一种可靠的芯片指纹 PUF 电路

白 创[1,2],唐立军[1]
(1. 长沙理工大学物理与电子科学学院,湖南长沙 410114;
2. 柔性电子材料基因工程湖南省重点实验室,湖南长沙 4100114)

摘 要: 本文引入一种可靠的芯片指纹物理不可克隆函数(Physical Unclonable Function)电路. 该 PUF 包括基于电流饥饿型延迟单元的工艺敏感电路、时间偏差放大器、时间偏差比较器、表决机制与扩散算法五个部分. 通过捕获制造工艺的偏差,每一个工艺敏感电路可以稳定产生两路具有微弱延时差的延迟信号,然后比较生成指纹 ID;设计一种新型的扩散算法改善 PUF 的唯一性,引入时间偏差放大器与表决机制增强 PUF 相对于温度与电源电压变化的稳定性. 文中 PUF 在 0.18μm CMOS 工艺下实现. 仿真结果表明,该 PUF 的输出具有均匀统计分布特征,同时在温度从 -40℃至 100℃,电源电压从 1.7V 至 1.9V 变化条件下,其输出 ID 具有 97.5% 的稳定性.

关键词: 物理不可克隆函数; 电流饥饿型延迟单元; 时间偏差放大器; 表决机制; 扩散算法
中图分类号: TN47 **文献标识码:** A **文章编号:** 0372-2112 (2019)10-2116-10
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.10.013

A Reliable Physical Unclonable Function for Chip Fingerprint

BAI Chuang[1,2], TANG Li-jun[1]
(1. *School of Physics and Electronic Science, Changsha University of Science and Technology, Changsha, Hunan* 410114, *China*;
2. *Hunan Provincial Key Laboratory of Flexible Electronic Materials Genome Engineering, Changsha, Hunan* 410114, *China*)

Abstract: A reliable physical unclonable function (PUF) for chip fingerprint using current starved delay element (CSDE) is described in this paper. The proposed PUF is composed of CSDE-based sensors, time difference amplifier, time difference comparator, voting mechanism and diffusion algorithm circuit. By capturing manufacturing process variations, each sensor produces two slightly different delay-time values that can be compared in order to create a digital identification (ID) for the chip. A new diffusion algorithm is designed to further improve the uniqueness of PUFs. Time difference amplifier and voting mechanism are introduced to simultaneously improve the reliability of PUFs across temperature and supply voltage variations. The proposed PUF is designed in 0.18μm CMOS technology. Simulated results show that the proposed PUF has a good output statistical characteristic of uniform distribution, and a high stability of 97.5% with respect to temperature variation from -40℃ to 100℃, and supply voltage variation from 1.7V to 1.9V.

Key words: physical unclonable functions; current starved delay element; time difference amplifier; voting mechanism; diffusion algorithm

1 引言

随着芯片攻击技术的发展,存储于 ROM 等非易失介质中的芯片指纹很容易通过版图反向工程和微探测技术等物理攻击方式被截取并且被复制,导致大量的克隆芯片的出现而破坏我国集成电路产业的良性发展. 物理不可克隆函数(PUF)电路通过捕获器件与连线制造时的工艺偏差,能够产生大量不同的 ID,作为芯片指纹标识芯片的合法身份. PUF 具有良好的安全性和不可克隆性,能够有效的抵御物理攻击且很难被复制,因此 PUF 电路正在逐步的被应用于芯片指纹的生成领域.

近些年,国内外出现了许多种芯片指纹 PUF 电路结构. 根据 PUF 构成单元的不同类型,PUF 主要分为两大类:基于延迟单元的 PUF 电路,其中包括基于判决器的 PUF 电路[1]、基于环路振荡器的 PUF 电路[2]等;基于

收稿日期:2018-04-23;修回日期:2019-01-09;责任编辑:梅志强
基金项目:国家自然科学基金资助项目(No.61604020);湖南省教育厅科学研究项目(No.18B164)

分压单元的 PUF 电路,其中包括基于电源线网格的 PUF 电路[3]、基于电流镜单元的 PUF 电路[4]、基于 SRAM 单元的 PUF 电路[5]、基于敏感放大器单元的 PUF 电路[6]等. PUF 的唯一性主要取决于 PUF 单元对工艺变化的敏感性,PUF 的稳定性则主要取决于 PUF 单元对温度和电源电压等环境条件变化的稳定性,而上述文献中的 PUF 单元都不能同时具备良好的工艺敏感与稳定性. 相比于基于电源线网格的 PUF 电路,基于 SRAM 单元的 PUF 电路的唯一性更好,原因在于 SRAM 单元对工艺的变化更加敏感,相反由于电阻比随着温度的变化基本保持不变,所以基于电源线网格的 PUF 电路对温度的变化表现出较高的稳定性;双堆叠型延迟单元相对于晶闸管型延迟单元工艺敏感性更强,故基于双堆叠型延迟单元的 PUF 具有更好的唯一性,然而在大的电源电压变化范围内,基于晶闸管型延迟单元的 PUF 具备更高的稳定性,原因是晶闸管型延迟单元对电源电压变化不敏感. 因此,亟需设计新型的 PUF 单元,保证其同时具备良好的工艺敏感性和稳定性;同时这些 PUF 电路都基于传统的体系结构设计,其体系结构仅包含工艺敏感电路与偏差比较器,工艺敏感电路产生的微弱的物理特性偏差信号很容易被噪声淹没,导致偏差比较器产生误判,从而降低 PUF 的稳定性. 因此需要对传统 PUF 体系结构进行改造和优化,提高 PUF 电路的稳定性;另外目前已出现了很多稳定性增强机制电路,通过增加稳定性增强机制到 PUF 电路中,PUF 的稳定性得到进一步改善. 文献[7]引入一种模式匹配技术完成误码矫正,提高 PUF 的稳定性,虽然这个方案能够有效的改善 PUF 电路的稳定性,但是其需要实现复杂的误码矫正逻辑,如 BCH decoder 等,同时存储在非易失介质中的 syndrome 很容易被窃取进而导致指纹 ID 的泄露;文献[8]提出了一种基于监测芯片工作温度,通过反馈进行电源电压控制的 PUF 设计方案,即根据反馈温度信息的不同,PUF 电路选择在不同的电源电压下工作,这样可以有效的提高 PUF 输出 ID 相对于温度变化的稳定性. 但是对电源电压浮动的情况无效. 因此,需要建立新的稳定性增强机制电路,要求实现简单,无需 syndrome 解码,并且可以改善 PUF 电路相对于温度和电源电压变化的稳定性.

