

基于电平转换器的物理不可克隆函数电路设计

韩丽娟¹, 钱蕾¹, 姚恩义^{2,3}, 娄鑫⁴, 曹元¹, 刘宴华⁵

(1. 河海大学物联网工程学院, 江苏 常州 213022;

2. 华南理工大学微电子学院, 广东 广州 511442;

3. 人工智能与数字经济广东省实验室(广州), 广东 广州 511442;

4. 上海科技大学信息科学与技术学院, 上海 201210;

5. 上海空间电源研究所, 上海 200245)

摘要: 提出一种基于通用交叉耦合电平转换器的低开销新型物理不可克隆函数的电路设计。该设计只需在传统电平转换电路中引入一个额外的开关晶体管, 用来切换电平转换器的差分工作模式和共模工作模式, 利用交叉耦合网络中两个 PMOS 晶体管由于开关速度不同所引起的输出电压的不确定性, 通过共模模式输出获取所必需的熵值。该电路采用标准 65 nm CMOS 工艺进行设计, 仿真结果显示该 PUF 的唯一性为 49.11%, 接近理想值。在电压为 1.0~1.5 V 内, 可靠性可达 96.09%, 而在环境温度为-20~100 °C 内, 可靠性可达 95.31%。同时在高速吞吐率为 20 Mbit/s 时, 每比特输出能耗仅为 0.72 pJ (1.2 V, 27 °C)。

关键词: 物理不可克隆函数; 工艺偏差; 电平转换器

中图分类号: TN402

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021024

Novel level shifter based physical unclonable function circuit design

HAN Lijuan¹, QIAN Lei¹, YAO Enyi^{2,3}, LOU Xin⁴, CAO Yuan¹, LIU Yanhua⁵

1. College of Internet of Things Engineering, Hohai University, Changzhou 213022, China

2. School of Micro-Electronics, South China University of Technology, Guangzhou 511442, China

3. Guangdong Artificial Intelligence and Digital Economy Laboratory (Guangzhou), Guangzhou 511442, China

4. College of Information Science and Technology, Shanghai Tech University, Shanghai 201210, China

5. Shanghai Institute of Space Power-Sources, Shanghai 200245, China

Abstract: Level shifters are widely used in low-power, multi-threshold integrated circuit chips. A novel physical unclonable function (PUF) design based on cross-coupled level shifter was proposed. In this work, a single

收稿日期: 2020-08-27; 修回日期: 2021-01-22

通信作者: 姚恩义, yaoenyi@scut.edu.cn

基金项目: 江苏省自然科学基金(BK20191160); 计算机架构国家重点实验室开放研究项目(CARCH201901); 青蓝工程; 常州市应用基础研究计划(CJ20200071); 常州市科技成果转化专项基金(2020029)

Foundation Items: The Natural Science Foundation of Jiangsu Province, China (BK20191160), Open Research of the State Key Laboratory of Computer Architecture (CARCH201901), QingLan Project, Changzhou Applied Basic Research Plan (CJ20200071), The Special Fund of Changzhou for the Transformation of Scientific and Technological Achievements (2020029)

论文引用格式: 韩丽娟, 钱蕾, 姚恩义, 等. 基于电平转换器的物理不可克隆函数电路设计[J]. 网络与信息安全学报, 2021, 7(2): 86-93.

HAN L J, QIAN L, YAO E Y, et al. Novel level shifter based physical unclonable function circuit design[J]. Chinese Journal of Network and Information Security, 2021, 7(2): 86-93.

switching transistor was inserted in the level shifter, which was the only overhead per response bit to change the operation mode of the cross-coupled level shifter from differential to common. The signature of the PUF was extracted while in common mode, by exploiting the uncertainty of the output voltage due to the difference of the switching time of the two PMOS in the cross-coupled network. Simulated with a standard 65 nm CMOS process, the results show the proposed PUF can produce a uniqueness of 49.11% and a reliability of 96.09% with the power supply voltage ranged from 1.0 V to 1.5 V and 95.31% with the temperature ranged from -20°C to 100°C . The energy per bit is only 0.72 pJ at a high throughput of 20 Mbit/s (1.2 V, 27°C).

