基于数据残留时间的SRAM-PUF预选算法

陈泽亮[1],孔德珠[2],尹爱国[2],陈泽福[2],张培勇[1*]
(1. 浙江大学微纳电子学院,浙江杭州 310000;2. 珠海奔图电子有限公司,广东珠海 519000)

摘 要: 静态随机存取存储器(Static Random-Access Memory,SRAM)物理不可克隆函数(Physical Unclonable Function,PUF)利用参数设计完全相同的晶体管在制造过程中存在的工艺偏差,生成每块芯片无法克隆的密钥响应.由于SRAM-PUF内部错误分布的随机性,密钥重构需要使用纠错码,而纠错电路的面积与其纠错能力呈正相关,为了降低SRAM-PUF错误分布,减小纠错电路面积,本文通过对SRAM数据残留特性的研究,提出一种数据残留预选算法,对SRAM单元进行筛选,提高PUF响应稳定性,使用区块择优算法筛选SRAM区块,减小响应的分散度,以更短的时间和资源消耗生成SRAM-PUF响应,测试结果表明,在不同温度(–40 ℃~80 ℃)和±10%电压波动下,256位SRAM-PUF响应拥有99.8%的稳定性及1.9×10^{-8}的误码率,相对于通用的临时多数表决(Temporal Majority Voting,TMV)算法提升了1.7%的稳定性,降低2.1×10^{5}倍误码率,与1 000次TMV相比,时间复杂度从$O(2\,000n)$线性降低到$O(900n)$.经过72小时老化测试后,采用数据残留算法预选的SRAM-PUF稳定性仅下降0.2%.

关键词: 物理不可克隆函数;SRAM;预选算法;数据残留;临时多数表决
基金项目: 国家重点研发计划(No.2021YFB2206200)
中图分类号: TN4 **文献标识码:** A **文章编号:** 0372-2112(2024)05-1478-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20221413

SRAM-PUF Preselection Algorithm Based on Data Remanence Time

CHEN Ze-liang[1], KONG De-zhu[2], YIN Ai-guo[2], CHEN Ze-fu[2], ZHANG Pei-yong[1*]
(1. *School of Micro-Nano Electronics, ZheJiang University, Hangzhou, Zhejiang* 310000, *China*;
2. *Zhuhai Bentu Electronics Co., Ltd, Zhuhai, Guangdong* 519000, *China*)

Abstract: Static random-access memory (SRAM) physical unclonable function (PUF) makes use of the process deviation in the manufacturing process of transistors with identical parameter design, which generates the key response that cannot be cloned for each chip. Due to the randomness of SRAM-PUF internal error distribution, key reconstruction requires the use of error correction codes, and the area of error correction circuits is positively related to its error correction capability. In order to reduce the error distribution of SRAM-PUF and reduce the area of error correction circuits,this paper proposes a data remanence preselection algorithm through the research on characteristics of SRAM data remanence, screening SRAM cells, improving the stability of PUF response, and screening SRAM blocks using block optimization algorithm, reduce the dispersion of the response, which generates SRAM PUF response in a shorter time and resource consumption. Experimental results show that 256 bits SRAM-PUF response has 99.8% stability and 1.9×10^{-8} bit error rate under different temperatures (–40 ℃~80 ℃) and ±10% voltage fluctuations. Compared with the general temporary majority voting (TMV) algorithm, the stability is improved by 1.7% and the error rate is reduced by 2.1×10^{5} times, compared with 1 000 times of TMV, linear reduction of time complexity from $O(2\,000n)$ to $O(900n)$. After 72 hours of aging testing, the stability of the SRAM-PUF pre-selected using the data remanence algorithm only decreased by 0.2%.

Key words: physically unclonable function; sram; preselection algorithm; data remanence; temporary majority voting
Foundation Item(s): National Key Research and Development Program of China (No.2021YFB2206200)

收稿日期:2022-12-21;修回日期:2023-03-31;责任编辑:孙瑶
*通讯作者:张培勇

1 引言

随着半导体技术的发展,芯片安全成为了一个至关重要的问题,在提升芯片安全的同时保证面积以及功耗的平衡,需要做出相应的取舍. 传统的密钥管理方案在出厂前将密钥存在非易失性存储器中(Non-Voltatile Memory, NVM),例如 EFLASH 和 EEPROM 等. 然而传统的密钥存储方案存在弊端,容易受到物理攻击,如探针攻击而造成密钥的泄露. 为防止此类物理攻击,需在物理上加入成本较高的防护层,这对低成本嵌入式设备来说非常不友好. 因此,在低成本嵌入式设备中,权衡芯片安全以及芯片成本成为了研究的重点.

物理不可克隆函数(Physical Unclonable Function, PUF)目前作为芯片安全的一种可靠解决方案,依靠制造过程中每一个器件存在的差异,使得每一块芯片都是独一无二的,根据差异性提取出来的密钥具有很好的随机性.

目前流行的PUF结构主要有 A-PUF[1]、RO-PUF[2]、蝶形 PUF[3]、电流镜 PUF[4]、SRAM-PUF 等. SRAM-PUF 由 Guajardo 等人[5]提出,静态随机存取存储器(Static Random-Access Memory, SRAM)由于其自身天然的随机性,不需要额外的PUF硬件电路生成熵源,近年来成为国内外研究的热门,已经将SRAM-PUF商用的公司有 Intrinsic ID公司[6]、Verayo公司[7]等.

SRAM作为PUF,其单元本身由于工艺的误差,有"0"和"1"两个不定的初始状态,且SRAM作为嵌入式系统中的标准器件,无需像其他类型的PUF一样增加额外的电路. 然而一些SRAM单元上电时受到环境如温度、电压的影响无法生成稳定的响应. 虽然纠错电路(Error Checking and Correction, ECC)和模糊提取(Fuzzy Extractor, FE)[8]算法能够在一定程度上纠正错误的SRAM-PUF响应,但随着纠错能力的增加,这些处理开销也随之增大. 因此,提高SRAM-PUF的可靠性以保持尽可能低的错误率是非常重要的.

近年来提出了许多提高SRAM-PUF稳定性的方案,这些方案大致分为两类:

(1)对原有SRAM结构进行调整,使得SRAM单元从制造出厂就具有非常强的偏向性,从源头提高其稳定性.

