基于CNFET的高性能三值SRAM-PUF电路设计

汪鹏君,龚道辉,张会红,康耀鹏
(宁波大学电路与系统研究所,浙江宁波 315211)

摘 要: 通过对碳纳米管场效应晶体管(Carbon Nanotube Field Effect Transistor,CNFET)和物理不可克隆函(Physical Unclonable Functions,PUF)电路的研究,提出一种高性能三值SRAM-PUF电路结构.该电路结构首先利用交叉耦合三值反相器产生随机电流,并对其电流进行失配分析;然后结合三值SRAM单元的电流竞争得到随机的、不可克隆的三值输出信号"0"、"1"和"2".在32nm CNFET标准模型库下,采用HSPICE对所设计的三值SRAM-PUF电路进行Monte Carlo仿真,分析其随机性、唯一性等性能.模拟结果表明所设计的三值SRAM-PUF电路归一化随机性偏差和唯一性偏差均为0.03%,且与传统二值CMOS设计的PUF电路相比工作速度提高33%,激励响应对数量为原来的$(1.5)^n$倍.

关键词: 碳纳米管场效应晶体管;三值逻辑;SRAM-PUF;随机性;唯一性
中图分类号: TP331 **文献标识码:** A **文章编号:** 0372-2112 (2017)05-1090-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.05.010

High Performance Ternary SRAM-PUF Circuit Based on CNFET

WANG Peng-jun, GONG Dao-hui, ZHANG Hui-hong, KANG Yao-peng
(*Institute of Circuits and Systems, Ningbo University, Ningbo, Zhejiang* 315211, *China*)

Abstract: By researching the Carbon Nanotube Field Effect Transistor(CNFET) and the Physical Unclonable Functions(PUF) circuit, a structure of high-performance ternary SRAM-PUF circuit is proposed. In this circuit structure, the cross-coupling ternary inverters generate random current, which is analyzed according to the mismatch feature. After competing the random current of ternary SRAM, it produces three-valued signal, such as "0", "1" and "2". Under Stanford University 32nm CNFET standard model, HSPICE is used for Monte Carlo simulation to analysis the randomness, uniqueness and other features. And simulation results show that the randomness variation and uniqueness can be achieved at 0.03% after normalization. Comparing with conventional binary CMOS PUF circuit, the proposed circuit improves the speed by 33%, and increases the number of challenge-response by $(1.5)^n$ times.

Key words: carbon nanotube field effect transistor(CNFET); three-valued logic; SRAM-PUF; randomness; uniqueness

1 引言

物理不可克隆函数(Physical Unclonable Function,PUF)电路利用集成电路制造过程中的随机工艺偏差产生密钥,并将其应用于密码系统[1].由于随机工艺偏差,相同结构的不同芯片在同一激励下,将得到不同的输出响应.因此攻击者尽管知道PUF电路结构,但由于工艺偏差的不可控,也无法克隆出具有相同输出响应的PUF电路.PUF电路不可克隆的特性,使得PUF电路可防御多种传统攻击模式.Pappu等首先提出PUF的概念,并设计光学PUF来实现系统认证等应用[2].随后Gassend等以硅参数的随机函数概念为基础,提出PUF

收稿日期:2016-08-11;修回日期:2016-11-25;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61474068, No. 61234002);浙江省公益性技术应用研究计划项目(No. 2016C31078);浙江省自然科学基金(No. LQ14F040001);宁波市自然科学基金(No. 2015A610107)

电路[3]. 因此对 PUF 电路的研究和应用越来越深入,如知识产权保护、设备认证、硬件识别、密钥产生等[4,5].

