基于石墨烯电极 RRAM 的混合型 PUF 指纹电路

白 创[1,2]，张 伟[1*]，吕 豪[1]，米莲娜·朱卡诺维奇[3]

(1. 长沙理工大学物理与电子科学学院 长沙 410114；2. 柔性电子材料基因工程湖南省重点实验室 长沙 410114；
3. 黑山大学电气工程学院 黑山共和国 波德戈里察 81000)

【摘要】该文提出了一种基于阻变存储器 (RRAM) 的混合型物理不可克隆函数 (PUF) 芯片指纹电路。RRAM 器件采用石墨烯电极、对称山型结构实现，具有阻值分布宽、开关比大的特点；通过引入对称 RRAM 阻值偏差作为 PUF 单元的随机熵源，提升 PUF 的唯一性；采用 RRAM 不同阻态阻值放大存储 PUF 单元初始偏差，提升 PUF 的稳定性；利用 RRAM 循环间随机性实现指纹 ID 的重构，提升 PUF 的安全性。混合型 PUF 芯片指纹电路在 0.35 μm CMOS 工艺下设计实现。仿真结果表明，PUF 输出具有良好的稳定性与唯一性，标准温度电压下片间汉明距离为 49.95%，同时温度在−40 ℃～100 ℃，电源电压在 4.6 V～5.4 V 范围内变化时，PUF 比特错误率为 0。

关 键 词 芯片指纹识别； 硬件安全； 物理不可克隆函数； 阻变存储器

中图分类号 TP319.56 **文献标志码** A doi:10.12178/1001-0548.2021023

A Hybrid Physical Unclonable Function for Chip Fingerprint Based on Graphene Electrode RRAM

BAI Chuang[1,2], ZHANG Wei[1*], LÜ Hao[1], and MILENA Djukanovic[3]

(1. School of Physics & Electronic Science, Changsha University of Science & Technology Changsha 410114;
2. Hunan Provincial Key Laboratory of Flexible Electronic Materials Genome Engineering Changsha 410114;
3. Faculty of Electrical Engineering, University of Montenegro Podgorica Montenegro 81000)

Abstract A resistive random access memory (RRAM)-based hybrid physical unclonable function (PUF) for chip fingerprint is described in this paper. The “E” shape central symmetrical RRAM uses graphene thin film as electrode layer, and has wide distribution of resistance and high on-off resistance ratio; the resistance variation of RRAM is introduced to PUF cell as an entropy source to improve the uniqueness of PUFs; the different resistance states of RRAM are used to amplify initial deviation of PUF cell and improve the stability of PUFs; the cycle-to-cycle variation of RRAM is utilized to reconstruct the chip ID and improve the security of PUFs. The proposed PUF is designed in a 0.35μm CMOS technology. Simulation results show that the proposed PUF has good characteristics of uniqueness and stability, the inter-chip hamming distance (HD) in normal conditions is 49.95%, and the bit error rate is zero when temperature varies from −40 ℃ to 100 ℃, and supply voltage changes from 4.6 V to 5.4 V.

Key words chip fingerprint identification; hardware security; physical unclonable function; RRAM

PUF 芯片指纹技术是一种新型的硬件安全原语，在电子信息产品合法身份认证领域具有广泛研究。目前国内外出现了许多种 PUF 芯片指纹电路结构，包括基于延时的仲裁器 PUF[1]、环形振荡器 PUF[2] 以及基于分压的静态随机存储器 (static radom access memory, SRAM)PUF[3]、电流镜 PUF[4] 等。这类 PUF 通过捕获芯片制造过程中器件和连线的随机工艺偏差，生成独一无二的指纹 ID，用于标识不同的电子产品的合法身份。然而在噪声、温度、电压等因素的影响下，PUF 的输出结果可能产生变化，限制了其在身份认证领域的应用。文献 [5] 提出通过降低电源电压来改善环形振荡器 PUF 稳定性，能起到一定的改善作用，但仍不能保证获得完全稳定的输出。文献 [6] 提出一种利用多组激励

