(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107483172 A
(43)申请公布日 2017.12.15

(21)申请号 201710765535.1

(22)申请日 2017.08.30

(71)申请人 哈尔滨工业大学(威海)
地址 264209 山东省威海市文化西路2号

(72)发明人 王晨旭 罗敏 韩良 王安
王新胜 刘晓宁

(74)专利代理机构 哈尔滨市松花江专利商标事务所 23109
代理人 岳泉清

(51)Int.Cl.
H04L 9/00(2006.01)

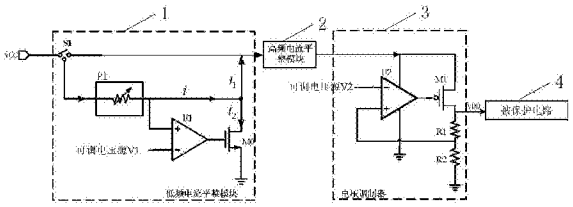
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种用于防御能耗攻击的密码防护电路

(57)摘要

一种用于防御能耗攻击的密码防护电路，涉及电子电路领域。解决了现有加密电路易受到功耗攻击，导致泄露密钥的问题。它包括低频电流平整模块、高频电流平整模块和电压调制器；低频电流平整模块，用于产生恒定的目标平整电流i，并利用该恒定的目标平整电流i对负载电流i_1进行补偿，负载电流i_1用于给被保护电路提供电能；其中，$i=i_1+i_2$，i_2为补偿电流；低频电流平整模块，还用于对电源VCC输出的电压进行高频滤波；高频电流平整模块，用于对低频电流平整模块输出的负载电流i_1进行低频滤波，并将滤波后的电流信号通过电压调制器进行电压转换，电压调制器输出的电压用于给被保护电路进行供电。本发明主要用于对加密电路进行防护。



CN 107483172 A

1.一种用于防御能耗攻击的密码防护电路，其特征在于，它包括低频电流平整模块(1)、高频电流平整模块(2)和电压调制器(3)；

低频电流平整模块(1)，用于产生恒定的目标平整电流i，并利用该恒定的目标平整电流i对负载电流i_1进行补偿，负载电流i_1用于给被保护电路(4)提供电能；其中，$i=i_1+i_2$，i_2为补偿电流；

低频电流平整模块(1)，还用于对电源VCC输出的电压进行高频滤波；

高频电流平整模块(2)，用于对低频电流平整模块(1)输出的负载电流i_1进行低频滤波，并将滤波后的电流信号通过电压调制器(3)进行电压转换，电压调制器(3)输出的电压用于给被保护电路(4)进行供电，

所述被保护电路(4)为加密电路。

2.根据权利要求1所述的一种用于防御能耗攻击的密码防护电路，其特征在于，所述的低频电流平整模块(1)包括单刀双掷开关S1、目标电流档位设定电路P1、放大器U1和N型MOS晶体管；

所述单刀双掷开关S1的控制端与电源VCC的电压输出端连接，单刀双掷开关S1的1号输出端与高频电流平整模块(2)的电流输入端连接，单刀双掷开关S1的2号输出端与目标电流档位设定电路P1的电信号输入端连接，目标电流档位设定电路P1的目标电流输出端与放大器U1的同相输入端、高频电流平整模块(2)的电流输入端和N型MOS晶体管M0的漏极同时连接，

放大器U1的反相输入端与可调电压源V1连接；

放大器U1的输出端与N型MOS晶体管M0的栅极连接，N型MOS晶体管M0的源极接电源地。

3.根据权利要求1或2所述的一种用于防御能耗攻击的密码防护电路，其特征在于，所述的电压调制器(3)包括放大器U2、电阻R1、电阻R2和P型MOS晶体管M1；

所述放大器U2的反向输入端用于接入可调电压源V2，放大器U2的同向输入与电阻R1的一端和电阻R2的一端同时连接，电阻R2的另一端接电源地，电阻R1的另一端与P型MOS晶体管M1的漏极连接，电阻R1的另一端作为电压调制器(3)的电压输出端；

