

基于电桥失衡效应的高随机性 PUF 电路设计

钱浩宇, 汪鹏君*, 李 刚

(宁波大学 电路与系统研究所, 浙江 宁波 315211)

摘要: 通过对物理不可克隆函数(Physical Unclonable Functions, PUF)电路和电桥失衡效应的研究, 提出一种高随机性 PUF 电路设计方案. 该方案首先利用工艺偏差导致电桥失衡产生随机偏差电压, 然后结合电压型灵敏放大器产生随机的、不可克隆的响应信号. 在 TSMC 65 nm CMOS 工艺下, 采用全定制方法设计 PUF 电路, PUF 单元电路的版图面积为 $2.23\ \mu\text{m} \times 2.43\ \mu\text{m}$. 通过 Spectre 软件, 在不同电压下对所设计 PUF 电路进行 Monte Carlo 仿真验证, 分析其逻辑功能、随机性等特性. 实验结果表明: 所设计的 PUF 电路在电源电压 1.2 V 和温度 25 °C 下随机性可达 51.8%.

关键词: 物理不可克隆函数; 电桥失衡效应; 随机性; 电路设计

中图分类号: TP331

文献标志码: A

文章编号: 1001-5132 (2016) 03-0056-06

随着网络技术和超大规模集成电路的发展, 电子设备在日常生活中已经得到广泛应用, 与此同时, 电子设备存在着泄露处理过程中信息的安全隐患, 这就对私人信息和经济社会生活等的安全性带来很大风险. 目前, 在诸多信息安全技术当中, 通常采用加密和身份认证技术两种信息安全保护手段^[1]. 其中, 加密技术是利用密码芯片对信息进行加密和解密, 进而保证信息的安全; 身份认证技术通常利用唯一的数字标识完成对用户身份识别和认证. 然而随着新型攻击技术的发展, 包括旁道攻击(Side Channel Attack, SCA)^[2]、差分功耗分析(Differential Power Analysis, DPA)^[3]和错误注入攻击(Fault Injection Attack, FIA)^[4]等技术使密码芯片的有效性逐步降低. 借鉴当前普遍适用的人体唯一特征(指纹或虹膜)实施认证的思想, 研究人员提出物理不可克隆函数电路^[5]. PUF 电路是芯片领域的 DNA 特征识别技术, 具有唯一性、随机性和不可克隆性, 通过提取芯片制造过程中无法避免引入的工艺偏差^[6], 产生无限多个特有的数据信息. 唯一性是指每个 PUF 电路的输出响应都包含了该集成电路的唯一物理身份信息; 随机性是指 PUF 电路产生的输出响应逻辑值具有随机分布特性;

不可克隆性是指 PUF 电路制造过程中存在随机工艺偏差, 即使攻击者了解 PUF 电路结构等信息, 也难以克隆出具有相同物理身份信息的电路. PUF 电路的这些优越特性, 使其可以有效防御各种攻击.

随机性作为 PUF 电路的一个重要性能指标, 它不但标志着电路的性能好坏, 还严重影响着应用系统的安全性; 尤其是将 PUF 电路的输出响应应用到加密算法中作为密钥时, 密钥的随机性好坏决定了此加密算法安全与否. 鉴此, 笔者提出一种基于电桥失衡效应的高随机性 PUF 电路设计方案. 首先利用四臂电桥的失衡效应得到两路随机偏差电压, 然后通过电压型灵敏放大器比较输入的偏差电压的大小, 产生响应信号. 本文在 TSMC 65 nm COMS 工艺下进行全定制版图设计, 利用 Spectre 工具对其进行 Monte Carlo 仿真分析. 结果表明, 所设计 PUF 电路逻辑功能正确, 在不同电源电压偏差下响应信号具有较高的随机性; 该 PUF 电路可广泛应用于密钥产生等信息安全领域.

1 基于电桥失衡效应的 PUF 电路设计

在集成电路制造过程中必然会引入工艺偏差, 其主要影响 MOSFET 的沟道长度、宽度、氧化层

收稿日期: 2015-12-05.

宁波大学学报(理工版)网址: <http://journalg.nbu.edu.cn/>

基金项目: 国家自然科学基金(61474068, 61274132); 浙江省自然科学基金(LQ14F040001).