在硅 PUF 电路中,随着特征尺寸缩小到纳米量级,互连线寄生效应带来的门延时、互连线串扰等问题越来越严重[4]. PUF 电路唯一性代表区别相同结构的不同芯片的能力[5],随机性影响该电路不可克隆性的强弱[6],因此提高 PUF 电路的随机性和唯一性这两方面性能尤为重要. 碳纳米管(Carbon Nanotube,CNT)因弹性散射具有超长自由程,使其拥有弹道传输特性,准一维结构的 CNT 相比三维体硅和二维绝缘衬底上的硅具有更好的电子控制能力[7]. 碳纳米管场效应晶体管(Carbon Nanotube Field Effect Transistor,CNFET)以 CNT 为导电沟道,利用 CNFET 设计的 PUF 电路具有更好的随机性和唯一性. 文献[7]研究表明,CNFET 的栅极电容 C_{gate} 是 MOSFET 栅极电容 C_{gate} 的 4%,故利用 CNFET 设计的 PUF 电路具有更高的工作频率. 但 CNT 制备方法尚不成熟,不能任意调整 CNT 的直径、管长、螺旋角等参数,使制得的 CNT 杂质高、产率低,因此利用 CNT 构成的 CNFET 阈值电压不能精准控制[8]. 在 PUF 电路中,提高激励响应对(challenge-response pairs,CRPs)数量可以提高密钥的复杂度. 在二值 PUF 电路中,增加激励响应对的数量,势必会增加芯片面积. 三值逻辑相对于二值逻辑来说,其信号取值可以为"0"、"1"和"2",对于相同 n 位 PUF 电路,三值 PUF 电路的激励响应对数量是二值 PUF 电路的 $(1.5)^n$ 倍. 因此,三值 PUF 电路可提高密钥的复杂度. 本文通过对三值逻辑理论研究,利用 CNFET 设计高速、高性能的三值 SRAM-PUF 电路.

2　基于 CNFET 的三值 SRAM-PUF 电路设计

2.1　失配分析

将用 CNFET 设计的三值反相器交叉耦合,节点 Q 与 $\overline{Q}$ 有三个稳定状态"0"、"1"和"2",结构如图 1 所示. 将节点 Q 与 $\overline{Q}$ 均预充电为高电平,由于 CNFET 制造过程中存在工艺偏差,T2 与 T5 管或 T1 与 T4 管的电流必将存在偏差. 通过 1000 次 Monte Carlo 仿真,分析 T2 管电流 I_{T2} 和 T5 管电流 I_{T5},其电流失配统计结果如图 2 所示.

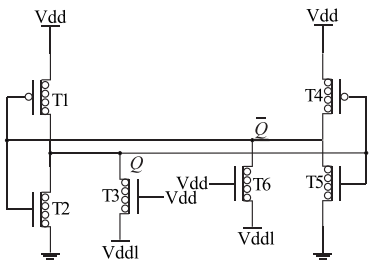

图1　基于CNFET的交叉耦合三值反相器

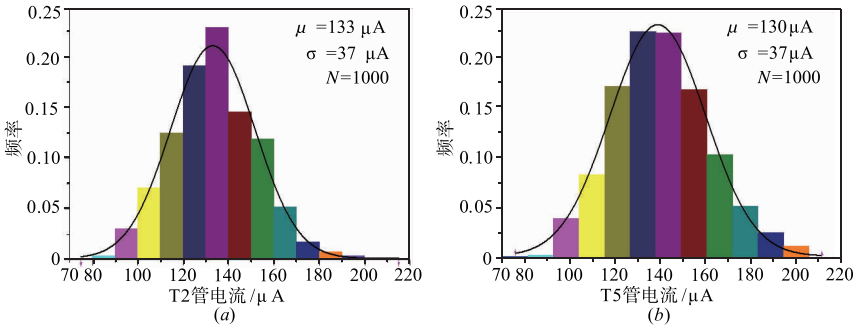

图2　电流失配统计 (a) T2管电流失配统计; (b) T5管电流失配统计

可以发现 T2 和 T5 管电流大小近似服从高斯分布,T2 管电流平均值 μ 为 133μA,标准差 σ 为 37μA;T5 管电流平均值 μ 为 130μA,标准差 σ 为 37μA,具有明显的电流失配. 断开节点 Q 和 $\overline{Q}$ 的预充电电压,通过 $T2$ 和 $T5$ 管电流竞争,节点 Q 与 $\overline{Q}$ 最终会到达一个稳定状态. 当 $I_{T2}-I_{T5}>1\mu A$,节点 Q 逻辑值为"0",如图 3(a);当 $I_{T5}-I_{T2}>1\mu A$,节点 Q 逻辑值为"2",如图 3(b);当 $|I_{T2}-I_{T5}|\leqslant 1\mu A$,即 I_{T2} 和 I_{T5} 相差不大时,节点 Q 逻辑值为"1",如图 3(c).

