



(12) 发明专利

(10) 授权公告号 CN 101943728 B

(45) 授权公告日 2012.03.28

(21) 申请号 200910088706.7

(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

(51) Int. Cl.

G01R 31/00 (2006.01)

(56) 对比文件

CN 2922277 Y, 2007.07.11, 全文 .

US 2008/0061843 A1, 2008.03.13, 全文 .

US 4857760, 1989.08.15, 全文 .

US 2003/0226082 A1, 2003.12.04, 全文 .

CN 101141123 A, 2008.03.12, 全文 .

审查员 汤莎亮

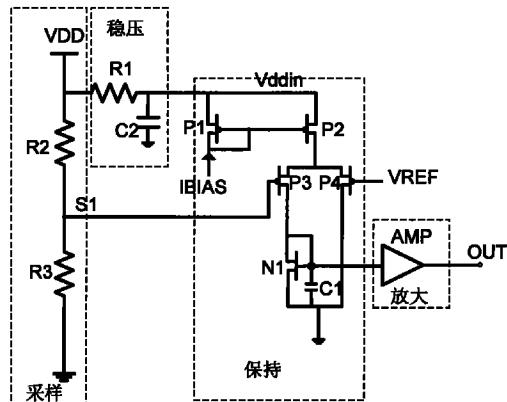
权利要求书 1 页 说明书 2 页 附图 1 页

(54) 发明名称

一种防电源毛刺攻击的检测电路

(57) 摘要

本发明提供一种易于在 CMOS 工艺集成的高速的负电源 Glitch 检测电路。传统电路如果检测集成电路电源上出现的高频毛刺，则需要较大的功耗才能对较高频率的电源毛刺响应，本发明的目的在于以较低的功耗代价来实现高频电源 Glitch 的检测。本发明的电源 Glitch 检测电路包括采样模块、稳压模块、保持模块、以及放大电路模块；采样模块由串联电阻连接电源、地实现对电源上毛刺的采样；稳压模块由 R、C 构成；保持模块通过输入对管、NMOS 管与电容参数的合理匹配实现；放大模块对于保持模块的输出信号放大输出检测标志位。



1. 一种防电源毛刺攻击的检测电路，其特征在于：包括有稳压模块、采样模块、保持模块、放大模块，采样模块由串联电阻 R2、R3 连接电源、地，串联电阻 R2、R3 的公共节点 S1 为采样输出节点；所述稳压模块由电阻 R1、电容 C2 串联在电源、地之间，其公共节点 Vddin 作为输出节点；所述保持模块中 PMOS 管 P1、P2 的源端连接节点 Vddin，PMOS 管 P1、P2 棚端连接 PMOS 管 P1 漏端，并由 PMOS 管 P1 漏端输入外界偏置电流；所述保持模块输入对管为 PMOS 管 P3、P4，PMOS 管 P3、P4 源端均连接 PMOS 管 P2 管漏端，PMOS 管 P3 的栅端连接所述采样模块的输出节点 S1，PMOS 管 P4 的栅端连接参考电压 VREF，PMOS 管 P4 漏端连接地，PMOS 管 P3 漏端连接 NMOS 管 N1 漏端，NMOS 管 N1 漏端与 NMOS 管 N1 棚端连接，NMOS 管 N1 源端接地，NMOS 管 N1 棚端连接电容 C1 一端，电容 C1 另一端与地相连；所述放大模块输入端与所述保持模块中 NMOS 管 N1 棚端相连，放大模块输出端为检测电路输出端。

2. 如权利要求 1 所述一种防电源毛刺攻击的检测电路，其特征在于，所述保持模块中与 NMOS 管 N1 棚端连接的对地连接电容 C1 为 POLY-POLY 电容或 Metal-Metal 电容或 MOS 电容。

3. 如权利要求 1 所述一种防电源毛刺攻击的检测电路，其特征在于，所述保持模块中与 NMOS 管 N1 棚端连接的对地连接的电容 C1 为 NMOS 管 N1 棚端对地的寄生电容。

4. 如权利要求 1 所述一种防电源毛刺攻击的检测电路，其特征在于，所述稳压模块由电阻 R1、电容 C2 串联于电源、地之间，其公共节点 Vddin 作为所述保持模块的电源输入。