(2)对SRAM某方面特性进行分析,使用特定的预选算法对制造出来的SRAM进行预选,仅使用预选的稳定点作为PUF密钥.

文献[9]利用SRAM单元上电坡度的特性,提出了一种SRAM上电坡度预选算法,在SRAM两端(VDD和VSS)实现快速坡度上电,选出两次操作SRAM上电结果相同的单元作为PUF响应,虽然算法的复杂度很低,但此上电方式对于芯片来说会转化成额外的硬件资源,其次这种上电方式对外界噪声、器件老化等因素非常敏感,导致PUF性能并不优越. 文献[10]利用SRAM跳闸电压特性,提出了一种SRAM最大跳闸电压预选算法,比如考虑两个SRAM单元(1和2)具有强烈的"0"倾向性,但强度不同,将数据"1"写入两个单元,然后逐渐降低VDD电压,直到某一个单元翻转到"0",若单元1在VDD_1翻转,单元2在VDD_2翻转且$VDD_1>VDD_2$,说明单元1有更强的"0"倾向,在SRAM阵列中找到那些降低VDD程度最小就翻转的单元作为预选单元. 然而此方案对电源颗粒度提出了较高的要求,根据电源分级颗粒度决定其算法复杂度. 文献[11,12]通过对SRAM的VSS和VDD端施加正向、反向共两次电压激励,记录两次激励后SRAM单元倾向,若两次电压激励SRAM单元倾向一致,则认为其为稳定的单元. 然而此方案需要找到合适的电压激励阈值,过大会导致所有SRAM单元偏向"1"或"0",过小则无法定位稳定单元位置. 同样,文献[13]通过在SRAM单元内部节点加入偏置电容,施加内部激励,文献[14]在SRAM内部对称节点两端注入高低电压差,两者都对电压激励阈值提出了较高的要求.

目前较通用的算法为临时多数表决(Temporal Majority Voting, TMV)算法,其在文献[15~17]中被提出. 该算法的核心思想是对每个SRAM单元的上电启动值进行多次评估,进行多数投票表决,在此过程中必须选择固定数量的测量值,例如1 000次评估,选择表决之后仍具有强烈偏向性的单元作为PUF响应,TMV1000的算法复杂度为$O(2\,000n)$. 但是许多在前1 000次评估中有相同偏向的单元在后续的评估中出现了相反的偏向性,用TMV预选算法需要大量的评估次数和相关数据,消耗较长的时间以及资源.

为了克服以上算法的缺点,本文提出了一种基于数据残留的预选算法,仅需两次实验测试即可找到SRAM阵列中具有强偏向性的稳定单元,与文献[9~14]相比,不需要对电源有较高的要求,降低了测试的复杂度,与文献[15~17]相比,不需要大量的测试,减少了测试时间,将算法复杂度降低到$O(900n)$. 最后的实验结果证明,本文的预选算法能够在不同外界电压、温度的影响下还能保持99.8%的稳定性.

2 SRAM数据残留特性

2.1 SRAM数据残留特性

SRAM单元上电电平取决于图1中PMOS管阈值电压差$\left|V_{\mathrm{th,P_1}}-V_{\mathrm{th,P_2}}\right|$. 当由于工艺误差或者环境影响导致$\left|V_{\mathrm{th,P_1}}\right|>\left|V_{\mathrm{th,P_2}}\right|$,在SRAM单元通电阶段,$P_2$先开始导通,

使得QB的电压位于高电平，同时阻止P_1管的开启．因此Q点的电压为低电平，此SRAM单元的上电值为“0”．因此$\left|V_{\mathrm{th,P_1}}-V_{\mathrm{th,P_2}}\right|$越大，单元趋于某一个电平的优先级就越高．

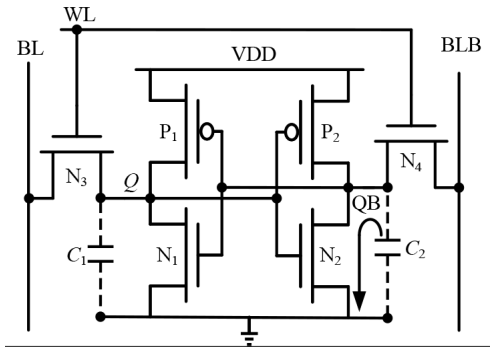


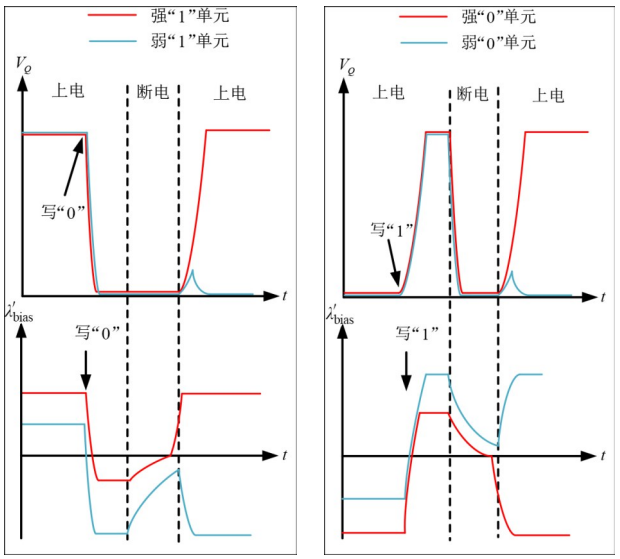
图1 6T-SRAM单元结构

假设SRAM单元Q点电压为“1”，寄生电容C_1充电到高电平，N_2处于线性区，在电场的作用下电子在栅极聚集形成反型层，反型层下面是由固定的负空间电荷构成的耗尽区．当断电时作用于N_2的外电场瞬间消失，在N_2栅极表面的电子仅能通过载流子扩散运动和衬底中的空穴复合，在复合过程中，电子和耗尽区中的固定的负空间电荷会吸引正电荷并将其存储于C_1之内，直到电子复合完、耗尽区消失，衬底中载流子达到新的动态平衡之后，残留在电容中的数据才算消散．因此影响SRAM数据残留时间长短的主要因素是载流子的输运时间，而影响载流子输运速率的主要因素是环境温度．

