可配置电阻分压型 DAC-PUF 电路设计

汪鹏君,李 刚,钱浩宇
(宁波大学电路与系统研究所,浙江宁波 315211)

摘 要: 物理不可克隆函数(Physical Unclonable Function,PUF)电路利用结构和设计参数相同的单元电路在制造过程中存在的随机工艺偏差,产生具有唯一性、随机性和不可克隆性的密钥. 通过对电阻失配和数模转换器(Digital to Analogue Conversion,DAC)的研究,提出一种可配置电阻分压型 DAC-PUF 电路设计方案. 该 PUF 电路由输入寄存器、电阻分压型 DAC、电压比较器和时序控制模块构成. 通过激励信号配置 DAC 单元,使该 PUF 电路无需更换硬件便可实现输出密钥的变化. 在 TSMC-LP 65nm CMOS 工艺下采用全定制方式进行版图设计,面积为 72.4μm×87.8μm. 实验结果表明该 PUF 电路唯一性高,且在不同温度(-40~125℃)和电压(1.08~1.32V)下随机性和可靠性分别大于 99.1% 和 97.8%,可广泛应用于信息安全领域.

关键词: 物理不可克隆函数; 数模转换器; 可配置; 电路设计
中图分类号: TP331 **文献标识码:** A **文章编号:** 0372-2112 (2016)07-1630-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.07.016

Design of Configurable Resistance Divider Type DAC-PUF Circuit

WANG Peng-jun, LI Gang, QIAN Hao-yu
(*Institute of Circuits and Systems, Ningbo University, Ningbo, Zhejiang* 315211, *China*)

Abstract: Physical Unclonable Functions (PUF) exploits process variation across same structure and design parameter unit circuits during the manufacturing processes to generate numerous unique, random and unclonable security keys. In this paper, a configurable resistance divider type DAC-PUF scheme is proposed, which consists of input register, resistor-string based DAC, voltage comparator and timing control module. After configuring the DAC cell by applying input challenges, the PUF circuit updates keys without physically replacement. In TSMC-LP 65nm CMOS technology, the layout occupies 72.4μm × 87.8μm with custom designing. Experimental results show that the PUF circuit possesses nice statistical characteristic of uniqueness, high randomness of 99.1% and high stability of 97.8%, both with respect to supply voltage variation from 1.08V to 1.32V, and temperature variation from -40℃ to 125℃. It can be effectively used in information security field.

Key words: physical unclonable function; digital to analogue conversion; configurable; circuit design

1 引言

随着信息技术的飞速发展,信息安全越来越受到人们关注. 物理不可克隆函数(Physical Unclonable Function,PUF)电路[1,2]从硬件纹理特性上提供一种增强信息安全的途径. PUF 的概念最早由 Pappu[3]等研究人提出,它是集成电路领域的"DNA 特征识别技术". 目前硅基 PUF 电路是最主要的一个研究方向,它利用结构和设计参数完全相同的单元电路之间存在的微小工艺偏差(表现在电学特性上为电压、电流、延时等大小不同),产生具有唯一性、随机性和不可克隆性的响应. 唯一性是指一个给定的 PUF 电路具有唯一的函数功能,即能够产生满足唯一标识其自身的激励相应对(Challenge Response Pairs, CRPs);随机性是指 PUF 电路输出逻辑 0 和逻辑 1 的概率基本相同且具有随机分布特征;物理不可克隆性是指复制一个具有相同函数功能的 PUF 电路难度极大. PUF 电路的上述三大特性使得它在 IP 保护[4]、设备认证和密钥生成[5]等领域具有广阔的应用前景.

物理不可克隆性是 PUF 电路的固有属性,因此在 PUF 电路的设计中应当着重考虑输出响应的唯一性、随机性和可靠性,而这些属性主要取决于 PUF 电路偏差信号的大小及分布,并受限于比较器的灵敏度. 传统的 PUF 电路利用数字电路中 MOSFET 的几何尺度偏差

收稿日期:2015-11-19;修回日期:2016-01-18;责任编辑:马兰英
基金项目:国家自然科学基金(No.61474068,No.61274132);浙江省自然科学基金(No.LQ14F040001);浙江省教育厅项目(No.Y201430798)

(宽度和长度偏差)和工艺参数偏差(掺杂浓度、氧化层厚度、扩散深度等)来设计偏差信号产生电路,如 Arbiter-PUF[6] 电路中的延时单元,SRAM-PUF[7] 电路中的交叉耦合反相器以及 RO-PUF[8] 电路中的环形振荡器等. 与数字电路相比,模拟电路对器件工艺偏差更加敏感,因此可利用模拟器件设计偏差信号产生电路.

