

基于最优控制电压的高鲁棒性 PUF 电路设计

汪鹏君, 张学龙, 张跃军

(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 Functions, PUF)电路作为一种新型的信息安全电路, 依赖集成电路制造过程中硅器件的固有工艺偏差产生密钥. 本文提出一种高鲁棒性 PUF 电路设计方案, 首先分析 MOSFET 在零温度系数点(Zero Temperature Coefficient, ZTC)的工作特性, 然后结合提高 PUF 电路鲁棒性的途径, 确定 PUF 电路的结构及最优控制电压, 最终达到密钥稳定可靠的目的. 在 TSMC 65nm CMOS 工艺下对所设计的 PUF 电路进行版图设计, 面积为 $14.89\mu\text{m} \times 12.14\mu\text{m}$. 实验结果显示在最优控制电压下 PUF 电路的鲁棒性最低为 96%.

关键词: 物理不可克隆函数; 零温度系数点; 鲁棒性; 电路设计

中图分类号: TP331 **文献标识码:** A **文章编号:** 0372-2112 (2015)05-0907-04

电子学报 URL: <http://www.ejournal.org.cn> **DOI:** 10.3969/j.issn.0372-2112.2015.05.011

Design of Highly Robust PUF Based on the Optimal Gate Voltage

WANG Peng-jun, ZHANG Xue-long, ZHANG Yue-jun

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

Abstract: Physical Unclonable Functions (PUF), as a kind of innovative secure circuits, extract key relying upon the intrinsic process variations in silicon devices. This paper proposes a scheme of highly robust PUF. First, we analyze the properties of the MOSFET working at the point of Zero Temperature Coefficient. And then we determine the structure and the optimal gate voltage of PUF by combining the approaches that improve the robustness of PUF circuits. All of which lead to the goal of making the keys stable and reliable at last. This design is implemented in TSMC 65nm CMOS technology and the layout area occupies $14.89\mu\text{m} \times 12.14\mu\text{m}$. The simulation results show that the reliability of PUF is not less than 96%, which is better than other PUF circuits.

Key words: physical unclonable functions; zero temperature coefficient; robustness; circuit design

1 引言

物理不可克隆函数(Physical Unclonable Functions, PUF)电路^[1]是一种依赖集成电路本身特性的函数发生电路, 产生的数字信号可以作为芯片的身份标识. 其中, 集成电路的本身特性是指在其制造过程中由于不可控的工艺偏差存在, 致使相同电路产生信号的大小及传输延迟出现偏差. PUF 电路借助集成电路的这种内在特性, 通过对比或其它方式处理偏差信号, 最终产生响应信号, 因此, 每个 PUF 电路拥有唯一的函数功能, 称为 PUF 电路的唯一性^[2]; 同时对响应信号中的每一位而言, 输出逻辑 0 和逻辑 1 的概率几乎相等, 称为 PUF 电路的随机性^[3]. 由于工艺偏差的不可控性, 即使攻击者已明确 PUF 电路的结构信息, 同样难以克隆出具有相同函数功能的 PUF 电路, 称为 PUF 电路的不可克隆性.

以上特点使得 PUF 电路可以有效地防御包括侵入式攻击^[4]的多种攻击模式. 因此, PUF 电路可作为安全芯片应用于身份认证^[5]、密钥产生^[6]和硬件知识产权保护等多种安全系统中.

由于 PUF 电路的设计是基于集成电路制造过程中微弱的工艺参数偏差, 电路的函数功能容易受电源电压、温度以及老化^[7](包括负偏压温度不稳定性、氧化层击穿和热载流子效应等)等因素的影响. 鲁棒性是指在各种因素影响下 PUF 电路仍保持正常工作的属性, 是 PUF 电路的一个重要性能指标. PUF 电路的鲁棒性严重影响应用系统的安全性, 高鲁棒性 PUF 电路已经成为当前研究和设计的重点. 目前提高 PUF 电路鲁棒性的方法主要采用纠错电路^[8]和改变电路的操作时序^[9]等, 但是存在芯片面积开销较大等问题. 鉴此, 本文提出一种高鲁棒性 PUF 电路设计方案, 通过分析 MOSFET 的工作特

性,确定 PUF 电路的最优控制电压,进而输出可靠性较高的密钥.本方案在 TSMC 65nm COMS 工艺下进行版图设计,利用 Spectre 工具对其进行基于 Monte Carlo 的仿真分析,结果表明所设计的 PUF 电路具有较高鲁棒性.