收稿日期：2021－01－21；修回日期：2021－03－31
基金项目：柔性电子材料基因工程湖南省重点实验室开放基金 (202005)；中国−黑山科技合作委员会第 3 届例会交流项目 (3-7)
作者简介：白创 (1983－)，男，博士，主要从事超大规模集成电路与 PUF 芯片指纹电路方面的研究.
通信作者：张伟，E-mail：1369231507@qq.com

响应对 (challenge-response pairs, CRPs) 作为辅助数据的错误校正方案，然而辅助数据的存储与传输可能会对 PUF 的安全性产生影响。文献 [7] 通过采用具有微小偏差的电源电压上电来确定并剔除不稳定位，但筛选和剔除过程都需要额外的时间和成本。

PUF 单元随机偏差的大小从根本上决定了 PUF 芯片指纹 ID 的稳定性，因此通过增大 PUF 单元的随机偏差是改善 PUF 稳定性最有效的方法之一。RRAM 是一种新型非易失存储器件，其阻值分布具有较强的随机性，可以用来构建 PUF 对称单元增强其随机偏差。文献 [8] 研制了国际首款基于 RRAM 的可重配置 PUF 芯片，使用分裂阻值法极大提高了 RRAM PUF 的稳定性。文献 [9] 提出了一种基于模拟 RRAM 交叉阵列的 RX-PUF，实现了 20×20 阵列的 600 kb CRPs 对 RRAM PUF，采用 SHA 提高抗攻击能力。文献 [10] 利用 RRAM 写入速度差实现了比特错误率小于 0.35% 的 RRAM PUF。然而现有的 RRAM PUF 也存在随机性不足，以及开关比较小导致读取错误率高等问题，同时多 CRPs 的强 PUF 面积开销和功耗开销都相对较大，不适合直接用作芯片指纹电路应用于身份认证领域。本文针对 PUF 指纹芯片应用需求，设计具有良好随机性和高开关比的 RRAM 器件，构建基于 RRAM 的 PUF 单元，实现基于 RRAM 的新型混合型 PUF 芯片。

1　石墨烯电极 RRAM 器件

采用 RRAM 器件构建 PUF 单元增强其随机偏差时，要求 RRAM 阻值分布范围宽，随机性好，同时开关比足够大，高低阻态易区分。为实现这一目标，文中引入了一种新型的石墨烯电极 RRAM 器件，结构如图 1 所示。器件为中心对称的山形结构，包括铝电极、铝氧化物阻变层、石墨烯薄膜电极、镍电极、二氧化硅/硅衬底。RRAM 器件在实验室制备完成后，通过加−5 V RESET 和+5 V SET 电压分别配置到高阻态和低阻态，阻值转变过程如图 2 所示。

RRAM 配置到不同状态后，在电极两端接 0.1 V 读取电压，通过测量电流来计算 RRAM 阻值。统计 2 000 个 RRAM 器件的高低阻值后计算累积概率分布，并与文献 [8, 11] 中其他两种典型 RRAM 进行比较，结果如图 3 所示。图中可以看出，3 种 RRAM 都在高阻态分布更广，所以通常选取高阻态 RRAM 作为随机熵源。石墨烯电极 RRAM 的高阻态阻值范围约为 10^8～10^{11} Ω，相比于其他两种 RRAM 的分布范围明显更广，是更好的随机源；同时其开关电阻比始终大于 10^3，比其他两种 RRAM 要高 2 个数量级左右，存储稳定性更高。因此，采用石墨烯电极 RRAM 构建的 PUF 指纹芯片将具有更好的随机性和稳定性，同时外围电路可以更加简单，实现 PUF 功能的芯片面积和功耗开销更小。