在标准 CMOS 工艺中,扩散区、阱区以及多晶硅等都可用来制作电阻,然而由于电阻边缘效应,电子迁移率和电阻厚度随机变化等因素,使得实际电阻值偏离理论值,且电阻几何尺寸越小阻值偏差范围越大.

鉴此,利用电阻的随机工艺偏差来设计 PUF 电路. 首先对电阻分压型数模转换器(Digital to Analog Converter,DAC)进行偏差分析,理论推导其输出电压的偏差大小与电阻变异系数(标准差/均值)的关系. 然后对 TSMC-LP 65 nm 工艺库中各类电阻偏差进行统计和分析,选出变异系数最大的电阻类型并结合电阻分压型 DAC 设计偏差电压产生电路,继而构建 PUF 电路. 最后在 TSMC-LP 65nm CMOS 工艺下对所提出的 PUF 电路进行版图设计,提取版图寄生参数并运用 Spectre 进行计算机仿真,验证其性能.

2　PUF 电路设计

2.1　电阻分压型 DAC 偏差分析

DAC 用于将数字信号转换成模拟信号,然而由于器件的随机工艺偏差使得输出模拟量偏离理论值,因此可利用 DAC 的此类偏差构建 PUF 电路的偏差电压产生模块. 一种 n 位电阻分压型 DAC 结构如图 1 所示,由电阻串(R_0,R_1,…,R_{2^n})、开关管、译码器和运算放大器(Operational Amplifier,OA)构成. 串联在参考电压 V_{ref} 与地之间的 2^n+1 个等值电阻产生分压电平 V_j($j=0,1,\cdots,2^n-1$). 译码器输出信号对各级开关管进行控制,将所选电压通过 OA 构成的缓冲器输出. 各级分压电平 V_j 可由式(1)表示:

$$V_j = \frac{\sum_{i=0}^{j} R_i}{\sum_{i=0}^{2^n} R_i} V_{ref} \tag{1}$$

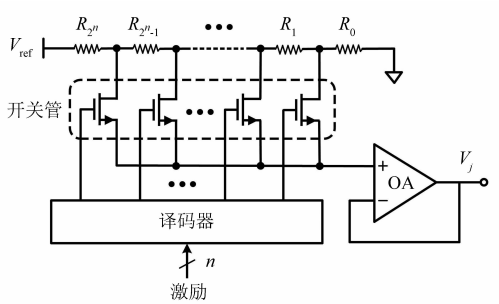


图1　电阻分压型DAC

令 $X=\sum_{i=0}^{j} R_i$,$Y=\sum_{i=j+1}^{2^n} R_i$,$U=u(X,Y)=\frac{X}{X+Y}$,由于 R_i($i=0,1,\cdots,2^n$)服从均值为 μ,方差为 σ^2(σ 为标准差)的高斯分布,则 U 近似服从高斯分布[9],其概率密度函数可表示为式(2):

$$f_U(u)=\frac{1}{\sqrt{2\pi}\sigma_0}e^{-\frac{(u-u_0)^2}{2\sigma_0^2}} \tag{2}$$

其中均值 u_0 和标准差 σ_0 分别为式(3)和式(4):

$$u_0=\frac{j}{2^n} \tag{3}$$

$$\sigma_0=\sqrt{\frac{u_0(1-u_0)}{2^n}}\frac{\sigma}{\mu} \tag{4}$$

将式(3)代入式(4)并乘以 V_{ref} 可获得第 j 级输出电压的偏差 ΔV_j,如式(5)所示:

$$\Delta V_j=\sigma_0 V_{ref}=\sqrt{\frac{j}{(2^n)^2}\left(1-\frac{j}{2^n}\right)}\frac{\sigma}{\mu}V_{ref} \tag{5}$$

可知当 DAC 位宽(n)、电阻变异系数(σ/μ)及参考电压(V_{ref})一定时,ΔV_j 仅与 DAC 输出的级数 j 相关,且当 $j=2^{n-1}$ 时,ΔV_j 取得最大值 $\sqrt{\frac{1}{2^{n+2}}}\frac{\sigma}{\mu}V_{ref}$.

