

基于气敏传感器的高稳态物理不可克隆函数发生器

汪鹏君^{*①②} 李乐薇^② 郑雁公^② 李刚^①

^①(温州大学电气与电子工程学院 温州 325035)

^②(宁波大学信息科学与工程学院 宁波 315211)

摘要: 物联网(IoT)作为战略性新兴产业已经上升为国家发展重点,但在实际应用中面临各种安全威胁。确保资源受限物联网系统数据传输、处理和存储的安全已成为研究热点。该文通过对物理不可克隆函数(PUF)和传感器制备工艺偏差的研究,提出一种基于气敏传感器的高稳态物理不可克隆函数发生器设计方案。该方案首先采用静电喷雾沉积(ESD)方式生成具有高比表面积特性的纳米材料,结合高温煅烧技术制备Pd-SnO₂气敏传感器;其次采集Pd-SnO₂气敏传感器在不同气体浓度、环境温度、加热电压条件下对甲醛气体的响应数据;然后利用随机阻值多位平衡算法比较不同簇气敏传感器响应的阻值,进而产生多位高稳态PUF数据;最后对所设计PUF发生器的安全性和可靠性进行评估。实验结果表明,该PUF发生器的随机性为97.03%、可靠性为97.85%、唯一性为49.04%,可广泛应用于物联网安全领域。

关键词: 物理不可克隆函数; 气敏传感器; 物理不可克隆函数发生器; 物联网安全

中图分类号: TN919; TP212

文献标识码: A

文章编号: 1009-5896(2021)06-1596-07

DOI: 10.11999/JEIT201104

High Steady-state Physical Unclonable Function Generator Based on Gas Sensors

WANG Pengjun^{*①②} LI Lewei^② ZHENG Yangong^② LI Gang^①

^①(College of Electrical and Electronic Engineering, Wenzhou University, Wenzhou 325035, China)

^②(Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China)

Abstract: As a strategic emerging industry, the Internet of Things (IoT) has become a national development focus, but it also faces various security threats in practical applications. Ensuring the security of data transmission, processing and storage of resource-constrained IoT systems has become a research hotspot. In this paper, a high steady-state Physical Unclonable Function(PUF) generator scheme is proposed by studying PUF and the deviation of the sensor preparation process. Firstly, the Electrostatic Spray Deposition (ESD) is used to generate nanofibers with high specific surface area characteristics and high-temperature calcination technology is combined to prepare Pd-SnO₂ gas sensors. Secondly, the response data of gas sensors to formaldehyde gas is collected under different gas concentration, ambient temperature and heating voltage conditions. Then, a random resistance multi-bit balance algorithm is used to compare the response data of different clusters of gas sensors and then multiple high steady-state PUF data is generated. Finally, the safety and reliability of the designed PUF generator are evaluated. Experimental results show that the randomness of the PUF generator is 97.03%, the reliability is 97.85%, and the uniqueness is 49.04%, which can be widely used in IoT security field.

Key words: Physical Unclonable Function(PUF); Gas sensor; Sensor PUF; Internet of Things(IoT) security

收稿日期: 2020-12-31; 改回日期: 2021-04-12; 网络出版: 2021-04-21

*通信作者: 汪鹏君 wangpengjun@wzu.edu.cn

基金项目: 国家自然科学基金(61874078, 61871244), 国家重点研发计划(2018YFB2202100), 宁波市公益性计划(202002N3134), 宁波大学大学生科技创新项目(2021SRIP1327)

Foundation Items: The National Natural Science Foundation of China(61874078, 61871244), The National Key Research and Development Program of China(2018YFB2202100), The Ningbo Public Welfare Projects(202002N3134), The Science and Technology Innovation Project of Ningbo University(2021SRIP1327)

1 引言

物联网(Internet of Things, IoT)通过网络技术和各类信息传感器,按照协定方式将能够被独立标识的机器、人和物等按需求连接起来,进行信息传输和协同交互,实现“万物互联”^[1]。传感器作为物联网系统的神经末梢,获取所需外界数据信息,是将数字世界和物理世界连接的核心。随着物联网应用范围的拓展,传感器级的安全问题越来越受到重视。一方面,传感器节点通常部署在无人值守的地理环境,只有很少或没有安全保护^[2],存在信息泄露的安全隐患。另一方面,传感器附件配备可用内存较少,计算能力有限^[3],一个典型的传感器附件可能只备用512 B的内存,诸如高级加密标准(Advanced Encryption Standard, AES)之类的传统加密技术无法使用。如何以较小的计算和存储开销,实现传感器产生数据的安全、可信传递,已经成为物联网安全的迫切需求。