本文首先引入电流饥饿型延迟单元作为 PUF 单元,其同时具备良好的工艺敏感性和稳定性;然后构建新型的 PUF 体系结构,其中包括基于电流饥饿型延迟单元的工艺敏感电路、时间偏差放大器和时间偏差比较器,有效改善 PUF 的稳定性;最后通过设计表决机制电路,增强 PUF 电路的稳定性,通过实现新的 ID 扩散算法,增强 PUF 电路的唯一性.

2　电流饥饿型延迟单元

电流饥饿型延迟单元的电路结构如图 1 所示,其中包括一个电流饥饿型反相器、一个 MOS 开关和一个整形反相器. MOS 开关 M_4 是用于控制延迟单元的工作状态,整形反相器用于对输出延迟信号进行整形,电流饥饿型反相器采用小尺寸器件增强对工艺的敏感性.

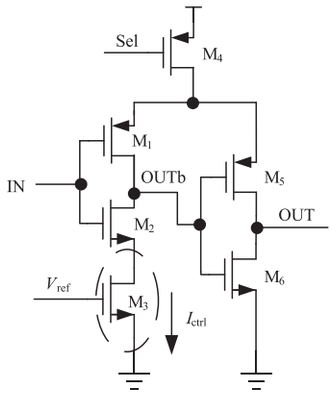


图1　电流饥饿型延迟单元结构

假如初始状态 OUTb 被预充电为 V_{DD},OUT 就被放电为 0,那么电流饥饿型延迟单元就处于关闭状态. 当输入信号 IN 出现一个上跳沿,晶体管 M_2 开启,OUTb 开始通过压控电流源晶体管 M_3 放电,放电电流为 I_{ctrl}. 直到 OUTb 被放电到 $V_{DD}/2$ 时,整形方向器的输出 OUT 立刻完成从 0 到 V_{DD} 的跳变,也即是说 IN 的上跳沿到达节点 OUT. 当输入 IN 出现一个下跳沿时,其过程正好相反,同时 OUT 完成从 V_{DD} 到 0 的跳变.

通过分析,电流饥饿型延迟单元的延迟时间计算如式(1)所示.

$$t_d = \alpha_1 \frac{C}{I_{ctrl}} V_{sw} + \alpha_2 \frac{1}{\mu_n C_{ox} \frac{W_2}{L_2}(V_{DD} - V_{Tn})} C\ln 2 + \delta t \quad (1)$$

其中,C 表示节点 OUTb 的等效电容,I_{ctrl} 表示压控电流源的电流,V_{sw} 表示电压阈值,当节点 OUTb 的电压为 V_{sw} 时,整形反相器输出 OUT 的状态完成即时转变,这里 $V_{sw} = V_{DD}/2$,α_1 和 α_2 为比例系数,同时 δt 表示整形方向器的整形延迟时间,由于 δt 是非常短的延迟时间,所以可以忽略. 显然通过公式可知延迟时间 t_d 同电源电压和温度都具有直接关系,也就是说电流饥饿型延迟单元对电源电压和温度的变化很敏感. 为了改善延迟单元相对于电源电压和温度变化的稳定性,文中采用通过量化计算 PUF 单元的延时特性,利用延时特性对温度和电源电压求导获取相关设计量最优值的增强 PUF 单元稳定性的设计方法. 通过式(2)和(3)联合可以计算得到最优的偏置电压 $V_{ref,opt}$ 和晶体管 M_3 的最优的宽长比 $(W_3/L_3)_{opt}$,当选择

$V_{ref,opt}$作为压控电流源的控制电压,$(W_3/L_3)_{opt}$作为晶体管M_3的尺寸时,电流饥饿型延迟单元的延迟时间就对电源电压和温度的变化不再敏感.

$$\left.\frac{\partial t_d}{\partial T}\right|_{V_{ref}=V_{ref,opt},W_3/L_3=(W_3/L_3)_{opt}}=0 \quad (2)$$

$$\left.\frac{\partial t_d}{\partial V_{DD}}\right|_{V_{ref}=V_{ref,opt},W_3/L_3=(W_3/L_3)_{opt}}=0 \quad (3)$$

其中,T表示电路工作时的温度,V_{DD}是指电路工作时的电源电压.

在0.18μm CMOS工艺下,分别设计SVT反相器链型延迟单元(SVT Inverter Chain),HVT反相器链型延迟单元(HVT Inverter Chain),双堆叠型延迟单元(Double Stacked Delay Element)和电流饥饿型延迟单元(Current Starved Delay Element).当电源电压为1.8V和工作温度为30℃时,各种延迟单元的延迟时间均约等于22.4ns.

在电源电压1.8V和工作温度30℃条件下,对每种延迟单元分别进行10000轮MonteCarlo分析,统计延迟时间随工艺变化的偏差特性.表1总结了不同延迟单元相对于工艺变化的延迟时间的标准方差.显然电流饥饿型延迟单元的延迟时间相对于工艺变化的标准方差最大,这意味着电流饥饿型延迟单元对工艺变化最敏感,基于电流饥饿型延迟单元的PUF的唯一性也最好.

表1 不同延迟单元相对于工艺变化的延迟时间标准方差

延迟单元	SVT反相器链型	HVT反相器链型	双堆叠型	电流饥饿型
标准方差	1.2643	3.6275	2.8145	10.7358

在电源电压从1.5V到2.1V、温度从-50℃到100℃的变化范围内,对各种延迟单元进行仿真.延迟单元的延迟时间相对于电源电压变化的稳定性如图2所示,延迟单元的延迟时间相对于温度变化的稳定性如图3所示,表2总结了不同延迟单元相对于电源电压与温度变化的延迟时间的标准方差.显然电流饥饿型延迟单元的延迟时间相对于电源电压与温度变化的标准方差均最小,这意味着电流饥饿型延迟单元在电源电压与温度变化时稳定性高,基于电流饥饿型延迟单元的PUF的稳定性也最好.