2.2　电阻类型选择

由式(5)可知,电阻分压型 DAC 输出电压偏差大小正比于电阻的变异系数 σ/μ,因此需对所选工艺库中不同类型的电阻进行偏差估计,以选择最适合的电阻类型. 表 1 为对 TSMC-LP 65nm 工艺库中各类型的电阻进行 10000 次 Monte Carlo 仿真的统计结果,其中 W_{min} 和 L_{min} 分别代表相应类型电阻在 DRC 规则中能够取到的最小宽度和长度,变异系数用于横向比较各类型电阻偏差范围.

由表 1 知在各类电阻中,Rppoly 电阻的 W_{min} 和 L_{min} 最小(对应版图面积最小)且变异系数最大,因此选用 Rppoly 电阻作为电阻分压型 DAC 的分压电阻.

表 1　TSMC-LP **65**nm **工艺库中各类型电阻参数统计**

电阻类型	W_{min} (μ)	L_{min} (μ)	均值 μ (Ω)	标准差 σ (Ω)	变异系数 σ/μ (%)
Rnwod	1.8	9	1916.34	125.53	6.55
Rnwsti	1.8	9	3640.77	238.49	6.55
Rnod	0.4	0.4	145.04	17.45	12.03
Rpod	0.4	0.4	187.79	22.06	12.20
Rnpoly	0.4	0.4	556.09	71.03	12.77
Rppoly	0.4	0.4	550.02	70.55	12.83
Rnodwo	0.4	0.8	302.39	26.61	8.00
Rpodwo	0.4	0.8	580.80	67.11	11.56
Rnpolywo	0.4	0.8	437.11	46.40	10.61
Rppolywo	0.4	0.8	1412.69	67.66	4.79

2.3 PUF 电路结构设计

利用电阻的随机工艺偏差,结合电阻分压型 DAC 所设计的可配置电阻分压型 DAC-PUF 电路结构如图 2 所示. 它由输入寄存器、上下两路可配置电阻分压型 DAC、电压比较器以及时序控制模块构成. 工作过程为:在时序控制的作用下,输入寄存器输出的片选信号 E_u 和 E_d 分别在上下两路可配置电阻分压型 DAC 中各选一个 DAC 单元电路. 公共字线-位线信号 *W-B*,通过行列译码器的输出电平,控制 DAC 单元电路节点电压的输出. 由于电阻失配的影响,上下两路 DAC 输出电压 V_u 和 V_d 具有随机偏差,偏差值经电压比较器判决产生输出响应. 判决规则为:当 $V_u > V_d$ 时输出逻辑值 1,反之输出逻辑值 0.

可配置电阻分压型 DAC 是该 PUF 电路的核心,决定偏差信号的大小及分布. 它由 4 个结构和参数完全相同的 DAC 单元电路(Cell_0-Cell_3)、行译码器、列译码器、单元译码器和输出缓冲器构成.

其中,单元译码器输出信号用于 DAC 单元电路片选,行译码器和列译码器输出信号用于选择 DAC 单元电路的节点电压. 以 Cell_0 为例,参数完全相同的电阻 R($W = L = 0.4\mu$)和 NMOS 管($W = 0.24\mu$,$L = 0.06\mu$)组成 1*R*1*N* 结构,其中每 4 个横向相邻的 NMOS 管的漏极连接在一起,构成类似数字存储器中的字线;纵向相邻的 4 个 NMOS 管栅极连接在一起构成相应的位线. 字线信号(w_0-w_3)和位线信号(b_0-b_3)选择一个电阻分压值输出,输出值的大小取决于各级电阻 R 的随机偏差. 1*R*1*N* 结构的 DAC 需两个 2-4 译码器,输出线上仅有 8 个 NMOS 管结电容,而图 1 中直接译码的 DAC 需一个 4-16 译码器,输出线上有 16 个 NMOS 管结电容,两者相比,前者有效减小了译码域的规模和负载电容,从而节省电路面积,提高工作速度.

