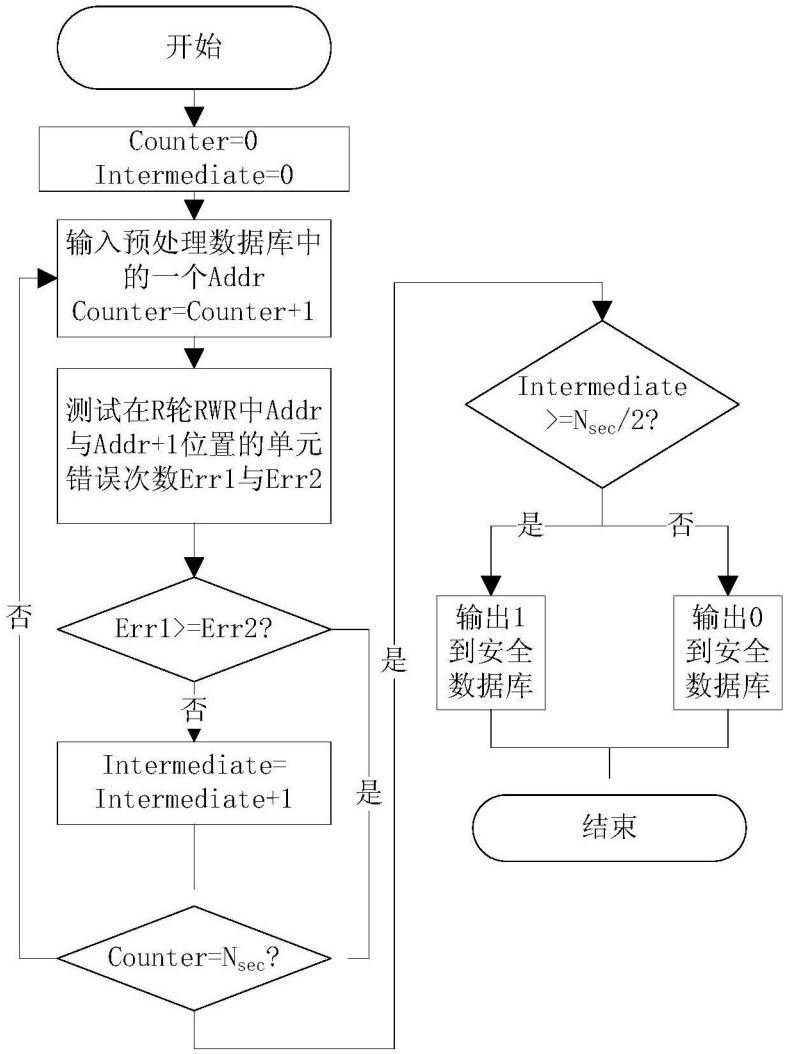

开始
Counter=0
Intermediate=0
输入预处理数据库中的一个Addr
Counter=Counter+1
测试在R轮RWR中Addr与Addr+1位置的单元错误次数Err1与Err2
Err1>=Err2?
否
是
Intermediate=Intermediate+1
Counter=Nsec?
否
是
Intermediate>=Nsec/2?
是
否
输出1到安全数据库
输出0到安全数据库
结束

图2

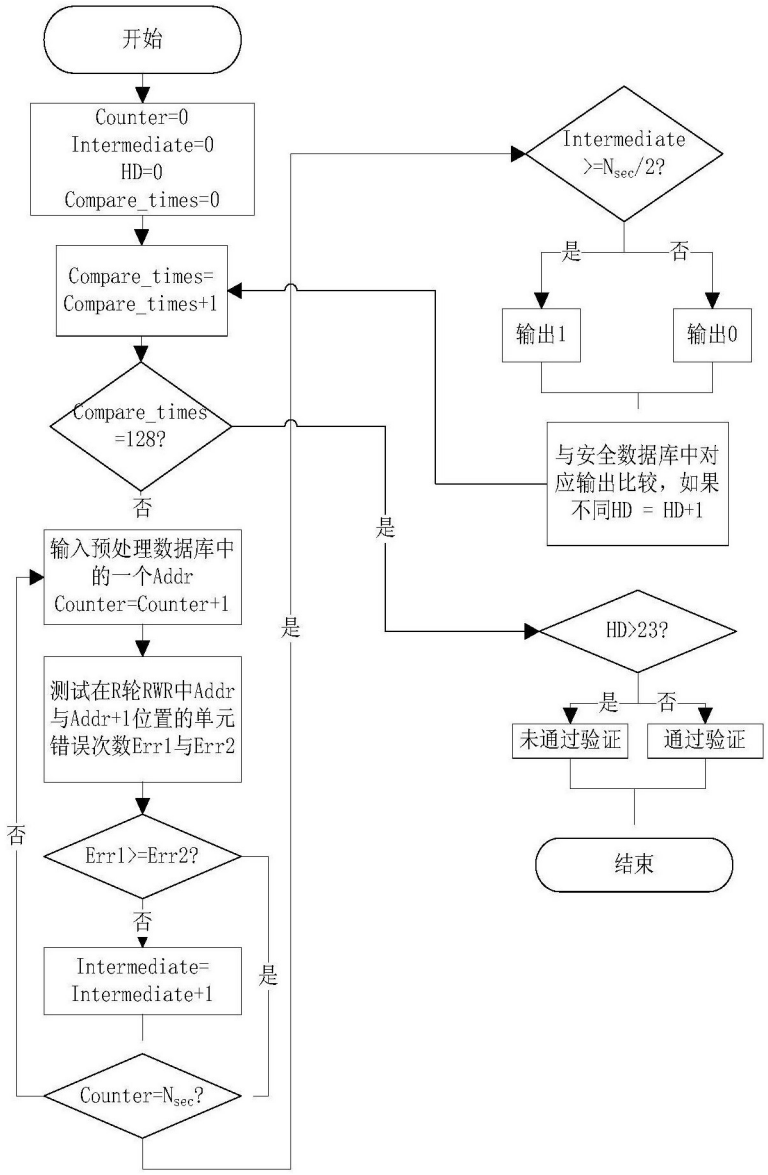

开始
Counter=0
Intermediate=0
HD=0
Compare_times=0
Compare_times=
Compare_times+1
Compare_times
=128?
否
是
输入预处理数据库中
的一个Addr
Counter=Counter+1
测试在R轮RWR中Addr
与Addr+1位置的单元
错误次数Err1与Err2
Err1>=Err2?
否
是
Intermediate=
Intermediate+1
Counter=Nsec?
否
是
Intermediate
>=Nsec/2?
是
否
输出1
输出0
与安全数据库中对
应输出比较，如果
不同HD = HD+1
是
HD>23?
是
否
未通过验证
通过验证
结束

图3