Keywords: physical unclonable function, process variation, level shifter

1 引言

在新兴的物联网 (IoT, internet of thing) 时代, 新一代信息技术逐渐向各个领域渗透, 各种智能设备应运而生, 其数量呈现爆破式增长。因此, 安全性能和隐私问题也随之受到了人们的广泛关注。为了在资源受限的 IoT 设备上实现低成本但高安全性的功能, 各行业学者正致力于研究更优的轻量级解决方案^[1]。物理不可克隆函数 (PUF, physical unclonable function) 作为一种新型的轻量级硬件安全原语正逐渐被应用于密钥管理、安全防伪和设备身份认证等领域^[2]。与传统的将机密密钥信息存储在非易失性存储器 (NVM, non-volatile memory) 中的加密算法不同的是, PUF 的产生得益于芯片制造过程中的不可预测且不受控制的工艺变化, 从中能够提取可靠且独特的物理差异, 而且其所含的密钥信息不需要任何存储器存储, 同时能够抵抗各种物理攻击 (侵入式攻击等) 诱发的密钥泄露等安全威胁, 具有防篡改和轻量级等良好特性^[3]。

自 2001 年 PUF 的概念被提出^[4], 多年来人们对 PUF 的研究从未止步。根据 PUF 电路结构生成 CRP (每个 PUF 输入和其对应的输出被称为该 PUF 的激励-响应对 (challenge-response pair) 数量的不同, PUF 可以大致分为两类: 强 PUF 和弱 PUF。强 PUF 拥有庞大的 CRP, 并随着电路单元的增加而呈指数增长, 在针对重放攻击的身份验证协议、通信验证协议开发等环节中具有广泛的应用场景^[5]。而弱 PUF 的 CRP 数量有限, 随结构单元的增加呈线性或多项式增长, 因此更适用于 ID 生成或密钥管理等应用。2016 年, Li 等^[1]提出了一种基于模拟电路的弱 PUF 设计,

该电路的输出电压正比于绝对温度, 通过读取放大器的输出电压产生随机数字 “0” 或 “1”。Yuan 等^[6]在 2019 年提出了一种基于对称 MOS 电容充电差异的 PUF 电路结构, 该方法可以有效抑制模拟电路中的上电复位噪声等问题。

相对于模拟电路, 数字电路更不容易受到芯片工艺波动的影响, 而且往往具有更小的面积及功耗, 更加容易与其他数字系统集成。利用现有芯片上的硬件资源构建 PUF 则更能节省成本、降低开销。利用数字电路模块, 一种可以在芯片内部自由分配的基于 D 触发器的 PUF 被提出。然而, 当温度在 $40\sim 85^{\circ}\text{C}$ 内变化时, 这种 PUF 的可靠性将会降低至 80%^[7]。Simons 等^[4]利用总线管理器提出了一种替代 D 触发器的弱 PUF。尽管与基于 D 触发器的 PUF 相比, 总线管理器 PUF 消耗更少的资源, 但它仍然容易受到温度和电压等因素的影响, 并且仅有 36% 的唯一性。诸如此类设计概念 (利用 D 触发器、总线管理等) 的 PUF 结构还有许多。然而, 利用电平转换器结构构建 PUF 的成功实例并未出现。

电平转换器广泛用于低功耗电路设计^[8], 设计示例如图 1 所示。电平转换器用于连接不同电源域之间的信号^[9], 起到至关重要的作用。为了有效提高传统数字 PUF 的可靠性和唯一性, 本文将电平转换器结构应用于 PUF 领域, 提出了一种基于数字电平转换器的新型 PUF 电路结构设计。该电路结构在原有的电平转换器电路中仅额外引入一个单独的 NMOS 开关晶体管开销, 并利用共模交叉耦合电平转换器输出电压的不确定性来生成数字化响应位。通过控制数字开关的状态使电路工作模式可以在电平转换器 (差模输入) 和 PUF (共模输入) 之间随意切换。

