(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 104579631 A
(43)申请公布日 2015.04.29

(21)申请号 201410776039.2

(22)申请日 2014.12.15

(71)申请人 天津大学
地址 300072 天津市南开区卫津路92号

(72)发明人 赵毅强 何家骥 束庆冉 杨松

(74)专利代理机构 天津市北洋有限责任专利代理事务所 12201
代理人 李丽萍

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)

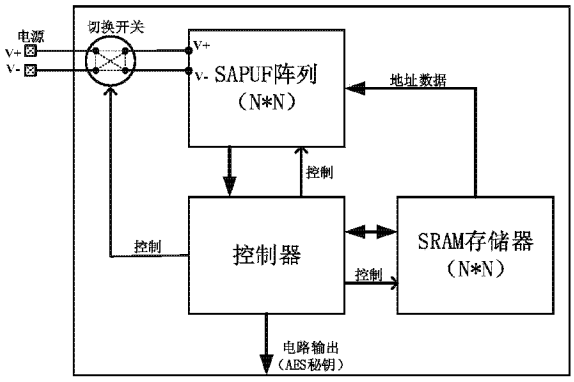
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于锁存型电压灵敏放大器PUF的AES密钥产生结构及方法

(57)摘要

本发明公开了一种基于锁存型电压灵敏放大器PUF的AES密钥产生结构，包括核心单元和外围电路，所述核心单元SAPUF结构是一种利用StrongARM型锁存灵敏放大器差分结构作为PUF的结构；所述外围电路包括一个SRAM存储器。SAPUF结构上电后，对其施加正偏压，得到N*N的码值，存储到SRAM中，对SAPUF施加负偏压，同时读取预存在SRAM中的码值，与新码值进行同或比较，将结果写入SRAM中，若结果为1，则选定的SAPUF结构稳定，若结果为0，则结构不稳定，以此作为可靠PUF的地址标记存储下来；对AES密钥产生结构施加零偏压，控制器参照预先存储在SRAM中的可靠PUF的地址，从SAPUF阵列中读取相应数目的码值，作为密钥进行输出。本发明为AES加解密电路提供密钥，保证密钥的唯一性、不可复制性和可靠性。



CN 104579631 A

1.一种基于锁存型电压灵敏放大器PUF的AES密钥产生结构，其特征在于，包括核心单元和外围电路，所述核心单元为SAPUF结构，所述SAPUF结构是一种利用StrongARM型锁存灵敏放大器作为PUF的结构；所述外围电路包括一个SRAM存储器；

所述StrongARM型锁存灵敏放大器为差分结构，包括七个场效应管：N1管、N2管、N3管、N4管、N5管、P1管和P2管，其中，N3管和N4管构成MOS对管，所述N3管和N4管的栅极接位线；N5管为使能管，N5管的栅极接使能控制信号EN，该使能控制信号EN控制放大器的开启与关断；N1管、N2管、P1管和P2管构成正反馈的锁存结构，该锁存结构相对于所述的MOS对管为负载；N1管和P1管的栅极为放大器的输出端OUT，所述P1管和P2管的源极为放大器的电源端。

2.一种基于锁存型电压灵敏放大器PUF的AES密钥产生方法，其特征在于，采用如权利要求1所述基于锁存型电压灵敏放大器PUF的AES密钥产生结构，并包括以下步骤：

步骤一、利用StrongARM型锁存灵敏放大器在位线零压差下的输出特性作为PUF结构：

当StrongARM型锁存灵敏放大器两输入端BL和BLA电压差为零时，其中，作为MOS对管的N3管和N4管失配，使StrongARM型锁存灵敏放大器的输出电压不为零，将该输出端电压折算到StrongARM型锁存灵敏放大器的输入端即为输入失调电压V_{OFFSET}：

$$V_{OFFSET}=(V_{th1}-V_{th2})+\sqrt{I}\left(\frac{1}{\sqrt{K_1}}-\frac{1}{\sqrt{K_2}}\right)+\frac{1}{2}\sqrt{\frac{1}{K}}\frac{\Delta R_0}{R_0}$$

$$K_1=\frac{1}{2}\mu c\frac{W_1}{L_1}$$

$$K_2=\frac{1}{2}\mu c\frac{W_2}{L_2}$$

$$K=\frac{1}{2}(K_1+K_2)$$

上式中，V_{th1}为N3管的阈值电压，单位为V，V_{th2}为N4管的阈值电压，单位为V，I为流过N5管的电流，单位为A，R_0为由从N1和N2管源极看进去的等效电阻，单位为Ω，μ为器件表面迁移率，单位为$cm^2/V\cdot s$，c为器件单位面积栅氧化物电容，单位为F/cm^2，W_1/L_1是N3管的宽长比，W_2/L_2是N4管的宽长比；