第一作者: 钱浩宇(1991—), 男, 湖南耒阳人, 在读硕士研究生, 主要研究方向: 逻辑电路. E-mail: 1473614428@qq.com

*通信作者: 汪鹏君(1966—), 男, 浙江奉化人, 博导/教授, 主要研究方向: 逻辑电路和低功耗集成电路. E-mail: wangpengjun@nbu.edu.cn

厚度、离子掺杂浓度等, 从而影响 MOSFET 阈值电压、漏电流和等效阻值等参数. 而 PUF 电路主要利用由工艺偏差引起电路中特定节点电压、电流和延迟等信号差异, 产生随机、不可预测的输出响应.

1.1 电桥失衡效应分析

如图 1(a)所示, 电阻 R_1 、 R_2 、 R_3 和 R_4 称为电桥的臂, 检流计 G 接于结点 CD 间称为“桥”. 一般情况下 R_1 、 R_3 两端的电压不相等, 即结点 C 、 D 之间的电势不等, 检流计 G 中有电流流过. 当 $R_1 \times R_4 = R_2 \times R_3$, 此时检流计 G 中没有电流流过, 即结点 C 、 D 之间的电势相等, 电桥处于平衡状态.

在超大规模集成电路中, 电阻通常使用多晶硅、MOS 管及电容电阻等进行等效替代. 在 CMOS 工艺条件下, 制作同阻值的有源电阻尺寸要比无源电阻小得多. 因此本文采用 MOS 管的二极管连接方法等效电阻. 通过适当连接 MOS 管的 4 个端点, MOS 管实现两端有源电阻. 有源电阻是指将 MOS 晶体管进行适当的连接, 使其工作在一定的状态, 利用它的直流导通电阻和交流导通电阻作为电路中的电阻元件使用. 一般可在 MOS 管栅极施加适当的偏压或将其栅极和漏极短接, 使其漏源电压大于它的过驱动电压, 则此 MOS 管始终工作在饱和区. 图 1(b)给出增强型 NMOS 管作为有源电阻时的一种接法, 图 1(c)为转移特性曲线, 图 1(d)为晶体管电流—电压特性曲线.

图 1(b)中, NMOS 的栅极和漏极短接, 源极接较低电位, 电流从漏极流入, 则 NMOS 管工作在饱和区. 根据饱和区的萨式方程可知, 其转移特性曲线如图 1(c). 在不考虑沟道长度调制效应(即 $\lambda = 0$) 时, 直流电阻 R_{on} 公式如下:

$$R_{on} \Big|_{V_{GS}=V} = \frac{V}{I} = \frac{2t_{OX}}{\mu_n \epsilon_{OX}} \frac{L}{W} \frac{V}{(V - V_{TH})^2}, \quad (1)$$

式中, μ_n 为 NMOS 管载流子的迁移率; t_{OX} 为栅氧厚度; ϵ_{OX} 为栅氧介电常数; W 为沟道宽度; L 为沟道长度; V_{GS} 为栅源电压; V_{TH} 为阈值电压.

交流电阻为转移特性曲线在工作点 O 处的切线, 如图 1(c)所示. 在 O 点处, $V_{DS} = V_{GS}$, 所以交流电阻 r_{ds} 公式如下:

$$r_{ds} = \frac{\partial V_{DS}}{\partial I_{DS}} \Big|_{V_{GS}=V} = \frac{1}{g_m} = \frac{t_{OX}}{\mu_n \epsilon_{OX}} \frac{L}{W} \frac{1}{(V - V_{TH})}, \quad (2)$$

即交流电阻等于工作点为 V 的饱和区跨导的倒数.

