

基于 Ni-SnO₂ 纳米颗粒的 GS-PUF 设计

李乐薇¹, 汪鹏君^{2*}, 张跃军¹

(1. 宁波大学 信息科学与工程学院, 浙江 宁波 315211; 2. 温州大学 电气与电子工程学院, 浙江 温州 325035)

摘要: 气敏传感器具有气体识别、探测和监测等功能, 广泛应用于工业生产等领域, 但在泄漏预警时缺乏迅速识别和定位等功能. 本文基于传感器制备工艺偏差分析, 通过对传感器气敏机制的研究, 提出一种基于 Ni-SnO₂ 纳米颗粒的气敏传感器物理不可克隆函数(Gas Sensor-Physical Unclonable Function, GS-PUF)设计方案. 该方案利用掺杂 Ni 元素的方法, 结合静电喷雾沉积技术制备 Ni-SnO₂ 气敏传感器, 以获取更加稳定可靠的物理特征值, 然后采集气敏传感器对不同浓度下气体的响应数据, 最后利用随机阻值多位平衡算法比较不同组气敏传感器响应电信号值, 实现 PUF 数据输出. 制备每组样本可产生 128 位二进制数据的多组 PUF 样本, 进行对比实验. 结果表明, 所设计的 GS-PUF 具有气体泄漏源头识别定位的功能, 且随机性提升至 99%, 唯一性达 49.80%.

关键词: Ni-SnO₂ 纳米颗粒; 物理不可克隆函数; 气敏传感器; 静电喷雾沉积

中图分类号: TN79

文献标志码: A

文章编号: 1001-5132 (2021) 06-0061-06

物联网(Internet of Things, IoT)是新一代信息技术重要组成部分, 它被称为继计算机、互联网之后世界信息产业发展的第三次浪潮. 目前, 全球有 100 多亿台设备相互连接, 预计未来 5 年将部署超过 5 倍的设备^[1]. 按照最初设计, 大部分设备隔离运行, 攻击者很难访问它们. 但是随着世界互联性加强, 许多以前孤立的设备现在支持在各种网络上进行外部通信, 也引发了一些新型攻击手段^[2]. 同时, 这些设备通常具有低功耗、可用内存较少以及处理能力有限等特性, 将限制添加新安全功能单元的可能性. 为了解决此问题, 研究人员开始探索非标准解决方案.

物理不可克隆函数(Physical Unclonable Function, PUF)是应对物联网设备潜在安全问题的研究热点之一^[3], 其通过对一个物理实体输入激励, 利用制造过程引起的固有偏差生成一个不可预测的响应, 实现物理不可克隆, 能有效防御攻击. 同时对于资源有限的物理实体, 不仅可以实现与传统

公钥密码一样的功能, 而且可以大大减少计算、存储和通信开销. 随着物联网兴起, 对 PUF 研究不再局限于集成电路本身激励-响应特性, 而且开始设计基于传感器等器件的新型 PUF 结构^[4]. Cao 等^[5]利用 CMOS 图像传感器制造过程中的固有缺陷产生唯一且可靠数字签名, 用于智能手机识别和防伪. Kumar 等^[6]利用太阳能电池的内在变化, 使用 Tiva TM4C123GH6PM 微控制器设计基于太阳能电池的 PUF 方案. Valsesia 等^[7]从原始图像中提取光学传感器光响应不均匀性的高频分量, 并创建弱 PUF, 同时基于自适应随机投影和使用极性码的创新模糊提取器设计一种用于高效传输和服务端验证的新颖方案. Rahim 等^[8]提出基于区块链和传感器 PUF 组合身份验证机制, 用于物联网设备实时认证, 建立用户与 IoT 设备之间的智能交互身份认证系统.

近年来, 气敏传感技术获得跨越式发展, 相关传感器在工业安全领域销量最大. 当化工气体发

收稿日期: 2021-06-15.

宁波大学学报(理工版)网址: <http://journal.lg.nbu.edu.cn/>

基金项目: 国家自然科学基金(61874078, 61871244); 国家重点研发项目(2018YFB2202100); 宁波市公益性计划项目(202002N3134); 宁波大学研究生科研创新基金.

