(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 101943729 B
(45)授权公告日 2012.03.28

(21)申请号 200910088707.1

(22)申请日 2009.07.06

(73)专利权人 北京中电华大电子设计有限责任公司
地址 100015 北京市朝阳区高家园 1 号

(72)发明人 马哲 张建平

(51)Int.Cl.
G01R 31/00(2006.01)

(56)对比文件
US 2003/0226082 A1,2003.12.04, 全文.
CN 101141123 A,2008.03.12, 全文.
US 2008/0061843 A1,2008.03.13, 全文.
US 4857760 ,1989.08.15, 全文.
CN CN2922277 Y,2007.07.11, 全文.

审查员 汤莎亮

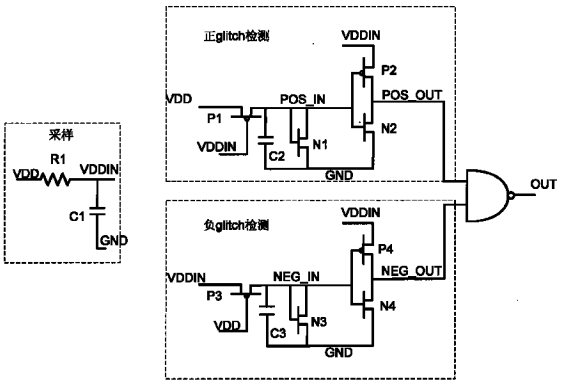
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

一种电源、地上毛刺的快速低功耗检测电路

(57)摘要

本发明提供一种对集成电路电源、地上出现的 glitch(毛刺)进行快速检测的电路,本发明的检测电路包括采样模块、正 glitch 检测模块、负 glitch 检测模块以及与非门;采样模块由电阻、电容构成,实现对电源、地上出现的 glitch 采样作用;正 glitch 检测模块由 MOS 开关管、下拉管、对地电容、反相器构成;负 glitch 检测模块由 MOS 开关管、下拉管、对地电容、反相器构成;与非门对正、负 glitch 的输出进行与非运算后作为本检测电路的输出。



CN 101943729 B

1. 一种电源、地上毛刺的快速低功耗检测电路，其特征在于：该检测电路包括采样模块、

正毛刺检测模块、负毛刺检测模块、与非门；其中：

所述采样模块由电阻 R1、电容 C1 串联构成，电阻 R1 一端为电源 VDD，电阻 R1 与电容 C1 的公共节点为 VDDIN、电容 C1 的另一节点接 GND；采样模块提供正、负毛刺检测模块的输入信号；

所述正毛刺检测模块由 PMOS 管 P1、P2，NMOS 管 N1、N2，电容 C2 构成；PMOS 管 P1 源端接 VDD、栅端接 VDDIN、漏端接 PMOS 管 P1 的漏端 POS_IN；电容 C2 一端接 PMOS 管 P1 的漏端 POS_IN、另一端接 GND；NMOS 管 N1 栅端、漏端接 PMOS 管 P1 的漏端 POS_IN，源端接 GND；PMOS 管 P2 栅端接 PMOS 管 P1 的漏端 POS_IN、漏端接 PMOS 管 P2 的漏端 POS_OUT、源端接 VDDIN；NMOS 管 N2，栅端接 PMOS 管 P1 的漏端 POS_IN、漏端接 PMOS 管 P2 的漏端 POS_OUT、源端接 GND；正毛刺检测模块实现对电源上出现的正毛刺进行实时检测，对地上出现的负毛刺进行实时检测；

所述负毛刺检测模块由 PMOS 管 P3、P4，NMOS 管 N3、N4，电容 C3 构成；PMOS 管 P3 源端接 VDDIN、栅端接 VDD、漏端接 PMOS 管 P3 的漏端 NEG_IN；电容 C3 一端接 PMOS 管 P3 的漏端 NEG_IN、另一端接 GND；NMOS 管 N3 栅端、漏端接 PMOS 管 P3 的漏端 NEG_IN，源端接 GND；PMOS 管 P4 栅端接 PMOS 管 P3 的漏端 NEG_IN、漏端接 PMOS 管 P4 的漏端 NEG_OUT、源端接 VDDIN；NMOS 管 N4，栅端接 PMOS 管 P3 的漏端 NEG_IN、漏端接 PMOS 管 P4 的漏端 NEG_OUT、源端接 GND；负毛刺检测模块实现对电源上出现的负毛刺进行实时检测，对地上出现的正毛刺进行实时检测；

