基于 65 nm 工艺的多端口可配置 PUF 电路设计

李 刚 汪鹏君* 张跃军 钱浩宇
(宁波大学电路与系统研究所 宁波 315211)

摘 要：物理不可克隆函数(Physical Unclonable Function, PUF)电路利用结构完全相同的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。该文通过对共源共栅电流镜的研究，提出一种基于电流镜工艺偏差的多端口可配置 PUF 电路。该 PUF 电路由输入寄存器、偏差电压源、复用网络、判决器阵列和扰乱模块构成，通过激励信号配置偏差电压源，无需更换硬件便可实现输出密钥的变化，且可在一个时钟周期内输出多位密钥。在 SMIC 65 nm CMOS 工艺下，采用全定制方式设计具有 36 个输出端口的 PUF 电路，版图面积为 24.8 μm×77.4 μm。实验结果表明，该 PUF 电路具有良好的唯一性和随机性，且工作在不同温度(-40~125°C)和电压(1.08~1.32 V)下的可靠性均大于 97.4%，可应用于信息安全领域。

关键词：电路设计；物理不可克隆函数；多端口；可配置
中图分类号： TP331 **文献标识码**：A **文章编号**：1009-5896(2016)06-1541-06
DOI: 10.11999/JEIT150968

Design of Multi-port Configurable PUF Circuit Based on 65 nm Technology

LI Gang WANG Pengjun ZHANG Yuejun QIAN Haoyu
(*Institute of Circuits and Systems*, *Ningbo University*, *Ningbo* 315211, *China*)

Abstract: Physical Unclonable Functions (PUF) exploits process variation across the same structure circuits during the manufacturing processes to generate numerous unique, random and unclonable security keys. In this paper, a multi-port configurable PUF scheme is proposed, which is based on random deviation of current mirrors. It consists of input register, deviation-voltage source, multiplexing-net, arbiter array and obfuscation circuit. After configuring deviation-voltage source by applying different input challenges, the PUF circuit updates keys without physically replacement, and it can generate multi-bit keys in a clock cycle. In SMIC 65 nm CMOS technology, the layout of 36 ports configurable PUF occupies 24.8 μm×77.4 μm with custom designing. Experimental results show that the PUF circuit possesses better statistical characteristic of uniqueness and randomness, and it has a high reliability of 97.4% with respect to temperature variation from −40 °C to 125 °C, and supply voltage variation from 1.08 V to 1.32 V. It can be effectively used in information security field.

Key words: Circuit design; Physical Unclonable Function (PUF); Multi-port; Configurable

1 引言

随着计算机技术和集成电路技术的飞速发展，信息安全与隐私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]，采用提取硬件纹理特性的方式，提供了一种增强信息安全的途径。这种技术最早由文献[3]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[4−6]是最主要的一个研究方向，利用结构和参数相同的电路之间存在的微小工艺偏差(表现在电学特性上为时延、电压、电流偏差等)，产生具有唯一性、随机性和不可克隆性的响应。这些微小工艺偏差可分为两类：第 1 类为工艺参数偏差，包括掺杂浓度、氧化层厚度、扩散深度等，是由沉积和掺杂剂扩散的非均匀性导致；第 2 类为几何尺度偏差，主要包括晶体管宽度和长度偏差，是由光刻技术的精度决定。PUF 电路输出相应的唯一性、随机性和不可克隆性这 3 大特性使得它在设备认证、密钥生成与存储[7]，IP 保护[8]以及安全芯片防攻击[9]等信息安全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 电路设计过程中应着重考虑输出响应的唯

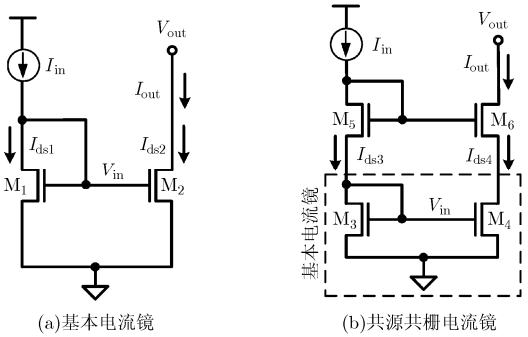
收稿日期：2015-08-24；改回日期：2016-01-20；网络出版：2016-03-14
*通信作者：汪鹏君 wangpengjun@nbu.edu.cn
基金项目：国家自然科学基金(61474068, 61274132)，浙江省自然科学基金(LQ14F040001)，浙江省教育厅项目(Y201430798)
Foundation Items: The National Natural Science Foundation of China (61474068, 61274132), The Natural Science Foundation of Zhejiang Provice (LQ14F040001), The Project of Department of Education of Zhejiang Provice (Y201430798)