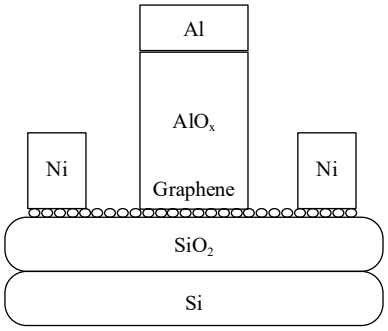


图 1　石墨烯电极 RRAM 结构

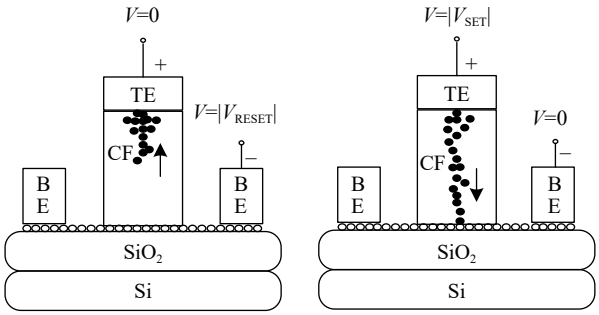


图 2　RRAM RESET 和 SET 过程

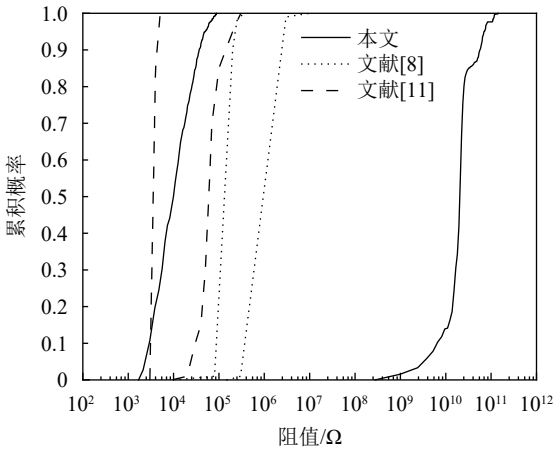


图 3　RRAM 阻值累积概率分布对比

2　混合型 SRAM-RRAM PUF 单元

基于 RRAM 的混合型 PUF 单元结构如图 4 所示，包含一个 6 T SRAM 单元、两个 RRAM 单元以及由 MOS 开关构成的配置单元等。单元为对称结构，SRAM 中 MOS 管 PM1 和 PM2 的阈值失配和两高阻态 RRAM 的阻值偏差共同作为随机熵源。

每个单元外接三路电源信号 PL1、PL2 和 PL3，两路控制信号 CL1 和 CL2，以及两路地址选择信号 SL1 和 SL2，输出端为 BL1 和 BL2。当 SL1 置高时，RRAM 单元被选中，此时将 CL1 和 CL2 置高，PL1 上电时，两 RRAM 被配置到高阻；配置完成后，将 SL1、SL2 和 CL2 置高，其他置低，PL3 上电即可生成初始值。利用 RRAM 可以对 PUF 初始值进行偏差放大。生成初始值后，将 PL3 保持上电，PL1 接地，SL1 和 SL2 置高，CL1 和 CL2 置低，PL2 上电时，初始值为高的一端 RRAM 被配置到低阻，初始值被放大后存储到 RRAM 中。偏差放大后，需要读取指纹值时，将 SL1、SL2 和 CL2 置高，其他置低，PL3 上电即可进行读取。各阶段 PUF 单元接口输入信号时序图如图 5 所示。由于本文所采用的 RRAM 器件在高低阻态的阻值差极大，偏差放大后再读取时，PUF 输出将完全由 RRAM1 和 RAM2 的高低组态决定，同时 RRAM 阻值受温度电压等因素影响极小，可保证指纹值的稳定读出。

