(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115840887 A
(43)申请公布日 2023.03.24

(21)申请号 202211570155.X

(22)申请日 2022.12.08

(71)申请人 电子科技大学长三角研究院(湖州)
地址 313099 浙江省湖州市西塞山路819号南太湖科技创新综合体B2幢8层

(72)发明人 李磊 周婉婷

(74)专利代理机构 成都虹盛汇泉专利代理有限公司 51268
专利代理师 陈婷

(51)Int.Cl.
G06F 18/213(2023.01)

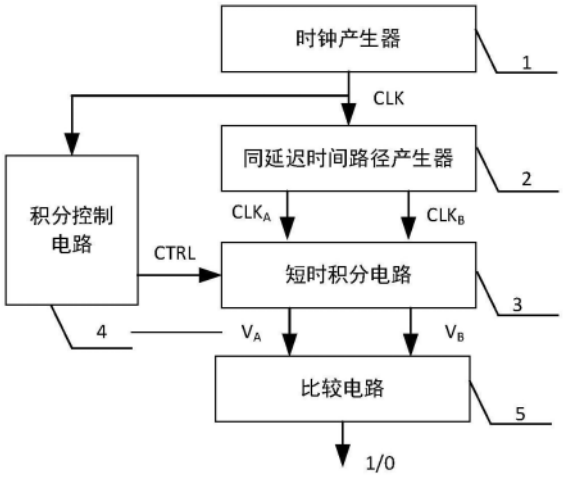
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种集成电路物理指纹的提取方法

(57)摘要

本发明公开一种集成电路物理指纹的提取方法,应用于信息安全和集成电路技术领域,针对现有的物理指纹提取电路存在结构复杂的问题;本发明基于时钟信号的处理,通过集成电路随机物理差异从而产生随机值,结合后端设计技术,通过采集时钟信号的差异提取集成电路随机物理差异,从而建立了一种新型的集成电路物理指纹的提取方法。该发明基于集成电路中的时钟信号进行处理,不需要额外增加太多电路。该专利处理简单,不需要后处理电路。



CN 115840887 A

1.一种集成电路物理指纹的提取方法,其特征在于,包括:时钟产生器、同延迟时间路径产生器、积分控制电路、短时积分电路和比较电路;时钟发生器用来提供时钟信号CLK,同延迟时间路径产生器通过所述时钟发生器提供的时钟CLK用来产生两个同延迟时间的时钟CLK_A和CLK_B,积分控制电路利用时钟信号CLK通过延迟链用于产生控制信号CTRL,短时积分电路在控制信号CTRL控制下通过内部的积分电路把CLK_A和CLK_B信号的短时时间转化为电平信号V_A和V_B,比较电路实现对电平信号V_A和V_B的对比,从而产生逻辑0或者逻辑1。

2.根据权利要求1所述的一种集成电路物理指纹的提取方法,其特征在于,时钟发生器采用锁相环或者延迟锁相环。

一种集成电路物理指纹的提取方法

技术领域

[0001] 本发明属于信息安全和集成电路技术领域,特别涉及一种实际硬件安全认证和硬件指纹提取技术。

背景技术

[0002] 在集成电路的身份认证中,使用者希望集成电路有唯一的标识。在现代的集成电路中,一般通过烧写设备给集成电路赋一个固定标识,例如序列号等信息等。这些标识作为集成电路的身份识别。但是这种方法很容易被仿制,已经无法满足安全需求。

[0003] 因此新型的技术被开发,例如物理不可克隆函数(Physical Unclonable Functions,PUF)是指在给定的输入下产生由电路物理特性决定的特定响应,也称“硬件指纹”。物理不可克隆函数来源于芯片制造过程中由于工艺偏差等因素引入的特定的物理信息,由于这些因素是无法预测且难以控制的,因此理论上响应输出是不可克隆的。

[0004] 现有的物理指纹的提取方法一般通过植入特定结构的方式来实现,常用的结构包括SRAM物理指纹提取、RO物理指纹提取和Anti-Fuse物理指纹提取等。

[0005] SRAM PUF是由两个完全相同的反相器耦合组成的。当对SRAM上电瞬间,SRAM会进入亚稳态,但是最终会进入某一个稳定的状态,理想情况下,SRAM进入两个稳定状态的概率应该是均等的。但是SRAM最终将偏向进入某个状态,这是由SRAM制造过程中工艺偏差决定的,并且是随机的,也是稳定的。Intrinsic ID的提出技术就是基于SRAM[www.intrinsic-id.com/zh-CN/sram-puf/]。基于SRAM的PUF的缺点是:(1)需要未初始化的SRAM,占用面积比较大;(2)后处理电路比较复杂,而且占用的集成电路面积也比较大。

[0006] RO PUF结构利用不同芯片间不同导线和晶体管固有延时特性。不同的RO具有不同的振荡频率,而真实的振荡频率是有物理信息决定。RO PUF的响应是通过比较被选中的两个RO的频率f_1和f_2得到的,例如,当$f_1 \geqslant f_2$时,响应输出0,反之响应输出1。也就是说RO PUF是通过RO与RO之间频率的随机变化来反应芯片工艺偏差的随机性的。基于RO的PUF的缺点是:(1)需要定制电路开发,开发周期长;(2)RO PUF稳定性不是很好,同样需要后处理电路,处理比较复杂,占用的集成电路电路面积比较大。