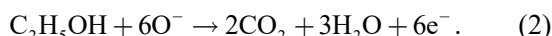
第一作者: 李乐薇(1997-), 女, 河南南阳人, 在读硕士研究生, 主要研究方向: 信息安全等技术及其相关理论. E-mail: 956876464@qq.com

*通信作者: 汪鹏君(1966-), 男, 浙江宁波人, 教授, 主要研究方向: 集成电路和信息安全等相关理论. E-mail: wangpengjun@wbu.edu.cn

生泄漏后,担任检测职能的气敏传感器可以及时可靠地探测空气中泄露气体的含量,但无法提供定位标签,也就是说难以找到气体泄露源头,常常耽误最佳抢修时间.如在江苏扬州发生的一起乙醇罐车泄露事件中,司机在发现险情后迅速报警,但因对道路状况不熟悉,无法说出准确地点,导致相关抢险救援人员 1 h 后才到达现场.汪鹏君等^[9]提出基于气敏传感器的物理不可克隆发生器设计,给出了气敏传感器 PUF 整体框架,但未对传感器组件性能对 PUF 数据的影响进行讨论.鉴此,本文基于掺杂机理分析,通过 Ni 掺杂方法以获得更加稳定可靠的物理特征信息,实现基于 Ni-SnO₂ 纳米颗粒的 GS-PUF.

1 掺杂机理分析

SnO₂ 作为一种 N 型半导体材料,当其暴露在空气中,吸附在表面上的氧分子会夺取部分电子成为氧离子,载流子电子浓度降低,SnO₂ 显示出高电阻性.本文的目标气体以乙醇为例进行阐述,当 SnO₂ 传感器暴露目标气体中,乙醇作为还原性气体与 SnO₂ 表面氧离子反应,并将捕获的电子释放回 SnO₂,SnO₂ 中载流子浓度增加,电阻降低.氧化物表面与乙醇之间的反应可以简单描述如下^[10]:



当向 SnO₂ 中添加 NiO 时,在 NiO 和 SnO₂ 粒

子界面处形成 pn 结.图 1 为被空气和乙醇包围时 Ni-SnO₂ 传感器简化模型.在这种情况下,由于 2 块半导体之间载流子浓度的梯度很大,SnO₂ 中的电子和 NiO 中的空穴向相反方向扩散.直到 pn 结的费米能级相等,整个过程在 NiO 和 SnO₂ 颗粒界面处建立一个耗尽层,对提高 Ni-SnO₂ 传感器的传感性能起着关键作用^[11].Ni-SnO₂ 气敏传感器以电子作为多数载流子,自由电子将在吸附过程中被氧气捕获,并导致 pn 结处耗尽层宽度增加,如图 1(a)所示.一旦传感器暴露在乙醇气体中,传感器表面的氧化物促进乙醇气体分子氧化为 CO₂ 和 H₂O,捕获的电子释放回传感器,从而降低传感器阻值.此外,C₂H₅OH 将电子释放到 NiO 中,电子-空穴复合运动导致 NiO 中空穴浓度降低,电子浓度增加.因此,pn 结两侧相同载流子的浓度梯度降低,载流子的扩散大大减少,界面处的耗尽层更薄,如图 1(b)所示.纳米颗粒中 pn 结的存在能大大提高传感器表面氧分子和乙醇的吸附和分解速率,使传感器显示出优异的传感性能,包括高灵敏度、重复性以及更短的响应和恢复时间,这些传感性能的提升不仅有助于更快地提取所需的物理特征信息,还能使物理特征信息更加稳定可靠,进一步提高生成 PUF 数据的性能.