电压比较器根据输入电压大小不同产生输出响应,它的灵敏度直接影响 PUF 电路输出响应的随机性. 所设计的电压比较器结构如图 3 所示,由交叉耦合的 PMOS 管(P_0-P_3)和 NMOS 管(N_0-N_3)、隔离管(N_4-N_5)以及两个与非门组成的 RS 锁存器构成. 当时钟信号 ACK 为低电平时,电路处于预充电阶段,P_0、P_3 管导通,N_4、N_5 管截止,节点 *s* 和 *r* 被充电至高电平,此时电路不工作. 当 ACK 变为高电平时,预充电结束,电路进入求值阶段,P_0、P_3 管截止,N_4、N_5 管导通. 电压比较器根据 V_u 和 V_d 的大小(假设 $V_u > V_d$),将节点 *a* 和 *b* 的电压差($V_a < V_b$)迅速放大,使节点 *s* 和 *r* 的电压被分别拉向低电平和高电平,从而 *Q* 输出逻辑值 1;反之当 $V_u < V_d$ 时,*Q* 输出逻辑值 0. RS 锁存器保证 *Q* 的输出值在预充电阶段保持不变.

PUF 电路的工作时序如图 4 所示,*CLK* 为总的时钟信号,*REN* 和 *AEN* 分别为输入寄存器和电压比较器的使能信号. 由于图 2 中输入寄存器由 8 个 D 触发器级联构成,因此 *AEN* 要比 *REN* 延迟 8 个时钟周期. *RCK* 为输入寄存器的时钟信号,*ACK* 为 DAC 和电压比较器的时钟信号. 当 *ACK* 为低电平时译码器输入数据,电压比较器处于预充电阶段,输出值保持不变;当 *ACK* 变为高电