所述与非门：由与非门构成，与非门输入接 PMOS 管 P4 的漏端 NEG_OUT、PMOS 管 P2 的漏端 POS_OUT，输出接 OUT，与非门对正、负毛刺检测模块的输出进行与非运算后输出标志信号 OUT。

2. 如权利要求 1 所述一种电源、地上毛刺的快速低功耗检测电路，其特征在于：所述正毛刺检测模块通过 PMOS 管 P1 作为开关管，由采样模块输出 VDDIN 作为所述 PMOS 管 P1 的开关控制端；所述 NMOS 管 N1 栅端、漏端短接于 PMOS 管 P1 的漏端 POS_IN，构成二极管接法，在电源、地上没有毛刺时，将 PMOS 管 P1 的漏端 POS_IN 拉至低电位，保证 PMOS 管 P2 的漏端 POS_OUT 输出为“高”。

3. 如权利要求 1 所述一种电源、地上毛刺的快速低功耗检测电路，其特征在于：所述负毛刺检测模块通过 PMOS 管 P3 作为开关管，由 VDD 作为所述 PMOS 管 P3 的开关控制端；所述 NMOS 管 N3 栅端、漏端短接于 PMOS 管 P3 的漏端 NEG_IN，构成二极管接法，在电源、地上没有毛刺时，将 PMOS 管 P3 的漏端 NEG_IN 拉至低电位，保证 PMOS 管 P4 的漏端 NEG_OUT 输出为“高”。

一种电源、地上毛刺的快速低功耗检测电路

技术领域：

[0001] 本发明涉及电源、地上毛刺的检测电路，尤其涉及在集成电路、智能卡集成电路中实现的一种电源、地上毛刺的快速低功耗检测电路。

背景技术：

[0002] 智能卡在各领域的广泛应用，尤其是身份认证、金融等高安全领域的智能卡对于防攻击能力提出了更高的要求，同样各方面的攻击者对该类智能卡攻击也日益严重；安全智能卡芯片通常包括 CPU、存储器（例如 EEPROM、FLASH）、以及嵌入式操作系统 (COS)。目前攻击者通过在智能卡芯片电源、地上施加一定条件的 glitch，然后利用 DFA 等分析技术就可以实现对密钥攻击、以及获取存储器内保密数据等。

发明内容：

[0003] 本发明的目的是针对在电源、地上出现的正、负 glitch 进行实时、快速检测，输出标志信号；并且本电路以超低功耗实现了快速检测目的。

[0004] 本发明公开了一种在集成电路中可以超低功耗、快速实时检测电源、地上 glitch 的电路，其特征在于：包括采样模块、正 glitch 检测模块、负 glitch 检测模块、与非门；其中采样电路提供正、负 glitch 检测模块的输入信号；正 glitch 检测模块实现对电源上出现的正 glitch 进行实时检测，对地上出现的负 glitch 进行实时检测；负 glitch 检测模块实现对电源上出现的负 glitch 进行实时检测，对地上出现的正 glitch 进行实时检测；与非门对正、负 glitch 检测模块的输出进行与非运算后输出标志信号 OUT。

[0005] 采用本发明公开的电路对电源进行实时检测，在电源、地上没有出现 glitch 时，本发明电路静态功耗仅为各个器件的漏电功耗，功耗极低；当电源、地上一旦出现 glitch 攻击信号，则本发明的电路就会实时检测并输出标志信号，系统据此可以对内部逻辑电路作实时的保护处理，防止被攻击；本电路具有功耗低、速度快，占用面积小、可移植性强、易于在标准 CMOS 工艺实现的特点。

[0006] 本发明的一种电源、地上毛刺的快速低功耗检测电路，其特征在于：包括采样模块、正 glitch 检测模块、负 glitch 检测模块、与非门；

[0007] 所述采样模块：由电阻 R1、电容 C1 串联构成，电阻 R1 一端为电源 VDD、电阻 R1 与电容 C1 的公共节点为 VDDIN、电容 C1 的另外节点接 GND；

[0008] 所述正 glitch 检测模块：由 PMOS 管 P1、P2，NMOS 管 N1、N2，电容 C2 构成；所述 PMOS 管 P1 源端接 VDD、栅端接 VDDIN、漏端接 POS_IN；所述电容 C2 一端接 POS_IN、另一端接 GND；所述 NMOS 管 N1 栅端、漏端接 POS_IN，源端接 GND；所述 PMOS 管 P2 栅端接 POS_IN、漏端接 POS_OUT、源端接 VDDIN；所述 NMOS 管 N2，栅端接 POS_IN、漏端接 POS_OUT、源端接 GND；