由上式得出，失调电压V_{OFFSET}由MOS对管的开启电压之差及K因子和负载电阻的失配决定，并且与偏置电流I的方根有关，利用该StrongARM型锁存灵敏放大器在位线零压差下的输出特性作为一种PUF结构从而形成SAPUF结构；

步骤二、对于步骤一确定的SAPUF结构进行筛选，：

在使用前首先对SAPUF施加一定的+ΔV以及-ΔV，通过判断SAPUF结构的输出是否稳定，来选出稳定的SAPUF结构，形成然后再使用，单个SAPUF筛选流程如下：

步骤2-1：给SAPUF结构施加+ΔV电压，记录此刻SAPUF结构的输出为OUT1；

步骤2-2：给SAPUF结构施加-ΔV电压，记录此刻SAPUF结构的输出为OUT2；

步骤2-3：将OUT1和OUT2进行比对，如果数值一样，则该SAPUF结构在偏压ΔV是稳定的，可以使用；

步骤 2-4 :重复上述步骤 1 ～ 3,直至选出足够多的 SAPUF 结构,用来产生固定位数的密钥 ;

步骤 2-5 :记录选定的 SAPUF 结构,需要密钥时,给选定的 SAPUF 施加零偏压的高电平,读取 SAPUF 的输出即可 ;

步骤三、使用步骤二筛选出的 SAPUF 结构构建 AES 密钥产生结构

对步骤二筛选出来的 SAPUF 结构上电之后,首先控制器控制切换开关对 SAPUF 施加 +ΔV 电压,得到 N*N 的码值,将该码值通过控制器存储到 SRAM 存储器当中,然后通过控制器控制切换开关对 SAPUF 施加 -ΔV 电压,与此同时,将预存在 SRAM 存储器当中的码值读取出来,然后与新得到的码值进行同或比较操作,将比较结果写入 SRAM 存储器当中,若同或比较结果为 1,则选定的 SAPUF 结构稳定,若同或比较结果为 0,则选定的 SAPUF 结构不稳定,以此作为可靠 PUF 的地址标记存储下来 ;

对 AES 密钥产生结构施加零偏压,即 ΔV 为 0,然后,控制器参照预先存储在 SRAM 当中的可靠 PUF 的地址,从 SAPUF 阵列中读取相应数目的码值,作为密钥进行输出,并且根据密钥长度,确定取出相应长度的密钥。

基于锁存型电压灵敏放大器 PUF 的 AES 密钥产生结构及方法

技术领域

[0001] 本发明使用一种 StrongARM 型锁存灵敏放大器作为 PUF(Physical Unclonable Function,物理不可复制结构),设计了可以为 AES(Advanced Encryption Standard, 高级加密标准算法)加解密模块产生密钥的结构。

背景技术

[0002] 21 世纪是信息的时代,一方面,信息技术和相关产业高速发展,呈现出空前繁荣的景象;另一方面,危害信息安全的事件不断发生,威胁国家安全和社会稳定,因此,必须采取措施确保我国的信息安全[1]。信息安全离不开密码学,作为信息安全的关键技术,密码学可以提供信息的保密性、完整性、可用性以及抗抵性。密码学主要由密码编码学和密码分析学两部分组成,密码编码学与密码分析学二者相互独立,又相互依存,从而推动了密码学自身的快速发展。