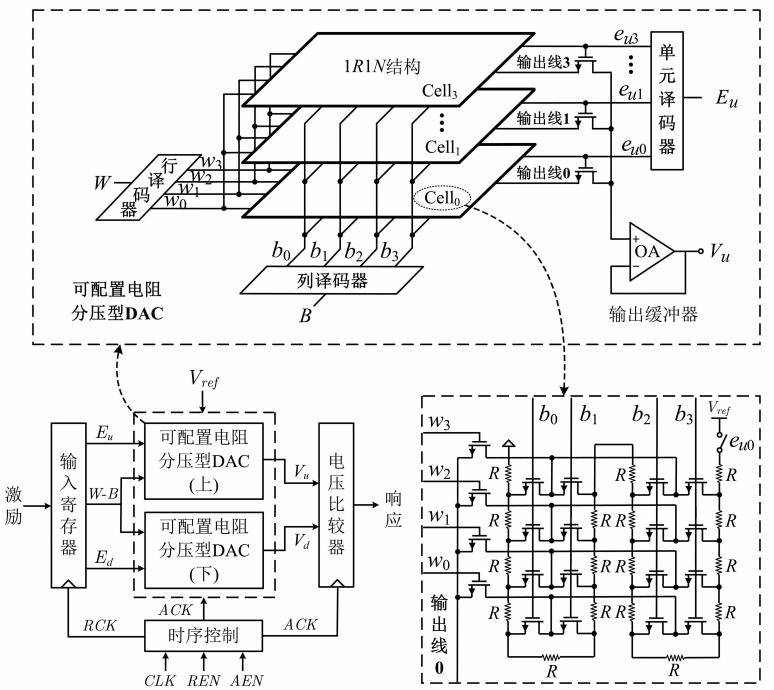


图2 PUF电路结构

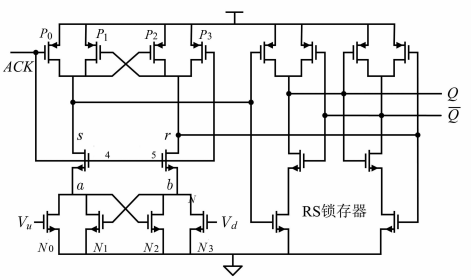


图3 电压比较器结构

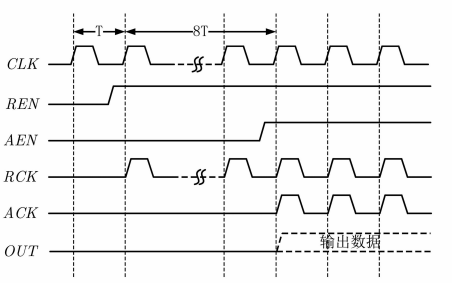


图4 PUF电路工作时序

平后译码器锁存,电压比较器处于求值阶段,输出判决值 0 或 1.

3　实验结果分析

在 TSMC-LP 65nm CMOS 工艺下采用全定制方式设计的 PUF 电路版图如图 5 所示. 输入寄存器、译码器及时序控制位于版图的左侧;电阻分压型 DAC 位于版图中间;运放及电压比较器位于版图右侧. 版图中各单元电路共用电源及地以减小面积. 整个版图共用到 3 层金属($M1$,$M2$,$M3$),$M1$ 用于单元电路内部信号及电源走线、$M2$ 用于各单元电路间连接,$M3$ 用于使能信号及输入-输出信号布线.

为减小各层金属线之间的电容耦合及信号串扰,相邻金属层采用垂直布线. 在最小尺寸下版图面积为 72.4μm×87.8μm,电路的动态功耗为 132μW. 提取版图寄生参数,利用 Spectre 对所设计的 PUF 电路进行计算机仿真,分别测试其输出响应的唯一性、随机性和可靠性.

3.1　唯一性

唯一性表征同一结构的 PUF 电路任意个体与其他个体的区分度,即产生唯一标识自身数字信息的能力. 通常采用统计相同条件下,同一 PUF 不同个体输出响应间汉明距离(Hamming Distance,HD)的方式衡量,理想情况下其值为 50%. k 个 PUF 个体的平均片间汉明距离 $E(\mathrm{HD}_{\mathrm{inter}})$ 可由式(6)[10]计算:

$$E(\mathrm{HD}_{\mathrm{inter}}) = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{\mathrm{HD}(r_i, r_j)}{n} \cdot 100\% \qquad (6)$$

其中,r_i 和 r_j 分别表示第 i 和第 j 个 PUF 电路在相同激励下产生的 n 比特响应.

为了测试的准确性,选取 256 组不同激励(每组激励长度为 8 比特,不重复),在每一组激励下对所提 PUF 电路进行 10000 次 Monte Carlo 仿真,继而得到 10000 个长度为 256 比特的输出响应,计算各响应间的 HD,统计结果如图 6 所示. 由图 6 可知所提 PUF 电路不同个体输出响应间的 HD 呈钟形分布,且通过式(6)计算 $E(\mathrm{HD}_{\mathrm{inter}})$ 为 51.3%,接近理想值.

3.2　随机性

随机性表征 PUF 电路输出数据中逻辑 0 和逻辑 1 的分布情况. 理想情况下,PUF 电路输出逻辑 0 和逻辑 1 的概率相同,此时随机性为 100%. PUF 电路输出数据的随机性可通过式(7)[10]计算:

$$Randomness = (1 - |2P(r=1) - 1|) \cdot 100\% \qquad (7)$$

其中,$P(r=1)$ 表示输出数据中逻辑 1 的概率.

选取 8 组汉明重量(Hamming Weight,HW)逐次加 1 的激励,对其在不同温度和电压下分别进行 10000 次 Monte Carlo 仿真,求每种环境下响应中逻辑 1 的平均值,并通过式(7)计算随机性,统计结果如图 7 所示. 由图 7 可知所提 PUF 电路在不同温度(电压为 1.2V)和工作电压(温度为 25℃)下随机性均大于 99.1%.