一性、随机性以及可靠性，而这些属性不仅取决于PUF电路偏差信号的大小及分布，还受比较器灵敏度的限制。传统的PUF电路，主要利用数字电路中MOSFET的工艺参数偏差和几何尺度偏差来设计偏差信号产生电路，如RO-PUF电路中的环形振荡器[4]，SRAM-PUF电路中的交叉耦合反相器[10]以及Arbiter-PUF电路中的延时单元[11]等。电流镜是模拟电路中必不可少的部分，用于实现复制输入电流到输出支路，然而由于输入-输出电路之间的随机工艺偏差和系统误差，使得复制到输出支路上的电流会围绕输入电流大小产生偏差。鉴此，利用电流镜的随机工艺偏差来设计偏差信号产生电路，继而构建PUF电路。首先对电流镜的工艺偏差进行分析，理论推导电流镜电流增益偏差与工艺参数偏差的关系，并通过Monte Carlo仿真得到共源共栅电流镜具有抑制沟道长度调制效应的特性，适合用于设计PUF电路的偏差信号产生电路。然后结合基准电流源和共源共栅电流镜设计偏差电压源，并采用偏差电压复用技术，实现所提PUF电路在一组激励下产生多位输出响应的目的。最后在SMIC 65 nm CMOS工艺下对所提PUF电路进行版图设计，并运用Spectre进行计算机仿真验证其性能。

2 电流镜工艺偏差分析

电流镜的主要功能是将输入支路上的电流复制到输出支路上，图1为两种不同类型的电流镜结构，图1(a)为基本电流镜，图1(b)为共源共栅电流镜。图1(a)中连接成二极管形式的晶体管M_1将输入电流转化为内部参考电压V_{in}，这个参考电压同时作用于晶体管M_2的栅极上，在该电压的驱动下M_2漏-源端产生电流，从而实现输入-输出支路上的电流镜像流动。忽略沟道长度调制效应，工作在饱和区的晶体管M_1,M_2的I-V方程可表示为

$$I_{ds1}=\frac{1}{2}\mu_{n1}C_{ox1}(W/L)_1\left(V_{in}-V_{th1}\right)^2=\frac{1}{2}k_{n1}\left(V_{in}-V_{th1}\right)^2 \tag{1}$$



(a)基本电流镜 (b)共源共栅电流镜

图1 两种电流镜结构

$$I_{ds2}=\frac{1}{2}\mu_{n2}C_{ox2}(W/L)_2\left(V_{in}-V_{th2}\right)^2=\frac{1}{2}k_{n2}\left(V_{in}-V_{th2}\right)^2 \tag{2}$$

其中，$k_{n1}=\mu_{n1}C_{ox1}(W/L)_1$和$k_{n2}=\mu_{n2}C_{ox2}(W/L)_2$分别表示$M_1$和$M_2$的增益因子，$\mu_{n1}$和$\mu_{n1}$分别表示$M_1$和$M_2$的电子迁移率，$C_{ox1}$和$C_{ox2}$分别表示$M_1$和$M_2$单位面积栅氧化层电容，$(W/L)_1$和$(W/L)_2$分别表示$M_1$和$M_2$的宽长比，$V_{th1}$和$V_{th2}$分别表示$M_1$和$M_2$的阈值电压。在$M_1$,$M_2$的尺寸完全相同且忽略体效应的情况下，根据式(1)和式(2)可知，流经M_1,M_2的电流I_{ds1},I_{ds2}应该完全相同。但事实上由于工艺偏差的影响，M_1和M_2的上述参数并不相同，使得I_{ds1},I_{ds2}产生偏差，进而造成电流镜输入-输出电流产生偏差。