[0003] AES全称是Advanced Encryption Standard,即高级加密标准算法,是美国联邦政府采用的一种区块加密标准,这个标准用来替代原先的 DES(Date Encryption Standard)算法,该算法由美国国家标准与技术研究院 (NIST) 于 2001 年 11 月 26 日发布于 FIPS PUB 197,并在 2002 年 5 月 26 日成为有效的标准,截至 2006 年,AES 已然成为对称密钥加密中最流行的算法之一[2,3]。AES 目前获得了广泛的应用,成为虚拟专用网、SONET(同步光网络)、远程访问服务器 (RAS)、高速 ATM/Ethernet 路由器、移动通信、卫星通信、电子金融业务等的加密算法,并逐渐取代 DES 在 IP-See、SSL 和 ATM 中的使用。此外,得益于密码技术的高速发展,政府及军事通信更多的采用高级的加密算法,以及网络保密系统,财政保密、游戏机密等方面 AES 加密算法都得到了广泛的应用。

[0004] PUF全称是Physical Unclonable Function,即物理不可复制结构[4],利用各种电路结构放大集成电路生产过程中因工艺等原因造成的各种偏差,形成稳定的、唯一的、不可预测结果的电路结构[5]。

[0005] [参考文献]

[0006] [1] 沈昌祥, 张焕国, 冯登国等;信息安全综述 [J],中国科学 E 辑 : 信息科学 ,2007,37(2):129-150。

[0007] [2] 杨帆;基于 AES 密码芯片的 DPA 攻击技术分析 [J],高速铁路移动通信信号覆盖优化初探与实践,2014:105。

[0008] [3] 刘上力,赵劲强,聂勤务;AES 差分故障攻击的建模与分析 [J],计算机工程,2010,36(1):189-190。

[0009] [4]Suh G E,Devadas S.Physical unclonable functions for device authentication and secret key generation[C]//Proceedings of the 44th annual Design Automation Conference.ACM,2007:9-14。

[0010] [5]Bhargava M,Mai K.An efficient reliable PUF-based cryptographic

key generator in 65nm CMOS[C]//Proceedings of the conference on Design,Automation&Test in Europe.European Design and Automation Association,2014:70。

发明内容

[0011] 针对现有技术存在的问题，本发明提供一种基于锁存型电压灵敏放大器PUF的AES密钥产生结构，为AES加解密电路提供加解密所需的密钥，可根据不同需要分别提供128位、192位和256位密钥，保证密钥的唯一性、不可复制性和可靠性。

[0012] 为了解决上述技术问题，本发明提出的一种基于锁存型电压灵敏放大器PUF的AES密钥产生结构，包括核心单元和外围电路，所述核心单元为SAPUF结构，所述SAPUF结构是一种利用StrongARM型锁存灵敏放大器作为PUF的结构；所述外围电路包括一个SRAM存储器；所述StrongARM型锁存灵敏放大器为差分结构，包括七个场效应管N1管、N2管、N3管、N4管、N5管、P1管和P2管，其中，N3管和N4管构成MOS对管，所述N3管和N4管的栅极接位线；N5管为使能管，N5管的栅极接使能控制信号EN，该使能控制信号EN控制放大器的开启与关断；N1管、N2管、P1管和P2管构成正反馈的锁存结构，该锁存结构相对于所述的MOS对管为负载；N1管和P1管的栅极为放大器的输出端OUT，所述P1管和P2管的源极为放大器的电源端。

[0013] 本发明中提出的一种基于锁存型电压灵敏放大器PUF的AES密钥产生方法，是采用上述AES密钥产生结构，并包括以下步骤：

[0014] 步骤一、利用StrongARM型锁存灵敏放大器在位线零压差下的输出特性作为PUF结构：

[0015] 当StrongARM型锁存灵敏放大器两输入端BL和BLA电压差为零时，其中，作为MOS对管的N3管和N4管失配，使StrongARM型锁存灵敏放大器的输出电压不为零，将该输出端电压折算到StrongARM型锁存灵敏放大器的输入端即为输入失调电压 V_{OFFSET}：

[0016] $$V_{OFFSET}=(V_{th1}-V_{th2})+\sqrt{I}\left(\frac{1}{\sqrt{K_1}}-\frac{1}{\sqrt{K_2}}\right)+\frac{1}{2}\sqrt{\frac{1}{K}}\frac{\Delta R_0}{R_0}$$