[0009] 所述负 gltich 检测模块：由 PMOS 管 P3、P4，NMOS 管 N3、N4，电容 C3 构成；所述 PMOS 管 P3 源端接 VDDIN、栅端接 VDD、漏端接 NEG_IN；所述电容 C3 一端接 NEG_IN、另一端接 GND；所述 NMOS 管 N3 栅端、漏端接 NEG_IN，源端接 GND；所述 PMOS 管 P4 栅端接 NEG_IN、漏

端接 NEG_OUT、源端接 VDDIN ;所述 NMOS 管 N4,栅端接 NEG_IN、漏端接 NEG_OUT、源端接 GND ;

[0010] 所述与非门 :由与非门构成,与非门输入接 NEG_OUT、POS_OUT,输出接 OUT。

[0011] 如图 1 电路所示,当电源 VDD、地 GND 上没有 glitch 出现时,二极管接法的 NMOS 管 N1、N3 分别将 POS_IN、NEG_IN 拉至低电位,保证 POS_OUT、NEG_OUT 输出为“高”,OUT 输出为“低”;此种状态下整体电路的静态功耗极低,仅为各器件的漏电功耗 ;

[0012] 如图 1 电路所示,当电源 VDD 上出现正 glitch 时,VDDIN 是经过采样模块的输出,不能实时跟随 VDD 变化,此时 PMOS 开关管 P1 打开,对电容 C2 充电、使得 POS_IN 至“高”电位,POS_OUT 输出为“低”,经与非门后 OUT 输出由“低”转变为“高”,标志有 glitch 出现 ;当电源 VDD 上出现负 glitch 时,VDDIN 是经过采样模块的输出,不能实时跟随 VDD 变化,此时 PMOS 开关管 P3 打开,对电容 C3 充电、使得 NEG_IN 至“高”电位,NEG_OUT 输出为“低”,经与非门后 OUT 输出由“低”转变为“高”,标志有 glitch 出现 ;

[0013] 如图 1 电路所示,当地 GND 上出现正 glitch 时,VDDIN 是经过采样模块的输出,能够采样到 GND 上的变化,此时 PMOS 开关管 P3 打开,对电容 C3 充电、使得 NEG_IN 至“高”电位,NEG_OUT 输出为“低”,经与非门后 OUT 输出由“低”转变为“高”,标志有 glitch 出现 ;当地 GND 上出现负 glitch 时,VDDIN 是经过采样模块的输出,能够采样到 GND 上的变化,此时 PMOS 开关管 P1 打开,对电容 C2 充电、使得 POS_IN 至“高”电位,POS_OUT 输出为“低”,经与非门后 OUT 输出由“低”转变为“高”,标志有 glitch 出现 ;

附图说明 :

[0014] 图 1 是在集成电路中实现电源、地毛刺快速低功耗检测电路的原理图 ;

[0015] 其中 VDD 是电源输入端,GND 是地输入端,OUT 是检测电路输出端。

[0016] 图 2 是电源、地毛刺快速低功耗检测电路的信号波形。

[0017] 其中 VDD 上出现正 glitch 时,正 glitch 检测模块输出端 POS_OUT 由“高”转变为“低”,电源毛刺快速检测电路输出 OUT 由“低”转变为“高”;

[0018] VDD 上出现负 glitch 时,负 glitch 检测模块输出端 NEG_OUT 由“高”转变为“低”,电源毛刺快速检测电路输出端 OUT 由“低”转变为“高”;

[0019] GND 上出现负 glitch 时,正 glitch 检测模块输出端 POS_OUT 由“高”转变为“低”,电源毛刺快速检测电路输出端 OUT 由“低”转变为“高”;

[0020] GND 上出现正 glitch 时,负 glitch 检测模块输出端 NEG_OUT 由“高”转变为“低”,电源毛刺快速检测电路输出端 OUT 由“低”转变为“高”;

[0021] 电源 VDD、GND 上没有 glitch 出现时,正、负 glitch 检测输出端 POS_OUT、NEG_OUT 输出均为“高”,电源毛刺快速检测电路输出端 OUT 为“低”。

具体实施方式 :

[0022] 下面结合附图和实例对本发明作进一步描述。

[0023] 本发明在集成电路中实现的电源、地毛刺快速低功耗检测电路工作情况如下 :

[0024] 包括采样模块、正 glitch 检测模块、负 glitch 检测模块、与非门 ;

[0025] 所述采样模块 :由电阻 R1、电容 C1 串联构成,电阻 R1 一端为电源 VDD、电阻 R1 与电容 C1 的公共节点为 VDDIN、电容 C1 的另外节点接 GND ;