物理不可克隆函数(Physical Unclonable Function, PUF)发生器可利用物理结构的随机、固有属性为物联网安全提供低开销、高可靠性的解决方案。Pappu等人^[4]依据光学操作原理实现物理单向函数以产生能够满足唯一标识功能的激励响应对(Challenge Response Pairs, CRP),最早提出PUF的概念。随之发展到目前以硅基为主的PUF发生器,它利用硅基电路制造过程存在的微小工艺偏差产生具有唯一性、随机性和不可克隆性的硬件指纹,包括仲裁器PUF^[5]、环形振荡器PUF^[6]、静态随机存取存储器PUF(Static Random Access Memory PUF, SRAM PUF)^[7,8]和触发器PUF^[9]等。然而将这些硅基PUF直接集成到资源受限的传感器节点将会增加设计难度和额外成本^[10]。学者已着手探索利用已有的传感器组件实现更低成本PUF发生器的研究^[11]。Rosenfeld等人^[12]利用传感器半透明底层所涂深色物质不均匀、光学透射率不一致,由此导致每个芯片光电二极管的光学灵敏度不尽相同等特点,提出一种消除传感器与加密技术分离的架构,但是该架构仍需利用传统的PUF将输入激励转换为初始向量以进行下一步工作,增加了额外的电路开销。Dey等人^[13]证明加速度计具有独特的指纹,对80个独立的加速度计芯片以及25个Android手机和2个平板电脑内部加速度计的测试数据表明这些指纹的确存在。Aysu等人^[14]利用陀螺仪的输出构建不可预测的PUF响应,但存在无法重复生成所需激励响应对的问题。Labrado等人^[15]对压电传感器建模,分析得到交流电压相同,由于制造过程的偏差,不同传感器的等效阻抗存在差异,

可利用此差异产生所需PUF数据,但该设计需要外加交流电压源。

气敏传感技术的发展推动了物联网在气体(油)等管理领域的广泛应用。通常将类型和数量众多的气敏传感器集成于物联网系统,安置在液化气储藏库、暖通市场、交通运输等场所。由于目前众多气敏传感器之间没有采取有效技术将其特征区分,不具备“一物一密”特性,所以当某观察点发生异常时难以精准判断哪个气敏传感器“报警”,也就是说难以找到气体(油)的泄露源头,耽误最佳抢修时间;同时也存在传输数据被盗或篡改数据等恶意破坏事故。鉴此,本文针对物联网智能体系中感知节点的安全性难题,拟利用气敏传感器识别到的外界环境变化,从中提取物理特征信息,设计高稳态PUF发生器,为传感器提供定位标签,实现物联网系统自底向上的安全防护。

2 半导体气敏传感器偏差分析

气敏传感器能将检测到的气体成分和浓度大小转换为电信号,但由于其制造过程的随机工艺偏差使得输出电信号值偏离理论值,因此可以利用气敏传感器制备工艺偏差构建气敏传感PUF发生器。气敏传感器检测系统主要由3部分组成:气体成分特异性识别和浓度识别的半导体气敏材料、非电信号转换为电信号的敏感组件和记录信号的辅助仪器,结构如图1所示。半导体气敏材料为纳米材料,具有高比表面积,气体与材料的接触面积大,为气体分子吸附提供更多的活性位点,有助于气敏性能的提高。

静电喷雾沉积(Electrostatic Spray Deposition, ESD)是制备纳米材料的常用方法^[16]。泰勒锥的形成和射流鞭动是两个随机性很强的静电喷雾关键环节。泰勒锥表面是液相和气相的边界,环境气体的快速吸附和溶剂蒸发两个过程并存,因此,不可避免地会引起泰勒锥内部扰乱,影响泰勒锥的形状^[17]。射流鞭动是静电喷雾时聚合物喷射流的运动轨迹,呈复杂的3维非直线型“鞭动”。刚开始喷的丝是直的,随后发生弯曲、不稳定。Shin等人^[18]针对射流的不稳定阶段提出鞭动模型,用线性不稳定性分析射流鞭动的发生。在已知流体性质和工艺参数条件下,给出式(1)扰动系数的数学方程

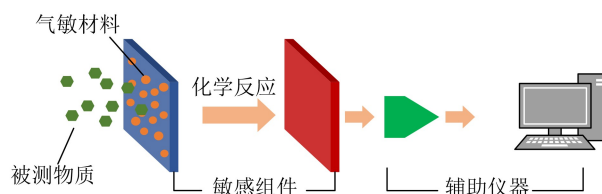


图1 气敏传感器检测系统结构示意图

$$\Gamma(E_{\infty}, Q) = \ln \left[\frac{A(s)}{A(0)} \right] = \int_0^s \frac{\omega(h, E, \sigma)}{Q} \pi h^2 dh \quad (1)$$