2 多比特输出 GS-PUF 设计

由于制造过程的随机工艺偏差使得每个气敏

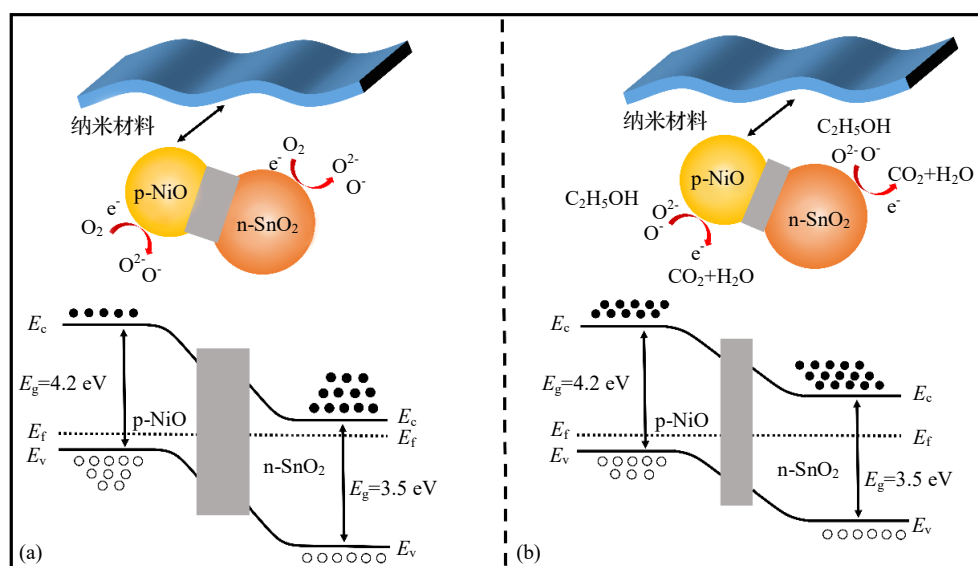


图 1 Ni-SnO₂ 传感器在空气和乙醇中气敏机理示意与能带结构图

传感器对气体的识别能力具有不可克隆性, 对不同气敏传感器信号值进行比较后, 可得到单比特 GS-PUF 输出. 多比特输出 GS-PUF 设计相应框架如图 2 所示, 具体实现方式参考作者前期发表的文章[9]. 整个设计包括外部激励源、气敏传感器阵列、传感器数据采集模块和阵列信号处理模块. 在阵列中放置 8 个气敏传感器, 制备传感器所需敏感材料采用静电喷雾沉积技术, 所需化学试剂如下: SnCl₄·5H₂O (525 mg)、NiCl₂·2H₂O (17 mg)、聚乙烯吡咯烷酮(1 200 mg)、N,N-二甲基甲酰胺(5 mL)、无水乙醇(5 mL). 使用乙醇气体作为外部激励源, 为阵列创造气体环境, 使 8 个气敏传感器分别产生一个输出阻值, 阻值采集模块通过搭建的信号传输平台, 采集 8 个气敏传感器的输出阻值, 并传输给数据处理模块, 数据处理模块将 8 个半导体气敏传感器中每 3 个作为 1 个传感器组, 并从不同的传感器组中选取 2 个组作为 1 个比较簇, 组选择和簇比较进行 128 次, 以得到 PUF 输出响应.

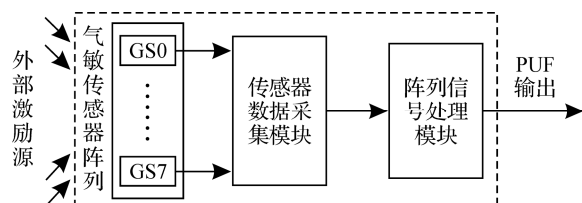


图 2 多比特输出 GS-PUF 设计框架

3 实验结果分析

实验过程制备多组基于 SnO₂ 和 Ni-SnO₂ 纳米颗粒的 GS-PUF 样本进行对比实验. 采用扫描电子显微镜(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; 采用 X 射线衍射分析仪(X-Ray Diffraction, XRD)测定并分析产物的晶相和成分; 搭建测试平台提取传感器偏差, 采用唯一性和随机性两种常用性能指标评估输出响应.

3.1 纳米材料特性分析

图 3 为 SnO₂ 和 Ni-SnO₂ 纳米颗粒 SEM 表征图. 由图可见, 氧化物表面是由形状不规则、带有棱角的纳米颗粒组成, 尺寸从几十纳米至几百纳米不等. 纳米颗粒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, 这导致每个区域

与气体分子的接触范围都不相同, 可实现气敏传感器 PUF 不可克隆的性质.