2 高鲁棒性 PUF 电路分析与设计

2.1 MOSFET 的零温度系数点理论

MOSFET 的漏电流 I_D 如式(1)所示^[10]:

$$I_D = \frac{1}{2} \mu C_{OX} \frac{W}{L} (V_{GS} - V_{TH})^2 \quad (1)$$

其中 μ 、 C_{OX} 、 W 、 L 、 V_{GS} 和 V_{TH} 分别表示 MOSFET 的载流子浓度、栅氧化层厚度、沟道宽度、沟道长度、栅极-源极电压和阈值电压,同时 V_{TH} 和 μ 是环境温度 (T) 的函数,分别如式(2)和式(3)所示:

$$V_{TH} = V_{TH}(T_0) + \alpha_{TH}(T - T_0) \quad (2)$$

$$\mu = \mu(T_0) \left(\frac{T}{T_0} \right)^{\alpha_\mu} \quad (3)$$

其中 T_0 是参考温度, α_{TH} 和 α_μ 是负数常量.

由文献[10]可知, MOSFET 的栅极-源极电压如式(4)所示:

$$V_{GS} = V_{TH}(T_0) - \alpha_{TH} T_0 \quad (4)$$

则 MOSFET 的漏电流如式(5)所示:

$$I_D = \frac{1}{2} C_{OX} \frac{W}{L} \mu(T_0) (\alpha_{TH} T_0)^2 \quad (5)$$

由式(5)可以发现, MOSFET 的漏电流 I_D 不受温度变化的影响.图1给出了 NMOS 管工作在不同温度下的 I - V 特性曲线.可以发现,在相同栅极控制电压下, NMOS 管的漏电流随着温度的变化而变化,表明温度影响 NMOS 管的漏电流;同时还可以发现不同温度下的 I - V 曲线存在一个交点,该点称为 NMOS 管的零温度系数 (Zero Temperature Coefficient, ZTC) 点,此时 NMOS 管的漏电流在温度变化时保持恒定,因此工作在零温度系数点的 NMOS 管具有较强的鲁棒性.

2.2 PUF 电路结构设计

PUF 电路主要是通过对比相同电路结构产生具有偏差的电压、电流和延迟等信号,产生随机的输出响应.影响 PUF 电路鲁棒性的因素可以分为工艺参数因

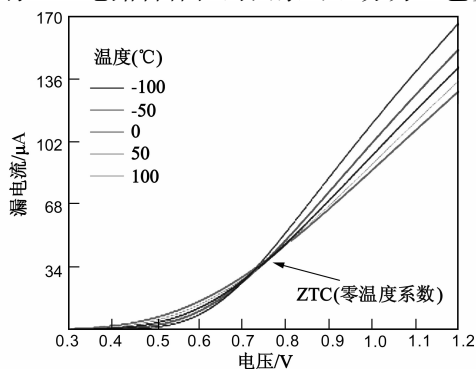


图1 NMOS管在不同温度下的 I - V 特性曲线

素和非工艺参数因素.其中工艺参数因素在集成电路制造过程中已经确定,包括 MOS 管的沟道宽长比、影响阈值电压的各项参数以及金属线延迟等;非工艺参数因素是指外部噪声,如温度和工作电压等.因此,可以采用以下两种途径提高 PUF 电路的鲁棒性:(1)是增加或固定进行对比的偏差信号差值;(2)是增强电路中各器件对非工艺参数的鲁棒性.

图2给出了单个 NMOS 管参数失配时的 I - V 特性曲线, M_0 、 M_1 、 M_2 、 M_3 和 M_4 分别表示不同失配参数下的 NMOS 管.可以发现不同参数偏差的 NMOS 管具有不同的 ZTC 点,同时发现不同 ZTC 点的栅极电压几乎相等,也就是说此时 NMOS 管具有不同的漏电流,并且均不受温度变化的影响,满足第二种提高 PUF 电路鲁棒性途径的条件.因此,可以利用 NMOS 管在 ZTC 点表现出的特性构建高鲁棒性 PUF 电路,其中 ZTC 点的横坐标值(栅极-源极电压)为 PUF 电路的最优控制电压.