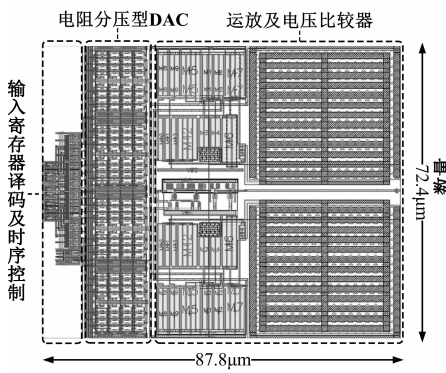


图5　PUF电路版图

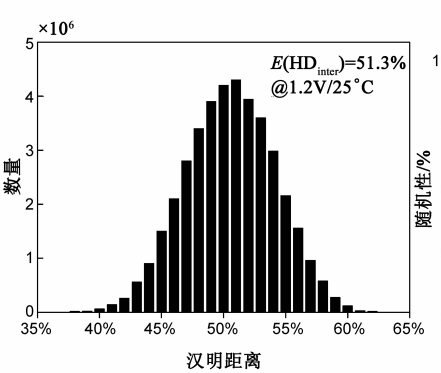


图6　PUF电路片间汉明距离

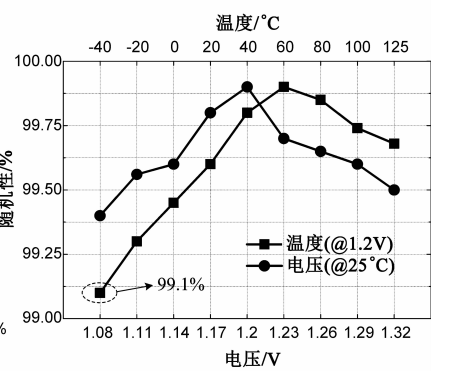


图7　PUF电路的随机性

3.3　可靠性

可靠性作为 PUF 电路的重要性能指标,用于说明 PUF 电路在不同工作环境中的性能. 在 m 个对比环境下,PUF 电路的可靠性可通过式(8)[10]衡量.

$$Reliability = 1 - E(\mathrm{HD}_{\mathrm{intra}}) = \left(1 - \frac{1}{m} \sum_{l=1}^{m} \frac{\mathrm{HD}(r_0, r_l)}{n}\right) \cdot 100\% \qquad (8)$$

其中,$E(\mathrm{HD}_{\mathrm{intra}})$ 表示平均片内汉明距离,r_0 和 r_l 分别表示在理想工作环境下(1.2V/25℃)和其他对比环境下长度为 n 比特的输出响应.

首先,在 1.2V/25℃条件下,对电路施加 256 组不同激励(每组激励长度为 8 比特,不重复),从而获得 256 比特长的输出,以此作为参考响应. 然后,使电路工作在不同的温度和电压下,施加与参考响应相同的激励,统计其输出响应相对于参考响应改变的位数,并通过式(8)计算可靠性. 统计结果如图 8 所示,图 8(a)和

图 8(*b*)分别代表可靠性随温度和电压的变化情况,可知所提 PUF 电路工作在不同温度(－40～125℃)和电压(1.08 ～ 1.32V)下的可靠性分别为 98.5%和 97.8%.

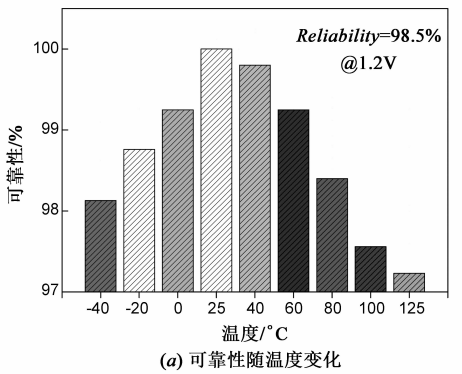


图8 PUF在不同温度和电压下的可靠性

表 2 为所设计的 PUF 电路与其他类型 PUF 电路性能对比. 所设计的可配置 DAC-PUF 电路在较大温度和电压变化情况下,依然能够保证较高可靠性.