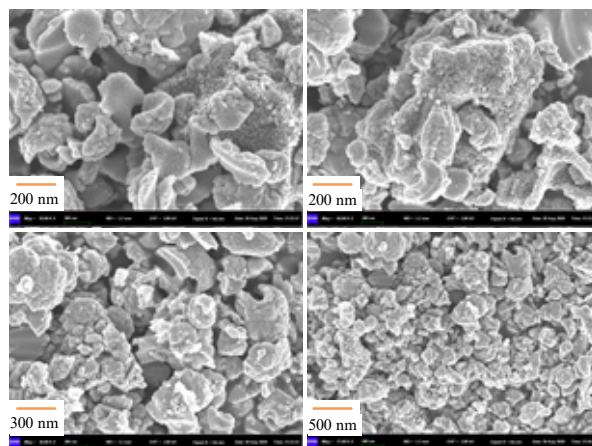
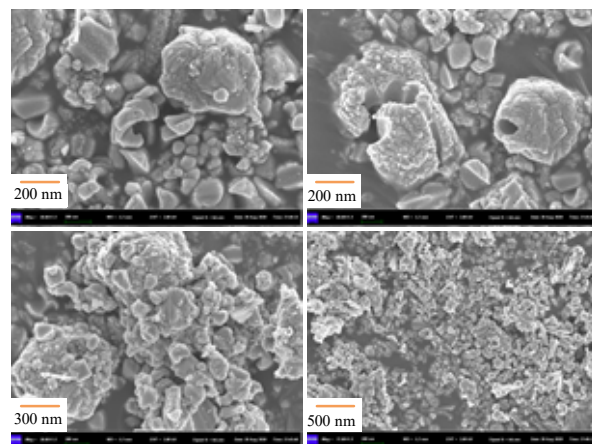
(a) SnO₂(b) Ni-SnO₂图 3 SnO₂ 和 Ni 掺杂 SnO₂ 纳米颗粒 SEM 图

图 4 为 2 种纳米颗粒样品经 600 °C 高温烧结后 XRD 图谱. 可以发现, (110)、(101)、(200)、(211) 等衍射峰与 SnO₂ 的 JCPDS(Joint Committee on Powder Diffraction Standards)标准卡片(PDF#77-

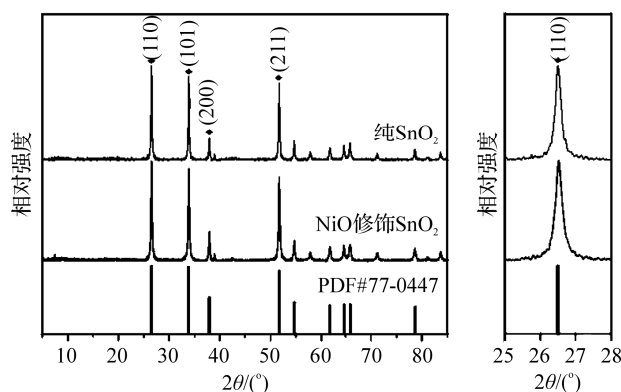


图 4 XRD 表征

0447)峰型吻合. 由于 NiO 占比很小, Ni 的掺杂并没有改变 SnO_2 的晶体结构, 所以也没有出现 NiO 的特征峰.

3.2 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. 传感器的响应定义为^[12]:

$$R = R_a / R_g, \quad (3)$$

式中: R_a 为气敏传感器在空气中的电阻值, R_g 为气敏传感器目标气体中的电阻值. 利用式(3)计算传感器响应随时间变化的趋势. 对制备的 Ni-SnO₂ 气敏传感器和 SnO_2 气敏传感器在 600×10^{-6} 和 500×10^{-6} 乙醇气体浓度下进行测试. 由图 5 可以发现, 在响应曲线较为平稳阶段, 传感器 1 和传感器 2 表现出偏差特性. 且 SnO_2 气敏传感器信号值进入平稳阶段需 48 s, Ni-SnO₂ 气敏传感器需 41 s. 通过掺杂, 传感器气敏特性得到提高, 同时也减少了 PUF 数据生成的等待时间.