根据以上结论，式(1)为SRAM单元偏向性强度变量λ'_{bias}(正数代表偏“1”，负数代表偏“0”，绝对值大小代表偏向性强度)、由电容电荷C_q造成的对SRAM单元偏向性强度影响的变量λ_{bias1}、由P管阈值电压差ΔV_{th}对强度影响的变量λ_{bias2}三者的关系式．其中η代表环境如电压、温度、噪声以及工艺对变量的影响，t表示时间．变量C_q、ΔV_{th}的大小与时间t成反比，即λ_{bias1}和λ_{bias2}与时间成反比，C_q变化的时间量级为毫秒或秒，即载流子复合时间，ΔV_{th}变化的时间量级为天，即由晶体管老化带来的影响，因此在控制环境变量相同的情况下，在电荷残留时间内可以忽略老化带来的对λ'_{bias}的微小影响，此时λ_{bias2}是常量．

$$\lambda'_{\mathrm{bias}}(t,\eta)=\lambda_{\mathrm{bias1}}(C_q(t,\eta))+\lambda_{\mathrm{bias2}}(\Delta V_{\mathrm{th}}(t,\eta)) \quad (1)$$

如图2(*a*)所示，上下两图分别是Q点的电压、SRAM单元偏向性强度λ'_{bias}和时间的关系．“1”偏向性的SRAM单元分为强偏向性单元和弱偏向性单元，强偏向性单元λ'_{bias}大于弱偏向性单元，在上电阶段将“0”写入SRAM，λ'_{bias}降为负，之后断电，由于λ_{bias1}和时间的负相关性，λ'_{bias}偏“0”强度减弱，之后再次上电，强SRAM单元λ_{bias2}强度大于弱SRAM单元，因此造成最终的偏向，强SRAM单元偏至“1”，弱SRAM单元偏至“0”，所以具有强偏向性的SRAM单元抗噪声干扰能力强、稳定性高，重复上电可取得同一上电值，正适合作为SRAM-PUF响应位，反之弱偏向性的SRAM单元抗噪声能力弱，稳定性差，重复上电无法取得同一上电值，无法作为SRAM-PUF响应位．图2(*b*)同理，偏向性强的SRAM单元会以更少的断电时间恢复到“1”，因此可以用数据残留时间长短来评估SRAM单元偏向性强度．



(*a*) 偏“1”单元识别 (*b*) 偏“0”单元识别

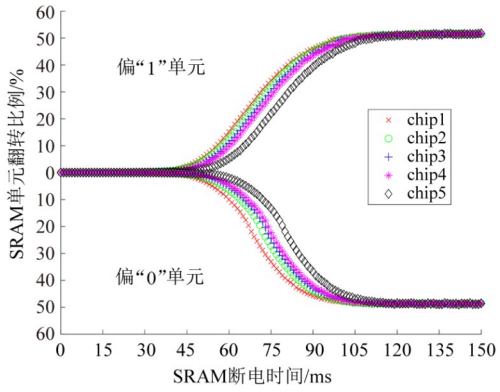
图2 SRAM偏向性单元识别

2.2 数据残留预选算法

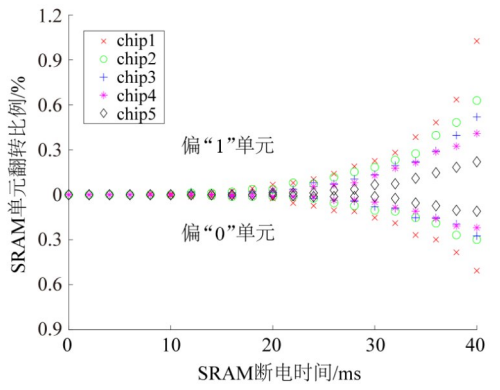
为了验证上述数据残留特性对SRAM单元偏向性的影响，使用型号为CY7C199-15PC的SRAM进行测试，每块芯片包含256K个SRAM单元．首先需要确定合适的断电时间，如果断电时间太短会导致SRAM残留电荷造成的偏向性强度λ_{bias1}大于所有SRAM单元自身偏向强度λ_{bias2}，如果断电时间太长，SRAM单元中的残留电荷将彻底放完电，λ_{bias1}降低到0就无法评估自身强度λ_{bias2}．对SRAM阵列全写“1”或“0”之后断电一段时间再上电读取SRAM阵列的数据，计算此时阵列中“0”或“1”的比例．

图3在标准VDD、室温25 ℃下对5块同一类型的芯片断电时间从0~150 ms进行扫描，并计算写0和1两类测试中SRAM单元的翻转比例．图3(*a*)断电时间为0~150 ms、扫描间隔为1 ms，为了更好地观察细节，图3(*b*)为图3(*a*)的细节图，断电时间0~40 ms、扫描间隔2 ms．每张图分为上下两部分，上部为偏“1”单元写“0”断电时间与翻转比例曲线，下部为偏“0”单元写“1”

断电时间与翻转比例曲线.



(*a*) 1 ms扫描间隔



(*b*) 2 ms扫描间隔

图3　全写“1”或“0”时SRAM单元翻转比例

写“0”和“1”时,偏向性强度最大的SRAM单元在断电约30 ms开始翻转,当断电时间增加到105 ms时,翻转比例达到50%,此时偏向性强度最小的SRAM单元基本翻转. SRAM单元的翻转比例随断电时间的增加而增加,同一种SRAM芯片的“0”和“1”数据残留时间曲线基本一致,波动范围在±5 ms之内,这也为采用本算法提供了很好的事实依据:同一类SRAM芯片或者说同一工艺下的SRAM整体的数据残留特性基本一致,也就说只要在此种工艺下首先进行一次数据残留时间的全面扫描得到断电时间曲线,即可大幅减少后续其他所有芯片的扫描时间,可以更快找到强偏向性的SRAM单元.

虽然基于数据残留时间的SRAM预选算法需要在每次断电之前写入SRAM单元“0”或“1”,但与清除SRAM单元数据残留所需要的时间相比,将数据写入SRAM所需要的时间可以忽略不计,只需要两类测试,全写“0”的测试用于筛选强偏向性的“1”单元,全写“1”的测试用于筛选强偏向性的“0”单元,在两次测试之间需要等待大约120 ms,这个时间是所有SRAM单元残留电荷释放所需要的时间.

用数据残留时间长短对SRAM单元偏向性进行评估,本文提出了数据残留预选算法. 根据数据残留时间、PUF长度以及断电扫描时间进行单元预选,伪代码如算法1所示,算法的复杂度以及函数说明如表1所示.