由式(1)和式(2)可以获得电流镜电流增益偏差[12]与工艺参数偏差的关系。首先讨论M_1,M_2阈值电压V_{th}完全相同，但导电因子k_{n1},k_{n2}存在工艺偏差的情况，此时电流镜电流增益偏差为

$$\varepsilon|_{\Delta k_n}=\frac{I_{ds2}-I_{ds1}}{(I_{ds2}+I_{ds1})/2}=\frac{(V_{in}-V_{th})^2(k_{n2}-k_{n1})}{(V_{in}-V_{th})^2(k_{n2}+k_{n1})/2}=\frac{\Delta k_n}{k_{n\_avg}} \tag{3}$$

$\Delta k_n=k_{n2}-k_{n1}$和$k_{n_avg}=(k_{n2}+k_{n1})/2$分别表示$M_1$,$M_2$的增益因子偏差和增益因子平均值。然后讨论$M_1$,$M_2$的增益因子$k_n$完全相同，但阈值电压$V_{th1}$,$V_{th2}$存在工艺偏差的情况，此时电流镜电流增益偏差为

$$\varepsilon|_{\Delta V_{th}}=\frac{I_{ds2}-I_{ds1}}{(I_{ds2}+I_{ds1})/2}=\frac{k_n\left((V_{in}-V_{th2})^2-(V_{in}-V_{th1})^2\right)}{k_n\left((V_{in}-V_{th2})^2+(V_{in}-V_{th1})^2\right)/2}\approx-\frac{\Delta V_{th}}{(V_{in}-V_{th\_avg})/2} \tag{4}$$

$\Delta V_{th}=V_{th2}-V_{th1}$和$V_{th_avg}=(V_{th2}+V_{th1})/2$分别表示$M_1$,$M_2$的阈值电压偏差和阈值电压的平均值。最后考虑到$M_1$,$M_2$增益因子偏差和阈值电压偏差互不相关，则电流镜电流增益偏差可表示为

$$\varepsilon=\varepsilon|_{\Delta k_n}+\varepsilon|_{\Delta V_{th}}=\frac{\Delta k_n}{k_{n\_avg}}-\frac{\Delta V_{th}}{(V_{in}-V_{th\_avg})/2} \tag{5}$$

以上分析建立在忽略沟道长度调制效应的基础上，事实上由于电流镜输入-输出支路并不完全对称，导致MOS管(M_1和M_2)的漏端电压不同，从而使得输出电流受沟道长度调制效应的影响。这种偏差由电流镜的结构决定，属于系统误差，可通过修

改电路结构加以改善。图 1(b)所示的共源共栅电流镜，是在基本电流镜的基础上增加两个晶体管 M_5, M_6 用于提高电流镜的输出阻抗，从而抑制沟道长度调制效应。

在 SMIC 65 nm CMOS 工艺下，对输入电流为 5 μA、增益系数为 1 的两类电流镜分别进行 50 次蒙特卡洛仿真，*I*-*V* 输出关系如图 2 所示。其中图 2(a)为基本电流镜的 *I*-*V* 输出关系，$V_{\rm ov}$ 为其最小输出电压；图 2(b)为共源共栅电流镜的 *I*-*V* 输出关系，$2V_{\rm ov}+V_{\rm th}$ 为其最小输出电压。由图 2 可知，当输出电压($V_{\rm out}$)大于最小输出电压时，两种电流镜的输出电流($I_{\rm out}$)都围绕输入电流大小($I_{\rm in}$=5 μA)产生了随机偏差，但仅共源共栅电流镜的输出电流不随输出电压的增大而改变。因此采用共源共栅电流镜设计偏差信号产生电路，可增强 PUF 电路的可靠性。