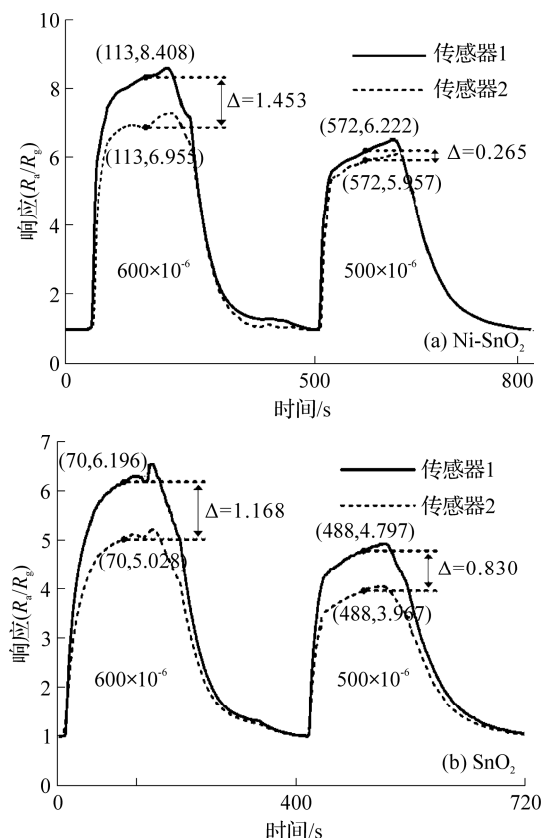


图 5 传感器响应偏差分析

3.3 GS-PUF 特性分析

3.3.1 随机性

信息熵是一个用来衡量比特流随机性的指标.

PUF 输出有 2 种状态, 即逻辑 1 和逻辑 0. 因此, 信息熵 E 可表示为^[13]:

$$E = -(p(r=0) \log_2 p(r=0) + p(r=1) \log_2 p(r=1)), \quad (4)$$

式中: $p(r=0)$ 和 $p(r=1)$ 分别代表了输出逻辑 0 和逻辑 1 的概率. 当且仅当 $p(r=0) = p(r=1) = 0.5$ 时, $E = 1$. 图 6 则给出所提取 PUF 各组样品输出响应熵值分布.

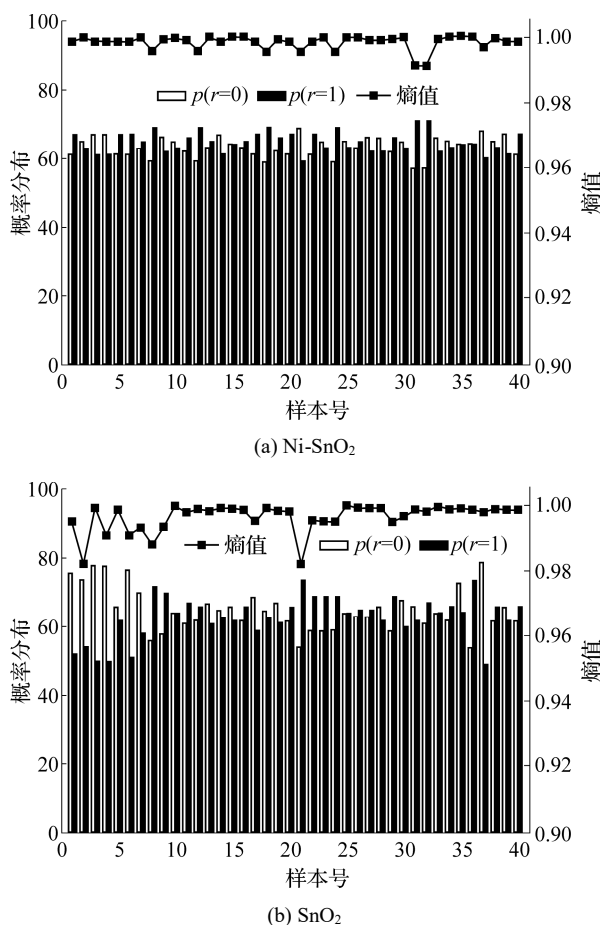


图 6 PUF 输出响应的随机性

其中图 6(a)各组输出响应信息熵均大于 0.98, 图 6(b)各组输出响应信息熵均大于 0.99. 这也由此表明基于 Ni-SnO₂ 纳米颗粒的 GS-PUF 输出响应具有更好的随机性.