表2 不同延迟单元相对于电源电压和温度变化的延迟时间标准方差

延迟单元	SVT反相器链型	HVT反相器链型	双堆叠型	电流饥饿型
电源电压	2.7265	4.2682	4.1509	2.3503
温度	5.7535	7.2255	3.8893	2.0621

3 新型的PUF体系结构

基于电流饥饿型延迟单元的新型PUF电路体系结构如图4所示,包括基于电流饥饿型延迟单元的工艺敏感电路(CSDE-based Sensor)、时间偏差放大器(Time Difference Amplifier)和时间偏差比较器(Time Difference Comparator)三个部分.一组选择线信号被定义为PUF的一个challenge,而输出的一位0/1比特信号被定义为PUF的一个response.基于电流饥饿型延迟单元的工艺敏感电路由两个相同的电流饥饿型延迟单元组成,N个工艺敏感电路在片上对称设计实现,通过捕获制造工艺的偏差,每一个工艺敏感电路能够产生两路具有微弱延时差的延迟信号,根据选择线的控制逻辑,不同的工艺敏感电路轮流被选择工作;时间偏差放大器用于对工艺敏感电路输出的微弱延时差进行放大,从而减小延时差对后级时间偏差比较器比较精度的敏感性,改善PUF输出的稳定性,文中设计的时间偏差放大器是基于交叉耦合式电流饥饿型反相器的一种对称性结构,具备62dB的增益;时间偏差比较器用于对时间偏差放大器输出的延时差进行比较,产生稳定的0/1输出,文中设计的时间偏差比较器是一种新型的基于SR锁存器的比较器,具有交叉耦合的对称性结构,时间比较精度约为2ps.时间偏差放大器与时间偏差比较器均采用大尺寸的器件和对称性的版图布局以减小系统性和随机性噪声的影响,提高比较精度,产生稳定的输出.

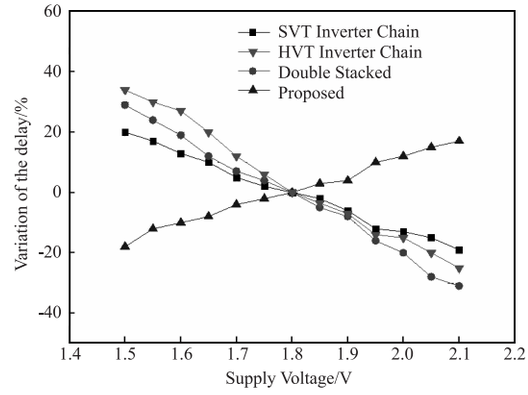


图2 不同延迟单元的延迟时间相对于电源电压变化的稳定性

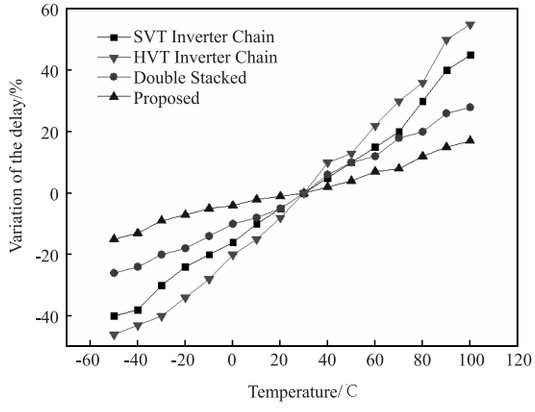


图3 不同延迟单元的延迟时间相对于温度变化的稳定性

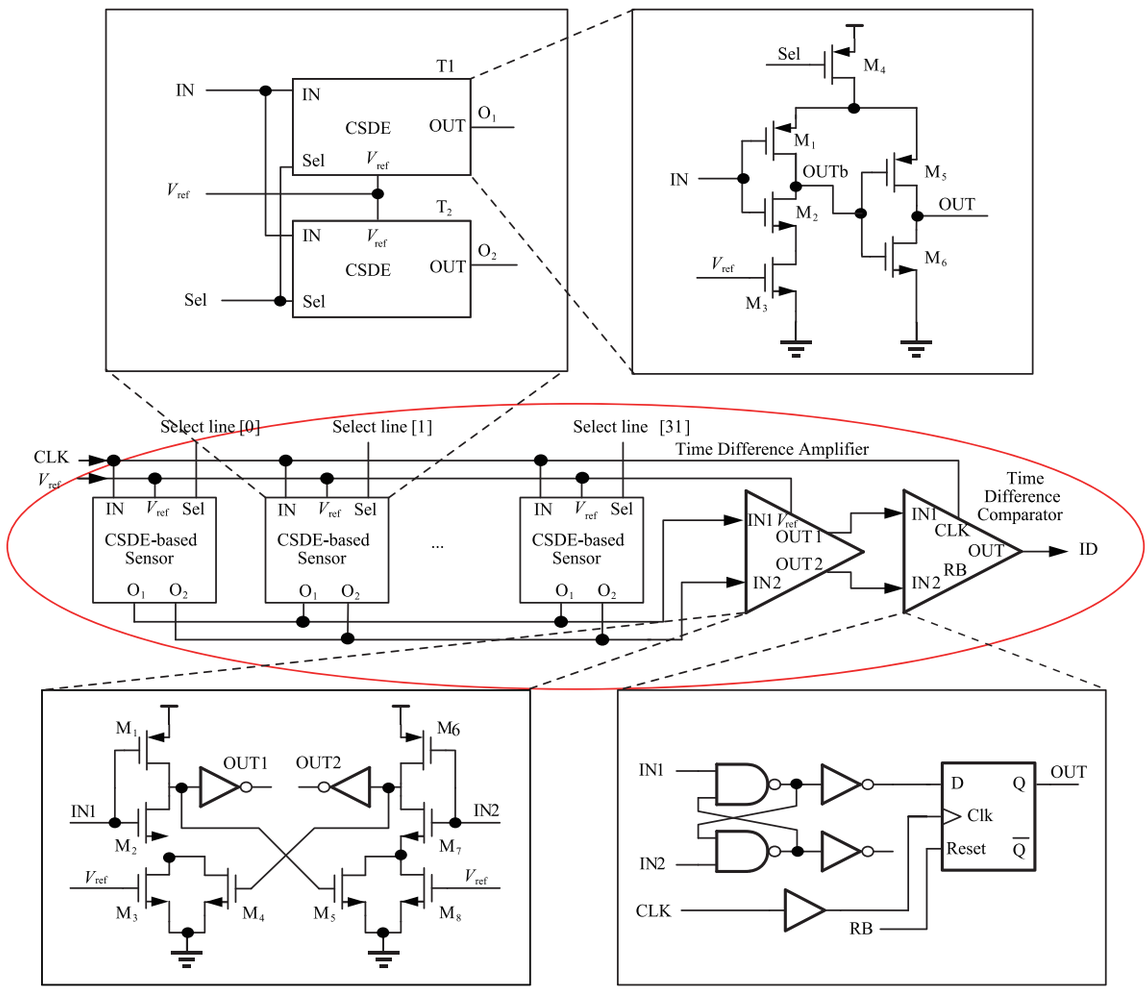


图4　基于晶闸管型延迟单元的新型PUF电路体系结构

相比于传统 PUF 体系结构,文中新型 PUF 结构增加了时间偏差放大器,从而改善 PUF 的稳定性. 如果时间偏差放大器没有被引入,那么基于电流饥饿型延迟单元的工艺敏感电路产生的具有微弱延时差的延迟信号就直接被送入时间偏差比较器. 当环境条件变化时,微弱的延时差可能变的小于时间偏差比较器的比较精度,就会导致比较器输出翻转或者不可预测. 另外微弱的延时差也很容易被电路本身和环境中的噪声淹没,导致比较器产生误判. 通过引入时间偏差放大器,放大微弱的延时差,减小其对时间偏差比较器的比较精度和各种噪声的敏感性,使得比较器能够产生稳定的输出,即提高了 PUF 的稳定性.