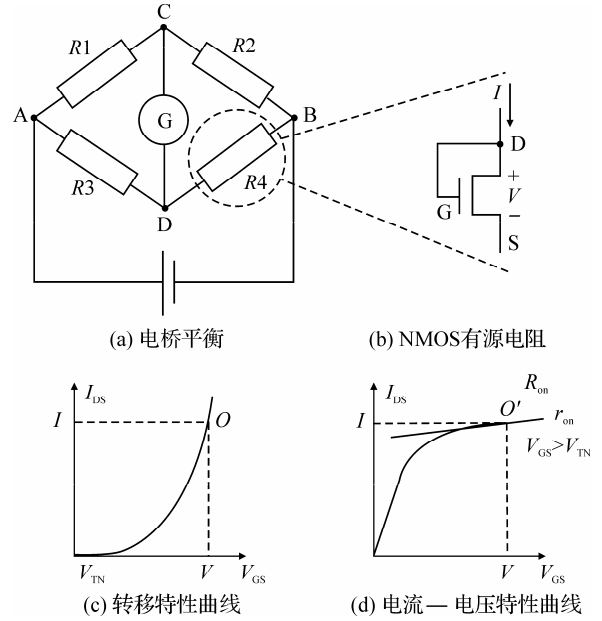


图1 电桥失衡效应分析

由(1)式和(2)式可见, 有源电阻的直流电阻、交流电阻阻值都易受到集成电路制造过程中沟道宽度 W 、沟道长度 L 和栅氧厚度 t_{OX} 等工艺参数的影响. 尤其是在 CMOS 工艺进入深亚微米后, 在光刻过程中必然会引起晶体管尺寸等参数的偏差, 从而导致有源电阻阻值偏差, 产生电桥失衡效应. 根据以上分析, 给出如图 2 所示的四臂电桥单元电路设计方案; 通过调节 NMOS 管的宽长比调节阻值, 使电桥处于理想平衡状态, 中间的检流计可用有源电阻代替.

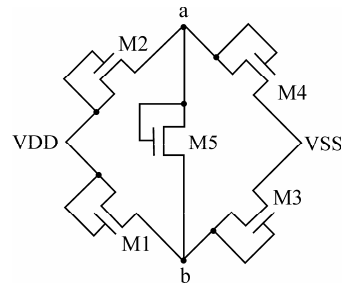


图2 四臂电桥单元电路

1.2 电桥失衡效应 PUF 电路单元设计

通过由上分析, 可得到如图 3 所示基于电桥失衡效应的 PUF 单元电路结构, 包括四臂电桥单元电路和对比输出单元电路. 其中对比输出单元电路由电压型灵敏放大器构成, 输入使能信号为 en , 输出响应为 out 和 $\overline{out}$. 在对比输出单元电路工作前, 灵敏放大器的输出端先利用使能信号 en 为低

电平进行预充电; 当 en 为高电平时, 电压型灵敏放大器通过比较 A、B 节点的电压大小, 得到互补输出信号 out 与 $\overline{out}$ 。

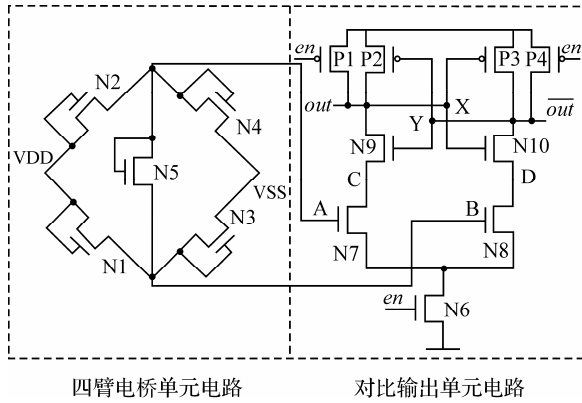


图3 基于电桥失衡效应的 PUF 单元电路

PUF 单元电路工作过程分为预充电阶段和求值阶段。在预充电阶段, 使能信号 $en = 0$, 此时电路通过预充电管 P1 和 P4 将输出信号 out 和 $\overline{out}$ 预充电至高电平, 从而使灵敏放大器的内部节点 C、D、X 和 Y 也全部达到高电平。随着使能信号 $en = 1$ 时, PUF 单元电路进入求值阶段。此时预充电管 P1 和 P4 截止, 电路输出端预充电结束, 同时 N6 导通, N7 和 N8 将全部处于饱和状态, 对比输出单元电路开始工作, PUF 单元电路开始求值, 输出响应信号。

理论上, 四臂电桥单元电路中有源电阻 N1、N2、N3、N4 的阻值应符合设计要求, 节点电压 V_A 和 V_B 也完全相等, 即电桥处于理想平衡状态。但由于在集成电路制造过程中不可避免会引入工艺偏差, 使 N1、N2、N3、N4 的参数不相同, 最终导致节点 V_A 和 V_B 电压不相等。电压型灵敏放大器通过比较两路存在随机偏差的电压信号大小, 产生

不可预测的输出响应信号, 电压型灵敏放大器的工作原理如下式所示:

$$out = \begin{cases} 1; V_A < V_B, \\ 0; \text{其他}. \end{cases} \quad (3)$$

因此, 若 N7 的栅电压 V_A 大于 N8 的栅电压 V_B , out 将优先被放电至低电平, $\overline{out}$ 被充电至高电平; 反之 out 被置为高电平, $\overline{out}$ 被置为低电平。同时, 灵敏放大器中的交叉耦合结构构成正反馈, 加快了 PUF 电路的响应速度。