2.2　基于 CNFET 的三值 SRAM-PUF 单元设计

由失配分析可知,预充电阶段结束后三值 SRAM-PUF 电路利用图 1 交叉耦合反相器 T2 和 T5 管电流的不同,通过竞争产生不同的逻辑值. 因此,可以利用三值 SRAM 来设计 PUF 电路. 交叉耦合反相器由于工艺偏差而引起的偏差电流,通过交叉耦合反相器的正反馈作用可将微小的电流偏差放大,从而得到稳定的输出值. 图 4 为基于 CNFET 的三值 SRAM-PUF 单元电路,它由两个三值反相器交叉耦合,并通过 T1 和 T8 管将存储节点的数据读出. T9 和 T10 管为预充电电路,在预充电阶段通过 Vdd 将节点 Q 和 $\overline{Q}$ 均预充为高电平.

三值 SRAM-PUF 电路工作分为两个阶段:预充电阶段和求值阶段,其工作过程如图 5 所示. 预充电阶段,字线信号 W 为低电平,T1 和 T8 管关闭;使能信号 EN 为低电平,T9 和 T10 管导通,节点 Q 与 $\overline{Q}$ 被预充为高电平,即为逻辑值"2". 求值阶段,EN 为高电平,T9 和 T10 管关闭,由于存在工艺偏差,两个反相器的竞争能力不同,节点 Q 和 $\overline{Q}$ 最终稳定于某一个确定的逻辑值. 从反相器开始竞争到节点 Q 和 $\overline{Q}$ 稳定所需的最小时间称建立时间 T_s,因此在 EN 为高电平后到数据读出前必须有一段等待时间 T_d,等待时间 T_d 大于建立时间 T_s,三值 SRAM-PUF 单元才能正常工作. 经过等待时间 T_d 后 W 为高电平,T1 和 T8 管导通,读出交叉耦合反相器竞争产生的数据,得到输出响应 BL 和$\overline{BL}$.