在电源电压为 1.8V 条件下,10000 个 PUF 实例分别在温度从 -40℃到 100℃变化的范围内进行仿真. 图 5 比较了包含时间偏差放大器和未包含时间偏差放大器两种 PUF 在不同温度条件下的稳定性. 当温度变化时,两种 PUF 的稳定性均降低;在不同的温度条件下,包含时间偏差放大器的 PUF 的稳定性均高于未包含时间偏差放大器的 PUF,这意味着包含时间偏差放大器的 PUF 在温度变化时具备更高的稳定性.

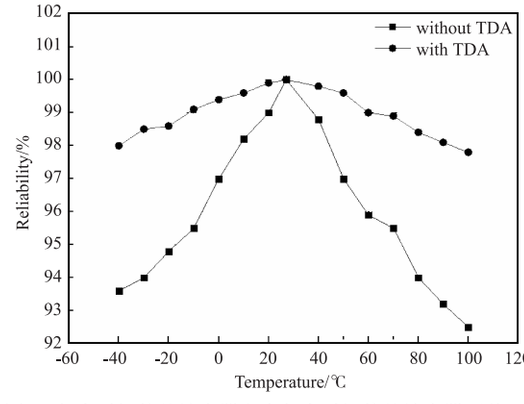


图5　包含时间偏差放大器和未包含时间偏差放大器两种PUF在不同温度条件下的稳定性

另外,在温度为 30℃ 条件下,这些 PUF 实例分别在电源电压从 1.7V 到 1.9V 变化的范围内进行仿真. 图 6 比较了包含时间偏差放大器和未包含时间偏差放大器两种 PUF 在不同电源电压条件下的稳定性. 当电源电压变化时,两种 PUF 的稳定性均降低;在不同的电源电压条件下,包含时间偏差放大器的 PUF 的稳定性均高于未包含时间偏差放大器的 PUF,这意味着包含时间偏差放大器的 PUF 在大的电源电压范围内具备更高的稳定性.

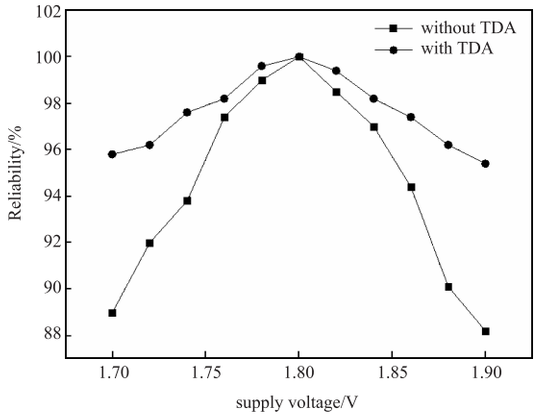


图6 包含时间偏差放大器和未包含时间偏差放大器两种PUF在不同电源电压条件下的稳定性

综合分析可知,在电源电压从 1.7V 到 1.9V 变化和温度从 40℃到 100℃变化的条件下,包含时间偏差放大器的 PUF 的稳定性约为 94.8%,远大于未包含时间偏差放大器的 PUF 的稳定性 87.4%. 因此时间偏差放大器的引入极大的改善了 PUF 相对于温度与电源电压变化的稳定性.

4 性能增强技术

为进一步提高 PUF 的性能,文中设计实现表决机制与扩散算法,分别用来改善 PUF 的唯一性与稳定性.

4.1 稳定性增强技术-表决机制

当环境条件尤其是电源电压随机抖动变化时,由于工艺敏感电路中的电流饥饿型延迟单元的延时特性会随之变化,所以导致时间偏差比较器的输出可能发生改变,同一个 PUF 芯片每次产生的 ID 有可能都是不一样的. 因此,文中引入表决机制(Voting Mechanism),通过对时间偏差比较器生成的 0/1 输出结果进行多次采样,并依据采样结果的概率分布,判决输出稳定的 ID 比特. 通过举手表决机制,可以极大的改善 PUF 的稳定性.

表决机制的电路结构如图 7 所示,包括一个采样器、两个控制器、两个计数器、一个判决器和两个寄存器. Voting Register 用来设置采样次数,Probability Register 用来设置比较阈值. 判决器的电路结构如图 8 所示,基于判决算法产生稳定 ID 比特. 表决机制具体工作过程为:首先对时间偏差比较器的输出进行多次采样,同时通过控制器 0 生成分别表示采样结果 0 和 1 个数的计数脉冲,然后通过计数器 0 与 1 分别对两路计数脉冲进行计数,最后判决器根据 0/1 计数值判决输出稳定 ID 比特. 分析可知不同的采样次数和比较阈值的组合决定表决机制具有不同的正确稳定的 ID 生成能力. 文中在标称电源电压为 1.8V,并叠加摆幅为 0.1V 的随机波动电压条件下,10000 个 PUF 实例分别在不同的温度、采样次数与比较阈值情况下进行仿真,通过比较仿真结果确定最优的采样次数与比较阈值组合.