其中, $\Gamma(E_{\infty}, Q)$ 为不稳定放大因子, $A(s)$ 为振幅, s 为向下移动距离, ω 为增长速率, h 为射流半径, Q 为流率, σ 为射流表面电荷密度。

纳米材料中纤维表面对气体分子的吸附能力赋予每个传感器独有的气敏特性。由于与喷雾效果相关的液体黏度、湿度、温度等参数在实验过程中不可避免地发生变化, 导致射流振动不完全可控, 致使纳米纤维的直径大小以及取向的排列发生差异。聚合物溶液通过电场到达收集板, 从喷射口喷射出无数方向不定、粗细不一的纤维层层堆叠, 导致每块纤维区域密度都具有随机性和唯一性。因此, 每块区域吸附气体能力不同, 可利用此特征得到随机的、不可克隆的气敏传感PUF发生器。

3 气敏传感PUF发生器设计

3.1 半导体气敏传感器的制备

采用ESD技术制备纳米材料, 装置如图2所示, 其具体制备过程如下: 将 $\text{Pd}(\text{NO}_3)_2 \cdot 2\text{H}_2\text{O}$ (5 mg), $\text{SnCl}_4 \cdot 5\text{H}_2\text{O}$ (701 mg)和聚乙烯吡咯烷酮 (1200 mg)溶解于二甲基甲酰胺 (5 ml)和乙醇 (5 ml)混合溶液中, 在室温下搅拌6 h, 使溶液均匀; 将其灌入注射器, 固定在推进泵上; 将高压电源的阳极连接注射器喷嘴, 阴极连接接地的收集板, 阴阳极距离保持15 cm; 在16 kV高压电场作用下, 注射器喷头开始喷射纤维材料; 将纤维材料放入马弗炉, 在空气氛围中以 $1^\circ\text{C}/\text{min}$ 的加热速率至 600°C , 并保持2 h, 然后冷却。

传感器一般分为内热式和旁热式两种结构。旁热式气敏器件的氧化铝陶瓷管内放置高阻加热丝,

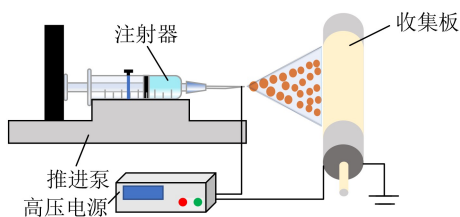
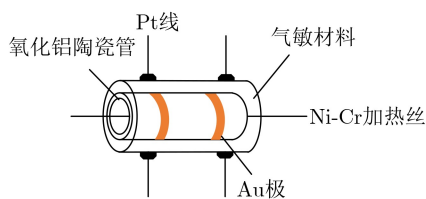
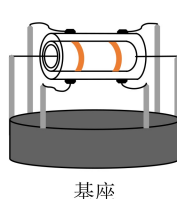


图2 静电喷雾装置示意图



(a) 传感器结构图



(b) 传感器实物图

图3 传感器示意图

陶瓷管外涂梳状金电极, 再在金电极外涂气敏半导体材料。这种结构克服了内热式器件热容量小、易受环境气流影响和测量不稳定的缺点, 明显提高器件稳定性。具体制作过程如下: 将制备好的纳米材料和去离子水按一定比例混合成糊状物; 将糊状物涂到两端固定铂金线的氧化铝管上, 也同样在空气氛围中以 $1^\circ\text{C}/\text{min}$ 加热速率至 600°C , 保持2 h; 待冷却后取出。在氧化铝陶瓷管轴心穿入一根直径为0.05 mm, 长度为10.5 mm细合金加热丝, 用于加热; 将加热丝和用作测量电极的铂金线焊在传感器基座上, 即完成旁热式气敏器件制备。传感器如图3所示。为使传感器具有更好的稳定性和重复性, 还需将其在 300°C 环境温度下老化2~7 d。

3.2 传感器响应提取

为完成传感器响应提取, 搭建如图4所示气敏传感PUF发生器测试平台, 由测试腔、气敏单元、蒸发台、推进泵、流量计等组成。在测试过程中, 开启阀门1~4; 将安装有8个气敏传感器(作为1个阵列)的电路放入测试腔, 并封闭; 为气敏单元电热丝提供4.5 V直流电源。用数据采集仪(如自带信号采集软件的安捷伦34970 A)观测时间-电阻曲线, 待曲线平稳, 即传感器已经进入准稳态; 用微量进样器抽取一定量目标物的液体, 通过推进泵将液体注射到蒸发台。由于蒸发台温度达 100°C , 液体将快速气化, 并均匀扩散。同时, 数据采集仪实时记录8个气敏传感器电阻值变化。待传感器电阻值稳定, 推进泵停止推进, 使空气重新充满测试腔。如此交替, 可得到传感器阵列对一定浓度目标气体响应性能。