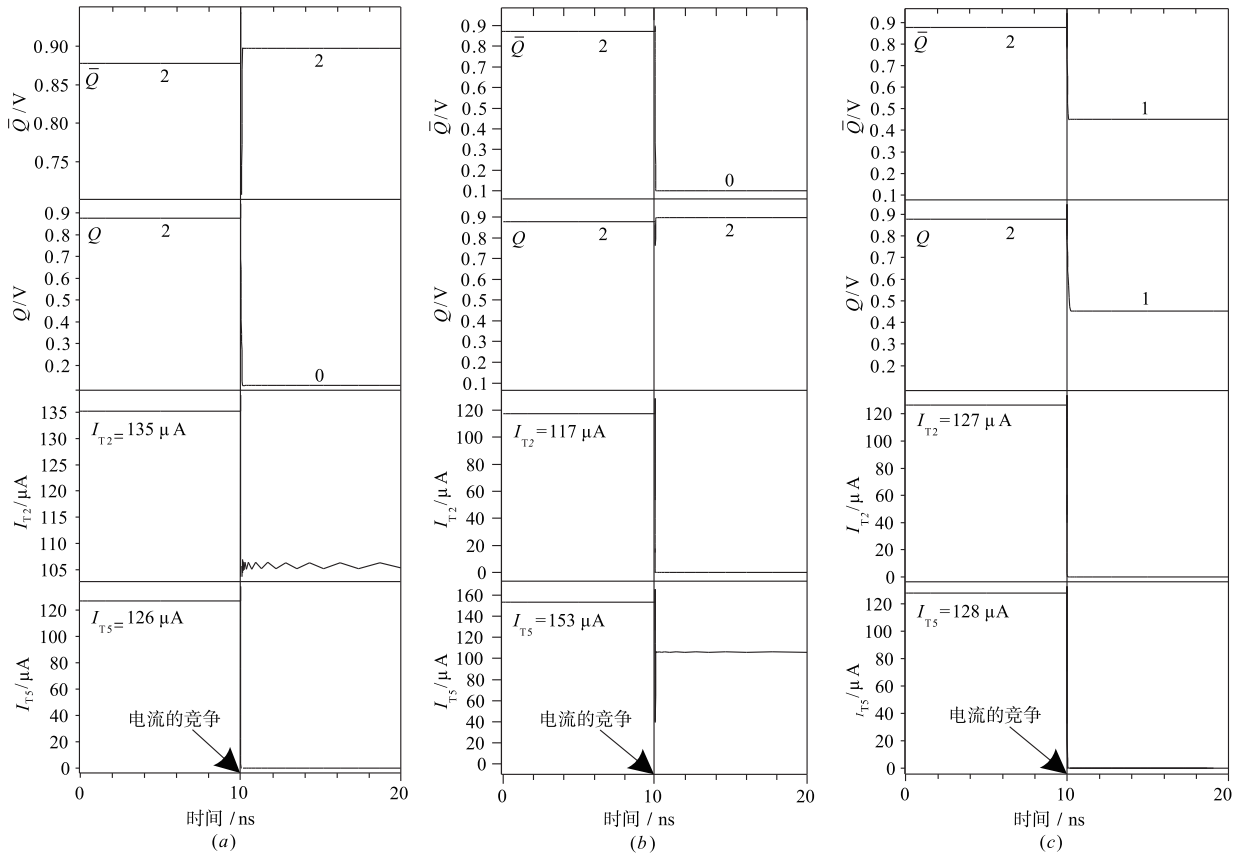

图3 交叉耦合反相器竞争结果 (*a*) 节点*Q*为“0”; (*b*) 节点*Q*为“2”; (*c*) 节点*Q*为“1”

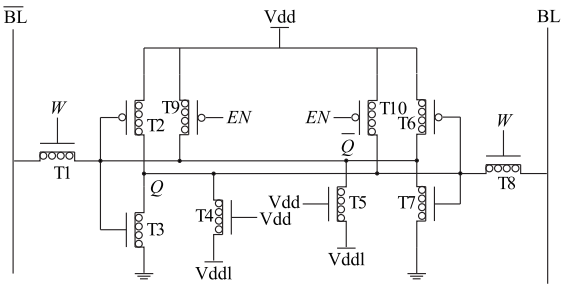

图4 基于CNFET的三值SRAM-PUF单元

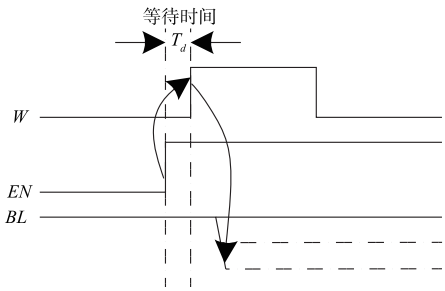

图5 三值SRAM-PUF单元工作时序

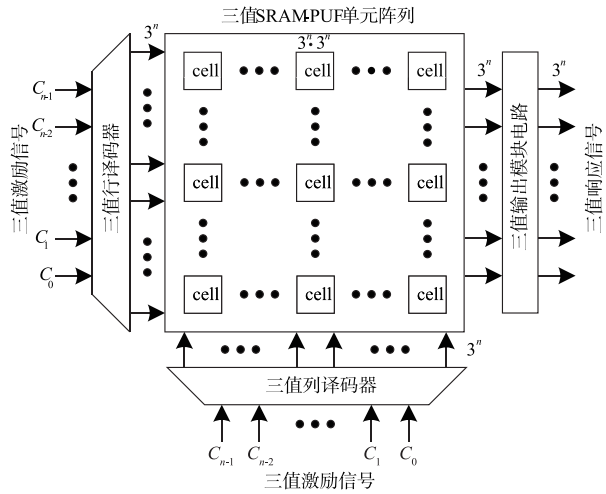

图6 *n*位SRAM-PUF电路

2.3 基于 CNFET 的三值 *n* 位 SRAM-PUF 电路设计

图 6 为基于 CNFET 的三值 *n* 位 SRAM-PUF 电路结构,由三值译码器、三值 SRAM-PUF 单元阵列和输出模块电路组成. 三值激励信号($C_0C_1C_2\cdots C_{n-1}$)通过三值行或列译码器选择相应 SRAM-PUF 单元,通过使能信号 *EN* 控制 SRAM-PUF 电路的工作,字线信号 *W* 为高电平时,输出模块电路输出三值响应信号.