放大器U2的电源输入端与高频电流平整模块(2)电压输出端、P型MOS晶体管M1的源极同时连接，放大器U2的接地端接电源地，

放大器U2的输出端与P型MOS晶体管M1的栅极连接。

4.根据权利要求1所述的一种用于防御能耗攻击的密码防护电路，其特征在于，所述的高频电流平整模块(2)为低通滤波器。

一种用于防御能耗攻击的密码防护电路

技术领域

[0001] 本发明涉及电子电路领域。

背景技术

[0002] 智能卡等密码设备在电信、金融、企业安全和政府等各种行业部门中得以广泛应用，其安全的重要性不言而喻。尽管密码设备的嵌入式特性使攻击者无法直接接触密码芯片中的密钥信息，但密码芯片工作时会泄漏一定的功耗、电磁辐射等侧信道信息，差分功耗分析(Differential Power Analysis,DPA)攻击技术利用密钥数据与这些信息之间的相关性，通过数理统计等方式可分析得出密钥的值。由于DPA攻击的非入侵性，普适性且简单易行等特点，其对智能卡等密码芯片的安全性造成了严重威胁。抵抗DPA攻击最基本的思想是消除密码芯片的工作电流与其执行算法时使用的数据的相关性。

[0003] 电路级防护独立于具体密码算法，是抗功耗攻击的一个重要研究方向。

发明内容

[0004] 本发明是为了现有加密电路易受到功耗攻击，导致泄露密钥的问题。本发明提供了一种可用于防御能耗攻击的密码防护电路。

[0005] 一种用于防御能耗攻击的密码防护电路，它包括低频电流平整模块、高频电流平整模块和电压调制器；

[0006] 低频电流平整模块，用于产生恒定的目标平整电流i，并利用该恒定的目标平整电流i对负载电流i_1进行补偿，负载电流i_1用于给被保护电路提供电能；其中，$i=i_1+i_2$，i_2为补偿电流；

[0007] 低频电流平整模块，还用于对电源VCC输出的电压进行高频滤波；

[0008] 高频电流平整模块，用于对低频电流平整模块输出的负载电流i_1进行低频滤波，并将滤波后的电流信号通过电压调制器进行电压转换，电压调制器输出的电压用于给被保护电路进行供电；

[0009] 所述被保护电路为加密电路。

[0010] 优选的是，所述的低频电流平整模块包括单刀双掷开关S1、目标电流档位设定电路P1、放大器U1和N型MOS晶体管；

[0011] 所述单刀双掷开关S1的控制端与电源VCC的电压输出端连接，单刀双掷开关S1的1号输出端与高频电流平整模块的电流输入端连接，单刀双掷开关S1的2号输出端与目标电流档位设定电路P1的电信号输入端连接，目标电流档位设定电路P1的目标电流输出端与放大器U1的同相输入端、高频电流平整模块的电流输入端和N型MOS晶体管M0的漏极同时连接，

[0012] 放大器U1的反相输入端与可调电压源V1连接；

[0013] 放大器U1的输出端与N型MOS晶体管M0的栅极连接，N型MOS晶体管M0的源极接电源地。

[0014] 优选的是，所述的电压调制器包括放大器U2、电阻R1、电阻R2和P型MOS晶体管M1；

[0015] 所述放大器U2的反向输入端用于接入可调电压源V2，放大器U2的同向输入与电阻R1的一端和电阻R2的一端同时连接，电阻R2的另一端接电源地，电阻R1的另一端与P型MOS晶体管M1的漏极连接，电阻R1的另一端作为电压调制器的电压输出端；

[0016] 放大器U2的电源输入端与高频电流平整模块电压输出端、P型MOS晶体管M1的源极同时连接，放大器U2的接地端接电源地，

[0017] 放大器U2的输出端与P型MOS晶体管M1的栅极连接。

[0018] 优选的是，所述的高频电流平整模块为低通滤波器。

[0019] 本发明具有高效易实施性以及可兼容性，适用于各种加密算法芯片的防护。本发明可以根据实际应用场景中的负载电压需求与负载电流变化范围来调节输出电压与平整电流档位。

[0020] 本发明所述的一种可用于防御能耗攻击的密码防护电路是一种基于电流平坦化的防御DPA攻击的方案。因为加密电路中的密码芯片能耗变化同密码具有强相关性，攻击者可以通过采集密码芯片的功耗曲线，破解出密钥。因此本发明将加密芯片电流平坦化，即可消除芯片功耗与密码的相关性，降低有效电流信息和噪声的信噪比，使得电流信息隐藏在噪声中，就可提升功耗攻击的难度。

[0021] 本发明带来的有益效果是，本发明将加密芯片电流平坦化，即可消除芯片功耗与密码的相关性，降低有效电流信息和噪声的信噪比，使得电流信息隐藏在噪声中，就可提升功耗攻击的难度，使得抵抗密码芯片的差分功耗分析攻击的强度提高了10％以上。本发明可以实现全频带电流信号的平整。对于低频段的信号，采用低频电流平整模块抑制，对于高频段电流信号滤除，可采用低通滤波器。