3.3 高稳态PUF发生器数据生成

由于气敏传感器制备工艺的随机偏差, 采集到的电阻值具有唯一性。将上述数据利用随机阻值多位平衡算法^[15]进行处理。其过程如下: 将3个传感器组合为1个传感器簇, 比较两个传感器簇总和电阻的大小, 结果用1位二进制数表示。如果第1个簇的阻值和较大, 则结果为1, 反之为0。从8个传感器中选出3个作为1簇, 共有 C_3^8 , 即56种选择; 再从中任选两簇进行阻值和比较运算, 则产生 C_2^{56} , 即

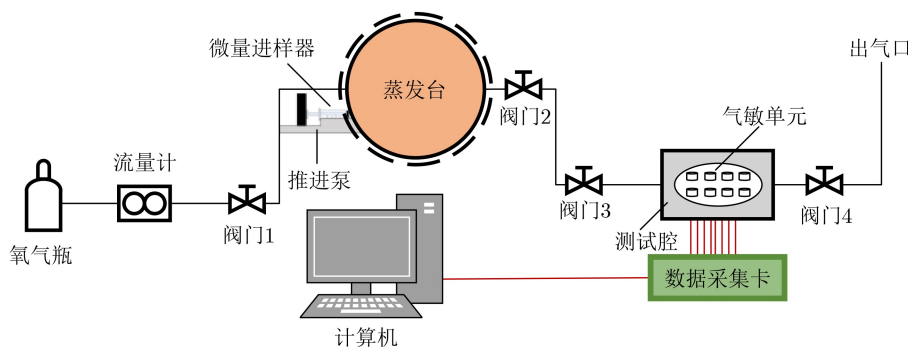


图4 测试平台示意图

128种可能性。簇选择和比较运算将不同传感器测量值随机比较,进而得到128位PUF响应。该响应不会偏向任意某个传感器,从而达到平衡。

具体数据生成方法使用8位随机阻值平衡算法,调用该算法16次生成128位响应,算法的伪代码如表1所示。算法假定8位子集包含在数组bit中,数组*v*包含8个气敏传感器关联的电阻值,传感器0的值位于数组*v*位置0,传感器1的值位于数组*v*位置1,依此类推。数组*lef*和*r*表示被选择的两簇传感器位置,取出数组*v*中与位置对应的电阻值,作阻值和比较运算。之后,place的值增加1,也就是将被选择的每个传感器位置都加1,以确定在随后的比较中使用哪几个传感器。进行8次比较后,一个过程完成,生成8个响应位。之后,改变*lef*与*r*的初始值以生成后续8位子集。

4 实验结果分析

主要包括3部分:(1)材料表征;(2)偏差特性分析;(3)PUF发生器性能分析。用扫描电子显微镜(Scanning Electron Microscope, SEM)对材料形貌进行表征,观察纳米材料外观结构和形貌;用X射

线衍射分析仪(X-Ray Diffraction, XRD)测定并分析产物物相结构;搭建测试平台提取传感器偏差。采用唯一性、可靠性和随机性3种常用性能指标评估输出响应。

4.1 材料表征

SEM表征纳米材料为颗粒状氧化物形貌,如图5所示。纳米颗粒的大小没有规律地散落分布,局部形成团聚,分布具有高度随机性。在不同分辨率情况下都可以观察到氧化物颗粒形态各异,每一个区域与气体分子的接触范围都不相同,是传感器PUF发生器差异性的原因所在。

图6为Pd-SnO₂纳米材料样品经600 °C高温烧结后的XRD图谱。可以发现,(110),(101),(200),(211),(220),(310),(321)等的衍射峰,与SnO₂的JCPDS(Joint Committee on Powder Diffraction Standards)标准卡片(PDF#77-0447)峰型吻合。Pd的掺杂并没有改变SnO₂的晶体结构,没有出现PdO的特征峰,其原因在于制备的纳米材料中PdO占比很小。

