(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111966329 B
(45)授权公告日 2023.03.21

(21)申请号 202010832075.1

(22)申请日 2020.08.18

(65)同一申请的已公布的文献号
申请公布号 CN 111966329 A

(43)申请公布日 2020.11.20

(73)专利权人 合肥工业大学
地址 230009 安徽省合肥市包河区屯溪路193号

(72)发明人 梁华国 王燕捷 王鑫宇 鲁迎春 蒋翠云 易茂祥 黄正峰

(74)专利代理机构 安徽省合肥新安专利代理有限责任公司 34101
专利代理师 陆丽莉 何梅生

(51)Int.Cl.
G06F 7/58(2006.01)

(56)对比文件
CN 103902930 A,2014.07.02
CN 106372539 A,2017.02.01
CN 108985105 A,2018.12.11
湛霍等.面向物理不可克隆函数的可靠性与随机性增强技术.《计算机应用》.2015,(第05期),
霍文捷等.一种基于FPGA的真随机数生成器的设计.《华中科技大学学报(自然科学版)》.2009,(第01期),

审查员 赵鹏翔

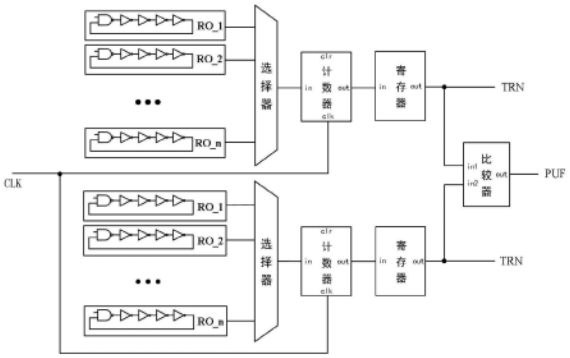
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种基于物理不可克隆函数PUF的真随机数发生器

(57)摘要

本发明公开了一种基于物理不可克隆函数PUF的真随机数发生器，是由两组RO振荡环、两个选择器、两个计数器、两个寄存器和一个比较器构成；任意一组RO振荡环与任意一个选择器的输入端连接，任意一个选择器的输出端与任意一个计数器的输入端相连，任意一个计数器的输出端分别与任意一个寄存器相连，任意一个寄存器的输出端输出真随机数TRN，两个寄存器的输出端还连接到比较器的输入端，比较器的输出端输出物理不可克隆函数PUF。本发明能在单个设备中同时实现puf和trng，从而减小能源开销，提升整体芯片电路性能。



CN 111966329 B

1.一种基于物理不可克隆函数PUF的真随机数发生器,其特征是由两组RO振荡环、两个选择器、两个计数器、两个寄存器和一个比较器构成;

任意一组RO振荡环与任意一个选择器的输入端连接,任意一个选择器的输出端与任意一个计数器的输入端相连,任意一个计数器的输出端分别与任意一个寄存器相连,任意一个寄存器的输出端输出真随机数TRN,两个寄存器的输出端还连接到比较器的输入端,比较器的输出端输出物理不可克隆函数PUF;

任意一组RO振荡环是由n个RO环组成,任意第i个RO环是由一个双输入与非门使能信号单元与四个反向器构成;

所述双输入与非门使能信号单元是由单输出双输入查找表LUT2配置,每个反相器由一个单输入查找表LUT1配置;

设定单输出双输入查找表LUT2的初值为4'b0111,单输入查找表LUT1的初值为2'b01;

令第一单输入查找表LUT1-1的输出端与第二单输入查找表LUT1-2的输入端相连;

令所述第二单输入查找表LUT1-2的输出端与第三单输入查找表LUT1-3的输入端相连;

令所述第三单输入查找表LUT1-3的输出端与第四单输入查找表LUT1-4的输入端相连;