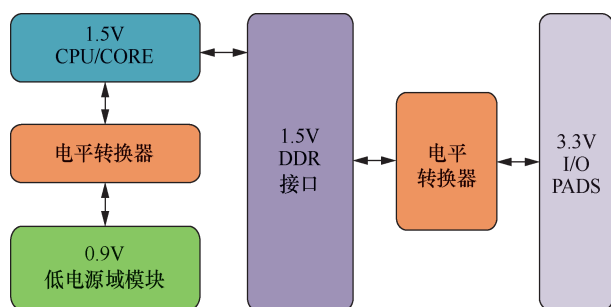


图1 低功耗电路设计示例
Figure 1 Example of low-power circuit design

2 新型 PUF 体系结构

图2显示了新型的基于交叉耦合电平转换器的 PUF 晶体管实现,它主要由具有低电压输入的 NMOS 差分输入对和在较高电源电压下工作的两个交叉耦合 PMOS 晶体管组成。图2(a)虚线框中的 NMOS 晶体管 MN5 是 PUF 每个响应位的唯一一片内开销,用于切换电路的工作模式(电平转换器模式和 PUF 模式)。两种模式的操作过程可以通过图2(b)的时序图进行说明。需要说明的是, VDDL 表示低电源电压, VDDH 表示高电源电压。本文中 VDDL=0.6V, VDDH=1.2V。在低电平电压域内, VDDL (0.6V) 为高电平;在高电平电压域内, VDDH (1.2V) 为高电平。

在电平转换器模式下, V_{ctr} 为低电平。当输入信号 “in” 为高电平 VDDL 时, 晶体管 MN1 和 MP2 导通, MN2 和 MP1 截止。由于交叉耦合电

平转换器的正反馈机制, 节点 B 被充电至 VDDH。随后, 输入信号 “in” 变为低电平, 节点 B 处被拉低至低电平, 晶体管 MN2 和 MP1 开启。在这个过程中, 具有差分共源共栅电压逻辑门的电平转换器可以将低输入电压信号转换为较高的电压信号。在 PUF 模式下, V_{ctr} 为高电平 VDDH, MN5 开启。当 NMOS 对的两个输入电压均为低电平时, 晶体管 MN1 和 MN2 均截止, 节点 A 和节点 B 将处于亚稳定状态。随后, 根据 MN1 和 MN2 之间具体的电流传导情况, 该亚稳态将锁存至高电源电压 VDDH 或 GND。当输入信号 “in” 升高至高电平 VDDL 时, 理论上晶体管 MN1 和 MN2 均导通, 节点 A 和节点 B 的电压随之下降。但是, 由于晶体管 MN1 和 MN2 的工艺波动, I_1 和 I_2 的电流略有不同, 导致晶体管 MP1 或 MP2 的打开时刻存在差异, 同时正反馈机制加速了各个晶体管的状态转换, 最终使输出位稳定为 “1” 或 “0”。

PUF 是电平转换器在共模输入情况下工作的, 为了避免两个输入端之间的反相器对共模输入时 PUF 性能的影响, 需要将其断开, 即 PUF 模式下不需要 VDDL 对电路供电。

新型 PUF 的主要熵源来自在共模输入情况下, NMOS 晶体管对 (MN1, MN2) 的工艺偏差会引起交叉耦合网络中两个 PMOS 晶体管的开关速度不同, 进一步将导致输出电压的不确定性。