4.2 偏差特性分析

偏差特性表示不同传感器对同一气体激励源的偏差情况。用安捷伦多路数据采集仪实时记录原始电信号,反映传感器电阻随测试腔中甲醛气体浓度变化而变化的信息。传感器的响应定义为^[19]

$$R = R_a/R_g \quad (2)$$

其中, R_a 和 R_g 为气敏传感器在空气和目标气体的电阻值。利用式(2)计算传感器响应随时间变化的趋势,如图7所示。在200 ppm甲醛气体浓度下,对所制备的Pd-SnO₂气敏传感器进行两次循环。可以发现,在响应曲线较为平稳阶段,传感器A和传感器B表现出偏差特性, R_A 和 R_B 变化趋势一致,且 $R_A > R_B$ 。有效降低阻值比较时响应翻转现象出现的可能性,提高输出响应的稳定性。

4.3 PUF发生器性能分析

4.3.1 随机性

随机性表示PUF发生器输出数据中逻辑0和逻

表1 8位随机阻值平衡算法伪代码

```

(1) int bit[place]
(2) int lef[3]
(3) int r[3]
(4) double v[8]
(5) i=0
(6) do {lsum=v[(i+lef[0]) mod 8]+v[(i+lef[1]) mod 8]+v[(i+lef[2]) mod 8]
(7) rsum=v[(i+r[0]) mod 8]+v[(i+r[1]) mod 8]+v[(i+r[2]) mod 8]
(8) if lsum>rsum
(9) then bits[place]=1
(10) else bits[place]=0
(11) place=place+1}
(12) while(i<8)
(13) return

```

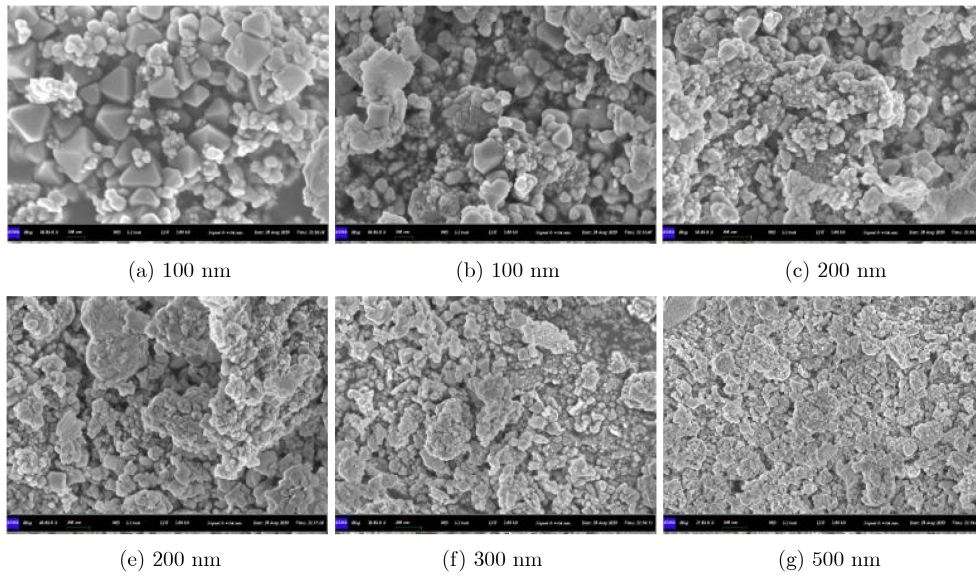


图5 不同分辨率下的SEM表征

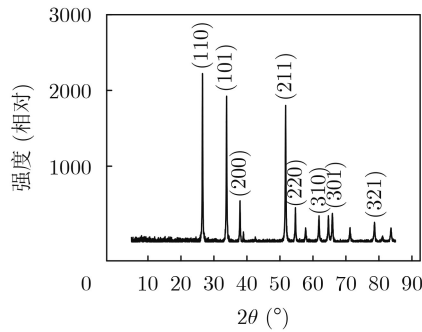


图6 XRD表征

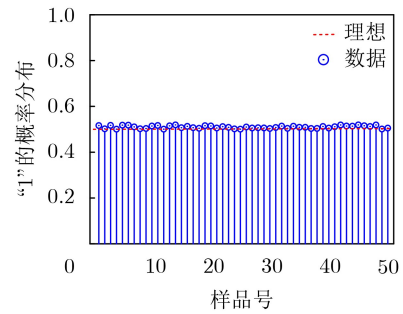


图8 随机性概率分布

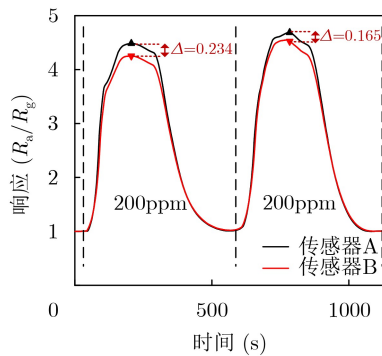


图7 传感器响应

辑1分布情况。在理想情况下，逻辑0和逻辑1的概率应相同，即随机性为100%。按式(3)计算^[20]

$$\text{Randomness} = (1 - |1 - 2P(r = 1)|) \times 100\% \quad (3)$$

其中， r 为输出响应， P 为输出响应中1的概率。实验制备了50组气敏传感PUF发生器样本，测试了6400位二进制响应。其中，“0”的数量为3138位，“1”的数量为3262位，则得该PUF发生器的随机性为98.06%，如图8所示。