令所述单输出双输入查找表LUT2的低位输入端与第四单输入查找表LUT1-4的输出端相连,所述单输出双输入查找表LUT2的高位输入端设为使能端EN,所述单输出双输入查找表LUT2的输出端与第一单输入查找表LUT1-1的输入端相连;以所述查找表LUT2的输出端作为第i个RO环的输出端,从而通过五个查找表实现一个双输入与非门使能信号单元与四个反向器之间的连接关系。

2.根据权利要求1所述的真随机数发生器的工作方法,其特征是按如下步骤进行:

步骤1、定义变量i并初始化i=1;

步骤2、定义当前计数周期数为t,并初始化t=1;

定义计数周期的总数为N;

定义采集周期的总数为M,且M<N;

步骤3、任意一个多路选择器从相应组RO振荡环的第i个RO环的输出端所输出的熵源值作为相应多路选择器的第i次输出;

步骤4、相应多路选择器将第i次输出的熵源值送到所连接的一个计数器C的输入端中;

步骤5、计数器C清零并接收第i次输出的熵源值;

步骤6、计数器C开始计数;

步骤7、判定当前计数周期t是否等于kM,若等于,则执行步骤8-步骤9;否则,执行步骤10,其中,k为正整数;

步骤8、相应的寄存器对所连接的计数器C的计数值进行采样,得到采样数据;并将所述采样数据的低三位作为真随机数输出;将采样数据的高位送入所述比较器中;

步骤9、所述比较器将两个寄存器输入的高位进行比较,得到的比较结果作为物理不可克隆函数PUF;

步骤10、判定当前计数周期t是否大于N,若大于N,则将i+1赋值给i后,执行步骤3,否则,则所述计数器C继续计数,并执行步骤7。

一种基于物理不可克隆函数PUF的真随机数发生器

技术领域

[0001] 本发明属于芯片认证、IP保护领域，具体的说是一种基于物理不可克隆函数PUF的真随机数发生器。

背景技术

[0002] 随着社会信息化发展的不断深入，信息安全问题越来越受到人们的重视。安全性被认为是未来物联网发展的最关键障碍之一。在较高级别的安全系统中，密码系统的安全性主要与密钥的强度有关。在不可信的环境中，为了保证系统安全，密钥不能在系统外部生成，因此，如果是在单个芯片中实现安全系统，密钥与待加密信息必须在相同的芯片上。由于有许多技术可以破解传统密钥，使得传统密钥不足以保证硬件的安全。为有效解决此安全问题，PUF和TRNG应运而生。

[0003] 在FPGA中设计PUF输出的信息不是来自于非易失性存储器中存储的易泄露数字位流，而是来自随机的制造过程物理特征，因此PUF技术虽然实现起来简单但却具有极高的安全性。同时，PUF的输出信息还具有不可篡改性，因为PUF本身是来源于芯片制造过程中无法避免工艺偏差，而这种偏差根植于深亚微米甚至是纳米级的物理结构中，任何可能的物理攻击都会对PUF的微小物理特征产生破坏从而使得其输出响应发生显著变化。这使得PUF成为提供密码密钥生成和存储的防篡改设计的主要手段。而TRNG利用的则是从电路工作时的亚稳态或热噪声引起的抖动提取随机性，这种随机性不是由算法产生的，而是通过环境中的电磁热噪声产生，因此很难预测。

[0004] 现有的独立设计的TRNG由于熵源数量少，导致其设计具有吞吐量不足的缺点；而独立设计的PUF由于电路结构复杂，需要手动放置或路由，使得电路稳定性变差，受环境影响程度高。且现有的独立设计还存在面积利用率低，电路开销大等问题，亟待找寻新的方法来解决以上问题。

发明内容

[0005] 本发明是为了解决上述现有技术存在的不足之处，提出一种基于物理不可克隆函数PUF的真随机数发生器，以期能在单个设备中同时实现puf和trng，从而减小能源开销，提升整体芯片电路性能。