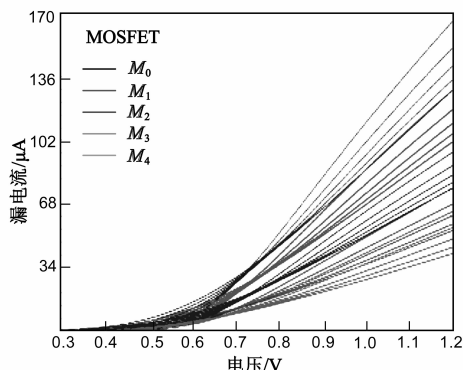


图2 NMOS管参数失配时 I - V 特性曲线

根据 NMOS 管的零温度系数点理论,结合常规的 PUF 电路设计方法^[1,11],本文提出一种高鲁棒性 PUF 电路设计方案,结构如图3所示,由偏差信号发生电路、信号选择电路和对比输出电路构成.偏差信号发生电路是 PUF 电路的核心,用于产生 PUF 电路所需的具有偏差的电压信号;信号选择电路用于选择进行对比的两路电压偏差信号;对比输出电路完成两路电压信号的对比,并产生 PUF 输出响应.

本文主要对偏差信号发生电路进行设计和分析,如图4所示,由8列 NMOS 管和电阻构成,输出电压 (V_1 、 V_2 , ..., V_8) 的大小由工艺参数决定,同时受非工艺参数的影响.偏差信号发生电路的鲁棒性决定整个 PUF 电路的函数功能, NMOS 管工作在 ZTC 点时漏电流不受温度影响,同时仿真发现当电阻值超过一定值时,温度对其阻值的影响可以忽略,因此偏差信号发生电路输出信号具有较高的鲁棒性.信号选择电路由数据选择器构成,受工艺偏差的影响,最初被选中的电压信号经过数据选择器后会再次出现偏差,将进一步扰乱 PUF 电路响应与

电路结构间的数据相关性,使得 PUF 电路的函数功能更加难以预测,从而提高 PUF 电路的安全性.偏差信号发生电路中各元器件的参数决定其输出偏差信号的大小,通过调整 NMOS 管的沟道宽长比以及电阻值的大小,可实现输出较大偏差信号的目的.在最优控制电压下,利用 Spectre 工具对所设计的偏差信号发生电路进行 1000 次 Monte Carlo 仿真,结果如图 5 所示.从图中可发现输出电压偏差信号的大小呈现正态分布,平均值为 243.34mV,标准差为 17.52,偏差电压的范围最大为 125mV.

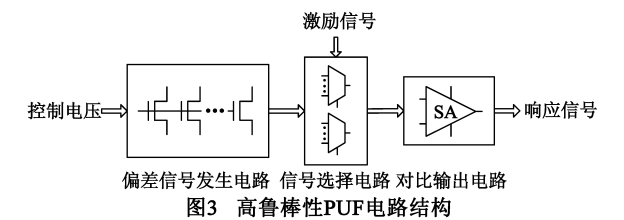


图3 高鲁棒性PUF电路结构

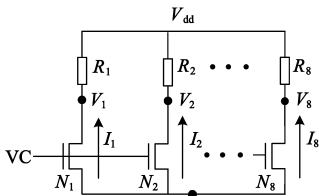


图4 偏差信号发生电路结构

对比输出电路由电压型灵敏放大器构成.PUF 电路的工作过程分为预充电和求值两个阶段.首先,预充电阶段,PUF 电路的栅极控制电压为低电平,偏差信号发生电路不工作,此时预充电模块将敏感放大器输入端充电至高电平,使其处于保持状态.其次,求值阶段,PUF 电路的栅极控制电压变为高电平,敏感放大器开始工作,对比输入端的电压信号产生随机的 PUF 电路响应.图 6 给出了 PUF 电路的工作时序图,其中,PRE、VC、EN_SA 和 OUT 分别为预充电信号、电压控制信号、敏感放大器的使能信号以及输出信号.