3.3.2 唯一性

唯一性表示多个设备对同一激励的响应区分度, 可由汉明距离(Hamming Distance, HD)衡量, 在理想情况下, 其值为 50%. 唯一性算式如下^[14]:

$$U_{\text{Uniqueness}} = \frac{2}{k(k-1)} \times$$

$$\sum_{i=1}^{k-1} \sum_{j=i+1}^k \frac{HD(R_i, R_j)}{n} \times 100\%, \quad (5)$$

式中: k 为 PUF 的数量; R_i 和 R_j 分别为第 i 和第 j 个 PUF 的输出响应; $HD(R_i, R_j)$ 为输出响应之间的汉明距离. 结果如图 7 所示, 基于 SnO₂ 纳米颗粒的 GS-PUF 唯一性为 45.16%, 基于 Ni-SnO₂ 纳米颗粒的 GS-PUF 唯一性为 49.80%, 唯一性得到提高, 接近理想值 50%. 由此表明, 每组 PUF 响应间具有明显区分度, 可将此响应作为定位标签赋在传感器上. 当气体发生泄漏, 即可通过唯一的标签找到泄露源头.

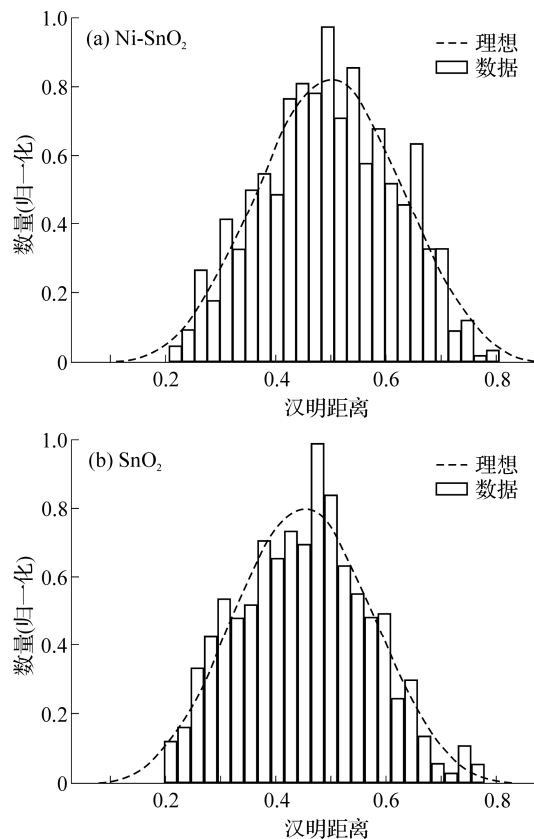


图 7 PUF 输出响应的唯一性

表 1 为本文与不同文献在唯一性和信息熵方面的数据比较, 基于 Ni-SnO₂ 纳米颗粒的 GS-PUF

表 1 相关文献比较

文献	PUF 类型	唯一性/%	信息熵/%
[3]	硅 PUF	49.60	>97
[13]	硅 PUF	50.30	>99
[15]	硅 PUF	48.60	>97
[9]	传感器 PUF	49.00	—
本文	传感器 PUF	49.80	>99

唯一性为 49.80%, 接近于理想值 50%, 信息熵高达 99% 以上, 表明所设计 PUF 输出响应具有良好的随机性, 且很难被预测.

4 结论

本文利用传感器制造过程工艺偏差, 结合静电喷雾沉积技术, 实现基于 Ni-SnO₂ 纳米颗粒的 GS-PUF 设计方案, 达到随机、不可克隆的气敏传感型 PUF 响应输出. 该方案通过提取传感器特征值, 利用响应生成算法来产生 PUF 输出响应. 实验过程制备了多组 GS-PUF 样本进行对比实验. 结果表明, 基于 Ni-SnO₂ 纳米颗粒的 GS-PUF 在改善传感器气敏特性基础上, 可以得到更稳定的特征值数据, 有效地改善了 PUF 的随机性和唯一性, 所设计的 GS-PUF 随机性高达 99% 以上, 且唯一性为 49.80%.