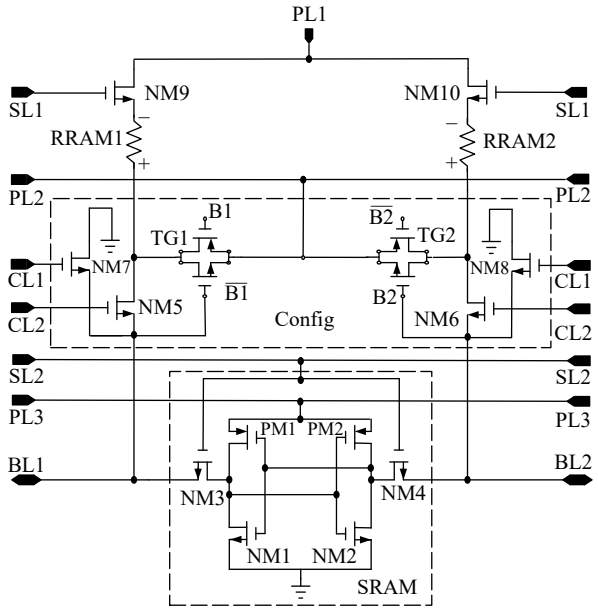


图 4 PUF 单元电路结构

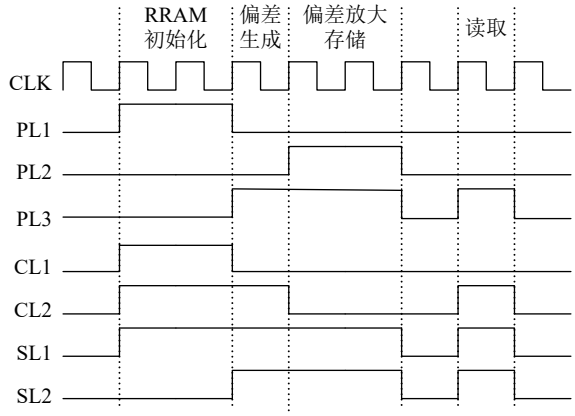
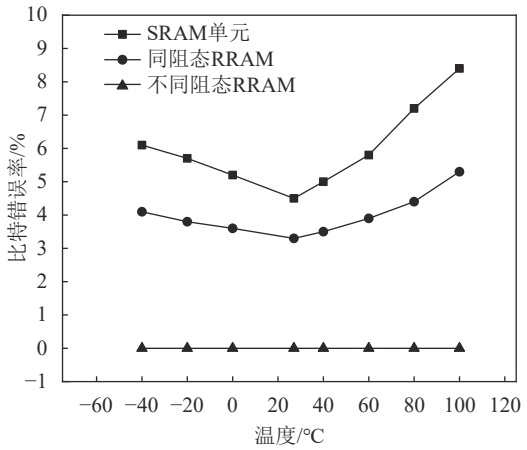
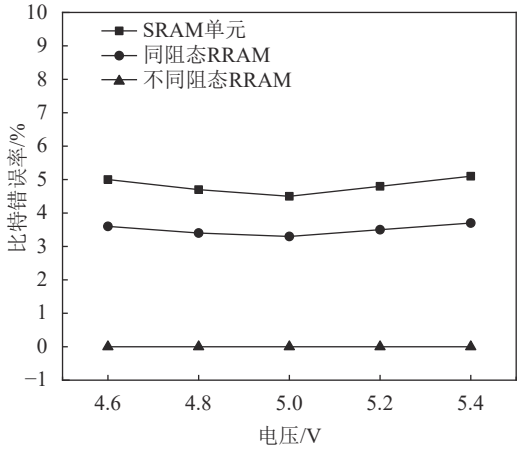


图 5 PUF 单元接口时序

本文分别对传统 SRAM 单元、同为高阻态 RRAM 的 PUF 单元、不同阻态 RRAM 的偏差放大 PUF 单元进行稳定性测试。测试条件分别为温度 27 ℃、电源电压 4.6～5.4 V、电源电压 5 V、温度−40 ℃～100 ℃，在每种条件下对每个单元进行 10 000 次蒙特卡洛仿真。并以电压 5 V、温度 27 ℃条件下的结果为参考值，计算了不同单元在不同条件下的比特错误率，结果如图 6 所示。可以看出，传统 SRAM PUF 单元在温度电压条件不变的情况下比特错误率仍不为 0，这是由于各种噪声的存在引起的比特翻转，在温度和电压变化的情况下比特错误率会进一步增加。引入同阻态 RRAM 作为混合熵源后，PUF 单元的稳定性在各种条件下都有所提升，但仍不能完全保证获得稳定的 PUF 指纹输出。采用不同阻态 RRAM 进一步对 PUF 进行偏差放大后，PUF 单元在任何条件下都得到了完全稳定的输出。