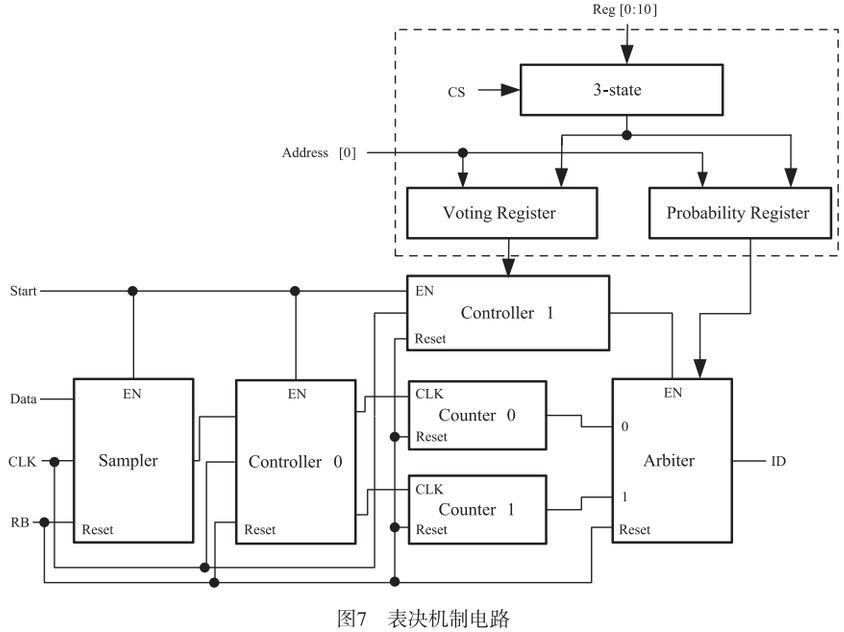


图7 表决机制电路

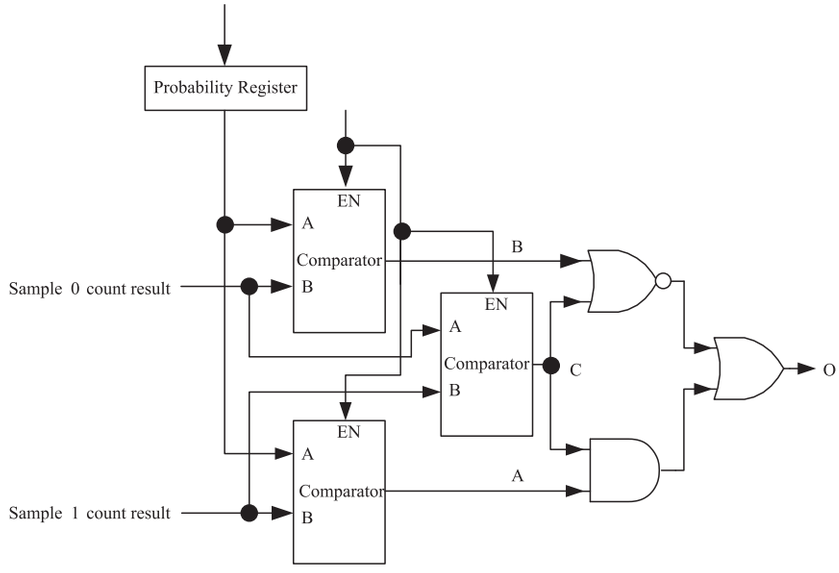


图8　判决器电路

在比较阈值为 50%、温度为 -40℃、30℃和 100℃三种条件下,选择不同的采样次数(范围为 100 到 1300)对 10000 个 PUF 实例进行仿真,统计 PUF 的稳定性如图 9 所示. 当采样次数接近 1200 时,PUF 在 -40℃到 100℃的温度范围内的 ID 稳定性均近似为 100%.

在比较阈值为 60%、温度为 -40℃、30℃和 100℃三种条件下,选择不同的采样次数(范围为 100 到 1300)对 10000 个 PUF 实例进行仿真,统计 PUF 的稳定性如图 10 所示. 当采样次数接近 1000 时,PUF 在 -40℃到 100℃的温度范围内的 ID 稳定性均近似为 100%.

在比较阈值为 70%、温度为 -40℃、30℃和 100℃三种条件下,选择不同的采样次数(范围为 100 到 1300)对 10000 个 PUF 实例进行仿真,统计 PUF 的稳定性如图 11 所示. 当采样次数接近 1300 时,PUF 在 -40℃到 100℃的温度范围内的 ID 稳定性均近似为 100%.

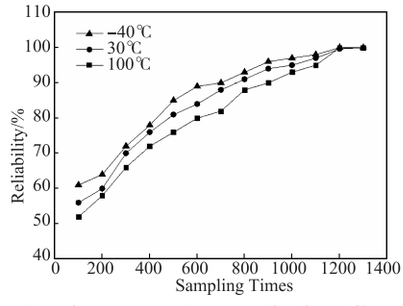


图9　在-40℃、30℃和100℃三种温度、比较阈值为50%、及不同采样次数的仿真条件下PUF的稳定性

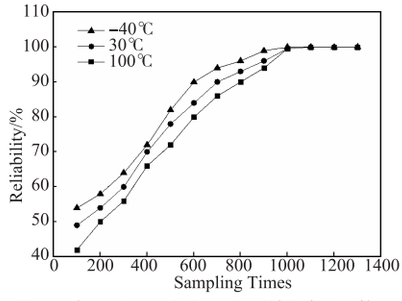


图10　在-40℃、30℃和100℃三种温度、比较阈值为60%、及不同采样次数的仿真条件下PUF的稳定性

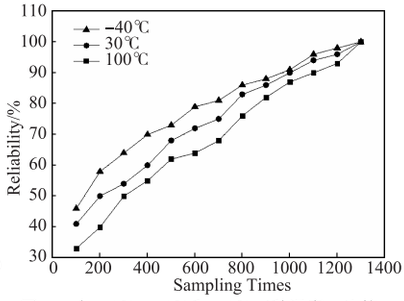


图11　在-40℃、30℃和100℃三种温度、比较阈值为70%、及不同采样次数的仿真条件下PUF的稳定性

通过比较分析可知,最优的组合是采样次数为 1000 和比较阈值为 60%. 在采样次数为 1200 和比较阈值为 50% 的组合、采样次数为 1300 和比较阈值为 70% 的组合情况下,PUF 在 -40℃到 100℃的温度范围内的稳定性也都近似为 100%,但是采样次数越大,PUF 的工作时钟频率越高,功耗越大,同时电流饥饿型延迟单元允许延迟时间范围越小,设计难度越大,因此选择采样次数为 1000 和比较阈值为 60% 的组合是最优的.

4.2　唯一性增强技术-扩散算法

表决机制生成的 ID 在分布上比较集中,任意两个 ID 之间不同比特位的数量(海明距离)较小,这增加了不同 ID 之间的碰撞的可能性. 为了减少 ID 重复改善 PUF 的唯一性,文中引入新型扩散算法(Diffusion Algorithm),将表决机制生成的 ID 进行扩散,使得扩散后的 ID 在较大的数值空间满足均匀分布特征,任意 ID 之间不同比特位的数量(海明距离)增大,从而减小了不同 ID 之间碰撞的概率,增强了 PUF 的唯一性. 文中实现两种扩散算法,电路结构分别如图 12 与图 13 所示.

通过仿真可知两种算法扩散后的 ID 都满足均匀分布特征,但是相比于扩散算法 1,扩散算法 2 面积开

销小,删除了非线性电路,减小了 ID 生成的复杂度,而且由原始 ID 很容易推出扩散后 ID,但是反之则非常困难,另外算法 2 扩散后 ID 的海明距离统计分布特性更好,即 ID 之间海明距离更大,ID 比特随机性更好,因此文中 PUF 设计实例均采用扩散算法 2 打散 ID 序列,增强 PUF 的唯一性.