附图说明

[0022] 图1为本发明所述的一种可用于防御能耗攻击的密码防护电路的原理示意图；

[0023] 图2为低频电流平整模块与高频电流平整模块集成的抑制效果图，其中，K为f_T处的电源电流信号和加密电路的电流比值。

具体实施方式

[0024] 具体实施方式一：参见图1说明本实施方式，本实施方式所述的一种用于防御能耗攻击的密码防护电路，它包括低频电流平整模块1、高频电流平整模块2和电压调制器3；

[0025] 低频电流平整模块1，用于产生恒定的目标平整电流i，并利用该恒定的目标平整电流i对负载电流i_1进行补偿，负载电流i_1用于给被保护电路4提供电能；其中，$i=i_1+i_2$，i_2为补偿电流；

[0026] 低频电流平整模块1，还用于对电源VCC输出的电压进行高频滤波；

[0027] 高频电流平整模块2，用于对低频电流平整模块1输出的负载电流i_1进行低频滤波，并将滤波后的电流信号通过电压调制器3进行电压转换，电压调制器3输出的电压用于给被保护电路4进行供电，

[0028] 所述被保护电路4为加密电路。

[0029] 本实施方式中，低频电流平整模块1，用于平整被保护电路4的低频电流成分，低频

电流平整模块1预先设定一个恒定的目标平整电流i，该电流i的值需要高于被保护电路4的电流峰值。低频电流平整模块1可实时检测负载电流i_1与恒定的目标平整电流i的差值，通过反馈环路，补偿相应的差值电流，使得负载电流i_1与补偿电流i_2的总和等于预先设定一个恒定的目标平整电流i，从而达到电流平坦化的目的。

[0030] 高频电流平整模块2用于滤除被保护电路4的高频电流成分。电压调制器3可以根据不同的被保护电路4的供电电压需求，设定相应的输出电压。

[0031] 在具体应用过程中，攻击者攻击时主要对被保护电路4输入的电源进行攻击，因此，在被保护电路4的前端加入了本发明所述的一种用于防御能耗攻击的密码防护电路，使得输入到被保护电路4的电流平坦化，提高对被保护电路4的防护能力。

[0032] 具体实施方式二：参见图1说明本实施方式，本实施方式与具体实施方式一所述的一种用于防御能耗攻击的密码防护电路的区别在于，所述的低频电流平整模块1包括单刀双掷开关S1、目标电流档位设定电路P1、放大器U1和N型MOS晶体管；

[0033] 所述单刀双掷开关S1的控制端与电源VCC的电压输出端连接，单刀双掷开关S1的1号输出端与高频电流平整模块2的电流输入端连接，单刀双掷开关S1的2号输出端与目标电流档位设定电路P1的电信号输入端连接，目标电流档位设定电路P1的目标电流输出端与放大器U1的同相输入端、高频电流平整模块2的电流输入端和N型MOS晶体管M0的漏极同时连接，

[0034] 放大器U1的反相输入端与可调电压源V1连接；

[0035] 放大器U1的输出端与N型MOS晶体管M0的栅极连接，N型MOS晶体管M0的源极接电源地。

[0036] 具体实施方式三：参见图1说明本实施方式，本实施方式与具体实施方式一或二所述的一种用于防御能耗攻击的密码防护电路的区别在于，所述的电压调制器3包括放大器U2、电阻R1、电阻R2和P型MOS晶体管M1；

[0037] 所述放大器U2的反向输入端用于接入可调电压源V2，放大器U2的同向输入与电阻R1的一端和电阻R2的一端同时连接，电阻R2的另一端接电源地，电阻R1的另一端与P型MOS晶体管M1的漏极连接，电阻R1的另一端作为电压调制器3的电压输出端；

[0038] 放大器U2的电源输入端与高频电流平整模块2电压输出端、P型MOS晶体管M1的源极同时连接，放大器U2的接地端接电源地，

[0039] 放大器U2的输出端与P型MOS晶体管M1的栅极连接。

[0040] 具体实施方式四：参见图1说明本实施方式，本实施方式与具体实施方式一所述的一种用于防御能耗攻击的密码防护电路的区别在于，所述的高频电流平整模块2为低通滤波器。

[0041] 本发明采用低频电流平整模块1与高频电流平整模块2结合的方案，实现对全频带的电流信号的抑制。利用高频电流平整模块2滤除加密电路的高频电流成分。整体的抑制效果取决于二者结合后叠加的频带是否足够。高频电流平整模块2的带宽f_{31}决定了可以滤除高频信号的频率范围，低频电流平整模块1的带宽f_{32}决定了可以抑制低频信号的范围，两个电路级联后，二者的可处理信号的频带相叠加，最差的抑制率出现在两个电路频带的交叠位置，如图2所示中f_T的位置。如果高频电流平整模块2的带宽和低频电流平整模块1的带宽混叠的频带的范围足够大，使得f_T处的电源电流信号和加密电路的电流比值K尽可能低，电