[0017] $$K_1=\frac{1}{2}\mu c\frac{W_1}{L_1}$$

[0018] $$K_2=\frac{1}{2}\mu c\frac{W_2}{L_2}$$

[0019] $$K=\frac{1}{2}(K_1+K_2)$$

[0020] 式中，V_{th1}为N3管的阈值电压，单位为V，V_{th2}为N4管的阈值电压，单位为V，I为流 过N5管的电流，单位为A，R_0为由从N1和N2管源极看进去的等效电阻，单位为Ω，μ为器件表面迁移率，单位为$cm^2/V\cdot s$，c为器件单位面积栅氧化物电容，单位为F/cm^2，W_1/L_1是N3管的宽长比，W_2/L_2是N4管的宽长比。

[0021] 由上式得出，失调电压V_{OFFSET}由MOS对管的开启电压之差及K因子和负载电阻的失配决定，并且与偏置电流I的方根有关，利用该StrongARM型锁存灵敏放大器在位线零压差

下的输出特性作为一种 PUF 结构从而形成 SAPUF 结构；

[0022] 步骤二、对于步骤一确定的 SAPUF 结构进行筛选，：

[0023] 在使用前首先对 SAPUF 施加一定的 +ΔV 以及 -ΔV，通过判断 SAPUF 结构的输出是否稳定，来选出稳定的 SAPUF 结构，形成然后再使用，单个 SAPUF 筛选流程如下：

[0024] 步骤 2-1：给 SAPUF 结构施加 +ΔV 电压，记录此刻 SAPUF 结构的输出为 OUT1；

[0025] 步骤 2-2：给 SAPUF 结构施加 -ΔV 电压，记录此刻 SAPUF 结构的输出为 OUT2；

[0026] 步骤 2-3：将 OUT1 和 OUT2 进行比对，如果数值一样，则该 SAPUF 结构在偏压 ΔV 是稳定的，可以使用；

[0027] 步骤 2-4：重复上述步骤 1 ～ 3，直至选出足够多的 SAPUF 结构，用来产生固定位数的密钥；

[0028] 步骤 2-5：记录选定的 SAPUF 结构，需要密钥时，给选定的 SAPUF 施加零偏压的高电平，读取 SAPUF 的输出即可；

[0029] 步骤三、使用步骤二筛选出的 SAPUF 结构构建 AES 密钥产生结构

[0030] 对步骤二筛选出来的 SAPUF 结构上电之后，首先控制器控制切换开关对 SAPUF 施加 +ΔV 电压，得到 N*N 的码值，将该码值通过控制器存储到 SRAM 存储器当中，然后通过控制器控制切换开关对 SAPUF 施加 -ΔV 电压，与此同时，将预存在 SRAM 存储器当中的码值读取出来，然后与新得到的码值进行同或比较操作，将比较结果写入 SRAM 存储器当中，若同或比较结果为 1，则选定的 SAPUF 结构稳定，若同或比较结果为 0，则选定的 SAPUF 结构不稳定，以此作为可靠 PUF 的地址标记存储下来；

[0031] 对 AES 密钥产生结构施加零偏压，即 ΔV 为 0，然后，控制器参照预先存储在 SRAM 当中的可靠 PUF 的地址，从 SAPUF 阵列中读取相应数目的码值，作为密钥进行输出，并且根据密钥长度，确定取出相应长度的密钥。

[0032] 与现有技术相比，本发明的有益效果是：

[0033] 本发明中利用 StrongARM 型锁存灵敏放大器作为 PUF 结构（以下简称 SAPUF），构成本发明中 AES 密钥产生结构的核心单元。

[0034] 由于 AES 的加密流程和算法是公开的，保护 AES 算法的核心在于保护密钥 (Key) 的安全，而近年来，针对预存储在 AES 加解密电路中的密钥攻击越来越多，为了保证密钥的安全，一部分研究者在电路增强方面进行了研究，还有一部分在如何产生不可复制的唯一的密钥方面进行了研究。经过相关文献和专利的检索，目前已有部分研究者提出基于不同种 类PUF 的密钥产生结构，但是需要进行 ECC(Error Correcting Code，错误检查和纠正）操作。利用本发明的密钥产生结构能够产生唯一的、不可复制的和可靠的 AES 加解密密钥，该结构简单易用，而且输出稳定，可以根据需要产生 128 位、192 位、256 位密钥，可以作为 IP 核来使用。由于本发明是利用 SAPUF 结构 (StrongARM 型锁存灵敏放大器结构作为 PUF 结构），无需进行 ECC 操作；此外，相比于其他结构本发明的密钥产生结构对于外围电路的需求极小，仅需额外配备一个 SRAM(Static RAM，静态随机存储器）。