[0026] 所述正 glitch 检测模块：由 PMOS 管 P1、P2，NMOS 管 N1、N2，电容 C2 构成；所述 PMOS 管 P1 源端接 VDD、栅端接 VDDIN、漏端接 POS_IN；所述电容 C2 一端接 POS_IN、另一端接 GND；所述 NMOS 管 N1 栅端、漏端接 POS_IN，源端接 GND；所述 PMOS 管 P2 栅端接 POS_IN、漏端接 POS_OUT、源端接 VDDIN；所述 NMOS 管 N2，栅端接 POS_IN、漏端接 POS_OUT、源端接 GND；

[0027] 所述负 gltich 检测模块：由 PMOS 管 P3、P4，NMOS 管 N3、N4，电容 C3 构成；所述 PMOS 管 P3 源端接 VDDIN、栅端接 VDD、漏端接 NEG_IN；所述电容 C3 一端接 NEG_IN、另一端接 GND；所述 NMOS 管 N3 栅端、漏端接 NEG_IN，源端接 GND；所述 PMOS 管 P4 栅端接 NEG_IN、漏端接 NEG_OUT、源端接 VDDIN；所述 NMOS 管 N4，栅端接 NEG_IN、漏端接 NEG_OUT、源端接 GND；

[0028] 所述与非门：由与非门构成，与非门输入接 NEG_OUT、POS_OUT，输出接 OUT。

[0029] 如图 2 所示，当电源 VDD、地 GND 上没有 glitch 出现时，二极管接法的 NMOS 管 N1、N3 分别将 POS_IN、NEG_IN 拉至低电位，保证 POS_OUT、NEG_OUT 输出为“高”，OUT 输出为“低”；此种状态下整体电路的静态功耗极低，仅为各器件的漏电功耗；

[0030] 如图 2 所示，当电源 VDD 上出现正 glitch 时，VDDIN 是经过采样模块的输出，不能实时跟随 VDD 变化，此时 PMOS 开关管 P1 打开，对电容 C2 充电、使得 POS_IN 至“高”电位，POS_OUT 输出为“低”，经与非门后 OUT 输出由“低”转变为“高”，标志有 glitch 出现；

[0031] 如图 2 所示，当电源 VDD 上出现负 glitch 时，VDDIN 是经过采样模块的输出，不能实时跟随 VDD 变化，此时 PMOS 开关管 P3 打开，对电容 C3 充电、使得 NEG_IN 至“高”电位，NEG_OUT 输出为“低”，经与非门后 OUT 输出由“低”转变为“高”，标志有 glitch 出现；

[0032] 如图 2 所示，当地 GND 上出现正 glitch 时，VDDIN 是经过采样模块的输出，能够采样到 GND 上的变化，此时 PMOS 开关管 P3 打开，对电容 C3 充电、使得 NEG_IN 至“高”电位，NEG_OUT 输出为“低”，经与非门后 OUT 输出由“低”转变为“高”，标志有 glitch 出现；

[0033] 如图 2 所示，当地 GND 上出现负 glitch 时，VDDIN 是经过采样模块的输出，能够采样到 GND 上的变化，此时 PMOS 开关管 P1 打开，对电容 C2 充电、使得 POS_IN 至“高”电位，POS_OUT 输出为“低”，经与非门后 OUT 输出由“低”转变为“高”，标志有 glitch 出现；