2 多位电桥失衡效应 PUF 电路设计

密码算法包括数据加密标准算法(Data Encryption Standard, DES)、椭圆曲线加密算法(Elliptic Curves Cryptography, ECC)和高级加密标准算法(Advanced Encryption Standard, AES)等, 都需要输入多位密钥数据。其中, DES 加密算法的密钥长度为 56 位, ECC 加密算法密钥长度为 106 位、160 位或 256 位, AES 加密算法密钥长度为 128 位、192 位或 256 位。因此, 在实际的密码算法与 PUF 电路的结合应用中, 需要具备多位密钥输出的功能。图 4 即为多位电桥失衡效应 PUF 电路的结构设计图, 由行译码器、列译码器、时序控制、PUF 阵列构成。N12 和 N13 为隔离管, 此种电路结构优点是在电路进行读操作时, 位线上的数据不会影响到 PUF 单元电路产生的数值, 降低扰乱内部数据的可能性, 进而提高电桥平衡效应 PUF 单元电路在读操作时的稳定性。电桥失衡效应 PUF 电路的读操作过程中, 首先, 电路通过对位线预充电至高电平, 然后选择使能行译码还是列译码, 字线信号(rd 或 rw)有效选中一行或一列, 从而一次性地输出 2^n 个数据。

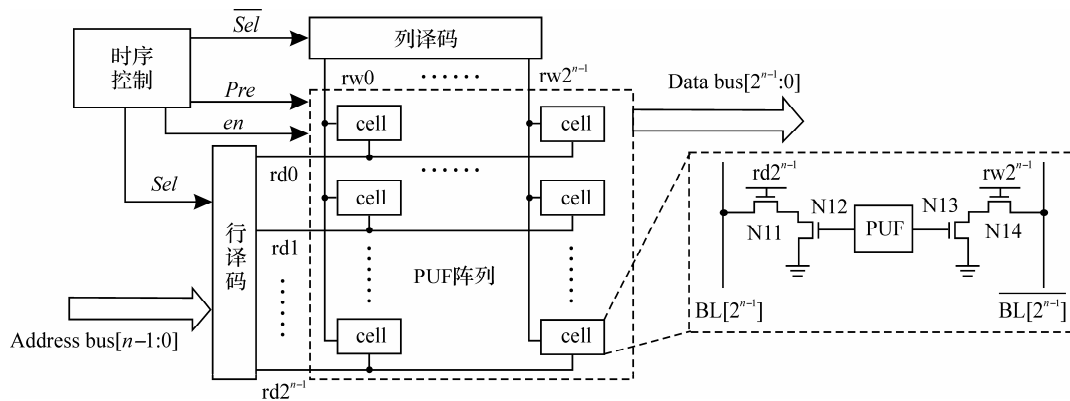


图4 多位电桥失衡效应 PUF 电路结构

图 5 为多位 PUF 电路工作时序图, 其中, Pre 、 en 、 Sel 和 $Data\ bus[2^{n-1}:0]$ 分别为预充电信号、PUF 单元电路预充求值信号、行列译码器选择信号以及输出信号。

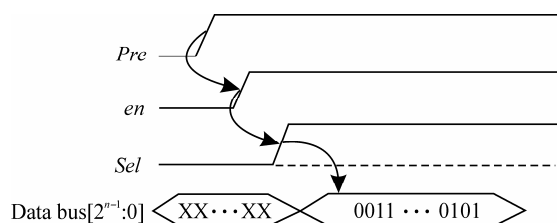


图 5 PUF 电路工作时序图

3 实验结果与分析

在 TSMC 65 nm CMOS 工艺下采用全定制方法设计电桥失衡效应 PUF 单元电路, 版图结构如图 6 所示。整个电路版图总共用到 3 层金属(M1、M2 和 M3)布线, 其中, M1 用于部分内部信号互连及电源走线(线宽为 90 nm), M2 为部分内部信号的