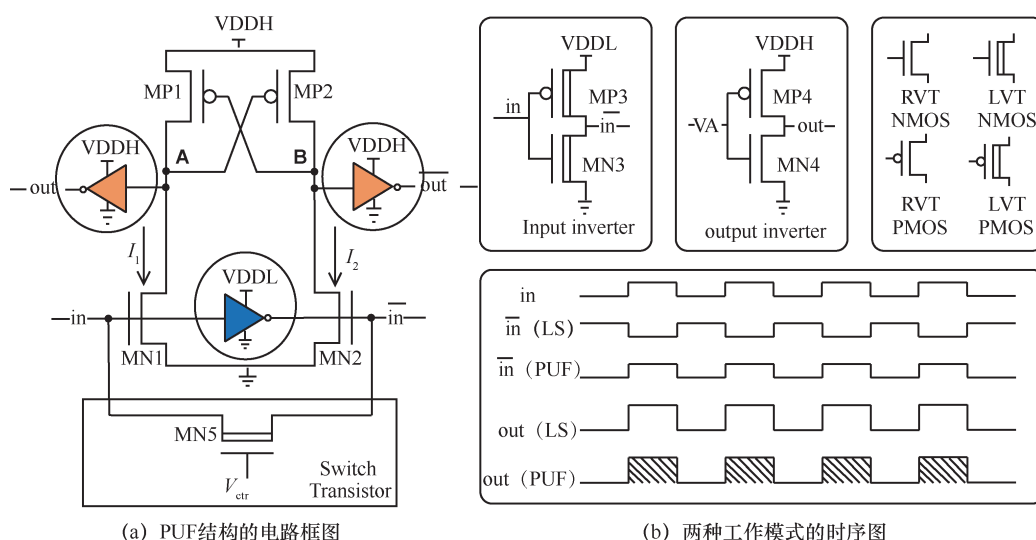


图2 新型的基于交叉耦合电平转换器的 PUF 晶体管实现
Figure 2 Implementation of a novel PUF transistor based on cross-coupled level shifter

例如, 输入信号“in”为高电平, 具体分析其主要熵源及最终所确定的输出状态 (在此假设理想情况下, 信号“in”和“ $\overline{\text{in}}$ ”完全同步, 没有时延、压降等一系列由 MN5 造成的问题)。当输入信号“in”为高电平时, “ $\overline{\text{in}}$ ”也为高电平, 此时晶体管 MN1 和 MN2 均导通。然而, 由于 NMOS 晶体管对 (MN1, MN2) 的工艺偏差, 同一时刻二者的漏极电压 (即 A、B 节点电压) 存在差异, 此差异会导致交叉耦合网络中两个 PMOS 晶体管的其中一个比另外一个优先导通, 同时导通一侧的节点 (A 与 B) 会被充电, 进一步引起另一侧 PMOS 晶体管的关闭。最终输出位会被稳定为“1”或“0”。正是由于 NMOS 对在电路工作时的重要作用, 优化 NMOS 对的类型、尺寸可以降低功耗、面积, 并增加工艺变化引起的随机性。此外, 为了避免电路结构的不完全对称性对输出特性的影响, 节点 A 和节点 B 处均添加了一个反相器作为缓冲器。同时, 晶体管 MN5 是一个低阈值器件, 用于衰减由 MN5 传输电阻形成的电压降, 尽可能使信号“in”和“ $\overline{\text{in}}$ ”对称。图 3 描绘了全局蒙特卡洛 (MC) 仿真得出的 PUF 输出电压的概率分布。随机比特位为“0”和“1”的百分比分别为 49.25% 和 50.75%。同时可以看出, 在微小偏置忽略不计的情况下, 输出位是对称分布的。

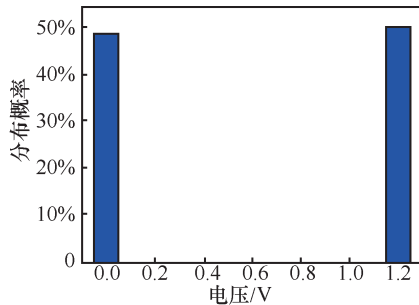


图3 基于电平转换器 PUF 输出电压的分布
Figure 3 Distribution of the level shifter based PUF's output voltages

3 仿真分析

本节将分析提出的新型 PUF 在唯一性、可靠性、随机性、速度与功耗等性能。在 1.2 V、65 nm CMOS 工艺下, 通过 Cadence Virtuoso Spectre 对所提出的 PUF 进行了仿真。收集的数据由

MATLAB 脚本进一步处理。

实验发现, 在工作频率为 20 MHz 时, 该新型电路能在 PUF 模式和电平转换器模式下正常工作且具有较好的性能。也就是说, 在工作频率为 20 MHz 时, 电平转换器电路能够很好地将 0.6 V 输入信号转换为 1.2 V, 同时保证了高性能 PUF 电路的唯一性、可靠性、随机性、功耗等。图 4 显示的则是 20 MHz、0.6 V 的输入信号转换为 1.2 V 的仿真波形, 可以看出该电平转换器能够很好地将亚阈值电压转换为标准电压。