[0006] 本发明为达到上述发明目的，采用如下技术方案：

[0007] 本发明一种基于物理不可克隆函数PUF的真随机数发生器的特点是由两组RO振荡环、两个选择器、两个计数器、两个寄存器和一个比较器构成；

[0008] 任意一组RO振荡环与任意一个选择器的输入端连接，任意一个选择器的输出端与任意一个计数器的输入端相连，任意一个计数器的输出端分别与任意一个寄存器相连，任意一个寄存器的输出端输出真随机数TRN，两个寄存器的输出端还连接到比较器的输入端，比较器的输出端输出物理不可克隆函数PUF。

[0009] 本发明所述的真随机数发生器的特点也在于，任意一组RO振荡环是由n个RO环组

成,任意第i个RO环是由一个双输入与非门使能信号单元与四个反向器构成;

[0010] 所述双输入与非门使能信号单元是由单输出双输入查找表LUT2配置,每个反相器由一个单输入查找表LUT1配置;

[0011] 设定单输出双输入查找表LUT2的初值为4'b0111,单输入查找表LUT1的初值为2'b01;

[0012] 令所述第一单输入查找表LUT1-1的输出端与第二单输入查找表LUT1-2的输入端相连;

[0013] 令所述第二单输入查找表LUT1-2的输出端与第三单输入查找表LUT1-3的输入端相连;

[0014] 令所述第三单输入查找表LUT1-3的输出端与第四单输入查找表LUT1-4的输入端相连;

[0015] 令所述单输出双输入查找表LUT2的低位输入端与第四单输入查找表LUT1-4的输出端相连,所述单输出双输入查找表LUT2的高位输入端设为使能端EN,所述单输出双输入查找表LUT2的输出端与第一单输入查找表LUT1-1的输入端相连;以所述查找表LUT2的输出端作为第i个RO环的输出端,从而通过五个查找表实现一个双输入与非门使能信号单元与四个反向器之间的连接关系。

[0016] 本发明所述的真随机数发生器的工作方法的特点是按如下步骤进行:

[0017] 步骤1、定义变量i并初始化i=1;

[0018] 步骤2、定义当前计数周期数为t,并初始化t=1;

[0019] 定义计数周期的总数为N;

[0020] 定义采集周期的总数为M,且M<N;

[0021] 步骤3、任意一个多路选择器从相应组RO振荡环的第i个RO环的输出端所输出的熵源值作为相应多路选择器的第i次输出;

[0022] 步骤4、相应多路选择器将第i次输出的熵源值送到所连接的一个计数器C的输入端中;

[0023] 步骤5、计数器C清零并接收第i次输出的熵源值;

[0024] 步骤6、计数器C开始计数;

[0025] 步骤7、判定当前计数周期t是否等于kM,若等于,则执行步骤8-步骤9;否则,执行步骤10,其中,k为正整数;

[0026] 步骤8、相应的寄存器对所连接的计数器C的计数值进行采样,得到采样数据;并将所述采样数据的低三位作为真随机数输出;将采样数据的高位送入所述比较器中;

[0027] 步骤9、所述比较器将两个寄存器输入的高位进行比较,得到的比较结果作为物理不可克隆函数PUF;

[0028] 步骤10、判定当前计数周期t是否大于N,若大于N,则将i+1赋值给i后,执行步骤3,否则,则所述计数器C继续计数,并执行步骤7。

[0029] 与现有技术相比,本发明的有益效果在于:

[0030] 1、本发明利用基于RO振荡环的PUF电路来产生TRNG的同时,仍会输出PUF,解决了对于可密钥系统面积较小的设备的面积利用率的问题,减小了电路面积开销。