在 *n* 位三值 SRAM-PUF 电路中,相同单元个数的三值 PUF 阵列相比二值 PUF 阵列可存储更多的信息,提高了信息存储密度. 同时,激励信号输入使用三值译码器,

$\log_3(2^n)$ 位三值激励信号输入对应的译码输出与 n 位二值激励信号对应的译码输出位数相同,相比二值译码器大大减小了电路布线面积. 对于 n 位二值 PUF 电路,其激励响应对数量为 2^n,而 n 位三值 PUF 电路中,其激励响应对数量为 3^n;相比传统的二值 PUF 电路,随着 PUF 电路位数的增加,三值 SRAM-PUF 电路激励响应对数量按照$(1.5)^n$ 指数函数的倍数增加. 从而可通过增加激励响应对的数量,提高 SRAM-PUF 电路的安全性.

3　模拟结果与分析

本文采用斯坦福大学的 32nm CNFET 标准模型库[9],利用 HSPICE 对三值 SRAM-PUF 电路进行仿真,并从电路的随机性、唯一性和工作速度来评估三值 SRAM-PUF 电路的性能. 标准模型库采用的电源电压为 Vdd = 0.9V 和 Vddl = 0.45V.

3.1　随机性

PUF 电路随机性越好,加密过程越安全,防御攻击的能力更强[5]. 在三值 SRAM-PUF 电路中,其随机性指的是对于每一位响应信号,输出逻辑"0"、"1"和"2"的概率相等. 三值 PUF 电路的随机性是通过测量输出响应逻辑值所占的比例来确定. 理想情况下,输出响应逻辑值"0"、"1"和"2"的比例应各占 33.3%. 当输入激励为 5 位三值信号时,三值译码器的输出为 243 位. 图 7(a) 是 243 × 243 三值 SRAM-PUF 阵列中 243 位的输出响应的随机性. 以逻辑值"1"为例,从图中可以看出,该阵列的随机性服从期望值为 33.21%、标准差为 5.6% 的高斯分布. 图 7(b)给出了 3 位输出响应的 27 种可能的取值,通过 HSPICE 仿真并统计数据,可以得出连续三位输出响应的概率几乎相等. 由图 7(a)中期望值为 33.21% 与理想情况的 33.3% 几乎相等,以及图 7(b)中 27 种可能取值概率基本相等可以得出:提出的三值 SRAM-PUF 具有很好的随机性.