算法 2 具体工作过程为:首先 32 位的移位寄存器初始状态复位为全"0";然后在原始 ID 比特位后补充 128 个比特"0",依次右移入 32 位移位寄存器,移位前数据源 $D_1 = Q_{32} \oplus Q_3 \oplus IN_m$,其中 IN_m是输入的第 m 个比特位. 当所有比特位全部按照上述方式移入后,寄存器的状态称为实际工作状态;最后将原始 ID 比特位重新依次右移入 32 位移位寄存器,移位前数据源 $D_1 = Q_{32} \oplus Q_3 \oplus IN_m$,其中 IN_m是原始 ID 中的第 m 个比特位,每右移入一位后从抽取寄存器第 32 位输出 Q_{32},并按照 $O_m = Q_{32} \oplus IN_m$运算产生新的 ID 位,其中 IN_m是原始 ID 中的第 m 个比特位,O_m为扩散后 ID 中第 m 个比特位. 如此循环直到产生最后一位 ID,新的 ID 同原始 ID 比特位数相同.

文中选择分别满足正态分布、指数分布和均匀分布的 3 组样本进行扩散测试,每组取 10000 个样本. 经过扩散后的 32 位二进制数值样本被转换为十进制数字,在大的数值空间内计算概率统计分布特性.

第 1 组样本满足正态统计分布特性,图 14(a)和图 14(b)分别展示了扩散前后第 1 组样本的统计分布特性. 第 2 组样本满足指数统计分布特性,图 14(c)和图 14(d)分别展示了扩散前后第 2 组样本的统计分布特性. 第 3 组样本满足均匀统计分布特性,图 14(e)和图 14(f)分别展示了扩散前后第 3 组样本的统计分布特性.

分析可知,满足正态分布、指数分布和均匀分布的三种类型样本,经过扩散算法 2 扩散后都在大的数值空间范围内满足均匀统计分布特性,扩散后样本的海明距离较大,样本间重复概率急剧下降,这意味着包含扩散算法 2 的 PUF 具有较好唯一性.

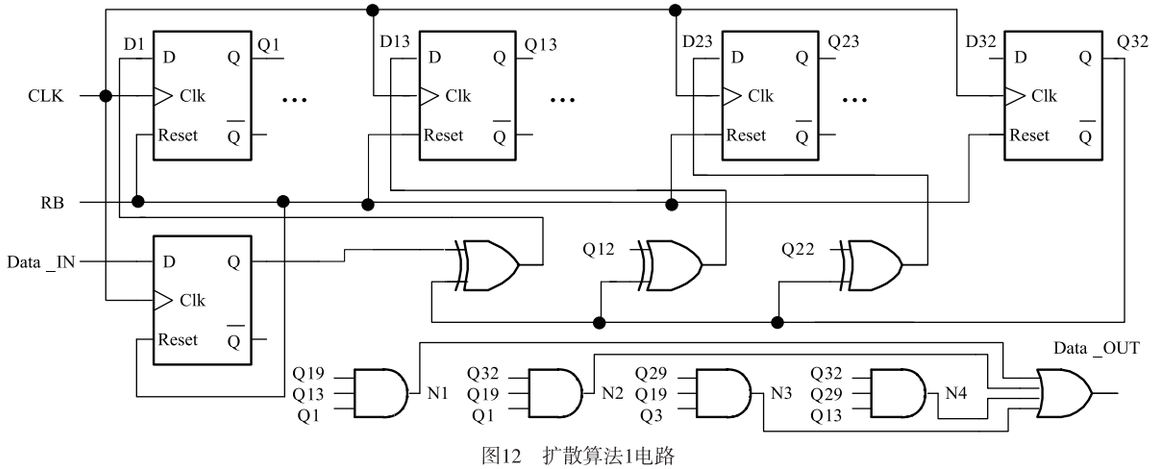


图12 扩散算法1电路

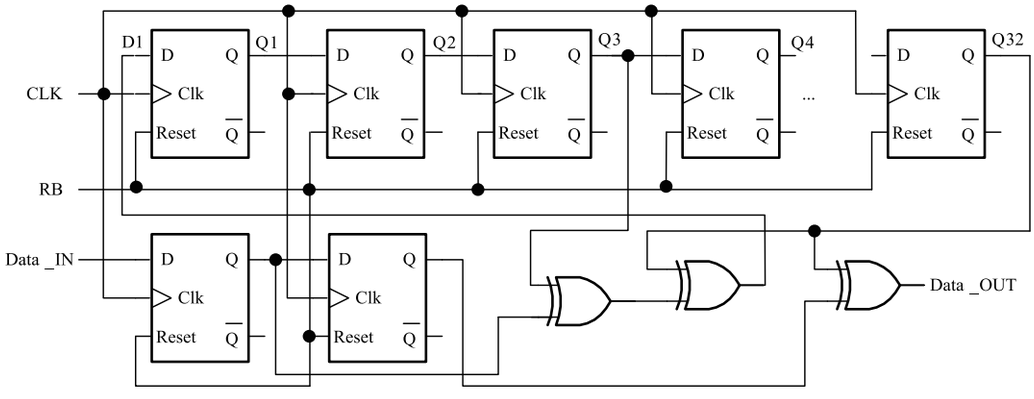


图13 扩散算法2电路

5 实验结果与分析

在 0.18μm CMOS 工艺下设计基于电流饥饿型延迟单元的 PUF(CSDE-based PUF),它包含 32 个基于电流饥饿型延迟单元的工艺敏感电路(CSDE-based Sensor)、时间偏差放大器(TDA)、时间偏差比较器(Time

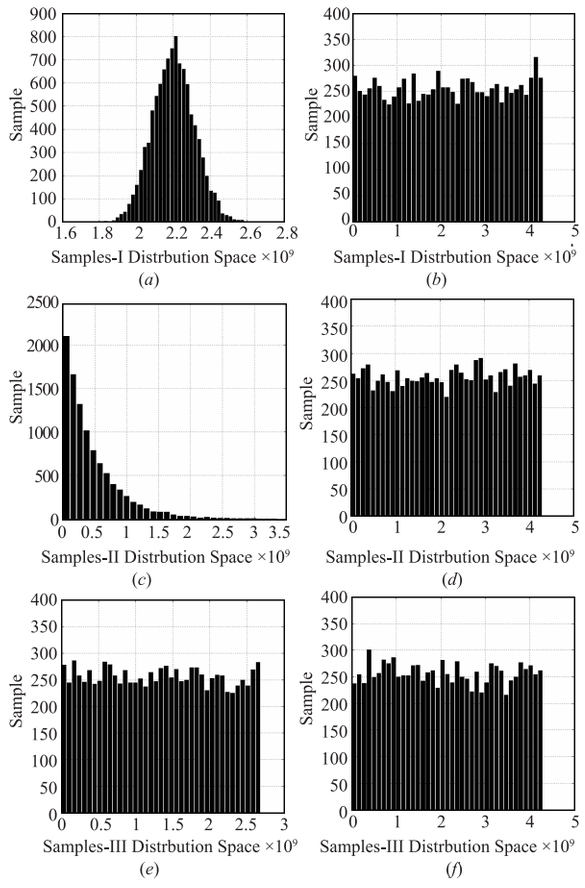


图14　不同类型样本扩散前后的概率统计分布特性图

Difference Comparator)、表决机制电路(Voting Mechanism)和扩散算法电路(Diffusion Algorithm),CSDE-based PUF 的版图实现如图 15 所示.