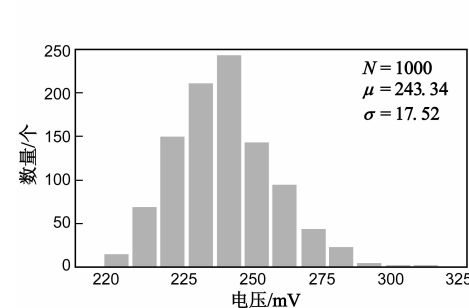


图5 偏差信号的蒙特卡洛仿真结果

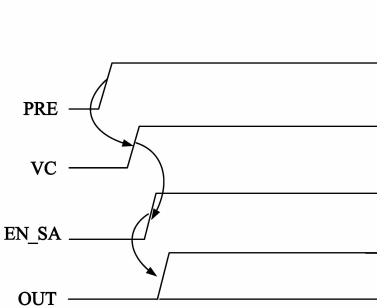


图6 PUF电路的工作时序图

2.3 PUF 电路版图设计

图 7 给出了在 TSMC 65nm CMOS 工艺下采用全定制方式设计的 PUF 单元电路版图,版图面积为 $14.89\mu\text{m} \times 12.14\mu\text{m}$,总共用了 4 层金属走线.其中版图的右侧部分为输出电路,左侧部分为偏差信号发生电路,中间部分为信号选择电路.

3 实验结果分析

本文对具有 25 位输出信号的 PUF 电路进行基于 Monte Carlo 的仿真分析,观察其在不同工作条件下输出响应的鲁棒性情况.

首先,分别仿真 PUF 电路在温度偏差为 $\pm 100^\circ\text{C}$ 和 $\pm 50^\circ\text{C}$ 情况下的输出响应结果,然后同参考温度下输出的响应信号进行对比,得出鲁棒性百分比.同时,为增加统计数据的可靠性,对 PUF 电路施加 10 组不同的激励信号,求鲁棒性的平均值,统计结果如图 8(a)所示,可以发现 PUF 电路在不同温度下鲁棒性最低为 96%.

然后,分析 PUF 电路在工作电压偏差下的鲁棒性情况.由于工作电压影响 MOS 管的 ZTC 工作点,因此分别仿真工作电压为 1.14V、1.17V、1.23V 和 1.26V(标准电压为 1.2V)情况下 PUF 电路的输出响应情况,同样对 PUF 电路施加 10 组激励信号,然后求其鲁棒性的平均值,统计结果如图 8(b)所示,可以发现 PUF 电路在不同电压下鲁棒性最低为 96.8%.

综上所述,PUF 电路在不同条件的鲁棒性最低为 96%.同时,对本文设计的 PUF 电路与其他类型 PUF 电路的进行对比,结果如表 1 所示,可以发现所设计的 PUF 电路与其他 PUF 电路相比具有较强的鲁棒性.

表 1 不同类型 PUF 电路对比

	文献[6]	文献[12]	文献[11]	文献[5]	本文
工艺	180nm CMOS	130nm CMOS	Xilinx Virtex 5	45nm SOI-CMOS	65nm CMOS
工作电压(V)	1.8	1	1	1	1.2
鲁棒性	95.2%	96%	90%	94.5%	96%