4.3.2 唯一性

唯一性表示多个设备对同一激励的响应区分度，通过片间汉明距离(Hamming Distance, HD)计算。在理想情况下，唯一性接近50%。按式(4)计算^[20]

$$\text{Uniqueness} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^k \frac{\text{HD}(R_i, R_j)}{n} \times 100\% \quad (4)$$

其中， k 为PUF发生器的数量， R_i 和 R_j 分别为第*i*和第*j*个PUF发生器的输出响应， $\text{HD}(R_i, R_j)$ 为输出响应的汉明距离，则得该PUF发生器的唯一性为49.04%，接近理想值50%，如图9所示。

4.3.3 可靠性

可靠性表示PUF发生器在给定输入激励始终产生正确响应的可能性。理想情况下，可靠性为100%，这意味着PUF发生器将始终产生正确的响应。按式(5)计算*n*位响应的可靠性^[20]

$$\text{Reliability} = 100\% - \frac{1}{m} \sum_{t=1}^m \frac{\text{HD}(R_u, R_v)}{n} \times 100\% \quad (5)$$

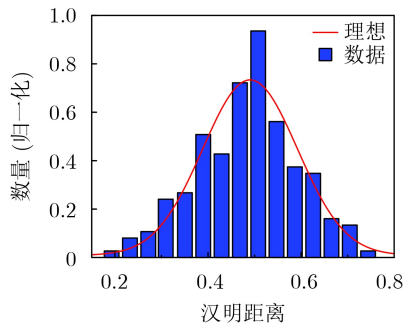


图9 汉明距离分布

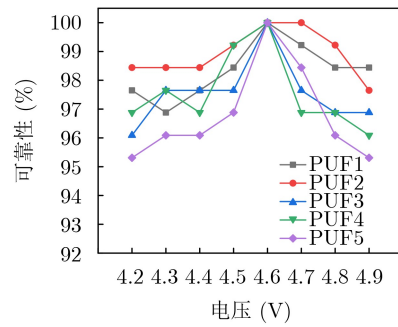


图10 不同电压下的可靠性

其中， m 为同一激励下测量的次数， n 为响应数据的位数， R_u 为选取的参考响应数据， R_v 为第 v 次测量的响应数据。在4.2 ~ 4.9 V电压范围内，以0.1 V为增量，以4.6 V为参考点，选取5个PUF发生器样本进行测试，统计结果如图10所示。可以发现，随着电压偏离参考点，其可靠性出现下降的总体趋势，具备PUF的典型特征。

可靠性还反映在一定时间内响应的变化情况。在常温常压下，选取5个PUF发生器样本进行400 s连续测试。用每个PUF发生器的第1个响应作参考响应，统计结果如图11所示。可以发现，前90 s的可靠性保持在100%，之后的310 s，也保持95%以上。

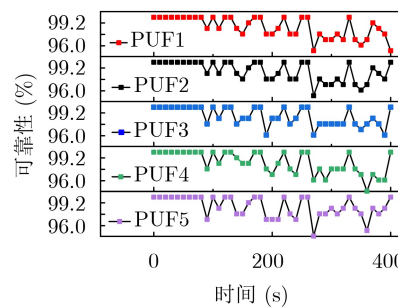


图11 400 s内的可靠性

表2为与其他类型PUF发生器之间的性能比较。所设计的PUF发生器随机性为98.06%，可靠性为97.85%，唯一性为49.04%。

表2 与相关文献的比较结果(%)

文献	PUF类型	响应机制描述	唯一性	可靠性
仲裁器 ^[5]	硅PUF	利用时延差异产生响应	49.88	92.88
SRAM ^[6]	硅PUF	利用SRAM单元上电差异产生响应	49.6	97.86
能量收集器 ^[11]	传感器PUF	利用太阳能电池对光强的偏差输出产生响应	-	92.97
MEMS传感 ^[14]	传感器PUF	利用陀螺仪的输出产生响应	42.64	92.17
压电传感器 ^[15]	传感器PUF	利用压电传感器对电压源的偏差输出产生响应	-	96.07
本文	传感器PUF	利用气敏传感器对气体感应偏差产生响应	49.04	97.85