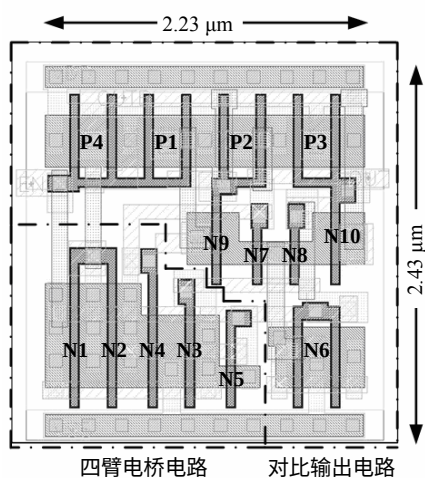


图 6 电桥失衡效应 PUF 单元电路版

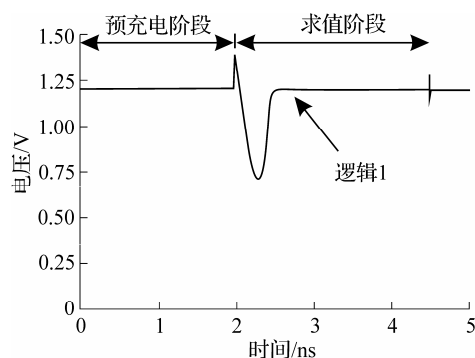
连接, M3 用于输出响应信号和输入使能信号的布线, M2 和 M3 线宽为 100 nm。同时, 为减小版图面积, 采用共用有源区和折叠等方法。最终, 所设计 PUF 单元电路的版图面积为 $2.23\ \mu\text{m} \times 2.43\ \mu\text{m}$ 。

3.1 PUF 电路逻辑功能

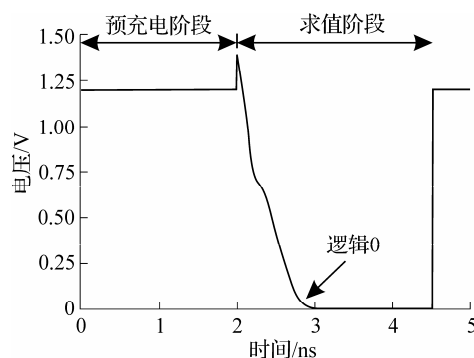
为验证 PUF 单元电路逻辑功能正确性, 需观察电压存在偏差时电路的输出响应是否正确。即当有源电阻 $N1$ 、 $N2$ 、 $N3$ 、 $N4$ 的阻值与所设计要求存在差异时, 输出响应为逻辑 1 或者逻辑 0。在理想条件下, 有源电阻 $N1$ 与 $N2$ 及 $N3$ 与 $N4$ 各项参数完全相同, 由其组成的四臂电桥处于平衡状态。图 7 即为电桥失衡时 PUF 单元电路的响应情况。有源电阻 $N1$ 和 $N2$ 沟道宽长比分别为 $720\ \text{nm}:60\ \text{nm}$ 和 $660\ \text{nm}:60\ \text{nm}$ 时的响应情况, 如图 7(a)所示。由于有源电阻 $N2$ 比 $N1$ 的阻值大, 所以节点电压 V_A 小于 V_B , 即 $N8$ 比 $N7$ 的栅电压大, 通过电压型灵敏放大器对比后 out 输出高电平; 反之 out 输出低电平, 如图 7(b)所示。因此, 所设计的电桥失衡效应 PUF 单元电路逻辑功能正确。

3.2 不同参数下电桥偏差分析

四臂电桥单元电路中各 MOSFET 的工艺参数偏差及二级效应决定输出偏差信号的大小, 通过适当调整 MOSFET 的沟道宽长比(即各个有源电阻阻值), 可以实现输出较大偏差信号的目的。在由不同宽长比的 MOSFET 构成四臂电桥单元电路情况下, 利用 Spectre 工具对所设计的四臂电桥单元电路进行 1 000 次 Monte Carlo 仿真, 结果如图 8 所示。图 8(a)为有源电阻 $N1$ 、 $N2$ 、 $N3$ 及 $N4$ 宽长相等, 图 8(b)为有源电阻 $N1$ 和 $N2$ 宽长相等大于 $N3$ 及 $N4$ 宽长, 图 8(c)为 $N1$ 和 $N2$ 宽长相等小于 $N3$



(a) 宽长比 $N1$ 大于 $N2$ 的 PUF 输出响应



(b) 宽长比 $N1$ 小于 $N2$ 的 PUF 输出响应

图 7 不同沟道宽长比下的 PUF 响应情况

及 N4 宽长情况. 由图可见, 输出电压偏差信号的大小呈现正态分布. 其中图 8(b)输出的偏差信号较大, 平均值为 589.45 mV, 标准差为 1.93 mV, 偏差电压的范围最大为 15 mV. 故可采用在图 8(b)条件下设计四臂电桥单元电路.