算法1　数据残留预选算法

输入:SRAM-PUF长度L,SRAM单元数据量N,扫描时间间隔Δt,扫描总时长T

输出:SRAM预选位置$\mathrm{Idx}=(n_1,n_2,\cdots,n_L)$,PUF响应$\mathrm{Rps}=(r_1,r_2,\cdots,r_L)$

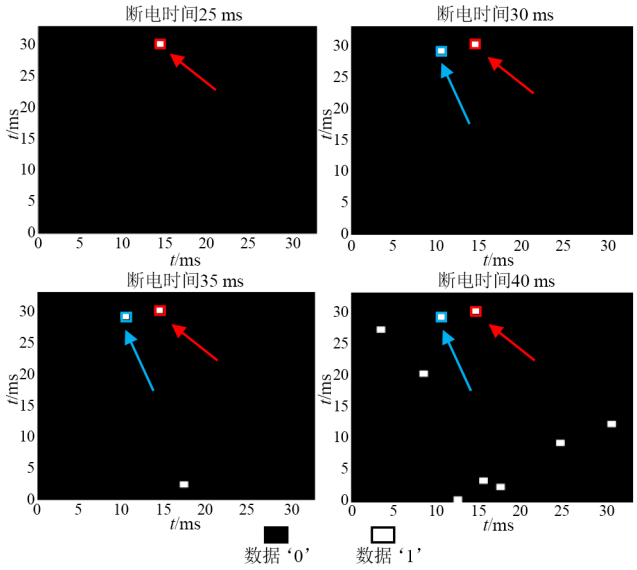
1. $\mathrm{Array}=\left[N\times\frac{T}{\Delta t}\times 2\right]$
2. FOR $w\leftarrow 1$ to 2
3. FOR $t\leftarrow 1$ to T by Δt
4. FOR $n\leftarrow 1$ to N
5. $\mathrm{Array}[n,t,w]=\mathrm{Get\_Val}(\cdot)$
6. FOR $t\leftarrow 1$ to T by Δt
7. $[\mathrm{num},\mathrm{Idx}_1]=\mathrm{Calculate\_Flip}\left(\mathrm{Array}\left((1,2,\cdots,N),t,1\right),0\right)$
8. IF num $\geqslant L/2$
9. BREAK
10. FOR $t\leftarrow 1$ to T by Δt
11. $[\mathrm{num},\mathrm{Idx}_2]=\mathrm{Calculate\_Flip}\left(\mathrm{Array}\left((1,2,\cdots,N),t,2\right),1\right)$
12. IF num $\geqslant L/2$
13. BREAK
14. $\mathrm{Idx}=\mathrm{Timsort}\left(\mathrm{Idx}_1\left[(1,2,\cdots,L)/2\right],\mathrm{Idx}_2\left[(1,2,\cdots,L)/2\right]\right)$
15. $\mathrm{Rps}=\mathrm{Array}[\mathrm{Idx}]$

表1　算法1复杂度计算

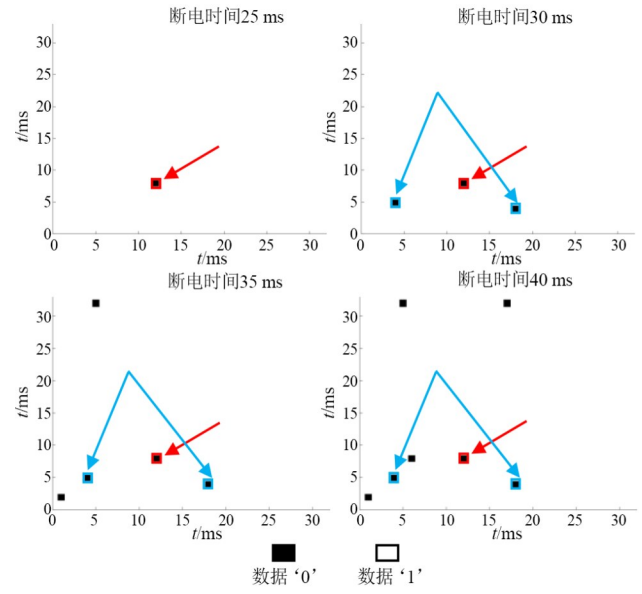
行号	复杂度	描述
1	$O(1)$	声明写“0”和“1”SRAM断电扫描数据存储矩阵
2~5	$O\left(2\times\frac{T}{\Delta t}\times N\right)$	Get_Val(·)获取当前断电时间此单元上电值
6~13	$O\left(4\times\frac{T}{\Delta t}\times N\right)$	Calculate_Flip(·)得到SRAM阵列中的“0”或“1”数量,返回对应位置
14	$O(L\log L)$	Timsort排序算法,将预选的SRAM单元下标升序排列
15	$O(L)$	从SRAM阵列中根据Idx生成PUF响应
总计	$O(1)+O\left(6\times\frac{T}{\Delta t}\times N\right)+O(L\log L)+O(L)=O\left(6\times\frac{T}{\Delta t}\times N+L\log L\right)$	

可以看出算法的复杂度跟PUF长度、SRAM阵列大小以及断电扫描频率呈正相关.

图4显示了1K个SRAM单元在不同断电时间下的翻转情况,SRAM单元上电值用黑白两种颜色表示,黑色表示数据“0”,白色表示数据“1”.



(a) 偏“1”单元在不同断电时间下翻转图



(b) 偏“0”单元在不同断电时间下翻转图

图4 1K个SRAM单元强偏向性单元翻转情况

图4(a)表示偏“1”单元在不同断电时间下的数据翻转情况,可以看到其中在较短断电时间内翻转的单元在之后更长时间的断电测试中始终处于翻转状态,如图中红色方框标明的最强“1”单元,蓝色方框表明的次强“1”单元. 将全“0”写入整片SRAM,然后关闭电源,设置断电时间,使得由于电荷残留带来的偏向性强度影响λ_{bias1}随时间衰减,当断电时间为25 ms时,1K个SRAM单元中第一个偏“1”单元诞生,此单元就是这1K个SRAM阵列空间内偏向性强度λ_{bias2}最大的单元. 当断电时间进一步增加时,会产生更多的偏“1”单元,这些单元出现的时间先后顺序跟λ_{bias2}成反比,先翻转的单元λ_{bias2}大,偏向性强. 也就是说,一旦确定了固定的断电时间和SRAM-PUF响应长度,即可找到SRAM阵列内偏向性强度最大的单元. 同样偏向“0”强度最大的单元也可以通过写全“1”,之后筛出断电时间最短翻转的SRAM单元,如图4(b)所示.