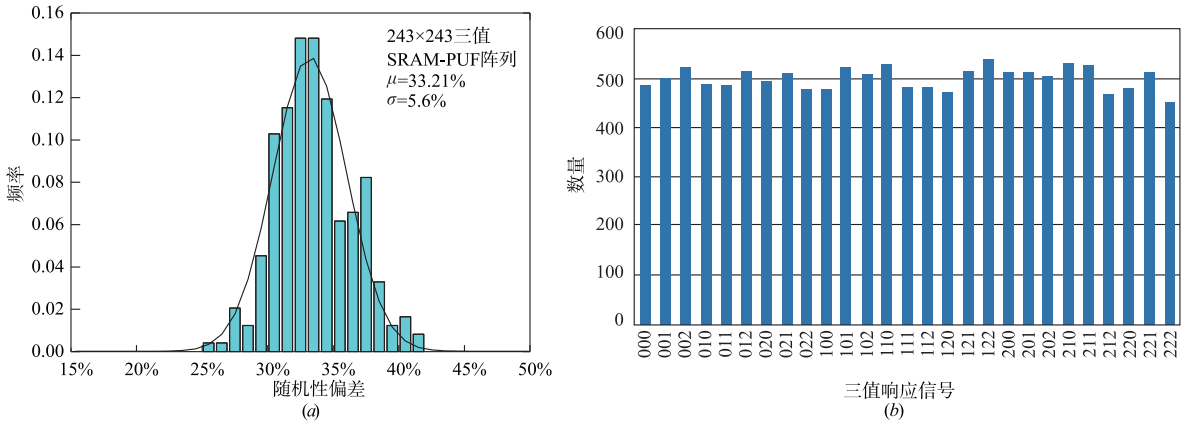

图7 三值SRAM-PUF随机性统计结果 (a) 243×243三值SRAM-PUF阵列的随机性"1"的分布;(b) 27种3位三值响应信号

相比二值 PUF 电路,三值 PUF 电路具有更多的逻辑值. 因此,在对比二值与三值 PUF 电路随机性时,需要将随机性偏差归一化. 归一化随机性偏差为:$R_u = |R_r - R_{id}|/d$. 其中,R_u 为归一化随机性偏差、R_r 随机性偏差测量值、R_{id}为理想随机性偏差、d 为逻辑基. 从表 1 可以看出本文提出的三值 SRAM-PUF 电路归一化偏差最小,具有很强的随机性.

表 1　与传统二值 PUF 电路的随机性偏差对比

文献	工艺	类型	随机性偏差测量值 %	归一化随机性偏差 %
[6]	45nm CMOS	Arbiter-PUFs	50.1	0.05
[10]	180nm CMOS	Arbiter-PUFs	65.6	7.8
[11]	65nm CMOS	DeMUX-PUFs	59.8	4.9
[12]	130nm CMOS	SRAM-PUFs	51.2	0.6
[13]	90nm CMOS	SRAM-PUFs	53.8	1.9
本文	32nm CNFET	SRAM-PUFs	33.2	0.03

3.2　唯一性

PUF 电路的唯一性越好,其不可克隆性越强,从而电路更安全. 唯一性可由平均片间汉明距离(Inter-Hamming Distances, HD_{Inter})来表示. HD_{Inter}的测量是在相同条件下对不同芯片给相同的激励,每片芯片得到特定的输出响应,测量这些输出响应的平均片间汉明距离. 理想情况下,三值 SRAM-PUF 电路的唯一性为 66.66%. 对于 K 片不同的芯片,其平均片间汉明距离可由公式(1) 计算得到[1]:

$$HD_{\text{Inter}} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \qquad (1)$$

其中,R_i 和 R_j 为芯片 i 和 j 的 n 位输出响应. 通过 Monte Carlo 仿真,图 8 给出了 200 片输出响应为 243 位的三值 SRAM-PUF 电路的片间汉明距离分布图. 由图 8 可知,本文提出的三值 SRAM-PUF 电路片间汉明距离期望值为 66.75%,标准差为 5.96%. 其期望值与理想值非常接近,因此三值 SRAM-PUF 电路具有很好的唯一性.

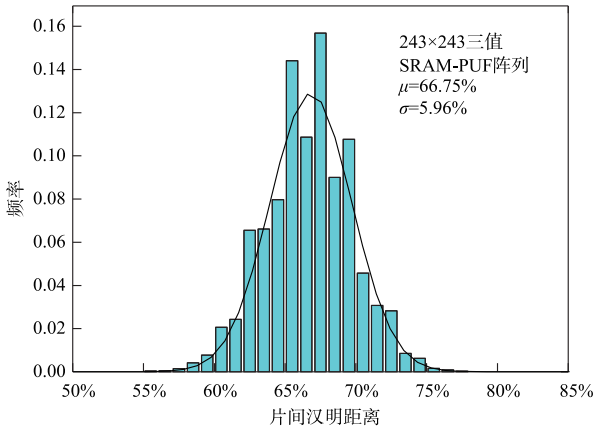

图8 片间汉明距离分布图

同样三值 PUF 电路与二值 PUF 电路唯一性的对比，需进行归一化处理. 归一化唯一性为：$U_u = |U_r - U_i|/d$. 其中，U_u 为归一化唯一性、U_r 为唯一性测量值、U_i 为唯一性理想值、d 为逻辑基. 从表 2 中可以看出，归一化后本文提出的三值 SRAM-PUF 归一化唯一性最小，具有很高的唯一性.

