郝嘉诚

2060434001@email.szu.edu.cn · +86 18558769035

教育背景

深圳大学，深圳 2023 – 至今

信息与通信工程，博士在读研究方向：集成电路硬件安全、智能图像传感芯片，以及面向事件相机的神经网络算法。

深圳大学，深圳 2020 – 2023

电子科学与技术，硕士研究方向：集成电路硬件安全，包括真随机数发生器与物理不可克隆函数芯片设计。

福州大学，福州 2014 – 2018

车辆工程，学士

科研与项目经历

CSRO-TRNG 低功耗真随机数发生器芯片设计 2023 – 2024

第一作者 / 40nm CMOS / 电路设计与流片实测 IEEE CICC 2024

- 设计基于多路异或电流饥饿环振的 TRNG 熵源架构，结合熵下界模型完成参数优化，将同类方案所需振荡器数量由 50–100 个压缩至 8 个。
- 负责前仿真、版图后仿真、测试板联调与芯片实测验证，完成从电路设计到硅后测试的完整闭环。
- 芯片面积为 331.5 μm^2，在 0.6 V 下实现 40 Mbps 输出速率，能效达到 97.9 fJ/bit。
- 完成 NIST SP 800-22、NIST SP 800-90B、PVT、老化与频率注入攻击测试，在 -65°C 至 140°C、0.6 V 至 1.3 V 范围内保持稳定随机性，并可承受 1 Vpp 频率注入。

Single-Chain TRNG 高 PVT 容忍真随机数发生器芯片设计 2024 – 2025

40nm CMOS / 电路设计与流片实测 IEEE TCAS-II 投稿方向

- 设计基于单个电流饥饿环振的 TRNG 架构，利用环振内部不同级节点的相位差提取抖动熵源，避免传统双环结构对片间失配校准和偏置调节的依赖。
- 构建三级高速环振与 3-bit 扩展单相时钟计数电路，实现紧凑型时间量化与随机比特生成。
- 完成芯片流片与实测分析，输出速率达到 69.8 Mbps，能效为 2.9 pJ/bit，核心面积约 241 KF^2。
- 通过 NIST SP 800-22、NIST SP 800-90B、FFT、ACF 与香农熵测试验证随机性，并在 -40°C 至 120°C、0.9 V 至 1.3 V 条件下验证 PVT 鲁棒性。

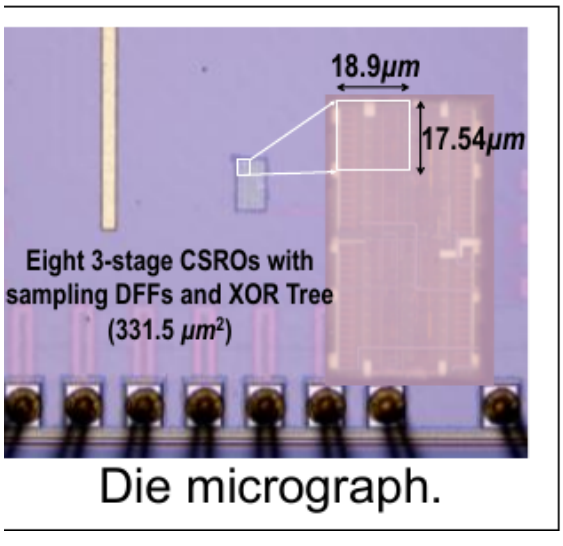
论文与成果

- 第一作者： “A 98fJ/Bit Current-Starved-Ring-Oscillator-Based TRNG with High PVT Tolerance and Resilience to Frequency Injection Attack Up to 1V”, **IEEE CICC**, 2024.
- 其他论文： “A 1.46pJ/bit, 149KF^2 RO TRNG Based on Reference-RO-Free Thresholding of Jitter Accumulation”, **IEEE TCAS-II**, 2025.
- “A 2.5 pJ/bit PVT-tolerant True Random Number Generator Based on Native-NMOS-Regulated Ring Oscillator”, **IEEE TCAS-II**, 2023.
- “A 3.02 pJ/bit 3T-APS-Based In-Sensor Strong PUF Featuring Near-100% Hardware Reuse Ratio and High Resilience to Machine Learning Attacks”, **IEEE TCAS-II**, 2023.
- “A Subthreshold-Inverter-Based Strong PUF with High Reliability and Energy Efficiency”, **IEEE ISCAS**, 2023.
- “A 166F^2/bit 0.0136%-Native-BER Physically Unclonable Function Based on Gate-Overhang-Shortened Transistor”, **IEEE CICC**, 2023.

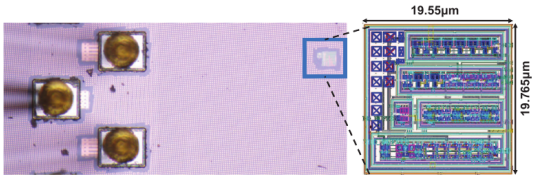
技能

- EDA / FPGA / PCB 工具：Cadence Virtuoso / Innovus / Vivado / Quartus / Altium Designer
- 编程与硬件描述：Python / Verilog / SystemVerilog

Chip Gallery



CICC 2024 CSRO-TRNG figure



Single-chain TRNG figure