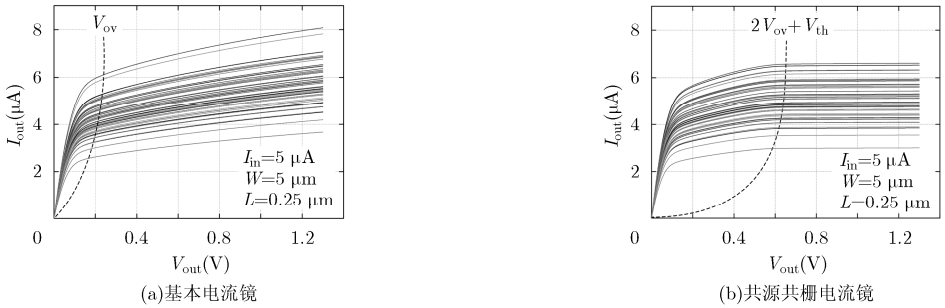
3　PUF 电路设计

由上节分析可知，共源共栅电流镜比基本电流镜具有更大的输出阻抗，可有效抑制沟道长度调制效应。因此，将利用共源共栅电流镜的随机工艺偏差设计 PUF 电路，结构如图 3 所示。该 PUF 电路由输入寄存器、偏差电压源、复用网络、判决器阵列及扰乱模块构成。输入寄存器由 m 个 D 触发器构成，用以保证输入的激励信号同步，避免不同步的激励信号对输出响应的干扰；偏差电压源由 n 个结构和参数完全相同的偏差电压单元(Deviation-voltage Unit, DU)构成，用于产生 n 组偏差电压($V_{\rm b0}$ - $V_{\rm b(n-1)}$, $V_{\rm c0}$ - $V_{\rm c(n-1)}$)；复用网络采用数学排列的方式从 n 个不同的偏差电压中任意选取 2 个偏差电压(C_n^2)，作为判决器阵列的输入信号；判决器阵列由 $2C_n^2$ 个电压比较器(Voltage Comparator, VC)构成，并根据复用网络提供的偏差电压大小产生判决输出；扰乱模块由 C_n^2 个异或门构成，用于扰乱判决器阵列输出值之间的相关性，从而增强防御攻击的能力，扰乱规则为 $R_i = R_{{\rm b}i} \otimes R_{{\rm c}i}$，其中 $R_{{\rm b}i}$,$R_{{\rm c}i}$ 分别表示上、下两路第 i 个判决器的判决输出，R_i 为 PUF 电路第 i 个输出端口的输出响应。

DU 和 VC 是 PUF 电路设计的关键，不仅决定输出响应的唯一性和随机性还影响 PUF 电路的可靠性。DU 由基准电流源($R_{\rm a}$,$\rm P_0$ - $\rm P_3$,$\rm N_0$ - $\rm N_4$)，多路共源共栅电流镜(短虚线框内所示)，开关阵列(S_0 - S_{m-1})和负载电阻($R_{\rm b}$,$R_{\rm c}$)构成。基准电流源用于产生不随温度和电压变化的电流 $i_{\rm REF}$($i_{\rm REF}$=1 μA)，共源共栅电流镜则将基准电流复制到各输出支路上，且各输出支路与基准电流源输出支路参数相同(W/L=120 n/60 n)，则理论上有 $i_{\rm REF}=i_k$(k=0,1,⋯, $m-1$)，然而受工艺参数偏差的影响 i_k 会围绕 $i_{\rm REF}$ 产生随机偏差。受激励信号控制的各输出支路偏差电流之和在电阻 $R_{\rm b}$ 和 $R_{\rm c}$ 上产生分压，从而产生偏差电压 $V_{\rm b}=V_{\rm DD}-R_{\rm b}\sum_{k=0}^{m-1} i_k S_k$ 和 $V_{\rm c}=V_{\rm DD}-R_{\rm c}\sum_{k=0}^{m-1} i_k \overline{S}_k$，$\overline{S}_k$ 表示对 S_k 逻辑取反。VC 由交叉耦合反相器($\rm N_5$-$\rm N_6$,$\rm P_5$-$\rm P_6$)、预充电管($\rm P_7$,$\rm P_8$)、差分电压探测管($\rm N_7$,$\rm N_8$)以及使能管($\rm N_{en}$)构成，其中 en_pre 和 en_sa 为使能信号端。当 en_pre 和 en_sa 为低电平时 VC 处于预充电阶段，此时 $\rm P_7$ 和 $\rm P_8$ 导通、$\rm N_{en}$ 截止，节点 a,b,c,d 被充电至高电平。当 en_pre 和 en_sa 相继变为高电平后 VC 处于求值阶段，此时 $\rm P_7$ 和 $\rm P_8$ 截止、$\rm N_{en}$ 导通，VC 则根据 $V_{\rm n}$ 和 $V_{\rm p}$ 大小产生判决输出。判决规则为当 $V_{\rm p}>V_{\rm n}$ 时 R 输出高电平，反之 R 输出低电平。