流平整电路的抑制效果达到最优。

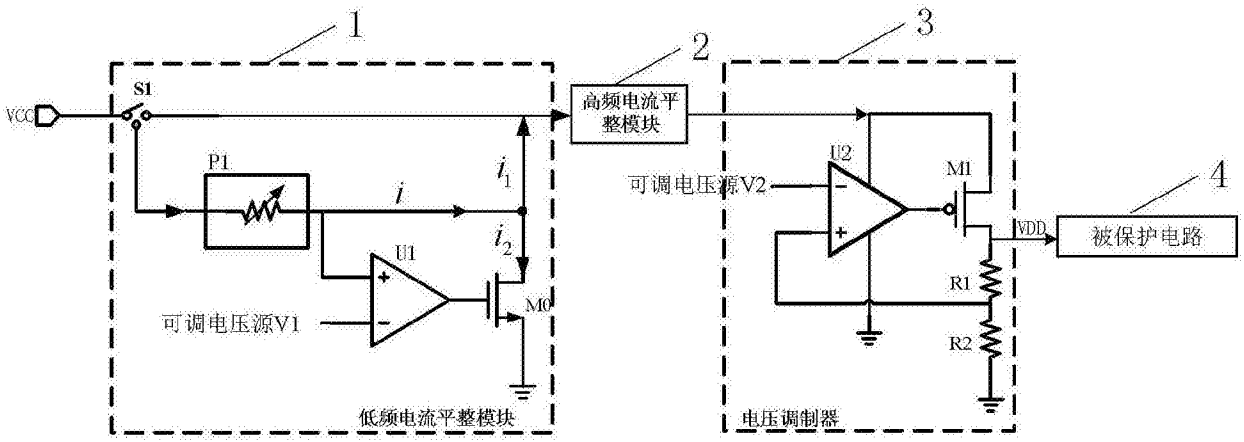

1
2
3
4
S1
VCC
P1
i
i1
i2
U1
M0
可调电压源V1
低频电流平整模块
高频电流平整模块
U2
M1
可调电压源V2
VDD
被保护电路
R1
R2
电压调制器

图1

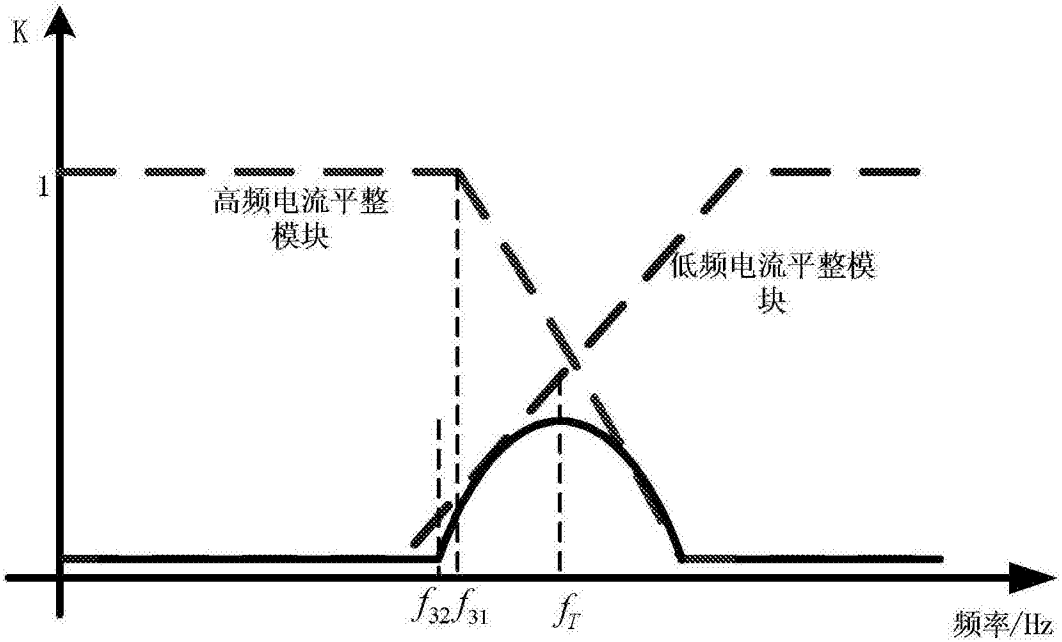

K
1
高频电流平整模块
低频电流平整模块
f32 f31
fT
频率/Hz

图2