表 2 不同类型 PUF 电路性能对比

文献	类型	可配置	工艺(nm)	温度范围(℃)	电压波动(%)	可靠性(%)
TVLSI 2016[6]	Arbiter-PUF	Y	180	－40～100	6	96.8
JSSC 2008[7]	SRAM-PUF	N	130	0～100	10	96.0
TCAD 2015[8]	RO-PUF	Y	65	－40～120	2.5	97.3
DEL 2015[11]	PCM-PUF	Y	–	0～120	10	80.0
HOST 2014[12]	CM-PUF	Y	30	0～75	9	96.0
AES 2015[13]	VM-PUF	Y	65	－40～125	5	96.0
本文	DAC-PUF	Y	65	－40～125	10	97.8

4 结论

PUF 电路利用 IC 制造过程中不可控的随机工艺偏差产生特有密钥,用于增强信息安全. 目前 PUF 电路主要利用数字电路中 MOSFET 的参数失配来设计,而本文采用数模混合方式,利用电阻分压型 DAC 电阻的失配来设计 PUF 电路. 通过激励信号配置电阻分压型 DAC,无需更换硬件电路便可实现输出密钥变化. 在 TSMC-LP 65nm CMOS 工艺下,采用全定制方式设计的电路版图面积为 72.4μm × 87.8μm. 实验结果表明该 PUF 电路唯一性强,且在不同工作环境下随机性和可靠性分别大于 99.1% 和 97.8%,可广泛应用于密钥生成和设备认证等领域.

参考文献

[1] Potkonjak M, Goudar V. Public physical unclonable functions[J]. Proceedings of the IEEE, 2014, 102(8): 1142－1156.

[2] Herder C, Yu M D, Koushanfar F, et al. Physical unclonable functions and Applications: a tutorial[J]. Proceedings of the IEEE, 2014, 102(8): 1126－1141.

[3] Pappu R, Recht R, Taylor J, et al. Physical one-way function[J]. Science, 2002, 297(5589): 2026－2030.

[4] Guajardo J, Kumar S S, Chrijen G J. FPGA intrinsic PUF and their use for IP protection[A]. Proceedings of the workshop on Cryptographic Hardware and Embedded Systems[C]. Vienna, 2007. 63－80.

[5] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[A]. Proceedings of Design A utomation Conference[C]. San Francisco, 2007. 9－14.

[6] BAI C, ZOU X, DAI K. A novel thyristor-based silicon physical unclonable function[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2016, 24(1): 290－300.

[7] Ying S, Holleman J, Otis B P. A digital 1.6 pJ/bit chip identification circuit using process variations[J]. IEEE Journal of Solid-State Circuits, 2008, 41(3): 69－77.

[8] Cao Y, Zhang L, Chang C H, et al. A low-power hybrid RO PUF with improved thermal stability for lightweight applications[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34(7): 1143－1147.

[9] Sergio S, Tommaso B, Luca F, et al. High-level modeling of resistor string based digital-to-analog converters[J]. Analog Integr Circ Sig Process, 2011, 66: 407－416.

[10] Lao Y J, Parhi K. 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.

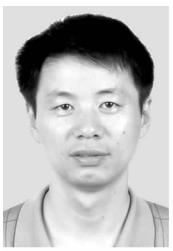
[11] Chen A. Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions[J]. IEEE Electron Device Letters, 2015, 36(2): 138－140.

[12] Kumar R and Burleson W. On design of a highly secure

PUF based on non-linear current mirrors[A]. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)[C]. Washington,2014. 38 - 43.

[13] 汪鹏君,等. 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.
Wang P J,Zhang X L,Zhang Y J. Design of robust PUF based on the optimal gate voltage[J]. Acta Electronica Sinica,2015,43(5):907 - 910. (in Chinese)

作者简介



汪鹏君(通信作者)　男,1966 年出生于浙江奉化,博士,教授,博士生导师,中国电子学会高级会员,中国计算机学会高级会员,中国电子学会电子线路与系统专业委员会委员,中国计算机学会多值逻辑与模糊逻辑专业委员会委员,目前主要从事低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计、多媒体技术及相关理论方面研究工作.

E-mail:wangpengjun@ nbu. edu. cn

李　刚　男,1988 年出生于陕西汉中,博士研究生,主要从事密码芯片攻击和防御理论研究.

钱浩宇　男,1991 年出生于湖南耒阳,硕士研究生,主要从事密码芯片攻击和防御理论研究.