a. 不同温度条件



b. 不同温度条件

图 6 不同环境下 3 种模式 PUF 单元的稳定性

3 混合型 PUF 芯片指纹电路

混合型 PUF 芯片指纹电路整体结构如图 7 所示，主要包含 PUF 核与外围电路两大部分。PUF

核包括 SRAM 阵列、RRAM 阵列与配置电路。外围电路主要包含 3 部分，即 PUF 芯片控制电路、译码器以及灵敏放大器 (sense amplifier, SA)。控制电路根据接收的输入信号，输出特定电源、控制和地址选择信号；译码器根据接收到的地址信号，通过 SL1 和 SL2 同时选中同一行 SRAM 和 RRAM；配置电路接收 CL2 和 CL2 的控制信号，确定 RRAM 与 SRAM 的电路连接方式，实现对 RRAM 的阻值配置；每个灵敏放大器接收 PUF 单元两端信号，输出一位指纹值。

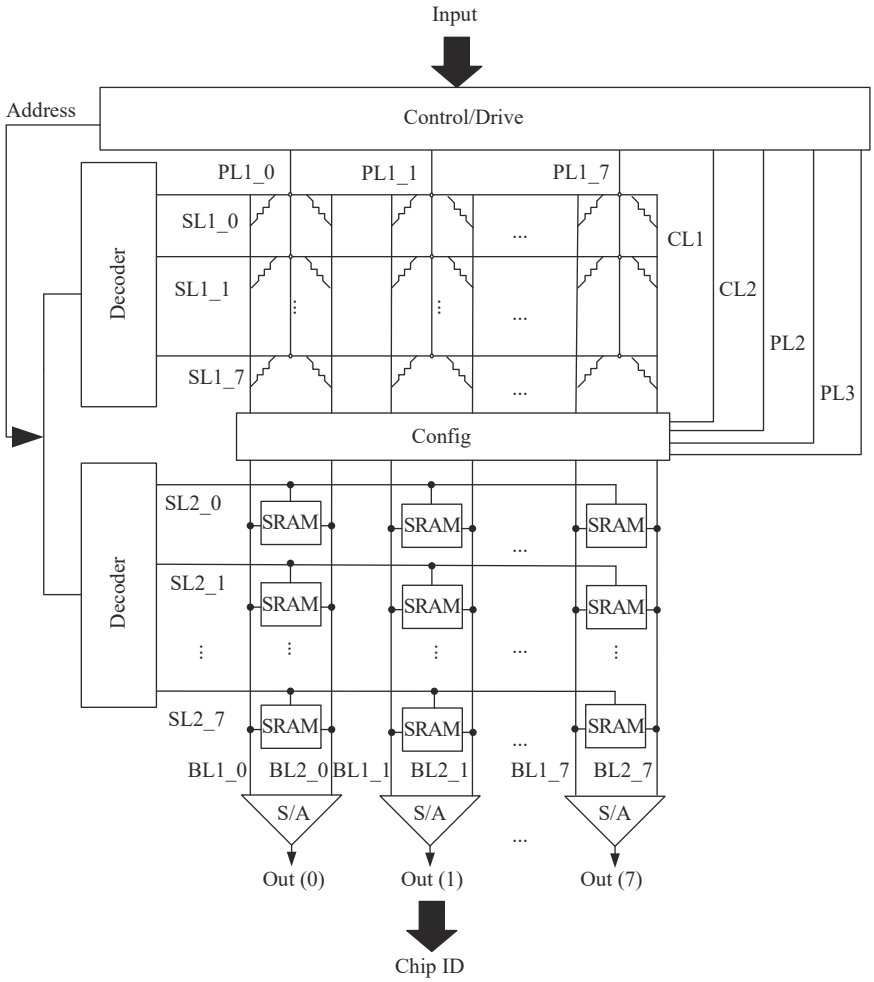


图 7　混合型 PUF 整体结构

混合型 PUF 芯片指纹电路包含 3 种工作模式：注册模式、读取模式与重构模式。模式切换与运行由控制电路实现，控制电路架构图如图 8 所示。输入模式选择信号被译码为 3 种不同的控制信号，内部控制单元根据控制信号执行 RRAM 初始化、偏差生成/读取、偏差放大操作，产生相应输出信号控制 PUF 运行。