4　实验结果与分析

采用 SMIC LP 65 nm mc 工艺库，利用 Spectre 对激励长度为 9 bit 具有 36 个输出端口(m=n=9)的 PUF 电路进行计算机仿真测试，分别验证其输出响应的唯一性、随机性和可靠性。图 4 给出了在 SMIC 65 nm CMOS 工艺下采用全定制方式设计的版图。输入寄存器位于版图的左侧；偏差电压源、复用网络及判决器阵列位于版图中间；扰乱模块位于版图右侧。版图中各单元电路共用电源及地以减小面积。整个版图设计共用到 4 层金属，第 1 层用于单元电



(a)基本电流镜　　(b)共源共栅电流镜

图 2　电流镜 *I*-*V* 输出关系的 Monte Carlo 仿真

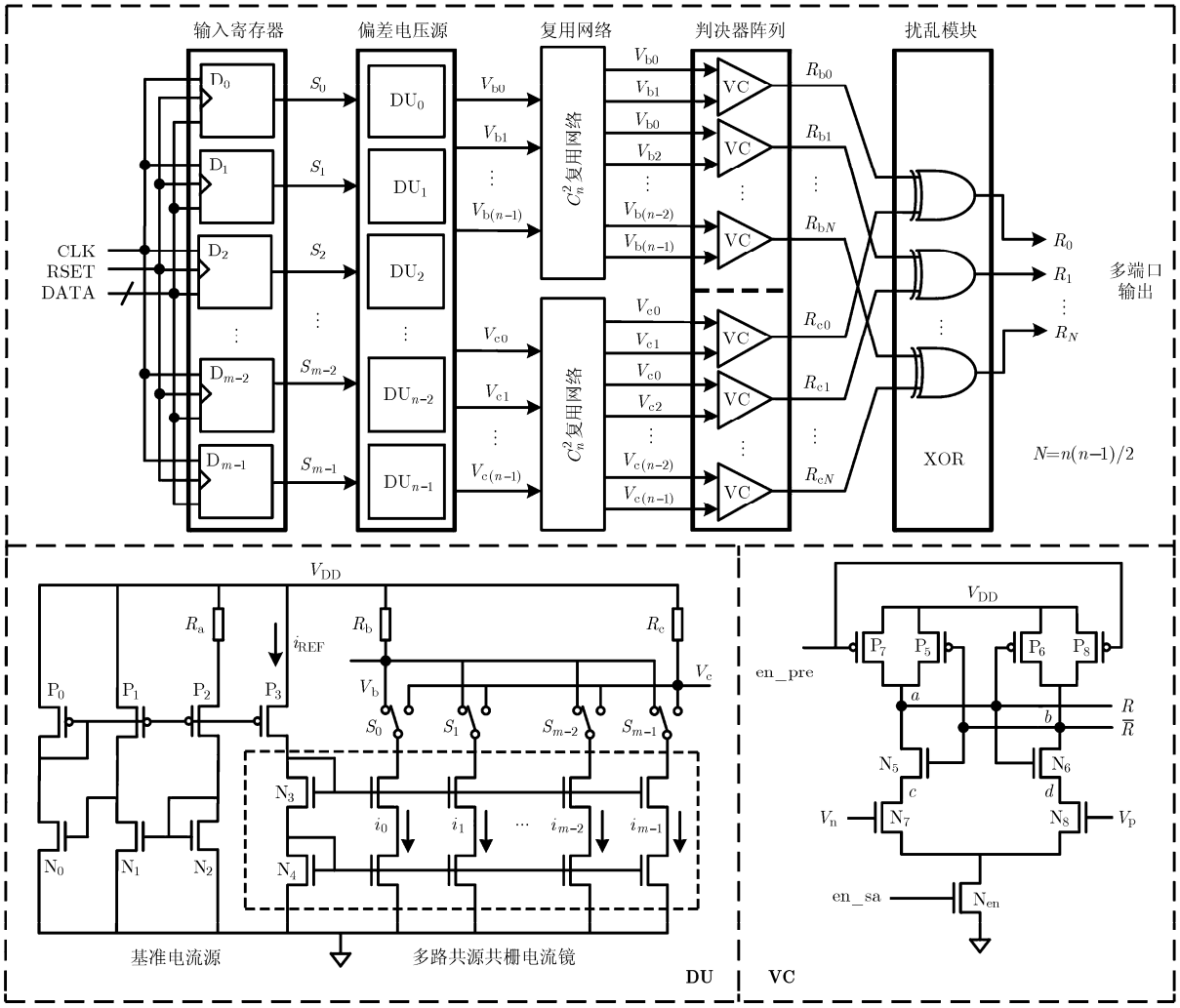


图 3 PUF 电路结构

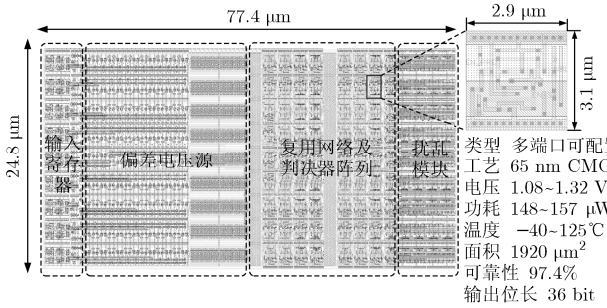


图 4 具有 36 个输出端口的 PUF 电路版图

路电源及内部信号走线、第 2 层用于各单元电路之间信号连接，第 3 层和第 4 层则对复用网络、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 24.8 μm×77.4 μm，其中电压比较器的面积为 2.9 μm×3.1 μm。

4.1 唯一性

唯一性表征同一类型的 PUF 电路的任意个体与其他个体的区分度，即产生唯一标识自身的数字信息的能力。通常采用统计同一类型 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 电路的片间汉明距离 $\mathrm{HD_p}$ 可由式(6)计算[6]：

$$\mathrm{HD_p}=\frac{2}{k(k-1)}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{\mathrm{HD}\left(R_i,R_j\right)}{N} \tag{6}$$

其中，R_i 和 R_j 分别表示第 i 和第 j 个 PUF 电路产生的 N bit 输出响应。则在 w 组不同激励下，k 个 PUF 电路的平均片间汉明距离 $\mathrm{E(HD_p)}$ 可由式(7)计算：

$$\mathrm{E}\left(\mathrm{HD_p}\right)=\frac{1}{w}\sum_{l=1}^{w}\mathrm{HD}_{pl}\times 100\% \tag{7}$$