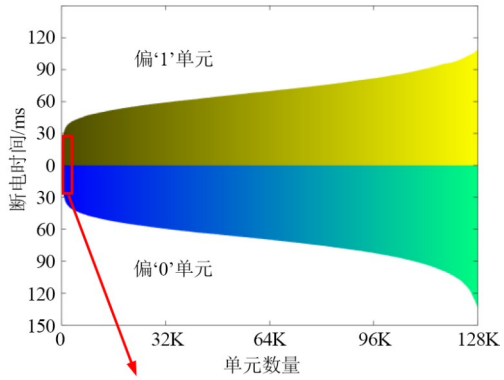
为了生成固定长度如64位、128位、256位的密钥,每一类密钥长度都存在一个断电时间与之对应,例如生成256位密钥需要128位“0”和“1”,对SRAM阵列进行两次写“1”和写“0”的扫描,直到要求数量的偏向性单元出现翻转,此刻的断电时间即为产生256位密钥所需要的时间.

对256K个的SRAM单元扫描并收集数据,根据每个单元的断电时间进行降序排列如图5所示,并使用算法1生成PUF响应,断电时间越短SRAM单元偏向性越强,其在多次上电评估中保持一致性的可能越大. 图5展示了使用256K个SRAM单元生成64位、128位、256位PUF密钥所需的断电脉冲时间,选取了256K个单元中偏向性最强的单元作为SRAM-PUF响应. 图5(a)和(b)分别代表128K偏“1”单元、偏“0”单元的数据残留时间,坐标轴最左边的单元具有最强的偏向性,改变断电时间即可得到对应长度的PUF响应. SRAM偏“1”和偏“0”单元并不完全对称,因此生成PUF响应所需的断电时间得同时满足两个扫描序列,例如生成256位PUF,产生64位偏“1”单元所需时间为22 ms,产生64位偏“0”单元所需时间为21 ms,则取较大断电时间22 ms作为PUF响应生成所需时间,然后记录下这些翻转单元的位置,将其作为重新提取PUF响应的来源. 同样可以得到64位、128位PUF响应生成所需要的断电脉冲为13 ms和18 ms.

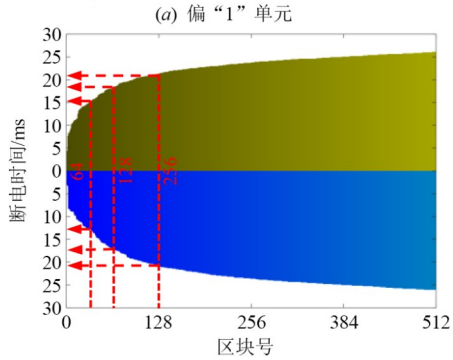
图6是选取的2K个SRAM单元在1 000次上电评估中稳定性,白色代表其在1 000次评估中始终保持稳定,颜色越深代表其变化的次数越多,可以看出其偏向性单元的分布具有随机性. 在1 000次上电评估中保持稳定的SRAM单元占比为74.7%,其对应的断电时间为69 ms,即断电时间小于69 ms的SRAM单元在1 000次上电评估中保持稳定.

2.3 区块择优算法

在实际应用中,由于生成PUF响应的SRAM单元分布的随机性,因此存储这些SRAM单元的位置是一个比较大的开销. 为了解决这个问题,本文提出了SRAM



(*a*) 偏“1”单元



(*b*) 偏“0”单元

图5　256K个SRAM单元数据残留时间降序排列

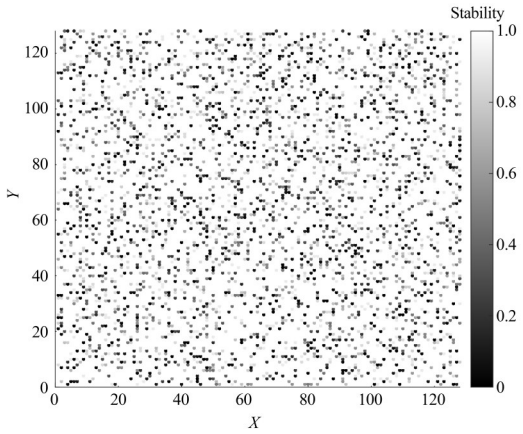


图6　2K个SRAM单元稳定性分布

区块择优算法,挑选出具有强偏向性SRAM单元最多的区块,减小响应的分散度,如此只需要记录区块号以及块内SRAM单元的偏移,可以大幅降低存储开销. 将SRAM根据所需PUF响应长度进行区块大小划分,64位、128位、256位PUF响应对应的SRAM区块大小分别为128位、256位、512位. 算法具体步骤如算法2所示,复杂度计算如表2所示.

算法2　区块择优算法

输入:SRAM-PUF长度L,SRAM单元数据量N,扫描时间间隔Δt,扫描总时长T

输出:SRAM预选区块号Addr,PUF响应Rps$=(r_1, r_2, \cdots, r_L)$,块内预选点Idx$=(r_1, r_2, \cdots, r_L)$

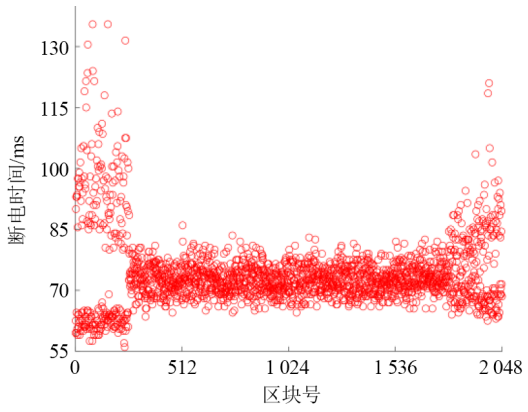
1. Array$=\left[N\times\frac{T}{\Delta t}\times 2\right]$
2. FOR $w\leftarrow 1$ to 2
3. FOR $t\leftarrow 1$ to T by Δt
4. FOR $n\leftarrow 1$ to N
5. Array$[n, t, w]$=Get_Val(·)
6. FOR $t\leftarrow 1$ to T by Δt
7. FOR block$\leftarrow 1$ to $N/2L$
8. $[\text{num}_1, \text{Idx}_1]$=Calculate_BlockFlip(Array(block, t, 1), 0)
9. $[\text{num}_2, \text{Idx}_2]$=Calculate_BlockFlip(Array(block, t, 2), 1)
10. IF $\text{num}_1\geqslant L/2$ and $\text{num}_2\geqslant L/2$
11. BREAK
12. Idx=Timsort([$\text{Idx}_1[1, 2, \cdots, L/2]$, $\text{Idx}_2[1, 2, \cdots, L/2]$])
13. Rps=Array[Idx]
14. Addr=block