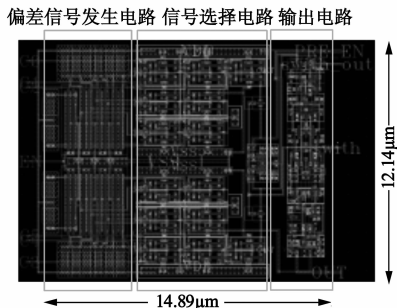


图7 PUF单元电路的版图

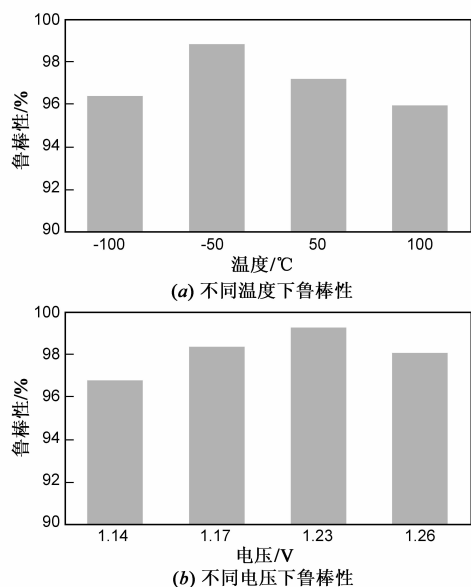


图8 PUF电路在不同工作条件下鲁棒性分析

4 结论

本文提出了一种新型的高鲁棒性 PUF 电路设计方案,主要利用 MOSFET 在工艺偏差情况下所有零温度系数点纵坐标相同的特点,确定 PUF 电路的最优控制电压.在 TSMC 65nm CMOS 工艺参数下,利用 Spectre 工具对电路进行基于 Monte Carlo 的仿真分析,在不同温度偏差下 PUF 电路的鲁棒性最低为 96%;同时,在不同电压偏差下 PUF 电路的鲁棒性最低为 96.8%,与其他 PUF 电路相比表现出较强的鲁棒性.

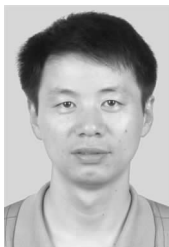
参考文献

- [1] Lofstrom K, Daasch W R, Taylor D. IC Identification circuit using device mismatch[A]. IEEE International Solid-State Circuits Conference (ISSCC)[C]. San Francisco, CA, USA: IEEE Xplore, 2000. 372 – 373.
- [2] Wang P J, Zhang Y J, Han J, et al. Architecture and physical implementation of reconfigurable multi-port physical unclonable functions in 65nm CMOS[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96-A(5): 963 – 970.
- [3] Zhang Y J, Wang P J, Li Y, et al. Model and physical implementation of multi-port PUF in 65nm CMOS[J]. International Journal of Electronics, 2012, 100(11): 112 – 125.
- [4] 汪鹏君,等.防御零值功耗攻击的 AES SubByte 模块设计及其 VLSI 实现[J].电子学报,2012,40(11):2183 – 2187. Wang Peng-jun, et al. Design of AES subByte module of anti-zero value power attack and its VLSI implementation[J]. Acta Electronica Sinica, 2012, 40(11): 2183 – 2187. (in Chinese)
- [5] Lang L, Srivathsa S, Krishnappa D K, et al. Design and valida-

tion of arbiter-based PUFs for sub-45-nm low-power security applications[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(4): 1394 – 1403.

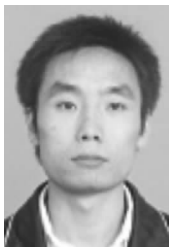
- [6] Lim D, Lee J W, Gassend B, et al. Extracting secret keys from integrated circuits[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2005, 13(10): 1200 – 1205.
- [7] Maiti A, Schaumont P. The impact of aging on a physical unclonable functions[J/OL]. <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&number=6612683>, 2013-09-26.
- [8] Yu M, Devadas S. Secure and robust error correction for physical unclonable functions[J]. IEEE Design & Test of Computers, 2010, 27(1): 48 – 65.
- [9] Bhargava M, Cakir C, Mai K. Reliability enhancement of bi-stable PUFs in 65nm bulk CMOS[A]. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)[C]. San Francisco, CA, USA: IEEE Xplore, 2012. 25 – 30.
- [10] Bendali A, Audet Y. A 1-V CMOS current reference with temperature and process compensation[J]. IEEE Transactions on Circuits and Systems-I: Regular Papers, 2007, 54(7): 1424 – 1429.
- [11] Majzoobi M, Koushanfar F. Time-bounded authentication of FPGAs[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 1123 – 1135.
- [12] 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, 43(1): 69 – 77.

作者简介



汪鹏君 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



张学龙 男, 1988 年出生于山东临沂, 硕士研究生, 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方面的研究工作.

张跃军 男, 1982 年出生于浙江台州, 博士, 讲师, 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方面的研究工作.