5 结论

本文所提基于气敏传感器的高稳态物理不可克隆函数发生器设计方案将感知器件和PUF发生器有效结合起来，通过分析传感器制造过程的随机偏差，测试多组外部激励下的传感器响应，利用随机阻值多位平衡算法生成高稳态PUF发生器数据，依靠传感器组件而不需要设计专用PUF电路模块，有效减少资源的开销。实验测试结果表明，基于气敏传感器的PUF发生器，在可靠性、随机性和唯一性上均有较理想的特性，可为解决极端资源受限系统的高安全性问题提供解决途径，为物联网的发展提供安全保障。

参考文献

- [1] BUTUN I, OSTERBERG P, and SONG H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(1): 616-644. doi: 10.1109/COMST.2019.2953364.
- [2] SAIRAM R, BHUNIA S, THANGAVELU V, et al. NETRA: Enhancing IoT security using NFV-based edge traffic analysis[J]. *IEEE Sensors Journal*, 2019, 19(22): 4660-4671. doi: 10.1109/JSEN.2019.2900097.
- [3] KOYUICEM D, BOUABDALLAH A, and LAKHLEF H. Internet of Things security: A top-down survey[J]. *Computer Networks*, 2018, 141(2018): 199-221. doi: 10.1016/j.comnet.