在同一组激励下对所提 PUF 电路进行 10000 次 Monte Carlo 仿真(k=10000)，继而得到 10000 个长度为 36 bit(N=36)的输出响应。为了实验结果的准确性，选取 9 组(w=9)汉明重量(Hamming Weight, HW)逐次加 1 的激励重复以上实验，记录数据并利用式(7)计算 $\mathrm{E(HD_p)}$ 为 48.6%。

4.2 随机性

随机性表征 PUF 电路输出逻辑 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 的概率相等, 随机性为 100%。PUF 电路输出数据的随机性可通过式(8)计算[6]：

$$\text{随机性}=\left(1-\left|2P(R=1)-1\right|\right)\times 100\% \tag{8}$$

其中，$P(R=1)$ 表示输出数值中逻辑电平 1 的概率。为准确测试所提 PUF 电路输出响应的随机性，选取 9 组 HW 逐次加 1 的激励，在每一组激励下进行 10000 次 Monte Carlo 仿真，统计各输出端口响应中逻辑 1 的概率，并通过式(8)计算随机性，各端口输出响应的随机性随激励 HW 增加的拟合曲线如图 5 所示。由图 5 可知所提 PUF 电路各端口输出数据的随机性均大于 97%。

4.3 可靠性

可靠性作为 PUF 电路重要的性能指标，用于说明 PUF 电路在不同工作环境中的性能。在 M 种不同环境下，PUF 电路的可靠性可通过式(9)衡量[6]。

$$\begin{aligned}\text{可靠性}&=1-\mathrm{E}\left(\mathrm{HD_q}\right)\\&=\left(1-\frac{1}{M}\sum_{i=1}^{M}\frac{\mathrm{HD}\left(R_{\mathrm{r}},R_i\right)}{N}\right)\times 100\%\end{aligned} \tag{9}$$

其中，$\mathrm{E}(\mathrm{HD_q})$ 表示平均片内汉明距离，R_{r} 和 R_i 分别表示工作在理想条件下(1.2 V/25℃) 和第 i 种对比条件下的 N bit 输出响应。首先在 1.2V/25°C 条件下，对电路施加 9 组 HW 逐次加 1 的激励，从而得到 9 组长度为 36 bit 的输出响应，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，在每一种环境下施加与参考响应相同的激励，统计输出响应相对于参考响应改变的位数，并通过式(9)计算可靠性。统计结果如图 6 所示，其中图 6(a)和图 6(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°C)和电压(1.08～1.32 V)下的可靠性均分别高于 97.8%和 97.4%。