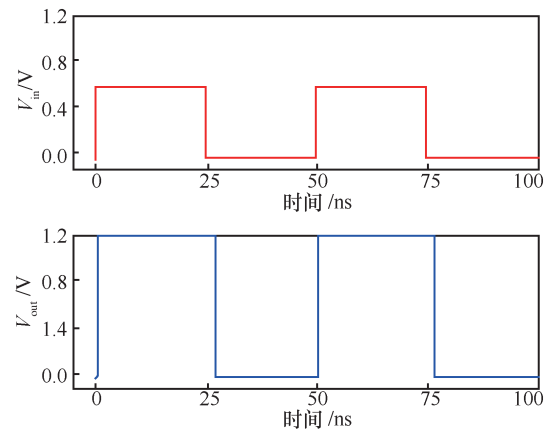


图4 交叉耦合电平转换器的仿真波形
Figure 4 Simulated waveform of the cross-coupled level shifter

在保证电平转换器正常工作的前提下, 本文将进一步对 PUF 的唯一性、可靠性、随机性、速度与功耗进行详细的分析验证。

3.1 唯一性

唯一性衡量的是不同的 PUF 实例产生的 CRP 之间的差异程度, 通过平均片间汉明距离 (HD, Hamming distance) 进行估计。PUF 的唯一性 U 表示如下:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^m \frac{\text{HD}(R_u, R_v)}{n} \times 100\% \quad (1)$$

其中, m 是 PUF 设备的总数。 R_u 和 R_v 是具有相同激励 C 的两个不同 PUF 设备的随机输出比特流。 n 是位长, 此处 $n=128$ 。在理想情况下, PUF 的唯一性应为 50%, 这意味着 PUF 实例能被完全区别, 并且具有最大的去相关性。本文在标称条件 (1.2 V, 27 °C) 下, 进行了 1 000 次迭代的 MC 仿真, 以评估 PUF 的唯一性。图 5 给出了提出的 PUF 的 HD 分布状况。与平均值 μ

为 49.11% 和标准偏差 δ 为 4.42% 的高斯分布曲线能很好地拟合。

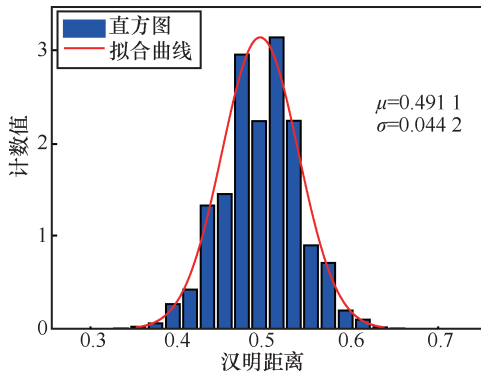


图5 片间汉明距离分布
Figure 5 Distribution of inter-die Hamming distance

3.2 可靠性

PUF 的另一个特性是可靠性。它评估的是在不同的工作条件（如不同的电源电压、温度、噪声等）下，PUF 在相同的激励下生成的 CRP 的稳定性，通常用误码率（BER, bit error rate）表示。BER 是指生成的比特流中错误的比特数相对于总比特数的百分比。可靠性 S 通常计算如下：

$$S = 1 - \text{BER} = 1 - \frac{1}{k} \sum_{j=1}^k \frac{\text{HD}(R_i, R_{i,j})}{n} \times 100\% \quad (2)$$

其中， R_i 是标称条件（1.2 V，27 °C）下随机激励 C 的响应。 $R_{i,j}$ 是在不同操作条件、相同激励 C 时的响应。 k 是相同激励 C 评估同一个 PUF 的次数。理想的 PUF 必须具有 100% 的可靠性。

PUF 的可靠性通过在不同的条件下的 BER（温度范围 -20 ~ 100 °C，电源电压范围 1.0 ~ 1.5 V）进行评估。本文中温度变化步长为 10 °C，电源电压变化范围为 0.1 V，在每种条件下收集 1 000 个 CRP 以计算可靠性。图 6 给出了仿真结果，最差情况下的可靠性位于 100 °C 和 1.0 V。最终在不同温度条件下的归一化 BER 为 1.98%，在不同电压变化条件下的归一化 BER 为 2.2%。