附图说明

[0035] 图 1 是 StrongARM 型锁存灵敏放大器结构示意图；

[0036] 图 2 是由 SAPUF 构成的 AES 密钥产生结构。

具体实施方式

[0037] 下面结合附图和具体实施例对本发明技术方案作进一步详细描述。

[0038] 本发明提出的一种基于锁存型电压灵敏放大器 PUF 的 AES 密钥产生结构是以 SAPUF 阵列为核心，加上相关外围电路构成。如图 2 所示，该 AES 密钥产生结构包括核心单元和外围电路，所述核心单元为 SAPUF 结构，所述 SAPUF 结构是一种利用 StrongARM 型锁存灵敏放大器作为 PUF 的结构；所述外围电路包括一个 SRAM 存储器。

[0039] 如图 1 所示，是 StrongARM 型锁存灵敏放大器（以下简称 SA 灵敏放大器）的结构图，该放大器为差分结构，包括七个场效应管：N1 管、N2 管、N3 管、N4 管、N5 管、P1 管和 P2 管，其中，N3 管和 N4 管构成 MOS 对管，N3 管和 N4 管为差分输入管，灵敏放大器失调电压 V_{OFFSET}的大小与 N3 管和 N4 管面积的平方根成反比，并且其栅极接位线；N5 管为使能管，N5 管的栅极接使能控制信号 EN，该使能控制信号 EN 控制放大器的开启与关断，使能管的宽长比对于放大器的速度影响最大；N1 管、N2、P1 和 P2 构成正反馈的锁存结构，该锁存结构相对于所述的 MOS 对管可以视为负载；N1 管和 P1 管的栅极为放大器的输出端 OUT，所述 P1 管和 P2 管的源极为放大器的电源端。

[0040] 结合图 1 说明本发明中的 SA 灵敏放大器理想情况下的工作原理：

[0041] 当使能信号 EN 为低电平时，N5 管关断，放大器不工作，输出端口 OUT 通过预冲管充电到高电平；理想情况下，如果两位线之间存在电压差，当使能信号 EN 变为高电平时，使能管 N5 开启，放大器开始工作，将两位线间的电压差进行放大。假设 BL 端电压大于 BLA 端电压，会使得流过 N3 的电流大于流过 N4 的电流，导致 b 点电位比 a 点电位下降快，当 b 点电位下降至 VDD-$|V_{th}|$ 时，P1 开启且开始对 a 点进行充电，当流过 P1 的充电电流大于流过 N1 的放电电流时，a 点电位上升，进而促使 b 点电位继续下降，开始正反馈，直至 a 点输出为高电平“1”，此时 b 点为低电平“0”，放大器输出“1”。相反，如果 BL 端电压 小于 BLA 端电压，最终 b 点为高电平“1”，放大器输出“0”。

[0042] 结合图 1 说明本发明中的 SA 灵敏放大器实际情况下的工作原理：

[0043] 理想情况下，放大器会将两位线之间的任意电压差进行放大，SA 灵敏放大器能够正确放大两位线间的电压差，强烈依赖于 N3/N4 管的匹配，而实际中，由于 MOS 管的匹配问题、工艺偏差等因素，导致 N3/N4 管不匹配。实际加工中，MOS 管的加工偏差，主要体现在宽长比的变化上，根据公式（1）：

[0044] $$I_D=\mu_n C_{OX}\frac{W}{L}[(V_{GS}-V_{TH})V_{DS}-\frac{1}{2}V_{DS}^2] \qquad (1)$$