注册模式为混合型 PUF 芯片出厂时的预操作模式。出厂时 RRAM 为高阻态，注册时控制电路执行 PUF 偏差生成/读取模块与偏差放大模块，实现指纹值的放大与稳定存储。读取模式为混合型 PUF 芯片的常规工作模式，芯片完成注册后，若需读取指纹值，控制电路将执行偏差生成/读取模块，根据偏差放大后 PUF 单元两端 RRAM 阻态高低读出指纹值。重构模式为指纹值暴露在风险环境后的安全更新模式。接收到重构信号后，控制单元首先执行 RRAM 初始化模块，将 RRAM 全部重新配置到高阻态，随后再次执行偏差生成/读取模块与偏差放大模块重新进行注册。由于噪声影响以及 RRAM 阻值在不同循环间的随机性，重构后读取时，PUF 芯片会生成新的指纹 ID。

4　电路仿真与分析

本文在 SMIC 0.35 μm 工艺下搭建了可重构式

混合型 RRAM PUF 芯片指纹电路，包含 64 个 RRAM 与 SRAM 单元构成的混合型 PUF 单元，可生成 64 位的芯片指纹 ID。通过在 Cadence 中进行仿真分析，计算了 PUF 芯片功耗和面积，通过蒙特卡洛分析，让芯片在不同条件下产生指纹值，计算了芯片指纹值的随机性、唯一性和稳定性。

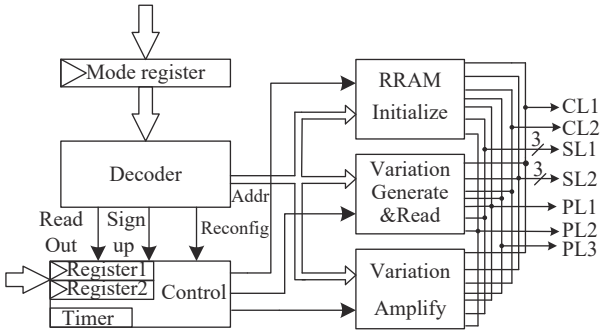


图 8 PUF 控制电路架构

4.1 面积和功耗

整个 PUF 芯片的面积约为 7200 μm^2。通过仿真可知，在电源电压为 5 V、温度为 27 ℃ 的条件下，单次注册过程能耗为 0.5 nJ，单次读取过程能耗为 96 pJ，单次重构过程能耗为 1.2 nJ。芯片出厂后正常工作时，重构次数相对读取次数而言极少，故生成每比特指纹值的能耗可近似为 2.5 pJ/bit。表 1 总结了混合 RRAM PUF 芯片各种性能的具体参数。

表 1 混合 RRAM PUF 芯片各性能参数值

性能	参数
工艺	0.35 μm CMOS
面积/μm^2	7650
工作电压/V	4.6～5.4
工作温度/℃	−40～100
注册能耗@5 V，27 ℃/nJ	0.5
读取能耗@5 V，27 ℃/pJ	96
重构能耗@5 V，27 ℃/nJ	1.2

4.2 随机性

随机性测试用于验证芯片生成的指纹 ID 是否具有真正的随机性，对于基于 RRAM 的混合型 PUF 芯片，通过 NIST 随机性测试验证指纹值。表 2 展示了详细的 NIST 随机性测试结果，可以看出，所提出的混合型 PUF 芯片平均 P_value 始终大于 0.01，通过了所有测试。这表明本芯片是理想的随机源。

表 2 混合型 RRAM PUF 芯片 NIST 随机性测试结果

Test item	Stream length	No. of runs	Avg. P_value	Pass rate	Pass?
Frequency	64	10	0.739918	10/10	YES
Block frequency	64	10	0.739918	10/10	YES
Cumulative sums	64	10	0.911413	10/10	YES
Runs	64	10	0.350485	10/10	YES
Longest run	64	10	0.739918	9/10	YES
FTT	64	10	0.739918	10/10	YES
Approximate entropy	64	10	0.213309	10/10	YES
Serial 1	64	10	0.066882	10/10	YES
Serial 2	64	10	0.350485	10/10	YES