5. 如权利要求 1 所述一种防电源毛刺攻击的检测电路，其特征在于，所述放大模块电路为反相器放大电路。

6. 如权利要求 1 所述一种防电源毛刺攻击的检测电路，其特征在于，所述放大模块电路为单端输入放大电路。

一种防电源毛刺攻击的检测电路

技术领域：

[0001] 本发明涉及电源 Glitch 攻击的检测电路,尤其涉及在集成电路、智能卡集成电路中实现的一种防电源 Glitch 攻击的检测电路。

背景技术：

[0002] 随着智能卡的广泛应用,在安全领域的智能卡成为了黑客等攻击者的重点攻击对象;安全智能卡芯片通常包括 CPU、存储器(例如 EEPROM)、以及操作系统(COS)。攻击者通过在智能卡芯片电源上施加适当的 Glitch 信号,可以利用 DFA 技术对密钥攻击、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上出现的 Glitch 信号进行实时检测,提供一种实时检测的电路。

[0004] 本发明公开了一种在集成电路中可实时检测电源 Glitch 的电路,其特征在于:包括有稳压模块、采样模块、保持模块、放大模块。其中稳压电路为检测单元提供稳定的电源,采样模块对电源上出现的 Glitch 信号进行采样,保持模块对采样得到的 Glitch 信号起到保持作用,放大模块对于保持模块保持的信号进行放大,电源上出现符合检测条件的 Glitch 信号,经过如上处理就能够被检测出来。

[0005] 采用以上电路对电源进行实时检测,则一旦检测出电源上出现了 Glitch 攻击信号,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、可移植性强等特点。

[0006] 所述检测电路包括有稳压模块、采样模块、保持模块、放大模块,采样模块由串联电阻 R2、R3 连接电源、地,串联电阻 R2、R3 的公共节点 S1 为采样输出节点;所述稳压模块由电阻 R1、电容 C2 串联在电源、地之间,其输出节点为 Vddin;所述保持模块中 PMOS 管 P1、P2 的源端连接节点 Vddin,P1、P2 栅端连接 P1 漏端,并由此端输入外界偏置电流;所述保持模块输入对管为 PMOS 管 P3、P4,P3、P4 源端均连接 P2 管漏端,P3 的栅端连接所述采样模块的输出节点 S1,P4 的栅端连接参考电压 VREF,P4 漏端连接地,P3 漏端连接 NMOS 管 N1 漏端,N1 漏端与 N1 栅端连接,N1 源端接地,N1 栅端连接电容 C1 一端,C1 另一端与地相连;所述放大模块输入端与所述保持模块中 N1 栅端相连,放大模块输出端为检测电路输出端。