可以看出区块择优算法是数据残留预选算法的变式,在据残留预选算法的基础上进行区块的预选,在区块内进行强偏性SRAM单元的预选. 两者的算法复杂度一致,区块择优算法降低了预选单元的分散度,降低了存储空间要求. 在本文测试中,参数$T=150$,$\Delta t=1$,$N=256\text{K}$,$L=64, 128, 256$,算法复杂度为$O(900n)$,相比于TMV1000复杂度降低55%.

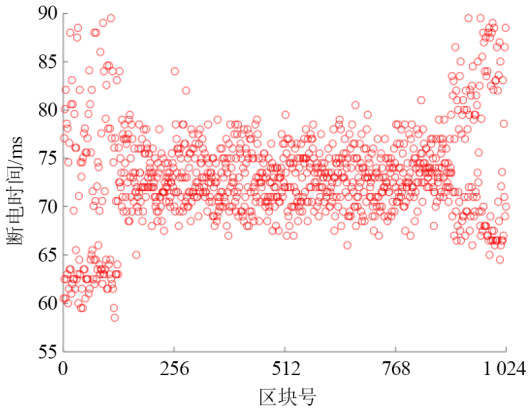
图7是3种PUF长度对应的各个区块产生对应PUF

表2　算法2复杂度计算

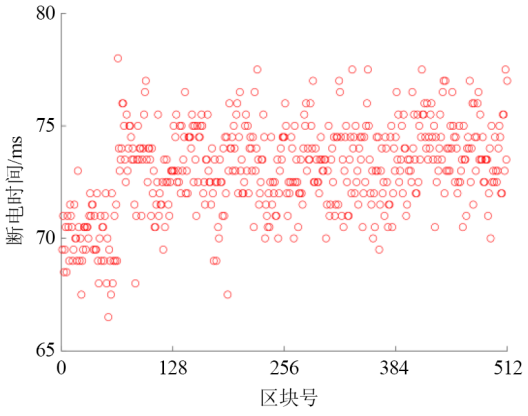
行号	复杂度	描述
1	$O(1)$	声明写“0”和“1”SRAM断电扫描数据存储矩阵
2~5	$O\left(2\times\frac{T}{\Delta t}\times N\right)$	Get_Val(·)获取当前断电时间此单元上电值
6~11	$O\left(4\times\frac{T}{\Delta t}\times N\right)$	Calculate_BlockFlip(·)根据区块号返回区块中“0”或“1”数量,返回对应位置
12	$O(L\log L)$	Timsort排序算法,将预选的SRAM单元下标升序排列
13	$O(L)$	从SRAM阵列中根据Idx生成PUF响应
14	$O(1)$	生成区块号
总计	$O(2)+O\left(6\times\frac{T}{\Delta t}\times N\right)+O(L\log L)+O(L)=O\left(6\times\frac{T}{\Delta t}\times N+L\log L\right)$	



(a) 64位PUF响应



(b) 128位PUF响应



(c) 256位PUF响应

图7 不同区块生成不同长度PUF响应所需的断电时间

响应所需要的数据断电时间,在使用256K个SRAM单元进行测试的情况下,3类PUF响应对应的区块数量分别为2 048、1 024、512块. 对每一个区块的断电时间进行扫描,直到有足够的SRAM偏向性单元构成对应长度的PUF响应. 图7(*a*)为64位PUF响应下,各个区块生成64位SRAM-PUF响应所需要的断电时间,其最小断电时间为56 ms,区块号为237;图7(*b*)为128位PUF响应,其对应的最小断电时间为58 ms,对应的区块号为119;图7(*c*)为256位PUF响应,其对应的最小断电时间为66 ms,对应的区块号为54.

可以根据所需要的SRAM-PUF响应长度来选择不同的断电时间,挑选出强偏向性SRAM单元最多的区块,同样也是基于两次测试:写"0"和写"1". 利用算法2计算对应PUF长度下的区块号以及响应,在每次断电后再次上电计算每一个区块出现的偏向性单元数量,直到有某个区块中的"0"和"1"偏向性单元数量到SRAM-PUF响应长度,此时这个区块即是当前SRAM-PUF长度下偏向性最强的区块,区块内的偏向性SRAM单元即为PUF响应序列.

3 SRAM-PUF测试结果

本节展示详细的测量结果,验证数据残留预选算法、区块择优算法预选的SRAM-PUF单元在不同温度、电压下的稳定性. 图8是SRAM的温度测试设备,FPGA产生SRAM的读写逻辑将采样的数据发到上位机,直流DC给SRAM芯片供电.

图8 SRAM-PUF温度测试

3.1 唯一性测试

PUF的唯一性由片间汉明距离大小来区分,理想情况其值为0.5,n个PUF实体之间其平均汉明距离由式(2)计算,s表示长度为k的PUF响应序列,xor代表按位异或.

$$\mathrm{FHD\_Inter}=\frac{2}{n(n-1)}\cdot\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\frac{\mathrm{xor}(s_i,s_j)}{k} \tag{2}$$

图9表示3类SRAM-PUF响应下不同芯片对的汉明距离,样本均值分别为0.495 8、0.498 7、0.502 6,标准差分别为0.032 2、0.047 1、0.025 2.