参考文献:

- [1] Butun I, Osterberg P, Song H. Security of the internet of things: vulnerabilities, attacks, and countermeasures[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 616-644.
- [2] Labrado C, Thapliyal H, Prowell S, et al. Use of thermistor temperature tensors for cyber-physical system security[J]. Sensors, 2019, 19(18):3905-3920.
- [3] Li G, Wang P J, Qian H Y. Highly reliable multiport PUF circuit based on MOSFET zero temperature coefficient point[J]. Chinese Journal of Electronics, 2018, 27(4):211-216.
- [4] Labrado C, Thapliyal H. Design of a piezoelectric-based physically unclonable function for IoT security[J]. IEEE Internet of Things Journal, 2019, 6(2):2770-2777.
- [5] Cao Y, Zalivaka S, Zhang L, et al. CMOS image sensor based physical unclonable function for smart phone security applications[C]. IEEE 14th International Symposium on integrated Circuits, 2014:392-395.
- [6] Kumar S D, 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, 2018:697-702.
- [7] Valsesia D, Coluccia G, Bianchi T, et al. User authentication via PRNU-based physical unclonable functions[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8):1941-1956.

- [8] Rahim K, Tahir H, Ikram N. Sensor based PUF IoT authentication model for a smart home with private blockchain[C]. 2018 International Conference on Applied and Engineering Mathematics, 2018:102-108.
- [9] 汪鹏君, 李乐薇, 郑雁公, 等. 基于气敏传感器的高稳态物理不可克隆函数发生器[J]. 电子与信息学报, 2021, 43(6):1596-1602.
- [10] Yun W, Hui Z, Xu H S. Electrospun nanowebs of NiO/SnO₂ p-n heterojunctions for enhanced gas sensing [J]. Applied Surface Science, 2016, 389(15):514-520.
- [11] Liu H C, Wang F P, Hu K L, et al. Superior hydrogen sensing property of porous NiO/SnO₂ nanofibers synthesized via carbonization[J]. Nanomaterials, 2019, 9(9):1250-1263.
- [12] Yi J, Lee J M, Park W. Vertically aligned ZnO nanorods and graphene hybrid architectures for high-sensitive flexible gas sensors[J]. Sensors & Actuators, 2011, 155(1): 264-269.
- [13] Li G, Wang P J, Zhang Y J, et al. A multi-port low-power current mode PUF using MOSFET current-division deviation in 65 nm technology[J]. Microelectronics Journal, 2017, 67:169-175.
- [14] Zhao Q, Wu Y H, Zhao X J, et al. A 1036-F2/bit high reliability temperature compensated cross-coupled comparator-based PUF[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2020, 28(6): 1449-1460.
- [15] 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.

Gas sensor physical unclonable function based on Ni-SnO₂ nanoparticles

LI Lewei¹, WANG Pengjun^{2*}, ZHANG Yuejun¹

(1.Factual of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China;

2.College of Electrical and Electronic Engineering, Wenzhou University, Wenzhou 325035, China)

Abstract: Gas sensors are widely used in industry and other fields with the functions of identification, detection, and monitoring, but they lack the functions of rapid identification and positioning in the early warning of leakage. In this paper, a GS-PUF (Gas Sensor-Physical Unclonable Function) design scheme is proposed. The method of doping heavy Ni elements is adopted to prepare Ni-SnO₂ gas sensor with electrostatic spray deposition technique to obtain more stable and reliable physical characteristics. Then the response data of gas sensors to different concentrations of gas are collected. Finally, the random resistance multi-bit balance algorithm is used to compare the response electrical signal values of different groups of gas sensors to achieve PUF data output. Multiple groups which can generate 128 bit binary data of PUF samples are implemented for comparison experiment. The results show that the designed GS-PUF has the function of identifying and locating the source of gas leakage, and the randomness is increased to 99%, and the uniqueness is 49.80%.

Key words: Ni-SnO₂ nanoparticles; physical unclonable function; gas sensor; electrostatic spray deposition

(责任编辑 章践立)