[0031] 2、本发明对于生成的PUF和TRNG各有用途和优势,可以用于非对称加密和非对称

密钥生成，且所设计的TRNG和PUF具有较好的随机性和稳定性。

[0032] 3、本发明利用可重配置的原理设计电路，使电路在较小的开销下仍具有较大的吞吐率。

附图说明

[0033] 图1为本发明基于物理不可克隆函数的真随机数发生器结构图；

[0034] 图2为本发明物理不可克隆函数的产生原理图；

[0035] 图3为本发明真随机数的产生原理图；

[0036] 图4为本发明真随机数发生器的工作流程图。

具体实施方式

[0037] 本实施例中，一种基于物理不可克隆函数PUF的真随机数发生器，是由两组RO振荡环、两个选择器、两个计数器、两个寄存器和一个比较器构成。

[0038] 如图1所示，熵源结构为两组RO振荡环，由选择器来选择每组RO振荡环中的一个RO环，作为选择器的输出，因此每组RO环与任意一个选择器的输入端连接。任意一个选择器的输出端与任意一个计数器的输入端相连，将从RO环组中取出来的变化值(0和1之间变化)送入计数器，使计数器进行计数。为了采样计数器的计数值，使用寄存器对计数器进行采样，将任意一个计数器的输出端分别与任意一个寄存器相连。任意一个寄存器的输出端输出真随机数TRN，两个寄存器的输出还需连接到比较器的输入端，进行比较，比较器的输出端输出物理不可克隆函数PUF。

[0039] 具体实施中，任意一组RO振荡环是由n个RO环组成，其中，任意第i个RO环是由一个双输入与非门使能信号单元与四个反向器构成，形成一个闭环结构。

[0040] 双输入与非门使能信号单元是由单输出双输入查找表LUT2配置，每个反相器由一个单输入查找表LUT1配置。

[0041] 依据真值表，设定单输出双输入查找表LUT2的初值为4’b0111，单输入查找表LUT1的初值为2’b01，查找表从左到右的顺序依次为：LUT2、LUT1-1、LUT1-2、LUT1-3和LUT1-4。

[0042] 单输出双输入查找表LUT2的输出端与第一单输入查找LUT1-1的输入端相连；

[0043] 第一单输入查找LUT1-1的输出端与第二单输入查找表LUT1-2的输入端相连；

[0044] 第二单输入查找表LUT1-2的输出端与第三单输入查找表LUT1-3的输入端相连；

[0045] 第三单输入查找表LUT1-3的输出端与第四单输入查找表LUT1-4的输入端相连；

[0046] 第四单输入查找表LUT1-4的输出端与单输出双输入查找表LUT2的低位输入端相连，单输出双输入查找表LUT2的高位输入端设置为EN端。以查找表LUT2的输出端作为第i个RO环的输出端，从而通过五个查找表实现一个双输入与非门使能信号单元与四个反向器之间的连接关系。

[0047] 为了对PUF输出的不稳定机理有更深入的理解，图2形象地描述了制造延时不匹配与噪声波动(包括电子热噪声与环境引起的延时偏移)对于PUF输出响应的影响。两大类路径延时影响因素分别对应于图中的灰色阴影区域和阴影区域中的垂直直线。制造延时不匹配是随机的，近似地符合高斯分布。如图2所示，当PUF单元映射到一个Slice中，如果工艺波动很小，受相对较大的噪声波动影响，PUF单元的输出响应将会在0和1之间波动，这就意味

着,当工作环境发生改变时,映射到该Slice的PUF单元不能够产生可靠的输出。换句话说,这个Slice不适合配置成PUF单元,因为对于0和1两个状态,相应的PUF单元没有表现出很强的偏移性。对于相反的情况,由于大的工艺波动,PUF的输出响应总是偏向于一个确定的状态(0或1),因此该Slice适合实现PUF单元。