4.3 唯一性

唯一性描述了芯片生成指纹 ID 的碰撞概率，通过芯片的片间汉明距离分布来进行衡量。为了衡量唯一性，仿真了 10000 块不同的 PUF 芯片，在 27 ℃、5 V 电压下产生指纹值，并计算这些指纹值的汉明距离，结果如图 9 所示。计算表明，本 PUF 芯片指纹电路的片间汉明距离为 49.95%，方差为 3.91%。这一结果与理想值 50% 非常接近，表明该芯片具有较为理想的唯一性。

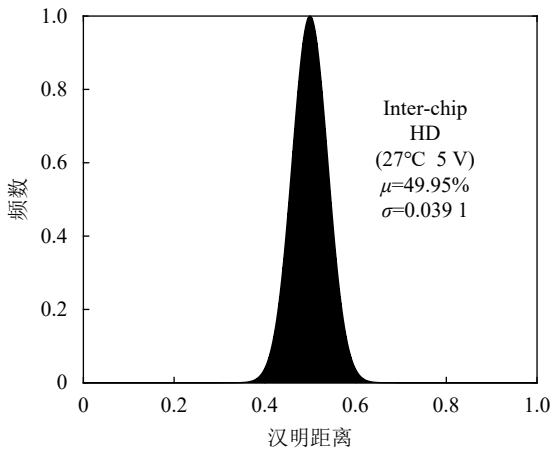
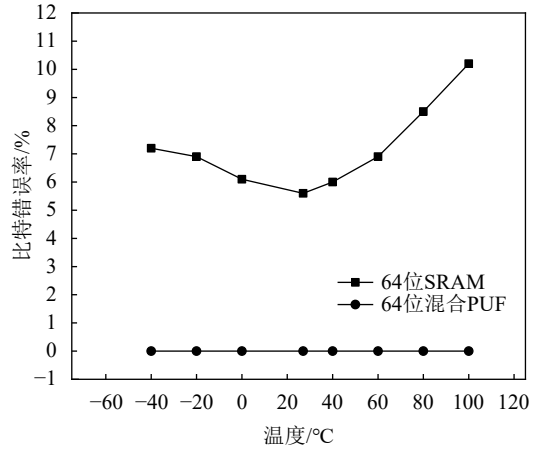


图 9 混合型 PUF 芯片片间汉明距离分布

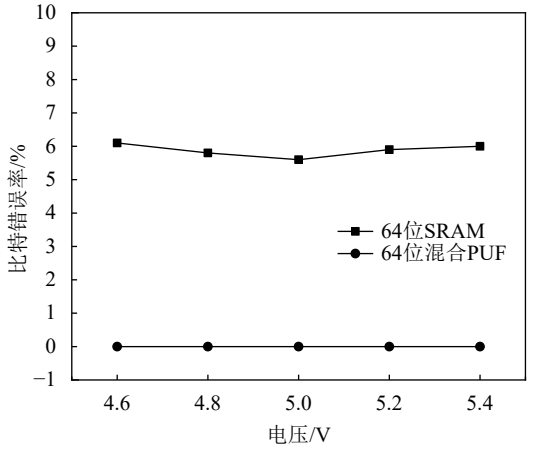
4.4 稳定性

稳定性指 PUF 芯片在外界环境变化的情况下保持输出不变的能力。本文在电源电压 5 V、温度 27 ℃ 的条件下，对提出的 PUF 芯片指纹电路进行了 100000 蒙特卡洛分析。同时还在电源电压为 4.6～5.4 V，温度−40 ℃～100 ℃ 的条件下进行了仿真，以 27 ℃、5 V 电压下第一次仿真的指纹值为标准，计算了温度电压变化条件下的比特错误率。为了验证本芯片指纹电路对 PUF 稳定性的提升，同时还搭建了 64 位 SRAM PUF 阵列，并在相同环境