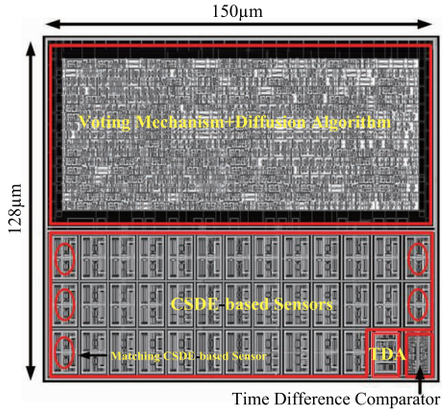


图15　PUF芯片版图

5.1　面积、功耗与速度

整个 PUF 芯片的面积是 19200μm². 经过仿真可知,CSDE-based PUF 在电源电压从 1.7V 到 1.9V 变化和温度从 -40℃到 100℃变化的条件下,能够稳定工作产生 32 位 ID,输出具有 1Mbps 的吞吐率;在电源电压为 1.8V,温度为 30℃的条件下,当芯片处于正常工作模式时,消耗的功率为 390μW;当芯片处于睡眠模式时,消耗的功率仅为 140nW. 表 3 总结了 CSDE-based PUF 芯片的各个性能参数值.

表 3　CSDE-based PUF 芯片不同性能参数值

工艺	0.18μm CMOS process
面积	19,200μm²
工作电压	1.7V ~ 1.9V
工作温度	-40℃ ~ 100℃
静态功耗@1.8V,30℃	140nW
动态功耗@1.8V,30℃	390μW
吞吐率	1Mbps

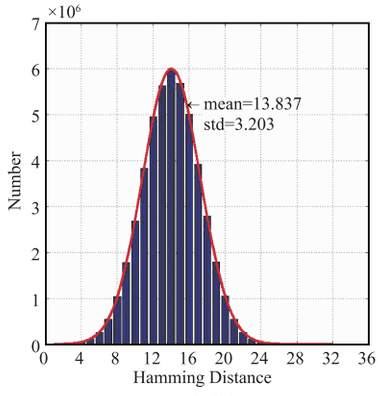
5.2　唯一性

唯一性是指 PUF 电路产生独立的、不重复的 ID 的能力. 唯一性越好,PUF 能够生成的独立的不重复的 ID 就越多. 为了验证 CSDE-based PUF 唯一性,文中在 0.18μm CMOS 工艺下、电源电压从 1.7V 到 1.9V 变化和温度从 -40℃到 100℃变化的仿真条件下,对 CSDE-based PUF 进行 10000 轮的 MonteCarlo 分析,比较 PUF 实例生成的 ID 的数值统计分布特性和海明距离分布特性. 在仿真中,一组 32 个不同的 challenges 被应用到每一个 PUF 实例,用来产生 32 位的 ID. 经过仿真可知,其中 9750 个实例可以产生不同的稳定的 32 位 ID,同时这些 ID 在大的数值空间上满足均匀分布特性.

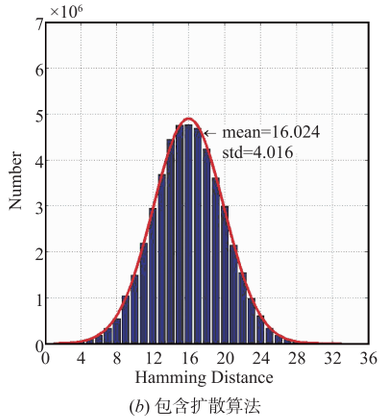
海明距离是指任何两个 ID 数字之间不同的二进制比特的数量. 图 16(*b*)展示了 9750 个包含扩散算法二的 CSDE-based PUF 芯片生成的 ID 的海明距离分布特性图,同时为了便于比较,图 16(*a*)展示了未包含扩散算法的 CSDE-based PUF 芯片生成 ID 的海明距离统计分布图. 通过计算分别给出了统计分布的平均值和标准方差值. 显然相比于未包含扩散算法 CSDE-based PUF 的海明距离统计分布平均值 13.837,包含扩散算法 2 的 CSDE-based PUF 的海明距离统计分布的平均值为 16.024,更接近于具有不相关特性的 PUF 的海明距离分布理想平均值 16. 另外相比于未包含扩散算法 CSDE-based PUF 的海明距离统计分布标准方差值 3.203,包含扩散算法 1 的 PUF 的海明距离统计分布标准方差值 3.624,包含扩散算法 2 的 CSDE-based PUF 的海明距离统计分布的标准方差值更大,为 4.016,即统计分布的宽度也越大. 总之,包含扩散算法 2 的 CSDE-based PUF 的海明距离统计分布具有更大的宽度,PUF 生成的不同 ID 之间存在更多的不同的二进制比特位,不同 ID 之间碰撞的可能性小,故包含扩散算法 2 的 CSDE-based PUF 就具有更好的唯一性.

5.3　稳定性

稳定性是指 PUF 电路在变化的环境条件下能够产生



(*a*) 未包含扩散算法



(*b*) 包含扩散算法

图16 CSDE-based PUF生成ID的海明距离分布特性图

稳定不变的 ID 的能力. 根据前文分析可知,在电源电压从 1.7V 到 1.9V 变化和温度从 -40℃到 100℃变化的条件下,CSDE-based PUF 具有 94.8% 的稳定性. 为了评估 CSDE-based PUF 的稳定性,根据参考文献[1,2,5,6]中 PUF 结构,文中在 0.18μm CMOS 工艺下分别实现了基于判决器的 PUF、基于环路振荡器的 PUF、基于 SRAM 单元的 PUF 和两种基于敏感放大器单元的 PUF(LS-SA 和 SA-SA),并在电源电压从 1.7V 到 1.9V 变化和温度从 -40℃到 100℃变化的仿真条件下,分别对每一种 PUF 进行 10000 轮的 MonteCarlo 分析. 图 17 展示了各种 PUF 在温度和电源电压变化条件下的 ID 错误率. 其中黑色柱代表当温度为 30℃、电源电压在 1.7V 到 1.9V 范围内变化时 PUF 的 ID 错误率,白色柱代表当电源电压为 1.8V、温度在 -40℃到 100℃范围内变化时 PUF 的 ID 错误率,灰色柱则代表温度和电源电压同时变化时 PUF 的 ID 错误率. 分析可知,当温度和电源电压同时变化时,CSDE-based PUF 的 ID 错误率最低,约为 5.2%,比其他 PUF 结构的低 1.4 ~ 4.2 倍. 这说明 CSDE-based PUF 具有更高的稳定性.