[0045] 式（1）中，I_D为流过 MOS 管的电流，单位为安培，μ_n为器件的表面迁移率，单位为 $cm^2/V\cdot s$，C_{ox}为器件单位面积栅氧化物电容，单位为 F/cm^2，W/L 为器件的宽长比，V_{GS}是器件栅极和源极电压差，V_{TH}是器件的阈值电压，V_{DS}是器件的漏极源极电压。流过一个 MOS 管的电流大小，取决于工艺常数 $\mu_n C_{ox}$，器件的尺寸 W 和 L 以及栅和漏极相对于源极的电位之间的关系。宽长比的变化会导致 N3 管、N4 管电流大小不同，最终会导致输入零电压差情况下输出不为零。例如，将两位线电压设为相同的高电平，让 N3 管和 N4 导通，假设工艺常数 $\mu_n C_{ox}$稳定，由于 N3 管和 N4 在加工过程中存在尺寸的匹配问题，即宽长比 W/L 不同，会导致流过 N3 管和 N4 的电流不同，若 N3 管电流大于 N4 管电流，OUT 最终会输出“1”，若 N3 管电

流大于 N4 管电流，OUT 最终会输出“0”。

[0046] 采用图 1 所示基于锁存型电压灵敏放大器 PUF 的 AES 密钥产生结构的实现方法主要考虑以下几个方面：

[0047] 利用 SA 灵敏放大器作为 PUF 结构形成 SAPUT:

[0048] 实际使用中，当 SA 灵敏放大器两输入端电压差为零时，由于 N3、N4 对管的失配，使输出电压不为零，该电压折算到输入端就称为输入失调电压 V_{OFFSET}，根据公式 (2)：

[0049] $$V_{OFFSET}=(V_{th1}-V_{th2})+\sqrt{I}(\frac{1}{\sqrt{K_1}}-\frac{1}{\sqrt{K_2}})+\frac{1}{2}\sqrt{\frac{1}{K}}\frac{\Delta R_0}{R_0} \qquad (2)$$

[0050] 式 (2) 中，V_{th1}为 N3 管的阈值电压，单位为 V，V_{th2}为 N4 管的阈值电压，单位为 V，I 为流过 N5 管的电流，单位为 A，R_0为由从 N1 和 N2 管源极看进去的等效电阻，单位为 Ω，K 为和 MOS 管密切相关的影响因子。失调电压 V_{OFFSET}由 MOS 对管 N3、N4 管的开启电压之差及 K 因子和负载电阻的失配决定，并且与偏置电流的方根有关。只有在两位线之间电压差大于一定的失调电压 V_{OFFSET}时，放大器才能够正确的放大位线之间的电压差。例如，如果将 BL 置为高电平，BLA 置为低电平，但是两位线间电压差小于 V_{OFFSET}，由电压差引起的 N3 管和 N4 管电流变化不足以抵消由于宽长比不同带来的电流大小差异，则会出现输出 OUT 不变的情况。由于加工过程中存在的匹配问题，具有很强的随机性，导致 OUT 的输出不受人为控制，因此利用放大器在位线零压差下的输出特性，作为一种 PUF 结构。

[0051] SAPUF 在实际使用中的稳定性：

[0052] 利用 SA 灵敏放大器作为 PUF，需要考虑其输出的稳定性问题，实际使用中失调电压 V_{OFFSET}会受到外界温度以及负载端电阻等的影响，V_{OFFSET}越大，SAPUF 的稳定性越高，故可以在一定的偏压 ΔV 下衡量 SAPUF 结构的稳定性。预设 BL 和 BLA 电压差为 ΔV，BL 电压高于 BLA 为 +ΔV，BL 电压低于 BLA 为 -ΔV。下面分情况讨论实际中 SAPUF 的工作过程。

[0053] 1)N3 比 N4 宽长比大，放大器工作失调电压电压 V_{OFFSET}，$\Delta V<V_{OFFSET}$。

[0054] 首先考虑施加 +ΔV 情况，EN 信号由低电平变为高电平之后，放大器开始工作，由于 N3 比 N4 宽长比大，且 BL 电压高于 BLA 电压，所以流过 N3 管电流大于 N4 管电流，最终导致输出为“1”；其次考虑施加 -ΔV 情况，EN 信号由低电平变为高电平之后，放大器开始工作，由于 $\Delta V<V_{OFFSET}$，并不能抵消由于 N3 比 N4 宽长比大导致的电流变化，最终结果仍然是流过 N3 管电流大于 N4 管电流，最终导致输出为“1”。在该情况下，作为 PUF 使用时，可以稳定保证 PUF 输出为“1”。