[0034] 综上，本发明通过以上技术方案，可以对于电源、地上出现的 glitch 攻击信号进行实时检测，并且电路具有功耗低、面积小、速度快、可移植性强的特点。

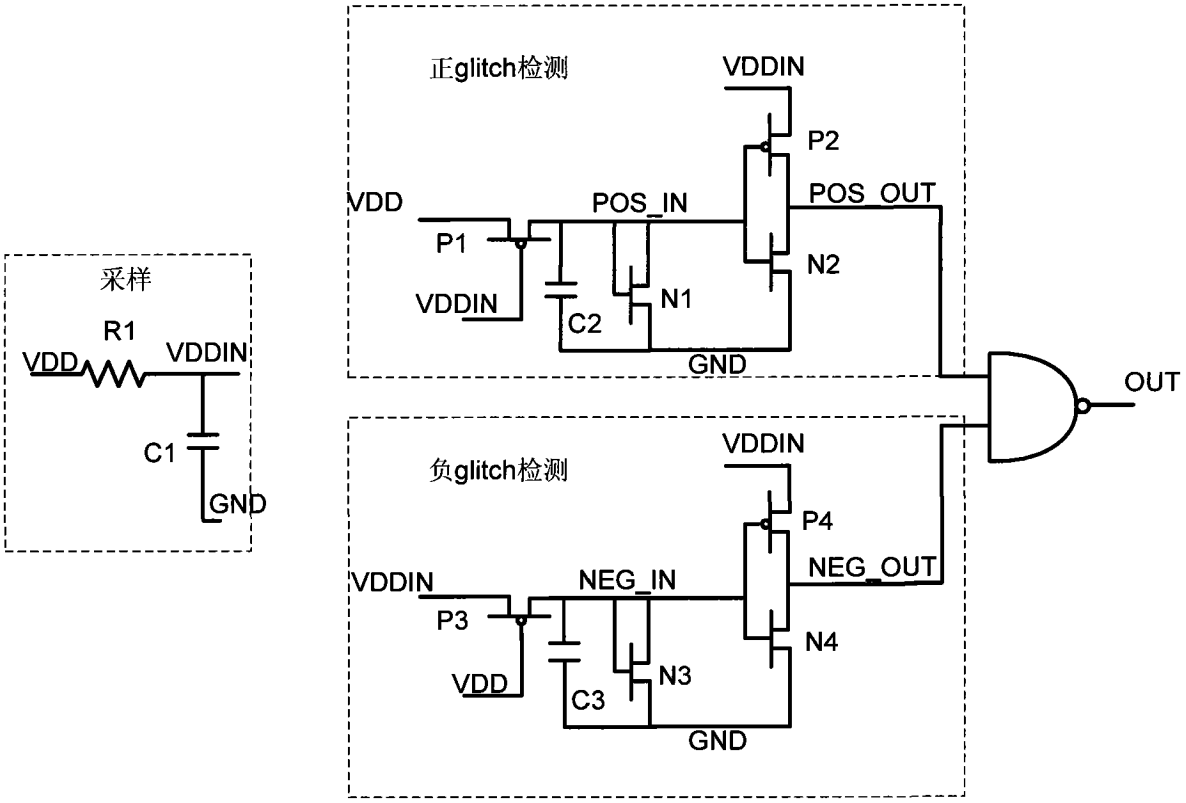

采样
R1
VDD
VDDIN
C1
GND
正glitch检测
VDDIN
P2
VDD
POS_IN
POS_OUT
P1
N2
VDDIN
C2
N1
GND
OUT
负glitch检测
VDDIN
P4
NEG_OUT
VDDIN
NEG_IN
P3
N4
VDD
C3
N3
GND

图 1

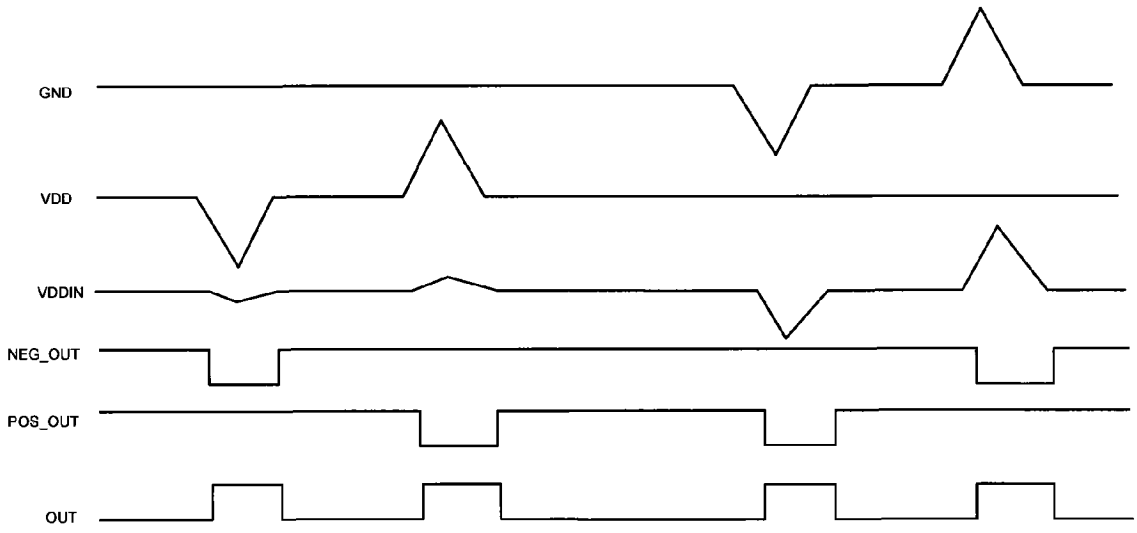

GND
VDD
VDDIN
NEG_OUT
POS_OUT
OUT

图 2