表 2 与传统二值 PUF 电路的唯一性偏差对比

文献	工艺	类型	唯一性测量值%	归一化唯一性%
[6]	45nm CMOS	Arbiter-PUFs	49.80	0.1
[12]	130nm CMOS	SRAM-PUFs	50.50	0.25
[13]	90nm CMOS	SRAM-PUFs	49.66	0.17
[14]	90nm CMOS	Arbiter-PUFs	46.14	1.93
[15]	65nm CMOS	RO-PUFs	50.42	0.21
本文	32nm CNFET	SRAM-PUFs	66.75	0.03

3.3 工作速度

由图 5 所示的三值 SRAM-PUF 单元工作时序图可知，等待时间 T_d 必须大于交叉耦合三值反相器竞争到数据稳定所用的建立时间 T_s，否则读出的数据将会出错. 图 9 为三值 SRAM-PUF 单元电路 Monte Carlo 仿真结果，得到 T_s 为 0.1ns. 表 3 给出了二值 SRAM-PUF 电路与本文的工作建立时间的对比，可得三值 SRAM-PUF 电路具有 T_s 最小，表明其工作速度比利用 CMOS 设计的 PUF 电路工作速度要快得多，工作速度至少提高了 33%. 文献[16]是在电压电压为 300mV 下的仿真结果，导致电路速度更慢.

表 3 SRAM-PUF 电路稳定信号建立时间

文献	工艺	类型	建立时间 T_s(ns)
[3]	65nm CMOS	SRAM-PUFs	0.15
[16]	65nm CMOS	SRAM-PUFs	100
本文	32nm CNFET	SRAM-PUFs	0.1

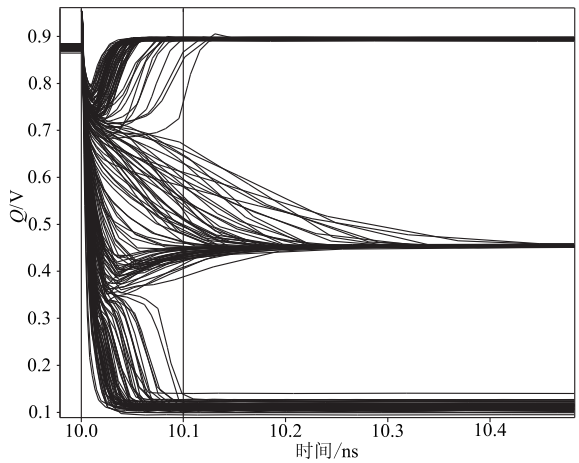

图9 三值SRAM-PUF单元电路Monte Carlo仿真结果

4 结论

本文设计了一种基于 CNFET 的三值 SRAM-PUF 电路. 利用 CNFET 在制造过程中产生的随机偏差，得到交叉耦合三值反相器的不同预充电电流，通过三值 SRAM 的竞争，产生唯一的、不可预测的输出响应. 通过 HSPICE 仿真，模拟结果表明该三值 SRAM-PUF 电路的随机性为 33.21% 与理想值的 33.33% 非常接近，唯一性为 66.75% 与理想值的 66.66% 几乎相等，具有很强的随机性和很高的唯一性. 相比传统的硅 PUF 电路，该三值 SRAM-PUF 大大提高了激励响应对的数量，且工作速度至少提高了 33%，因此该三值 SRAM-PUF 电路可以达到很高的工作频率. 本文提出的三值 SRAM-PUF 电路可以应用于身份认证和密钥产生等信息安全领域.

参考文献

[1] Chen A. Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions[J]. IEEE Electron Device Letters, 2015, 36(2): 138 – 140.

[2] Ravikanth P S. Physical one-way functions[J]. Science, 2002, 297(5589): 2026 – 2030.

[3] Zhang X L, Wang P J, ZHANG Y J. Highly stable data SRAM-PUF in 65nm CMOS process[A]. 2013 IEEE 10th International Conference on ASIC[C]. IEEE, 2013. 1 – 4.