为了进一步评估噪声对 PUF 可靠性的影响，通过进行瞬态噪声模拟来研究 PUF 在噪声环境下的可靠性。Spectre 瞬态噪声设置为： $f_{\max}=100$ GHz， $f_{\min}=1$ kHz，scale=1。以在标称条件（1.2 V，27 °C）下和不考虑噪声为参考值，通过式(2)计算噪声

存在情况下的误码率。最终得出 BER 为 1.56%，接近理想值 0。说明该新型 PUF 具有很好的抗噪声能力。

3.3 随机性

随机性估计的是 PUF 生成的 CRP 的不确定性或不可预测性。好的 PUF 具有高随机性，这意味着攻击者很难用收集的少量 CRP 成功预测。为了评估随机性，进行了美国国家标准技术研究所（NIST, National Institute of Standards and Technology）随机性测试和自相关测试。

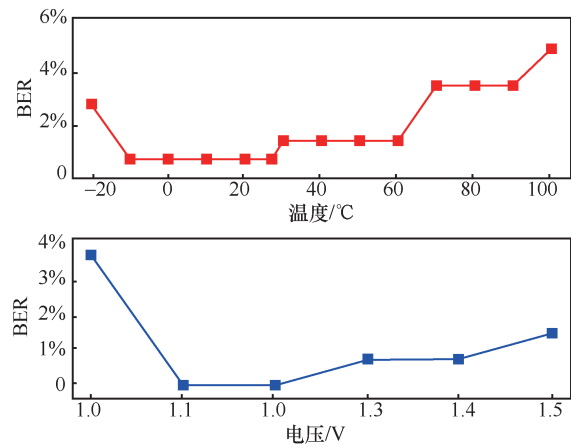


图6 在一定温度和电源电压范围内的 BER
Figure 6 The simulated native BER with varied operating temperature and supply voltage

(1) NIST 随机性测试：NIST SP800 统计测试套件是用于随机性分析的重要测试套件。本文实验收集了 10 000 个原始 PUF 响应位，表 1 给出了 NIST 测试结果。 P 值用于衡量随机程度，且所有 P 值均应大于 0.01，以使任意随机源的置信度达到 99%。从表 1 可以看出，该 PUF 通过了所有 NIST 测试（因比特流长度有限，未显示的其他项目未执行），这意味着 PUF 生成的随机比特序列具有较高的随机性。

(2) 自相关测试：自相关是信号在不同时间点与自身的互相关。自相关函数（ACF, autocorrelation function）可用于计算随机位序列的自相关，以确定其是否独立且均匀分布。图 7 显示了 50 000 CRP 的 ACF 测试结果，在置信水平为 95% 下，置信区间为 [-0.008 9, 0.008 9]。置信区间值表明 ACF 测试结果误差范围小，同时说明该 PUF 证明了不易受相关性分析攻击^[10]。

表 1 PUF 生成的随机序列的 NIST 测试结果
Table 1 Results of the NIST test on the random sequences generated by our proposed PUF

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P 值	PRPO	测试项
5	0	4	0	4	2	0	2	3	0	0.048 716	20/20	频率检验
5	0	4	0	4	2	0	2	3	0	0.048 716	20/20	块内频数检验
4	1	0	3	3	1	1	2	3	2	0.637 119	20/20	累加和检验（前向）
2	3	1	2	3	0	0	2	3	4	0.534 146	20/20	累加和检验（后向）
4	0	2	3	1	1	0	3	3	3	0.437 274	20/20	游程检验
0	1	2	1	3	2	1	6	0	4	0.066 882	20/20	块内最长游程检验
2	2	4	0	1	3	2	1	4	1	0.534 146	20/20	近似熵检验
4	1	1	1	3	2	4	2	1	1	0.637 119	20/20	序列检验（前向）
1	4	1	2	2	4	0	2	2	2	0.637 119	20/20	序列检验（后向）