[0048] 图3表示利用抖动产生TRNG的原理。由于环形振荡器由与非门和反相器组成,如果接出其输出我们可以观察到其理想的输出波形为规则的方波。然而,因为热噪声等环境因素的影响,其输出波形的上升沿和下降沿将会出现微小的偏置,这种现象我们称之为抖动。抖动的产生是无法预测的,输出的边沿位置可能提前可能延后,边沿位置的出现概率以理想边沿位置呈正态分布,如图3所示。抖动的范围很小,在SRAM型FPGA中仅为几个皮秒,如果在FPGA中直接实现环形振荡器并利用触发器对其采样将会使大量确定性的数值被提取,生成的序列的随机性比较差。为了提高随机性,通过组合多个环形振荡器作为熵源,通过将多个环形振荡器的输出进行异或来增加熵源的随机性,再将输出通过触发器进行采样生成随机序列。

[0049] 对于配置好的RO对,在RO环的输出端使用计数器统计各自的振荡频率;寄存器对计数器进行采样出来的多位数据,由于多位数据中的低三位数据变化很大且无规律可循,可将其作为TRN。再使用比较器比较两个计数器输出数据的高位,根据高位差的正负,得到1bit的PUF响应。流程图如图4所示,真随机数发生器的工作方法是按如下步骤进行:

[0050] 步骤1、定义变量i并初始化i=1,表明从每组n个RO振荡环中选择第i个RO振荡环;

[0051] 步骤2、定义当前计数周期数为t,并初始化t=1,表明计数器当前计数时钟周期数;

[0052] 定义计数周期的总数为N,表明当计数周期数超过N时,计数器清零;

[0053] 定义采集周期的总数为M,且M<N,表明每过M个周期采样一次;

[0054] 步骤3、任意一个多路选择器从相应组RO振荡环的第i个RO环的输出端所输出的熵源值作为相应多路选择器的第i次输出;

[0055] 步骤4、相应多路选择器将第i次输出的熵源值送到所连接的一个计数器C的输入端中;

[0056] 步骤5、计数器C清零并接收第i次输出的熵源值;

[0057] 步骤6、计数器C开始计数;

[0058] 步骤7、判定当前计数周期t是否等于kM,若等于,则执行步骤8-步骤9;否则,执行步骤10,其中,k为正整数;

[0059] 步骤8、相应的寄存器对所连接的计数器C的计数值进行采样,得到采样数据;并将采样数据的低三位作为真随机数输出;将采样数据的高位送入比较器中;

[0060] 步骤9、比较器将两个寄存器输入的高位进行比较,得到的比较结果作为物理不可克隆函数PUF;

[0061] 步骤10、判定当前计数周期t是否大于N,若大于N,则将i+1赋值给i后,执行步骤3,否则,则计数器C继续计数,并执行步骤7。

[0062] 在上述步骤之后还包括随机性测试步骤:

[0063] 采用NIST测试套件对结构产生的随机比特数据进行随机性测试,测试包含15个项目,NIST测试套件会对随机比特数据针对每个测试项目计算出相应的卡方分布的概率密度

曲线，通过先求出统计量计算其到无穷大的积分将积分结果P-value作为测试结果与显著水平α进行比较，若大于α则认为其具有随机性，典型的α取值区间在[0.001,0.01]内，本发明中所产生的TRN的所有结果均通过NIST测试具有真随机性。

[0064] 为了进一步说明本发明方案的积极效果，使用的Xilinx Sparten-6系列FPGA平台，对提出的硬件安全原语电路进行了设计与实现，得出所设计的PUF其误码率为5.2%，具有较好的唯一性和稳定性。