[4] 汪鹏君，张学龙，张跃军. 基于最优控制电压的高鲁棒性 PUF 电路设计[J]. 电子学报，2015，43(5)：907 – 910.
Wang P J, Zhang X L, Zhang Y Y. Design of highly robust PUF based on the optimal gate voltage[J]. Acta Electronica Sinica, 2015, 43(5): 907 – 910. (in Chinese)

[5] 汪鹏君，李刚，钱浩宇. 可配置电阻分压型 DAC-PUF 电路设计[J]. 电子学报，2016，44(7)：1630 – 1635.

Wang P J,Li G,Qiang H Y. Design of configurable resistance divider type DAC-PUF circuit[J]. Acta Electronica Sinica,2016,44(7):1630 – 1635. (in Chinese)

[6] Vijayakumar A,Kundu S. A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics[A]. 2015 Design, Automation & Test in Europe Conference&Exhibition[C]. EDA Consortium, 2015. 653 – 658.

[7] Deng J,Wong H S P. A compact SPICE model for carbon-nanotube field-effect transistors including nonidealities and its application-part I:model of the intrinsic channel region [J]. IEEE Transactions on Electron Devices, 2007, 54 (12):3186 – 3194.

[8] 唐伟童,汪鹏君,王谦. 一种 CNFET 的多位三值比较器设计[J]. 西安电子科技大学学报:(自然科学版),2016, 43(1):139 – 143.
Tang W T,Wang P J,Wang Q. Design of magnitude ternary comparator of CNFET[J]. Journal of Xidian University (Natural Science Edition), 2016, 43 (1): 139 – 143. (in Chinese)

[9] Stanford nanoelectronics lab. stanford CNFET model and schottky barrier CNFET model[EB/OL]. http://nano.stanford.edu/model.php? id = 23. 2015-12-18.

[10] Lim D,Lee J W,Gassend B,et al. Extracting secret keys from integrated circuits[J]. IEEE Transaction on Very Large Scale Intergration Systems, 2004, 13 (10): 1200 – 1205.

[11] Lao Y, Parhi K K. Statistical analysis of MUX-based physical unclonable functions[J]. IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems,2014,33(5):649 – 662.

[12] Su Y,Holleman J,Otis B P. A digital 1.6 pJ/bit chip identification circuit using process variations[J]. IEEE Journal of Solid-State Circuits,2008,43(1):69 – 77.

[13] Chellappa S,Clark L T. SRAM-based unique chip identifier techniques[J]. IEEE Transactions on Very Large Scale Integration Systems,2016,24(4):1213 – 1222.

[14] Suh G E,Devadas S. Physical unclonable functions for device authentication and secret key generation[A]. Paoc of Design Automation Conference[C]. New York: ACM, 2007. 9 – 14.

[15] Cao Y,Zhang L,Chang C H,et al. A low-power hybrid RO PUF with improved thermal stability for lightweight applications[J]. IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems,2015,34(7):1 – 5.

[16] Jang J W,Ghosh S. Design and analysis of novel SRAM PUFs with embedded latch for robustness[A]. International Symposium on Quality Electronic Design[C]. Sarta Clana,2015. 298 – 302.

作者简介

汪鹏君(通信作者)　男,1966 年出生于浙江奉化,博士,教授,博士生导师,中国电子学会高级会员,中国计算机学会高级会员,中国电子学会电子线路与系统专业委员会委员,中国计算机学会多值逻辑与模糊逻辑专业委员会委员,目前主要从事低功耗、高信息密度集成电路理论和设计、安全芯片理论和设计、多媒体技术及相关理论方面研究工作.
E-mail:wangpengjun@nbu.edu.cn

龚道辉　男,1991 年出生于湖南岳阳,硕士研究生,主要从事多值逻辑电路设计及理论的研究.

张会红　女,1976 年出生于河北定州,副教授,硕士研究生导师,主要主要从事高信息密度和低功耗集成电路理论及优化设计.

康耀鹏　男,1992 年出生于浙江台州,硕士研究生,主要从事多值逻辑电路设计及理论的研究.