3.2 随机性测试

美国国家计数与标准局(National Institute of Standards and Technology,NIST)发布的统计测试包(Statistical Test Suite,STS),用于测试序列随机性. 在此对256×5组SRAM-PUF选点序列进行测试,主要的测试结果如表3所示. 由于1K的序列长度有限,在15项NIST测试中仅对以下项目进行测试:频率、块内频率、累加和、游

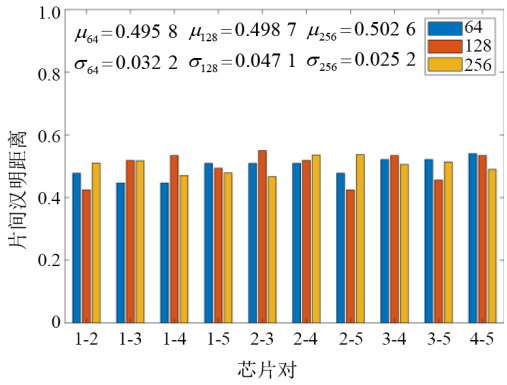


图9　预选点片间汉明距离

表3　基于SRAM-PUF的NIST测试结果

测试指标	P-Value	通过
Frequency	1.000 000	Yes
Block Frequency	0.157 083	Yes
Cumulative Sums	0.289 432	Yes
Runs	0.149 998	Yes
Longest Run	0.261 821	Yes
FFT	0.653 376	Yes
Approximate Entropy	0.044 108	Yes
Serial	0.288 588	Yes
Non-overlapping Template Matching	0.999 983	Yes

程、块内游程、FFT、近似熵、序列、非重叠模块匹配检验.

以上筛选产生的SRAM-PUF序列的p-value都大于0.01,表明生成的PUF序列都有较好的随机性.

3.3　电压和温度对稳定性影响

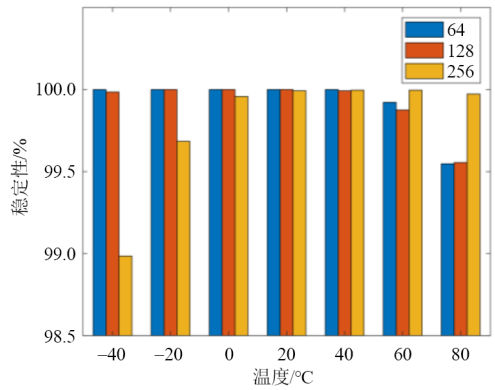
为了测试基于数据残留的预选技术在不同工作环境下的稳定性,通过改变SRAM-PUF的工作温度,评估在极限环境下SRAM-PUF的稳定性.

PUF稳定性的衡量可以使用片内汉明距离来衡量,如式(3),其中s表示长度为k的PUF响应序列,N表示不同环境下PUF响应序列的数量.

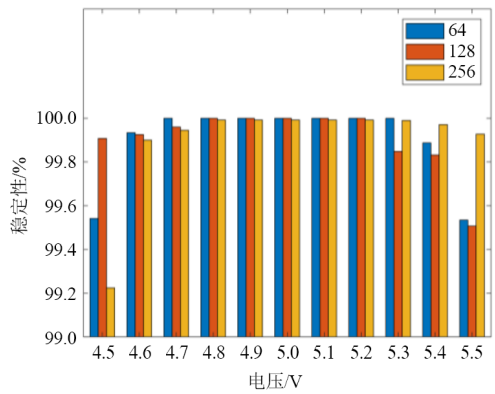
$$\text{Stability}=1-\frac{1}{N}\cdot\sum_{i=1}^{N}\frac{\text{xor}(s_1,s_i)}{k} \tag{3}$$

将在常温常压(5 V/20 ℃)下测得的PUF响应序列作为参考响应,之后改变SRAM-PUF的工作温度,统计不同温度下这些单元是否变化,并计算其稳定性. 测试结果如图10所示,图10(*a*)和(*b*)分别表示3种长度的PUF响应稳定性随温度以及电压的变化,预选出的SRAM单元在不同温度(–40~80 ℃)和电压(4.5~5.5 V)工作下,PUF长度64的稳定性为99.92%和99.90%;PUF长度128的稳定性为99.92%和99.91%;PUF长度256的稳定性为99.8%和99.90%.

对TMV1000预选单元进行了稳定性评估,其预选



(*a*) 稳定性随温度变化



(*b*) 稳定性随电压变化

图10　PUF在不同温度及电压下的稳定性

出的256位PUF响应稳定性为98.1%. 为了从误码率方面评估SRAM-PUF单元的稳定性进行对比,对预选出来PUF响应为256位的SRAM单元进行200 000次评估,由式(4)得出误码率,其中N为参与评估的PUF响应长度,#error为在#evaluations次评估中出错的次数.

$$\text{BER}=\frac{1}{N}\cdot\sum_{n=1}^{n=N}\frac{\#\text{errors}}{\#\text{evaluations}} \tag{4}$$

在此对区块号为54的256位SRAM-PUF在5 V/20 ℃环境下进行200 000次上电评估,由式(4)得到误码率为1.9×10^{-8}.

对TMV1000预选出的单元同样进行稳定性、误码率计算,合并得到结果如表4所示.

表4　TMV1000与本文算法性能比较

	稳定性	误码率	复杂度
TMV1000	98.1%	3.9×10^{-3}	$O(2\ 000n)$
本文	99.8%	1.9×10^{-8}	$O(900n)$

3.4　器件老化对稳定性影响

设备老化可能会导致SRAM-PUF响应在产品的生命周期内发生变化,负温度不稳定性是SRAM单元主要的老化机制,其主要表现为阈值电压的增加,当SRAM

单元上电时，PMOS对管电压差$\left|V_{\mathrm{th,P_1}}-V_{\mathrm{th,P_2}}\right|$随时间推移会变小，这将减少两个PMOS管之间的不匹配性．对SRAM芯片在静态直流条件下使用1.5×VDD进行72小时的压力测试，在每次施加电压力之前将读出新的SRAM-PUF响应作为参考，每隔1小时读出64位、128位、256位响应并计算其稳定性，如图11所示．

为了进行比较，将TMV1000和随机选点的SRAM单元进行稳定性的计算，可以看到，使用在72小时的压力测试后，TMV1000降低了2.5%，随机选择的单元则降低了5%，而采用本文算法的SRAM单元在老化压力测试下稳定性仅下降0.2%．