3.3 PUF 电路随机性

在一些加密等应用中, 需要 PUF 电路的输出响应具有很好的均匀分布特性. 输出为逻辑 0 或逻辑 1 的 PUF 响应的分布特性可以用随机性来表征. 设 N 为响应的位数, 则第 i 个响应 $r_i = [r_{i,1}, r_{i,2}, \dots, r_{i,N}]$ 的随机性可以定义为:

$$R(i) = \frac{1}{N} \sum_{j=1}^N r_{i,j} \times 100\%. \quad (4)$$

若其值为 100%则意味着响应位的值都为逻辑

1. 理想情况下 PUF 电路的随机性为 50%, 即输出逻辑 0 和逻辑 1 的概率相等. 对于 k 片不同的 PUF 芯片, 其平均随机性可以定义如下:

$$R_u = \frac{1}{k} \sum_{i=1}^k R(i). \quad (5)$$

本文所设计的电桥失衡效应 PUF 单元电路在正常环境(电压 1.2 V, 温度 25 °C)下, 通过 Monte Carlo 仿真($N=128, k=5$), 结果如图 9(a)所示, 计算出此时的平均随机性为 51.8%. 图 9(b)为电桥失衡效应 PUF 单元电路在不同电压下($(1.20 \pm 0.05)V$)输出逻辑 1 的平均随机性, 其中最大为 65.8%, 最小为 46.4%. 以上均可以表明, 所设计的电桥失衡效应 PUF 单元电路工作在不同电压环境中时具有较高的随机性.