[0065] 综上所述，本发明从密钥生成的角度来看，成功在单个设备中同时实现了PUF和TRNG两种结构，能有效减小能源开销。

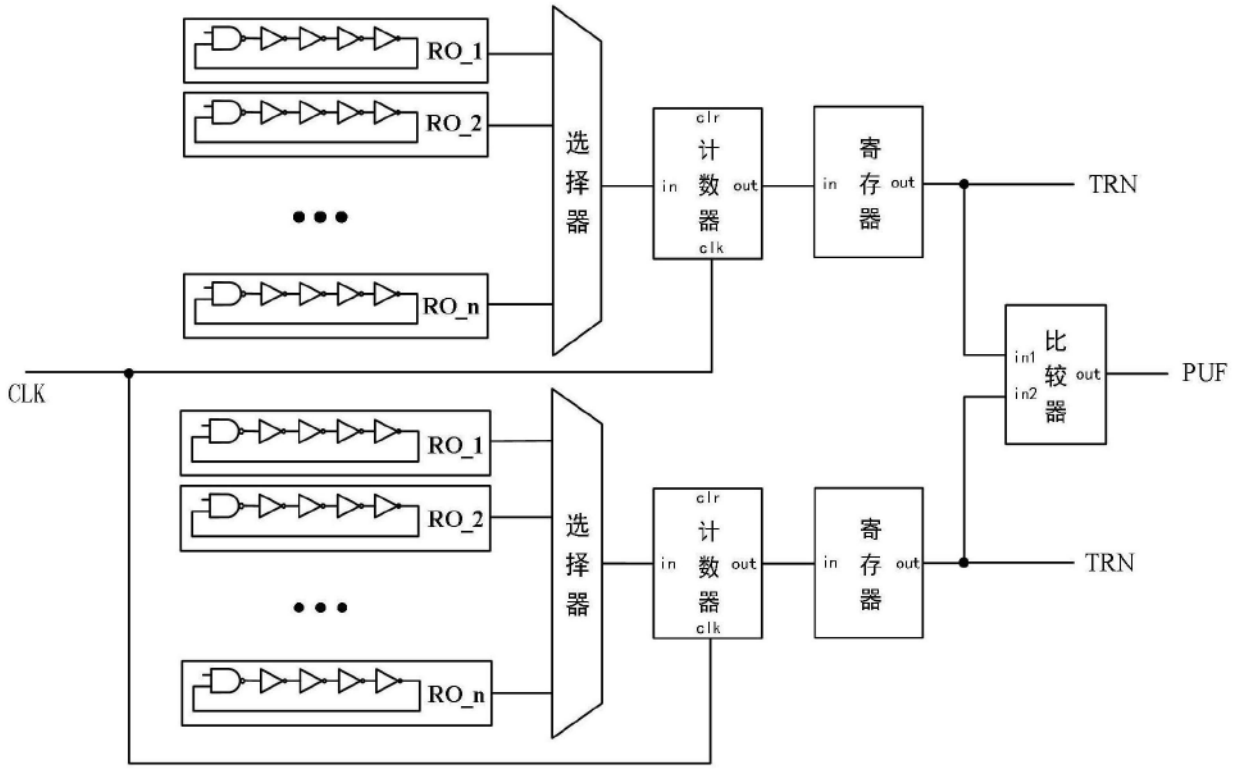

RO_1
RO_2
RO_n
选择器
clr
计数器
in
out
clk
寄存器
TRN
比较器
in1
in2
PUF
CLK

图1

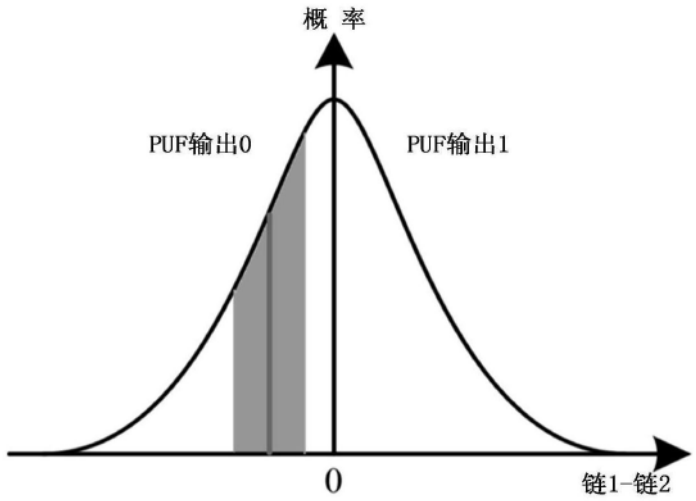