- 2018.03.012.
- [4] PAPPU R, RECHT B, TAYLOR J, *et al.* Physical one-way functions[J]. *Science*, 2002, 297(5589): 2026–2030. doi: [10.1126/science.1074376](https://doi.org/10.1126/science.1074376).
- [5] 龚越, 叶靖, 胡瑜, 等. 内建自调整的仲裁器物理不可克隆函数[J]. 计算机辅助设计与图形学学报, 2017, 29(9): 1734–1739. doi: [10.3969/j.issn.1003-9775.2017.09.018](https://doi.org/10.3969/j.issn.1003-9775.2017.09.018).
GONG Yue, YE Jing, HU Yu, *et al.* Built-in self-adjusting arbiter PUF[J]. *Journal of Computer-Aided Design & Computer Graphics*, 2017, 29(9): 1734–1739. doi: [10.3969/j.issn.1003-9775.2017.09.018](https://doi.org/10.3969/j.issn.1003-9775.2017.09.018).
- [6] 孙子文, 叶乔. 利用震荡环频率特性提取多位可靠信息熵的物理不可克隆函数研究[J]. 电子与信息学报, 2021, 43(1): 234–241. doi: [10.11999/JEIT191013](https://doi.org/10.11999/JEIT191013).
SUN Ziwen and YE Qiao. Study on the physical unclonable function of the reliable information entropy extracted by the frequency characteristic of oscillating ring[J]. *Journal of Electronics & Information Technology*, 2021, 43(1): 234–241. doi: [10.11999/JEIT191013](https://doi.org/10.11999/JEIT191013).
- [7] LI Gang, WANG Pengjun, MA Xuejiao, *et al.* A 215-F² bistable physically unclonable function with an ACF of < 0.005 and a native bit instability of 2.05% in 65-nm CMOS process[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2020, 28(11): 2290–2299. doi: [10.1109/TVLSI.2020.3014892](https://doi.org/10.1109/TVLSI.2020.3014892).
- [8] GOLANBARI M, KIAMEHR S, BISHNOI R, *et al.* Reliable memory PUF design for low-power applications[C]. The 19th International Symposium on Quality Electronic Design, Santa Clara, USA, 2018: 207–213. doi: [10.1109/ISQED.2018.8357289](https://doi.org/10.1109/ISQED.2018.8357289).
- [9] 张培勇, 袁晓东, 王雪洁, 等. 基于D触发器的物理不可克隆函数[J]. 浙江大学学报(理学版), 2019, 46(1): 35–41. doi: [10.3785/j.issn.1008-9497.2019.01.005](https://doi.org/10.3785/j.issn.1008-9497.2019.01.005).
ZHANG Peiyong, YUAN Xiaodong, WANG Xuejie, *et al.* D flip-flop based physical unclonable function[J]. *Journal of Zhejiang University (Science Edition)*, 2019, 46(1): 35–41. doi: [10.3785/j.issn.1008-9497.2019.01.005](https://doi.org/10.3785/j.issn.1008-9497.2019.01.005).
- [10] FUKUSHIMA K, YOSHIMURA A, KIYOMOTO S, *et al.* Evaluation of software PUF based on gyroscope[C]. The 15th International Conference on Information Security Practice and Experience, Kuala Lumpur, Malaysia, 2019: 232–247. doi: [10.1007/978-3-030-34339-2_13](https://doi.org/10.1007/978-3-030-34339-2_13).
- [11] KUMAR S, LABRADO C, BADHAN R, *et al.* Solar cell based physically unclonable function for cybersecurity in IoT devices[C]. 2018 IEEE Computer Society Annual Symposium on VLSI, Hong Kong, China, 2018: 697–702. doi: [10.1109/ISVLSI.2018.00131](https://doi.org/10.1109/ISVLSI.2018.00131).
- [12] ROSENFELD K, GAVAS E, and KARRI R. Sensor physical unclonable functions[C]. 2010 IEEE International Symposium on Hardware-Oriented Security and Trust, Anaheim, USA, 2010: 112–117. doi: [10.1109/HST.2010.5513103](https://doi.org/10.1109/HST.2010.5513103).
- [13] DEY S, ROY N, XU Wenyuan, *et al.* AccelPrint: Imperfections of accelerometers make smartphones trackable[C]. Network and Distributed System Security Symposium, San Diego, USA, 2014: 1–16. doi: [10.14722/ndss.2014.23059](https://doi.org/10.14722/ndss.2014.23059).
- [14] AYSU A, GHALATY N, FRANKLIN Z, *et al.* Digital fingerprints for low-cost platforms using MEMS sensors[C]. Workshop on Embedded Systems Security, Montreal Quebec, Canada, 2013: 1–6. doi: [10.1145/2527317.2527319](https://doi.org/10.1145/2527317.2527319).
- [15] LABRADO C and THAPLIYAL H. Design of a piezoelectric-based physically unclonable function for IoT security[J]. *IEEE Internet of Things Journal*, 2019, 6(2): 2770–2777. doi: [10.1109/JIOT.2018.2874626](https://doi.org/10.1109/JIOT.2018.2874626).
- [16] KANG D, KIM J, KIM I, *et al.* Experimental qualification of the process of electrostatic spray deposition[J]. *Coatings*, 2019, 9(5): 294–312. doi: [10.3390/coatings9050294](https://doi.org/10.3390/coatings9050294).
- [17] 刘兆香, 刘勇, 王欣, 等. 静电纺丝过程中泰勒锥、射流鞭动和电晕现象分析[J]. 塑料, 2012, 41(3): 29–34. doi: [10.3969/j.issn.1001-9456.2012.03.010](https://doi.org/10.3969/j.issn.1001-9456.2012.03.010).
LIU Zhaoxiang, LIU Yong, WANG Xin, *et al.* Phenomena analysis of taylor cone, jet whipping and corona in process of electrospinning[J]. *Plastic*, 2012, 41(3): 29–34. doi: [10.3969/j.issn.1001-9456.2012.03.010](https://doi.org/10.3969/j.issn.1001-9456.2012.03.010).
- [18] SHIN Y, HOHMAN M, BRENNER M, *et al.* Experimental characterization of electrospinning: The electrically forced jet and instabilities[J]. *Polymer*, 2001, 42(25): 9955–9967. doi: [10.1016/S0032-3861\(01\)00540-7](https://doi.org/10.1016/S0032-3861(01)00540-7).
- [19] YI J, LEE J, and PARK W. Vertically aligned ZnO nanorods and graphene hybrid architectures for high-sensitive flexible gas sensors[J]. *Sensors & Actuators*, 2011, 155(1): 264–269. doi: [10.1016/j.snb.2010.12.033](https://doi.org/10.1016/j.snb.2010.12.033).
- [20] 李刚, 汪鹏君, 张跃军, 等. 基于65 nm工艺的多端口可配置PUF电路设计[J]. 电子与信息学报, 2016, 38(6): 1541–1546. doi: [10.11999/JEIT150968](https://doi.org/10.11999/JEIT150968).
LI Gang, WANG Pengjun, ZHANG Yuejun, *et al.* Design of multi-port configurable PUF circuit based on 65 nm technology[J]. *Journal of Electronics & Information Technology*, 2016, 38(6): 1541–1546. doi: [10.11999/JEIT150968](https://doi.org/10.11999/JEIT150968).
- 汪鹏君: 男, 1966年生, 教授, 研究方向为集成电路设计、信息安全等技术及其相关理论。
李乐薇: 女, 1997年生, 硕士生, 研究方向为集成电路设计、信息安全等技术及其相关理论。
郑雁公: 男, 1983年生, 副教授, 研究方向为气敏材料以及沸石相关理论。
李刚: 男, 1988年生, 讲师, 研究方向为集成电路设计、信息安全等技术及其相关理论。