表 2 性能比较
Table 2 Performance comparison

方法	采用的电路	温度/℃	电源电压/V	唯一性	可靠性（温度）	可靠性（电压）	比特率/Mbit·s ⁻¹	功耗/μW	能耗/位/pJ·bit ⁻¹
本文	电平转换器	-20~100	1.0~1.5	49.11%	95.31%	96.09%	20	14.39	0.72
HOST'12 ^[4]	Buskeeper	-40~85	1.08~1.32	49.01%	80.00%	95.00%	—	—	—
ACM CCS'10 ^[7]	D 触发器	-40~80	—	36.00%	—	—	—	—	—
TCAS'17 ^[11]	环形振荡器	-40~120	0.9~1.3	49.97%	97.90%	—	—	—	38.33
ISCAS'19 ^[6]	差分电容	0~80	1.2~1.8	50.03%	97.70%	96.20%	27.78	20.86	0.75

注：“—”表示无法获得。

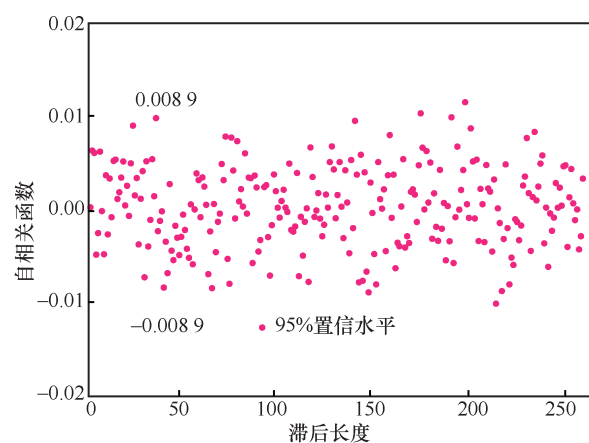


图 7 自相关测试结果
Figure 7 Autocorrelation test results

3.4 速度与功耗

为了进一步评估所设计的新型 PUF 的性能，本文对其功耗和比特率进行了测量。图 8 给出了

标称条件（1.2 V，27 ℃）下，功耗、每比特能耗与比特率之间的关系。在本设计中，能使两种工作模式均能正常操作且各项性能相对较好的最大比特率为 20 Mbit/s，此时功耗为 14.39 μW，每比特的能耗为 0.72 pJ。

3.5 性能比较

本文所提出的 PUF 性能与表 2 中最新的弱 PUF 设计进行了比较。与基于现有硬件资源的几种 PUF 相比，可以得出以下结论：各自的温度和电源电压范围内，本文所提出的 PUF 在可靠性和唯一性方面明显优于其他 PUF，同时噪声环境下的 BER 仅为 0.015 6，抗噪声能力强。与 ISCAS'19^[6]中的结构相比，所提出的 PUF 的每比特能耗（0.72 pJ）降低了 1%，并且具有更高的工作频率 20 MHz。本文利用电平转换器的思想创建一个弱 PUF 结构。在所设计的基于交叉耦合电