所设计的 PUF 电路与其他类型 PUF 电路性能对比如表 1 所示。由表 1 可知，设计的电流型(CM)多端口可配置 PUF 电路功耗相对较高，但单比特面积最小、可靠性最高。

5　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具有唯一性、随机性和不可克隆性的特有密钥。利用电流镜的工艺偏差，提出一种可配置多端口 PUF 电路设计方案，通过激励信号控制电流镜支路的开关，使得无需更换硬件电路便可实现输出密钥的变化，且可在一个时钟周期内产生多位输出数据。在 SMIC 65 nm CMOS 工艺下，采用全定制方法设计具有 36 个输出端口的 PUF 电路版图，面积为 24.8 μm×77.4 μm。与传统采用并联结构的 36 端口 PUF 电路相比，设计的 PUF 电路中偏差电压源面积利用率提高了 87.5%，整体电路面积利用率提高了 71.8%，面积利用率会随偏差电压单元数的增加进一步提高。实验结果表明所设计的多端口

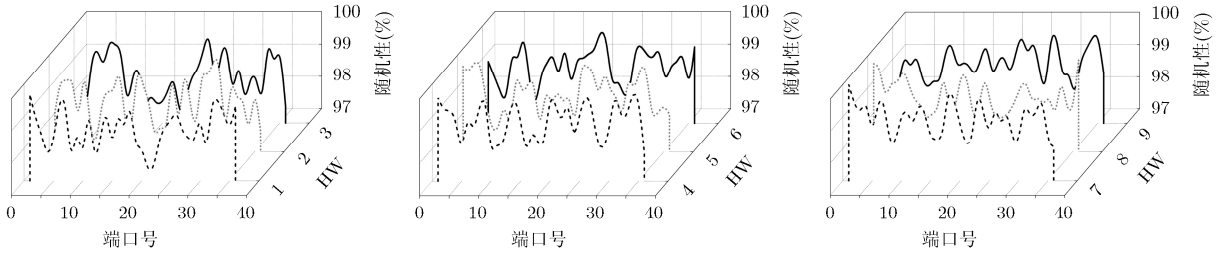


图 5 各端口输出响应的随机性随激励 HW 增加的拟合曲线

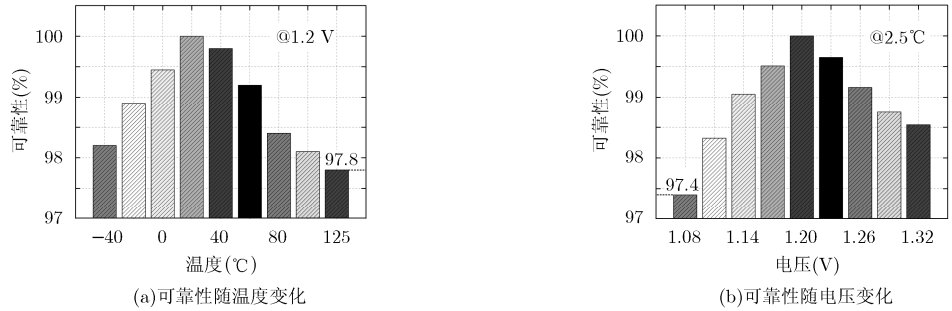


图 6　PUF 电路在不同温度和电压下的可靠性

表 1 不同类型 PUF 电路性能对比

文献	类型	可配置	工艺 (nm)	功耗 (μW)	单比特面积 (μm^2)	温度范围 (°C)	电压波动 (%)	可靠性 (%)
TVLSI 2016[11]	Arbiter-PUF	Y	180	380.0	21750	−40~100	6.0	96.8
JSSC 2008[10]	SRAM-PUF	N	130	1.6	119	0~100	15.0	96.0
TCAD 2015[13]	RO-PUF	Y	65	32.3	250	−40~120	2.5	97.3
VLSI 2011[14]	CM-PUF	Y	90	788.0	1110	−40~120	10.0	97.0
HOST 2013[15]	CM-PUF	Y	45	108.0	16000	−55~125	10.0	95.9
HOST 2014[16]	CM-PUF	Y	30	12.3	875	0~75	9.0	96.0
本文	CM-PUF	Y	65	152.0	53	−40~125	10.0	97.4

PUF 电路在不降低安全性能的前提下增加了可配置功能，且在不同工作环境下可靠性达到 97.4%以上，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 and GOUDAR V. Public physical unclonable functions[J]. *Proceedings of the IEEE*, 2014, 102(8): 1142–1156. doi: 10.1109/JPROC.2014.2331553.