附图说明：

[0007] 图 1 是在集成电路中防电源 Glitch 攻击的检测电路的原理图。

[0008] 其中 VDD 是电源输入端,IBIAS 是偏置电流输入端,VREF 是偏置电压输入端,OUT 是检测输出端。

[0009] 图 2 是防电源 Glitch 攻击检测电路的信号波形。

[0010] 其中 VDD 上出现负 Glitch 时,采样模块采样得到 VS1,如图中所示,VS1 幅度低于

VREF，则被检测到并输出低电平，如 OUT 信号波形。

具体实施方式：

- [0011] 下面结合附图和实例对本发明作进一步描述。
- [0012] 本发明在集成电路中防电源 Glitch 攻击的检测电路工作原理如下：
- [0013] 包括有稳压模块、采样模块、保持模块、放大模块，采样模块由串联电阻 R2、R3 连接电源、地，串联电阻 R2、R3 的公共节点 S1 为采样输出节点；所述稳压模块由电阻 R1、电容 C2 串联在电源、地之间，其输出节点为 Vddin；所述保持模块中 PMOS 管 P1、P2 的源端连接节点 Vddin，P1、P2 棚端连接 P1 漏端，并由此端输入外界偏置电流；所述保持模块输入对管为 PMOS 管 P3、P4，P3、P4 源端均连接 P2 管漏端，P3 的棚端连接所述采样模块的输出节点 S1，P4 的棚端连接参考电压 VREF，P4 漏端连接地，P3 漏端连接 NMOS 管 N1 漏端，N1 漏端与 N1 棚端连接，N1 源端接地，N1 棚端连接电容 C1 一端，C1 另一端与地相连；所述放大模块输入端与所述保持模块中 N1 棚端相连，放大模块输出端为检测电路输出端。
- [0014] 如图 1 所示，当电源 VDD 上出现了负 Glitch 时，采样电阻 R3、R2 就会获得一定比例的 Glitch 信号输入给后面的保持模块，而稳压模块 R1、C2 起到了滤除电源 VDD 上 Glitch 的作用，其能够提供给保持模块稳定的电源，以保证保持模块稳定的工作；如果 VDD 上出现了幅度足够大的 Glitch 的信号，使得电路中 S1 节点的电压低于输入的参考电压 VREF 后，保持模块中的 P3 管将打开，对 NMOS 管 N1 的栅节点电容进行充电，当 Glitch 消失后，电路中 S1 点电位恢复正常，P3 管关闭，此时 NMOS 栅节点的电容将通过 N1 管对地放电，调节 N1 管可以调节此处放电的时间常数，从而可将 Glitch 信号在此处保持设定的时间，后面的放大电路可以对此信号进行放大，从而可以将 VDD 上出现的 Glitch 信号检测输出。
- [0015] 本电路中用 NMOS 管 N1 代替了电阻，可以节省面积，也能够实现较大的阻值，提供较大的时间常数，同时放大模块则可以较小的功耗代价对高频的 Glitch 信号进行响应。
- [0016] 综上，本发明通过以上技术方案，可以对于电源上出现的 Glitch 攻击信号进行实时检测，而且电路不仅功耗低、面积小，而且速度快、可移植性强。

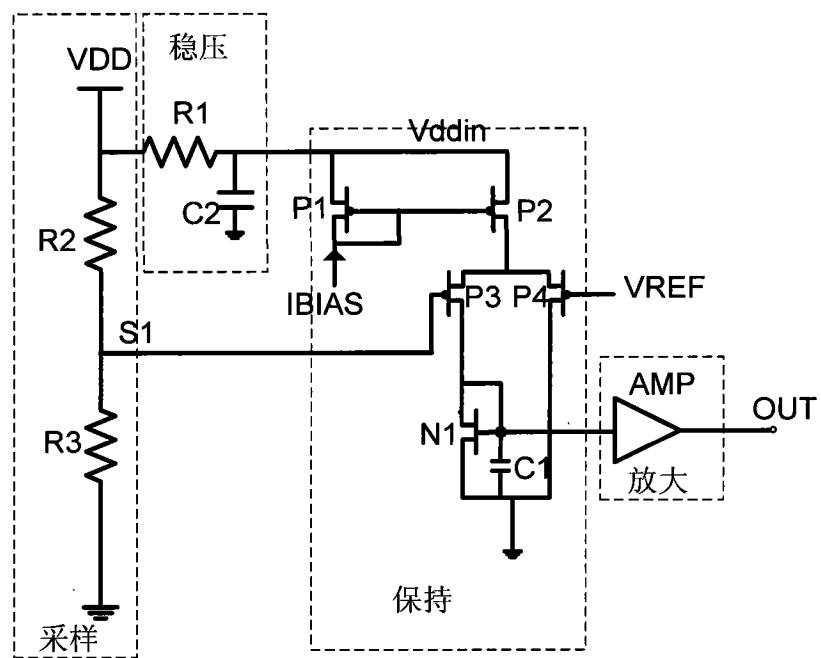


图 1

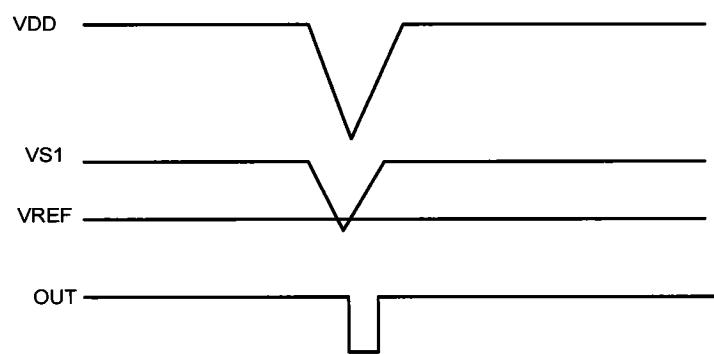


图 2