平转换器的 PUF 结构中, 每个响应位的开销仅为单个 NMOS 晶体管, 在整体布局中可以忽略不计, 这使所提出的设计具有低能耗和每个响应位低开销的特点。

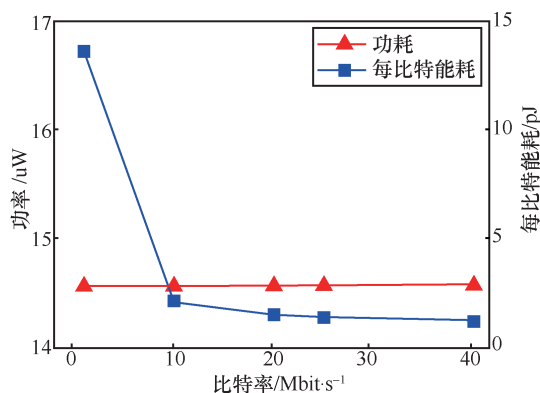


图 8 不同比特率下的功耗和能耗

Figure 8 Power dissipation and energy per bit across bit rate

4 结束语

本文介绍了一种高性能、低开销的弱 PUF 电路结构, 从电平转换器设计中提取熵。在原有的电平转换器电路基础上, NMOS 开关晶体管是 PUF 工作时每个响应位的唯一片内开销, 它使现有的交叉耦合电平转换器电路可以轻松地在差分模式和共模模式之间切换。本文提出的 PUF 单元通过利用由共模信号控制的两个 NMOS 晶体管的固有工艺变化来提取熵, 最终得到随机响应序列, 并使用标准的 65 nm CMOS 工艺执行 MC 仿真, 具有 49.11% 的唯一性。在最坏情况下, 在温度 $-20 \sim 100^{\circ}\text{C}$ 、电源电压 $1.0 \sim 1.5\text{ V}$ 内, 可靠性分别为 95.31% 和 96.09%。通过设置瞬态噪声仿真参数值, 得到最终噪声环境下的 BER 为 1.56%, 接近理想值 0。最大比特率和最佳的每比特能耗为 20 Mbit/s 和 0.72 pJ/bit。该设计可以在原有电平转换器电路上进行改进, 该电路是在原有电平转换器的基础上仅添加一个额外 NMOS 晶体管形成的, 低开销和低能效的优势使其成为物联网设备中具有应用前景的硬件安全原语。

参考文献:

[1] LI J, SEOK M. Ultra-compact and robust physically unclonable

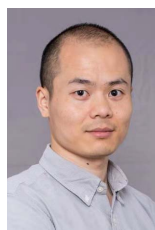
function based on voltage-compensated proportional-to-absolute-temperature voltage generators [J]. IEEE Journal of Solid-State Circuits, 2016, 51(9): 2192-2202.

- [2] MISPLAN M S, HALAK B, CHEN Z, et al. TCO-PUF: a subthreshold physical unclonable function [C]//2015 11th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME). 2015: 105-108.
- [3] 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 (HOST). 2014: 38-43.
- [4] SIMONS P, VAN DER SLUIS E, VAN DER LEEST V. Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs [C]//2012 IEEE International Symposium on Hardware-Oriented Security and Trust. 2012: 7-12.
- [5] BAI C, ZOU X, DAI K. A novel thyristor-based silicon physical unclonable function [J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2016, 24(1): 290-300.
- [6] YUAN H, GUO W, CHANG C, et al. A reliable physical unclonable function based on differential charging capacitors [C]//2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019: 1-5.
- [7] LEEST V, SCHRIJEN G J, HANDSCHUH H, et al. Hardware intrinsic security from D flip-flops[C]//Proceedings of the ACM Conference on Computer and Communications Security. 2010: 53-62.
- [8] SONG J. Level-shifter current influence to power loss of gate driver IC[C]// International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management. 2019: 1-4.
- [9] SINGH P. A 19nW, near-threshold to I/O voltage level shifter in 28nm FD-SOI using 1.8v/28A device for IoT systems[C]//2018 IEEE International Symposium on Circuits and Systems (ISCAS). 2018: 1-4.
- [10] MATHEW S K, SRINIVASAN S, ANDERS M A, et al. 2.4 Gbit/s, 7 mW all-digital PVT-Variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors[J]. IEEE Journal of Solid-State Circuits, 2012, 47(11): 2807-2821.
- [11] LIU C Q, CAO Y, CHANG H C. 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.

[作者简介]



韩丽娟（1996-），女，河南新密人，河海大学硕士生，主要研究方向为物理不可克隆函数、真随机数发生器。



娄鑫（1987-），男，浙江湖州人，博士，上海科技大学研究员，主要研究方向为 VLSI 信号处理集成电路与系统。



钱蕾（1999-），女，江苏南通人，河海大学硕士生，主要研究方向为物理不可克隆函数、真随机数发生器。



曹元（1985-），男，江苏南通人，博士，河海大学教授，主要研究方向为物理不可克隆函数、真随机数发生器。



姚恩义（1988-），男，黑龙江七台河人，博士，华南理工大学副教授，主要研究方向为类脑及其他新型智能计算芯片设计、存算融合、硬件安全等。



刘宴华（1986-），男，山东栖霞人，上海空间电源研究所工程师，主要研究方向为空间飞行器设计。