[2] HERDER C, YU M D, KOUSHANFA F, *et al.* Physical unclonable functions and Applications: a tutorial[J]. *Proceedings of the IEEE*, 2014, 102(8): 1126–1141. doi: 10.1109/JPROC.2014.2320516.

[3] PAPPU R, RECHT R, TAYLOR J, *et al.* Physical one-way function[J]. *Science*, 2002, 297(5589): 2026–2030.

[4] 项群良, 张培勇, 欧阳冬生, 等. 多频率段物理不可克隆函数[J]. 电子与信息学报, 2012, 34(8): 2007–2012. doi: 10.3724/SP.J.1146.2011.01249.
XIANG Qunliang, ZHANG Peiyong, OUYANG Dongsheng, *et al.* Multiple frequency slots based physical unclonable functions[J]. *Journal of Electronics & Information Technology*, 2012, 34(8): 2007–2012. doi: 10.3724/SP.J.1146.2011.01249.

[5] MATHEW S K, SATPATHY S K, ANDERS M A, *et al.* A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS[C]. IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), San Francisco, 2014: 278–279.

[6] LAO Y J and 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. doi: 10.1109/TCAD.2013.2296525.

[7] SUH G E and DEVADAS S. Physical unclonable functions for device authentication and secret key generation[C]. Proceedings of the Design Automation Conference, San Francisco, 2007: 9–14.

[8] GUAJARDO J, KUMAR S S, and CHRIJEN G J. FPGA intrinsic PUF and their use for IP protection[C]. Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, Vienna, 2007: 63–80.

[9] 汪鹏君, 张跃军, 张学龙. 防御差分功耗分析攻击技术研究[J]. 电子与信息学报, 2012, 34(11): 2774–2784. doi: 10.3724/SP.J.1146.2012.00555.
WANG Pengjun, ZHANG Yuejun, and ZHANG Xuelong. Research of differential power analysis countermeasures[J]. *Journal of Electronics & Information Technology*, 2012, 34(11): 2774–2784. doi: 10.3724/SP.J.1146.2012.00555.

[10] YING S, HOLLEMAN J, and 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. doi: 10.1109/JSSC.2007.910961.

[11] BAI C, ZOU X, and 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. doi: 10.1109/TVLSI.2015.2398454.

[12] 池保勇. 模拟集成电路与系统[M]. 北京: 清华大学出版社, 2009: 186–189.
CHI Baoyong. Analog Integrated Circuits and Systems[M]. Beijing: Tsinghua University Press, 2009: 186–189.

[13] 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. doi: 10.1109/TCAD.2015.2424955.

[14] GANTA D, VIVEKRAJA V, PRIYA K, *et al.* A highly stable leakage-based silicon physical unclonable functions[C]. IEEE International Conference on VLSI Design, Madras, 2011: 135–140.

[15] KALYANARAMAN M and ORSHANSKY M. Novel strong PUF based on nonlinearity of MOSFET subthreshold operation[C]. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, 2013: 13–18.

[16] KUMAR R and BURLESON W. On design of a highly secure PUF based on non-linear current mirrors[C]. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Washington, 2014: 38–43.

李 刚： 男，1988 年生，博士生，研究方向为密码芯片攻击和防御理论及其VLSI 实现.

汪鹏君： 男，1966 年生，教授，博士生导师，研究方向为低功、高信息密度集成电路理论和设计技术、电路设计综合和优化技术、安全芯片理论和设计技术等.

张跃军： 男，1982 年生，讲师，博士，研究方向为密码芯片攻击和防御理论及其VLSI 实现、多值逻辑电路理论和设计技术.

钱浩宇： 男，1991 年生，硕士生，研究方向为密码芯片攻击和防御理论及其VLSI 实现.