进一步而言,在电源电压存在 ±0.1V 的波动条件下,10000 个 CSDE-based PUF 实例分别在温度从 -40℃到 100℃变化的范围内进行仿真. 结果表明,表决前 PUF 输出

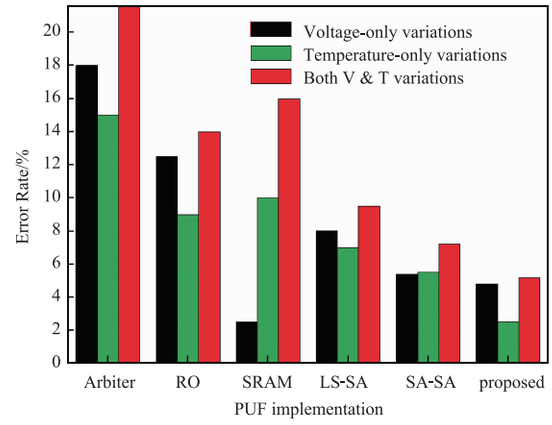


图17 在温度和电源电压变化条件下CSDE-based PUF与其他参考PUF结构的ID错误率的比较图

ID 的稳定性为 94.8%,而在经过表决后 PUF 输出 ID 的稳定性提高到 97.5%. 这意味着包含表决机制的 CSDE-based PUF 具有更好的稳定性. 表 4 比较了包含各种不同稳定性增强机制的 PUF 电路的 ID 错误率. 显然相比于其他 PUF 而言,CSDE-based PUF 在大的温度变化范围内(-40℃至 100℃)具有相对最低的错误率 2.5%,故文中设计的表决机制是一种非常有效的稳定性增强技术.

表 4 CSDE-based PUF 与其他包含不同稳定性增强机制的 PUF 的错误率比较

	温度	电源电压	错误率
文献[9]	-40℃ to 120℃	0.9V to 1.1V	4.2%
文献[10]	25℃ to 85℃	0.8V to 1.0V	2.8%
Proposed	-40℃ to 100℃	1.7V to 1.9V	2.5%

总之,相比于其他 PUF 结构,基于电流饥饿型延迟单元的 PUF 具有 97.5% 较高的稳定性,同时其输出的 ID 在大的数值空间满足均匀分布统计特性.

6 总结

本文从 PUF 单元、PUF 体系结构、表决机制和扩散算法等方面分别展开研究,以提高芯片指纹 PUF 电路的唯一性和稳定性. 通过设计电流饥饿型延迟单元作为 PUF 单元和 ID 扩散算法,增强 PUF 电路的唯一性;通过构建新型的 PUF 体系结构、设计新的表决机制电路,增强 PUF 电路的稳定性. 本文主要贡献如下:

(1)基于利用延时特性对温度和电源电压求导获取相关设计量最优值的增强 PUF 单元稳定性的设计方法,加固电流饥饿型延迟单元,使得电流饥饿型延迟单元在电源电压与温度变化时具有较强的稳定性;

(2)在传统 PUF 结构基础上,通过引入时间偏差放大器,构建新型的 PUF 体系结构,放大后的延时差,减小了对时间偏差比较器的比较精度和各种噪声的敏感性,使得比较器能够产生稳定的输出,提高 PUF 稳定性.

参考文献

[1] LIN C W, GHOSH S. A family of schmitt-trigger-based arbiter-PUFs and selective challenge-pruning for robustness and quality[A]. IEEE International Symposium on Hardware-Oriented Security and Trust[C]. McLean, VA, USA: IEEE, 2015. 32 – 37.

[2] RAHMAN M T, RAHMAN F, FORTE D, et al. ARO-PUF: An aging-resistant RO-PUF for reliable key generation[J]. IEEE Transactions on Emerging Topics in Computing, 2016, 4(3): 335 – 348.

[3] ZHANG J R, ZHAO Y F. Study on temperature effects based on measuring power distribution system of PUF [A]. 2013 IEEE International Conference on Anti-Counterfeiting, Security and Identification (ASID)[C]. Shanghai, China: IEEE, 2013. 1 – 3.

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

[5] XU X L, RAHMATI A, HOLCOMB D E, et al. Reliable physical unclonable functions using data retention voltage of SRAM cells[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34(6): 903 – 914.

[6] BHARGAVA M, CAKIR C, MAI K. Attack resistant sense amplifier based PUFs (SA-PUF) with deterministic and controllable reliability of PUF responses[A]. IEEE International Symposium on Hardware-Oriented Security and Trust [C]. Anaheim Convention Center, California, USA: IEEE, 2010. 106 – 111.

[7] PARAL Z, DEVADAS S. Reliable and efficient PUF-based key generation using pattern matching[A]. 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)[C]. San Diego, California, USA: IEEE, 2011. 128 – 133.

[8] VIVEKRAJA V, NAZHANDALI L. Feedback based supply voltage control for temperature variation tolerant PUFs[A]. 24th International Conference on VLSI Design[C]. Madras, Chennai, India: IEEE Computer Society, 2011. 214 – 219.

[9] LIU C Q, CAO Y, et al. ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 64(12): 3138 – 3149.

[10] TANEJA S, ALVAREZ A, et al. A fully-synthesizable C-element based PUF featuring temperature variation compensation with native 2.8% BER, 1.02fJ/b at 0.8 – 1.0V in 40nm[A]. 2017 IEEE Asian Solid-State Circuits Conference (A-SSCC)[C]. Seoul, South Korea: IEEE, 2017. 301 – 304.

作者简介

白　创　男, 1983 年生于陕西延安. 现为长沙理工大学物理与电子科学学院、柔性电子材料基因工程湖南省重点实验室讲师、硕士生导师. 主要研究方向为数模混合集成电路设计与实现.

E-mail: 154317586@qq.com

唐立军　男, 1963 年生于湖南邵阳. 现为长沙理工大学物理与电子科学学院教授、博士生导师. 主要研究方向为微弱信号检测及系统实现.

E-mail: tanglj2000@263.com