[0055] 2)N3 比 N4 宽长比大，放大器工作失调电压 V_{OFFSET}，$\Delta V>V_{OFFSET}$。

[0056] 首先考虑施加 +ΔV 情况，EN 信号由低电平变为高电平之后，放大器开始工作，由于 N3 比 N4 宽长比大，且 BL 电压高于 BLA 电压，所以流过 N3 管电流大于 N4 管电流，最终导致输出为“1”；其次考虑施加 -ΔV 情况，EN 信号由低电平变为高电平之后，放大器开始工作，虽然 N3 比 N4 宽长比大，但是 $\Delta V>V_{OFFSET}$，会导致流过 N3 管的电流小于流过 N4 管的电流，最终导致输出为“0”。在该情况下，作为 PUF 使用时，由于其输出不能保持一个稳定的数值，故是不稳定的。

[0057] 经过上述 1)、2) 的讨论，可以得出，为了保证 SAPUF 在工作过程中的稳定性，需要失调电压 V_{OFFSET}越大，以保证 PUF 的稳定性，同时由于在使用中需要能够保证一定数量的

PUF 结构可以使用，故需要选取合适的 ΔV，既要保证能够选出足够数量的 SAPUF 单元，又要保证选出的 SAPUF 单元可靠。

[0058] 可靠 SAPUF 的筛选流程

[0059] 实际使用中，我们会选取很多 PUF，共同构成 AES 密钥产生结构，由于加工过程的随机性，不同的 PUF 本身的失调电压 V_{OFFSET} 也不同，所以需要利用 PUF 本身的特性，对于 PUF 结构进行一个筛选，即在使用前首先对 PUF 施加一定的 +ΔV 以及 -ΔV，通过判断 PUF 结构的输出是否稳定，来选出稳定的 PUF 结构，然后再使用，单个 PUF 筛选流程如下所示：

[0060] 步骤 1：给 PUF 结构施加 +ΔV 电压，记录此刻 PUF 结构的输出，OUT1

[0061] 步骤 2：给 PUF 结构施加 -ΔV 电压，记录此刻 PUF 结构的输出，OUT2

[0062] 步骤 3：将 OUT1 和 OUT2 进行比对，如果数值一样，则该 PUF 结构在偏压 ΔV 是稳定的，可以使用

[0063] 步骤 4：重复步骤 1 ～ 3，直至选出足够多的 PUF 结构，用来产生固定位数的密钥

[0064] 步骤 5：记录选定的 PUF 结构，需要密钥时仅需给选定的 PUF 施加零偏压的高电平，读取 PUF 的输出即可。

[0065] 使用 SAPUF 结构构建 AES 密钥产生结构

[0066] 如图 2 所示，是利用 SAPUF 结构构成的 AES 密钥产生结构框图。

[0067] 在使用之前，首先需要对该密钥产生结构进行校正，即对于其中的 PUF 核心阵列进行筛选，对该结构上电之后，首先控制器控制切换开关对 SAPUF 施加 +ΔV 电压，可以得到 N*N 的码值，将该码值通过控制器存储到 SRAM 存储器当中，然后通过控制器控制切换开关对 SAPUF 施加 -ΔV 电压，与此同时，将预存在 SRAM 存储器当中的数据读取出来，然后与新得到的码值进行同或比较操作，将比较结果写入 SRAM 存储器当中，若选定的 SAPUF 结构稳定，则同或比较结果为 1，若选定的 SAPUF 结构不稳定，同或比较结果为 0，以此可以作为可靠 PUF 的地址标记存储下来。

[0068] 正常使用中，对 AES 密钥产生结构施加零偏压，即 ΔV 为 0，然后控制器参照预先存储在 SRAM 当中的可靠 PUF 的地址，按照系统需求，从 SAPUF 阵列中读取相应数目的码值，作为密钥进行输出，在使用过程中，一般会根据密钥长度，确定取出相应长度的密钥。

[0069] 尽管上面结合附图对本发明进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨的情况下，还可以做出很多变形，这些均属于本发明的保护之内。