条件下生成芯片指纹值，计算了比特错误率并进行比较，结果如图 10 所示。可以看出，本文提出的 64 位混合型 PUF 芯片指纹电路可以有效消除系统噪声和电路不对称因素的影响，并在温度电压变化的条件下仍然保持了理想的 100% 稳定性。



a. 不同温度下稳定性对比



b. 不同电压下稳定性对比

图 10　不同环境 SRAM 与混合型 PUF 稳定性对比

表 3 对比了 SRAM-RRAM 混合型 PUF 与其他几种最新的典型芯片指纹 PUF 方案。可以看出，相对于其他 PUF 结构，混合型 PUF 具有最好的稳定性；相比于文献 [12] 中低开销的 Inverter PUF，混合型 PUF 稳定性有显著提升；相比于文献 [7] 中具有高稳定性的 SRAM PUF，混合型 PUF 无需额外筛选和剔除过程；相比于文献 [13] 中的 Anti-fuse PUF，混合型 PUF 在能耗上降低了约 70%，同时还具有可重构功能；相比于文献 [8] 中结构和功能类似的 RRAM PUF，混合型 PUF 在能耗上降低了约 50%。混合型 PUF 每比特指纹值的芯片面积相对较大，通过减小工艺尺寸，增加 PUF 生成的 ID 位数即可有效提升面积效率。

表 3　与其他典型芯片指纹 PUF 方案对比

参数	文献[7]	文献[8]	文献[12]	文献[13]	本文
Technology/nm	65	130	65	55	350
Entropy source	SRAM	RRAM	Inverter	Anti-fuse	SRAM-RRAM
Area/$\mu m^2 \cdot bit^{-1}$	49.12	2.86	9.37	0.66	112.5
Efficiency/$fJ \cdot bit^{-1}$	73	3 028	40	5 200	1 500
Bit error rate/%	3×10^{-8}	0.000 6	0.3	0.05	0
Intra-HD	0	0	0.004 7	0	0
Inter-HD	0.499 3	0.499 9	0.499 8	0.499 999	0.499 5
Reconfigurable?	No	Yes	Yes	No	Yes

5　结 束 语

本文从 PUF 稳定性和随机性问题出发，引入 RRAM 器件来增强 PUF 单元的随机偏差。通过具有高随机性高开关比的石墨烯电极 RRAM 器件，提升了 RRAM PUF 的整体性能，采用 PUF 偏差放大技术提高了 PUF 芯片指纹电路的唯一性和稳定性，通过设计混合 RRAM PUF 芯片的整体结构和工作模式，提高了 PUF 芯片指纹电路的可靠性和安全性。

参　考　文　献

[1] LIN L, SRIVATHSA S, KRISHNAPPA D K, et al. Design and validation of arbiter-based pufs for sub-45-nm low-power security applications[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(4): 1394-1403.

[2] LU Zhao-jun, LI Dong-fang, LIU hai-long, et al. An anti-electromagnetic attack PUF based on a configurable ring oscillator for wireless sensor networks[J]. Sensors, 2017, 17(9): 2118.

[3] GUAJARDO J, KUMAR S S, SCHRIJEN G J, et al. FPGA intrinsic PUFs and their use for IP protection[J]. International Workshop on Cryptographic Hardware and Embedded Systems, 2007, 42(27): 63-80.

[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. Arlington: IEEE, 2014: 38-43.

[5] SAUVAGYA R S, SUDEENDRA K, KAMALAKANTA M. A novel configurable ring oscillator PUF with improved reliability using reduced supply voltage[J]. Microprocessors and Microsystems, 2018, 60: 40-52.

[6] SUN Kai, SHEN Yi-fei, LAO Ying-jie, et al. A new error correction scheme for physical unclonable function[C]//2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS). Chengdu: IEEE, 2018: 374-377.

[7] YIZHAK S, AVI M, OSNAT K, et al. A method to improve reliability in a 65-nm SRAM PUF array[J]. IEEE Solid-State Circuits Letters, 2018, 1(6): 138-141.

(下转第 550 页)