[0007] Anti-Fuse物理指纹提取技术通过Anti-Fuse制造过程形成的随机性提取物理指纹,可以实现高的稳定性。但是Anti-Fuse物理指纹提取技术缺点是:(1)需要特殊加工工艺的支持;(2)内部需要集成电路高压电路。

发明内容

[0008] 为解决上述技术问题,本发明从集成电路设计出发,基于时钟信号的处理,从而提出了一种物理指纹提取方法。

[0009] 本发明采用的技术方案为:一种集成电路物理指纹的提取方法,包括:时钟产生器、同延迟时间路径产生器、积分控制电路、短时积分电路和比较电路;时钟发生器用来提供时钟信号CLK,同延迟时间路径产生器通过所述时钟发生器提供的时钟CLK用来产生两个

同延迟时间的时钟CLK_A和CLK_B，积分控制电路利用时钟信号CLK通过延迟链用于产生控制信号CTRL，短时积分电路在控制信号CTRL控制下通过内部的积分电路把CLK_A和CLK_B信号的短时时间转化为电平信号V_A和V_B，比较电路实现对电平信号V_A和V_B的对比，从而产生逻辑0或者逻辑1。

[0010] 本发明的有益效果：本发明的一种集成电路物理指纹的提取方法基于对集成电路时钟信号的处理，结合后端设计技术，通过采集时钟信号的差异提取集成电路随机物理差异，从而建立了一种新型的集成电路物理指纹的提取方法。该发明基于集成电路中的时钟信号进行处理，不需要额外增加太多电路。该专利处理简单，不需要后处理电路。

附图说明

[0011] 图1为本发明的方法流程图。

具体实施方式

[0012] 为便于本领域技术人员理解本发明的技术内容，下面结合附图对本发明内容进一步阐释。

[0013] 以下为本发明的实施例过程：

[0014] 1、本发明中的时钟发生器用来提供时钟信号CLK，时钟发生器可以采用锁相环或者延迟锁相环等，该时钟发生器可以和集成电路用来产生时钟的时钟发生器采用一个。

[0015] 2、完成所述同延迟时间路径产生器设计

[0016] 通过所述时钟发生器提供的时钟CLK用来产生两个同延迟时间的时钟CLK_A和CLK_B。

[0017] 所述同延迟时间路径产生器的设计主要在后端工具(Cadence Innovus或者Snopsys ICC等)中实现。

[0018] 所述同延迟时间路径产生器设计步骤主要包括：设定相同的对称位置、设置相同的约束条件、生成相同延迟时钟路径。所述同延迟时间路径产生器产生的两个同延迟时间的时钟CLK_A和CLK_B，输入到短时积分电路中。

[0019] 3、完成所述积分控制电路设计

[0020] 所述积分控制电路利用时钟信号CLK通过延迟链用于产生控制信号CTRL。所产生的控制信号CTRL输出到所述短时积分电路。

[0021] 4、完成所述短时积分电路设计

[0022] 所述短时积分电路在控制信号CTRL控制下通过内部的积分电路把CLK_A和CLK_B信号的短时时间转化为电平信号V_A和V_B。所属电平信号V_A和V_B输出到比较电路中。

[0023] 5、完成所属比较电路设计

[0024] 所述比较电路实现对电平信号V_A和V_B的对比，从而产生逻辑0或者逻辑1。

[0025] 6、把本发明内容集成到原有集成电路设计中，用来产生物理指纹。物理指纹的长度根据需要进行定制开发。

[0026] 7、进行流片加工封装完成。一旦加工制造完成，相应的物理指纹也已经制造完成，并嵌入在所设计的集成电路中。

[0027] 8、在使用的时候，按照需要进行指纹提取，完成相应的安全功能即可。

[0028] 本领域的普通技术人员将会意识到，这里所述的实施例是为了帮助读者理解本发

明的原理，应被理解为本发明的保护范围并不局限于这样的特别陈述和实施例。对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的权利要求范围之内。

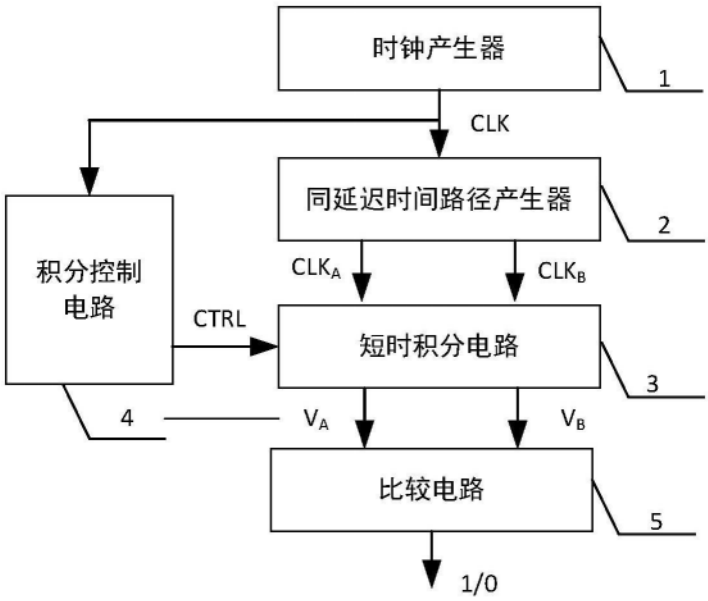

时钟产生器
1
CLK
同延迟时间路径产生器
2
积分控制
电路
CLK_A
CLK_B
CTRL
短时积分电路
3
4
V_A
V_B
比较电路
5
1/0

图1