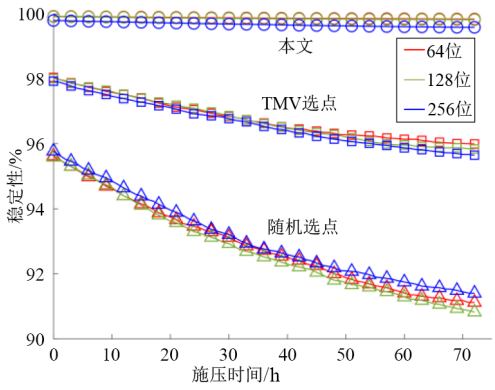


图11 PUF在老化效应下的稳定性

表5为本文所提出的预选算法和其他SRAM预选算法的性能对比．

表5 不同预选方式性能对比

文献	预选算法	“1”占比	片间汉明距离/%	误码率	供电电压/V	温度/℃
ASSCC 2018[11]	VSS倾斜	—	50.2	1.3×10^{-6}	0.8~1.2	–10~85
ISSCC 2021[12]	VDD倾斜	—	—	3.3×10^{-8}	0.7~1.4	–40~125
Access 2020[13]	电容倾斜	50.1%	49.3	2.6×10^{-6}	0.8~1.2	–10~85
DATE 2012[14]	充电注入	45.0%	50.2	1.0×10^{-6}	1.0~1.4	–20~80
VLSI 2016[17]	多重评估	—	—	1.4×10^{-2}	0.55~0.75	25~110
本文	数据残留	50.0%	50.3	1.9×10^{-8}	4.5~5.5	–40~80

4 结论

SRAM-PUF利用IC制造过程中随机的工艺偏差生成响应，但是其内部错误分布随机，用于密钥生成会使得ECC电路面积庞大，因此需要一定的预选算法降低SRAM-PUF错误率．目前主要采用基于TMV的预选算法，但其需要的测试量大、时间复杂度高且带来的稳定性提升并不可观．本文提出了数据残留预选算法，以两次测试，写“0”和写“1”之后记录其断电时间，找出偏向性强的SRAM单元．为了减小NVM存储空间，本文通过区块择优算法挑选出偏向性最强的SRAM区块，并记录其中断电时间最少的SRAM单元位置．通过实验，采用本文算法的SRAM-PUF在不同温度（–40~80 ℃）不同电压（–4.5~5.5 V）下产生256位PUF有99.8%的稳定性、1.9×10^{-8}的误码率，相比于TMV算法提升1.7%的稳定性，降低2.1×10^{5}的误码率，且跟1 000次TMV算法相比，在时间复杂度上降低55%，在经过72小时的老化测试后稳定性还能保持99.6%，可广泛用于SRAM-PUF密钥生成．

参考文献

[1] DEVADAS S, SUH E, PARAL S, et al. Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications[C]//2008 IEEE International Conference on RFID. Piscataway: IEEE, 2008: 58-64.

[2] MAITI A, CASARONA J, MCHALE L, et al. A large scale characterization of RO-PUF[C]//2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). Piscataway: IEEE, 2010: 94-99.

[3] KUMAR S S, GUAJARDO J, MAES R, et al. Extended abstract: The butterfly PUF protecting IP on every FPGA [C]//2008 IEEE International Workshop on Hardware-Oriented Security and Trust. Piscataway: IEEE, 2008: 67-70.

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

[5] HOLCOMB D E, BURLESON W P, FU K. Power-up SRAM state as an identifying fingerprint and source of true random numbers[J]. IEEE Transactions on Computers, 2009, 58(9): 1198-1210.

[6] SIMONS P W, VAN DER S E. Physical Unclonable Function: US20130234771[P]. 2013-09-12.

[7] KANG H, HORI Y, SATOH A. Performance evaluation of the first commercial PUF-embedded RFID[C]//The 1st IEEE Global Conference on Consumer Electronics. Piscataway: IEEE, 2012: 5-8.

[8] KANG H, HORI Y, KATASHITA T, et al. Cryptographie

key generation from PUF data using efficient fuzzy extractors[C]//16th International Conference on Advanced Communication Technology. Piscataway: IEEE, 2014: 23-26.

[9] WANG W D, SINGH A, GUIN U, et al. Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs[C]//2018 IEEE 19th Latin-American Test Symposium (LATS). Piscataway: IEEE, 2018: 1-6.

[10] SARAZA-CANFLANCA P, CARRASCO-LOPEZ H, BROX P, et al. Improving the reliability of SRAM-based PUFs in the presence of aging[C]//2020 15th Design & Technology of Integrated Systems in Nanoscale Era (DTIS). Piscataway: IEEE, 2020: 1-6.

[11] LIU K Y, MIN Y, YANG X, et al. A 373 F2 2D power-gated EE SRAM physically unclonable function with dark-bit detection technique[C]//2018 IEEE Asian Solid-State Circuits Conference (A-SSCC). Piscataway: IEEE, 2018: 161-164.

[12] HE Y, LI D, YU Z H, et al. 36.5 an automatic self-checking and healing physically unclonable function (PUF) with $<3\times10^{-8}$ bit error rate[C]//2021 IEEE International Solid-State Circuits Conference (ISSCC). Piscataway: IEEE, 2021: 506-508.

[13] SHIFMAN Y, MILLER A, KEREN O, et al. A method to utilize mismatch size to produce an additional stable bit in a tilting SRAM-based PUF[J]. IEEE Access, 2020, 8: 219137-219150.

[14] BHARGAVA M, MAI K. An efficient reliable PUF-based cryptographic key generator in 65nm CMOS[C]// 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE). Piscataway: IEEE, 2014: 1-6.

[15] BATURONE I, PRADA-DELGADO M A, EIROA S. Improved generation of identifiers, secret keys, and random numbers from SRAMs[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2653-2668.

[16] MATHEW S K, SATPATHY S K, ANDERS M A, et al. 16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS[C]//2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC). Piscataway: IEEE, 2014: 278-279.

[17] MATHEW S, SATPATHY S, SURESH V, et al. A 4fJ/bit delay-hardened physically unclonable function circuit with selective bit destabilization in 14nm tri-gate CMOS [C]//2016 IEEE Symposium on VLSI Circuits (VLSI-Circuits). Piscataway: IEEE, 2016: 1-2.

作者简介

陈泽亮　男,1998 年 6 月出生,浙江绍兴人. 现为浙江大学硕士研究生. 主要研究方向为数字IC设计.

E-mail: 22060644@zju.edu.cn

张培勇　男,1977 年 5 月出生,安徽安庆人. 博士,浙江大学微纳电子学院教授、博导. 主要研究方向为集成电路设计、DTCO 设计、嵌入式CPU及SOC设计.

E-mail: zhangpy@zju.edu.cn