概率
PUF输出0
PUF输出1
0
链1-链2

图2

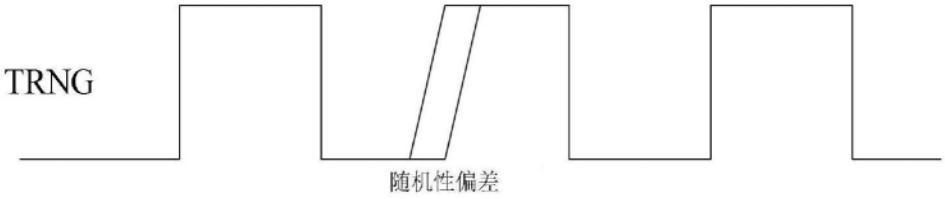

TRNG
随机性偏差

图3

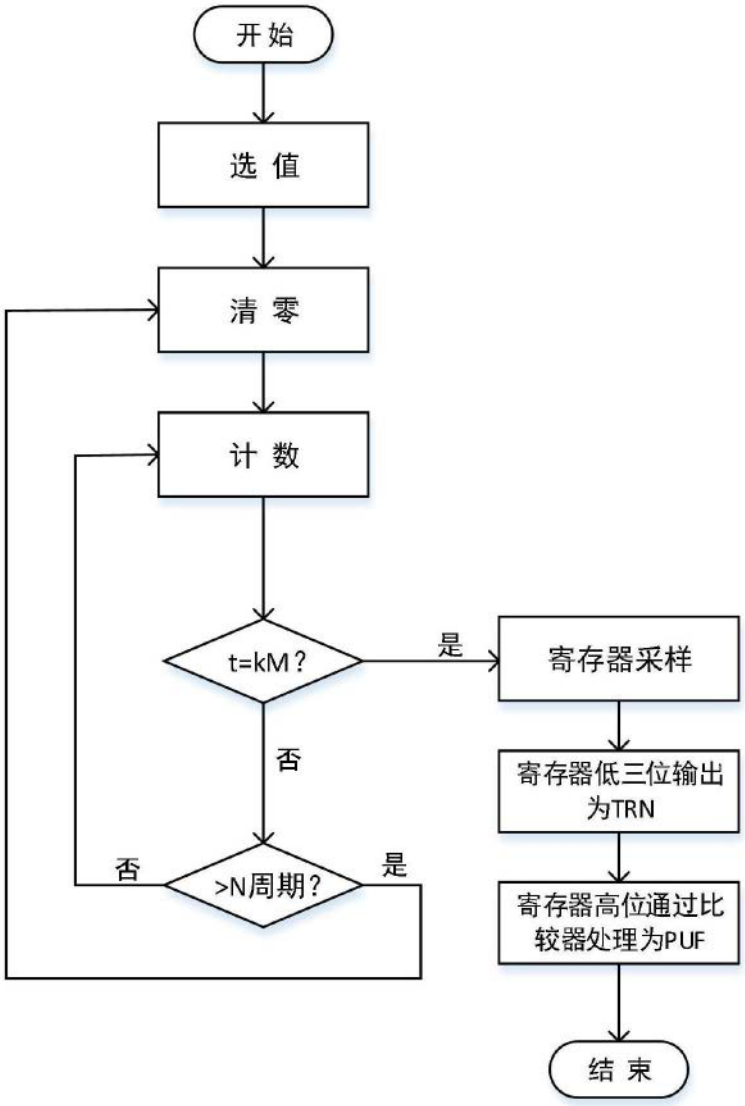

开始
选 值
清 零
计 数
t=kM?
是
寄存器采样
否
寄存器低三位输出为TRN
否
>N周期?
是
寄存器高位通过比较器处理为PUF
结 束

图4