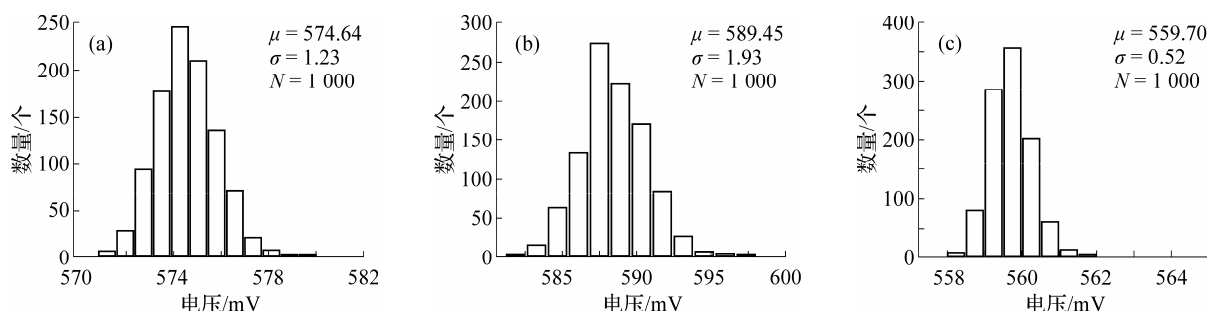


图 8 不同条件时偏差信号的蒙特卡洛仿真结果

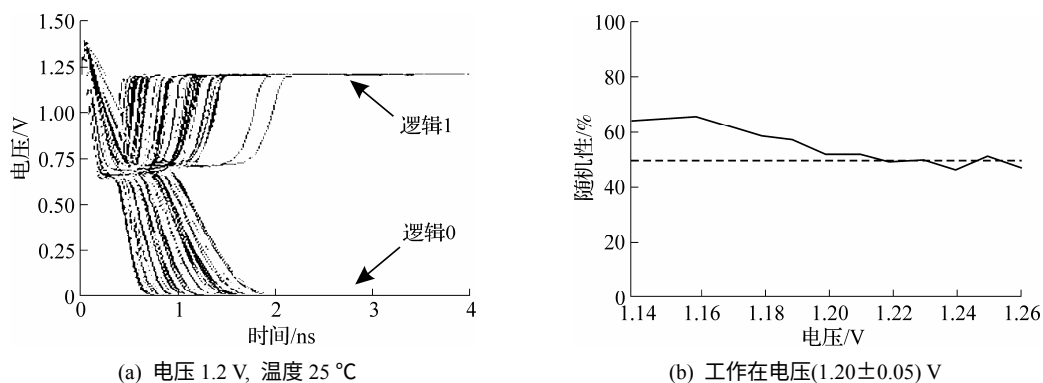


图 9 电桥失衡效应 PUF 电路的随机性

表 1 不同类型 PUF 电路对比

	文献[10]	文献[11]	文献[12]	本文
工艺	180 nm CMOS	65 nm CMOS	65 nm CMOS	65 nm CMOS
电压/V	1.8	1.2	1.2	1.2
类型	Arbiter-PUFs	DeMUX-PUFs	电压型-PUFs	电压型-PUFs
特点	延时	反馈	鲁棒性好	高随机性
随机性/%	65.6	59.8	52	51.8
单比特面积/ μm^2	183 618	-	180.76	5.42

同时, 对设计的 PUF 电路与其他类型 PUF 电路进行对比, 从表 1 可以发现, 所设计的 PUF 电路与其他 PUF 电路相比具有良好的随机性和较小的面积。

4 结论

设计了一种基于电桥失衡效应的高随机性 PUF 电路。首先利用四臂电桥作为偏差信号发生电路, 用电压型灵敏放大器构成对比输出电路, 然后通过对电桥失衡时产生的两路偏差电压的大小产生随机的 PUF 电路输出响应。结果表明所设计的 PUF 电路逻辑功能正确, 输出响应信号具有较高的随机性, 可应用于密钥产生等信息安全领域。

参考文献:

- [1] MAJZOBI M, KOUSHANFAR F. Time-bounded authentication of FPGAs[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3):1123-1135.
- [2] MANGARD S, OSWALD E, POPP T. Power Analysis Attacks: Revealing the Secrets of Smart Cards[M]. Austria: Springer Publish, 2007:1-306.
- [3] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Advances in Cryptology. Heidelberg: Springer Berlin, 1999:388-397.
- [4] CHRISTOPHE G, HUGUES T. A survey on fault attacks[C]. 6th Smart Card Research and Advanced Application Conference, 2004:159-176.
- [5] GASSEND B L. Physical random functions[D]. Massachusetts Institute of Technology, 2003.
- [6] ROEL M, INGRID V. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions[M]. Heidelberg: Springer Berlin, 2010:3-37.
- [7] MAITI A, KIM I, SCHAUMONT P. A robust physical unclonable function with enhanced challenge-response set[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(1):333-345.
- [8] MURPHY J, NEILL M. O, BURNS F, et al. Self-timed physically unclonable functions[C]. 5th IFIP International Conference on New Technologies, Mobility and Security, 2012:1-5.
- [9] MURPHY J. Asynchronous Physical Unclonable Functions-AsyncPUF[M]. Heidelberg: Springer Berlin, 2012:230-241.
- [10] LIM D, LEE J W, GASSEND B, et al. Extracting secret keys from integrated circuits[J]. IEEE Transactions on Very Large Scale Integration Systems, 2005, 13(10): 1200-1205.
- [11] LAO Y J, KESHAB K P. Statistical analysis of MUX-based physical unclonable functions[J]. IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, 2014, 33(5):649-662.
- [12] 汪鹏君, 张学龙, 张跃军. 基于最优控制电压的高鲁棒性 PUF 电路设计[J]. 电子学报, 2015, 43(5):907-910.
- [13] 乐大珩. 抗功耗攻击的密码芯片电路级防护关键技术研究[D]. 长沙: 国防科技大学, 2011.

Design of High Randomness PUF Circuit Based on Bridge Unbalance Effect

QIAN Hao-yu, WANG Peng-jun*, LI Gang

(Institute of Circuits and Systems, Ningbo University, Ningbo 315211, China)

Abstract: Through researching on the physical unclonable function (PUF) circuit and bridge unbalance effect, a high randomness PUF circuit is proposed in this paper. In this scheme, random deviation voltages are generated from bridge unbalance caused by process deviation. Then, random deviation voltages are inputted into sense amplifier to obtain response which is random and unclonable. Under TSMC 65 nm CMOS process, the full custom design method is adopted. The layout area of PUF circuit is $2.23 \mu\text{m} \times 2.43 \mu\text{m}$. Using Spectre software, Monte Carlo simulation results verify the designed PUF circuit under different voltage conditions. And also, the logical function and random characteristics are analyzed based on the simulation results. At 1.2 V & 25 °C, the randomness of the proposed PUF circuit achieves 51.8%.

Key words: PUF; bridge unbalance effect; randomness; circuit design

(责任编辑 章践立)