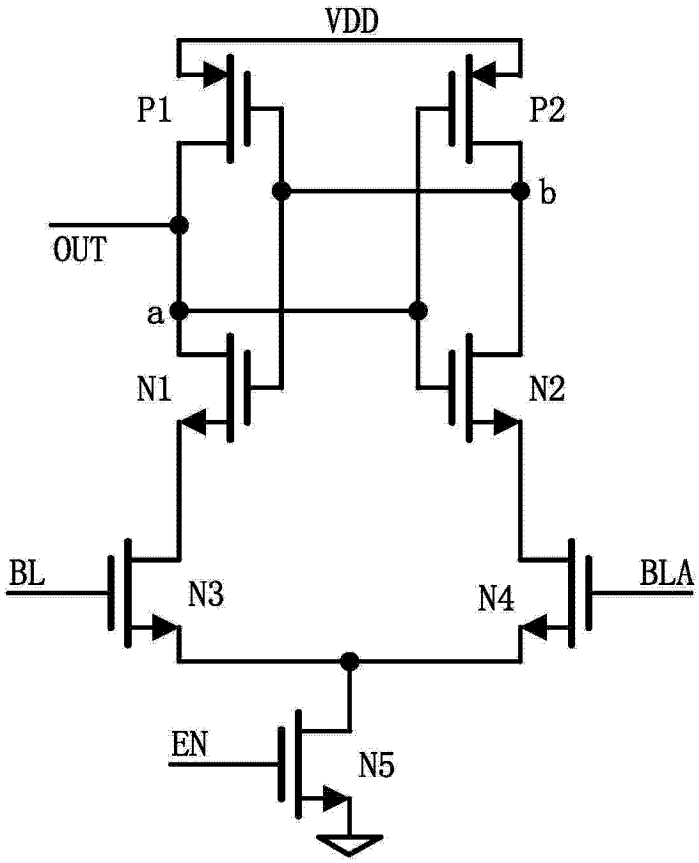


图 1

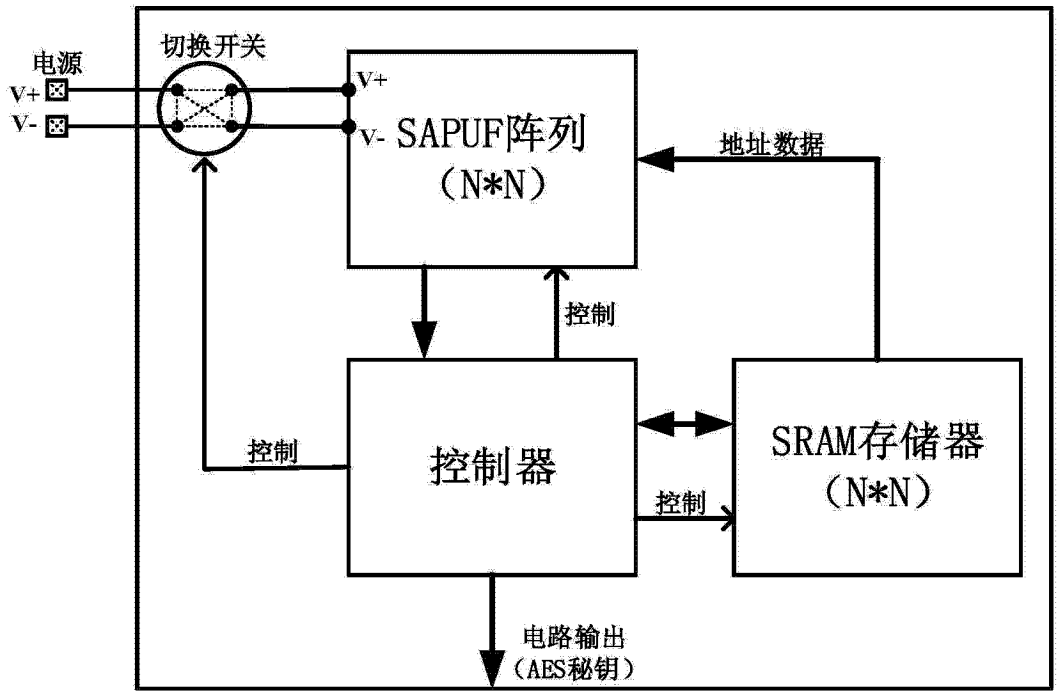

电源
V+
V-
切换开关
V+
V- SAPUF阵列
（N*N）
地址数据
控制
控制
控制器
控制
SRAM存储器
（N*N）
电路输出
（AES秘钥）

图 2