CNPUF: A Carbon Nanotube-based Physically Unclonable Function for Secure Low-Energy Hardware Design

S. T. Choden Konigsmark, Leslie K. Hwang, Deming Chen, Martin D. F. Wong

University of Illinois at Urbana-Champaign

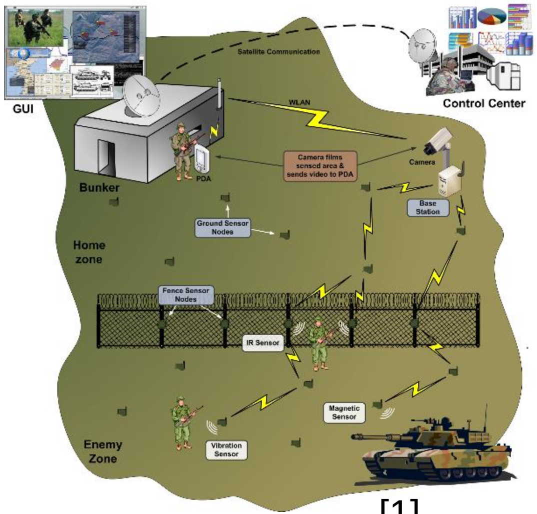
January 21, 2014

Outline

- Introduction
- Background
- Carbon Nanotube PUF (CNPUF)
- Extended CNPUF (ex-CNPUF)
- Experimental Evaluation
- Conclusion

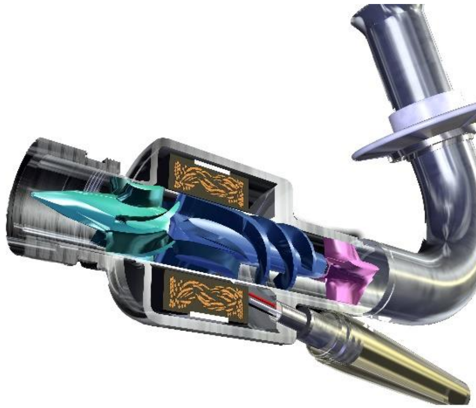
Introduction

- New devices and technologies: **New Risks**
  - Wireless sensor networks / military, crisis detection
  - Wearable technology / privacy
  - Medical electronics / health



[1]

[2]



[3]

Introduction (2)

- Security cannot be handled by software alone
  - Encryption, protocols, etc. assume secure hardware elements
  - Attacks against hardware possible, e.g. imaging, probing, reading memory
- Silicon Physically Unclonable Functions (PUFs) by Gassend et al. as a main building block of hardware security
  - Unique and unpredictable challenge (input) to response (output) mapping based on manufacturing process variations

Introduction (3)

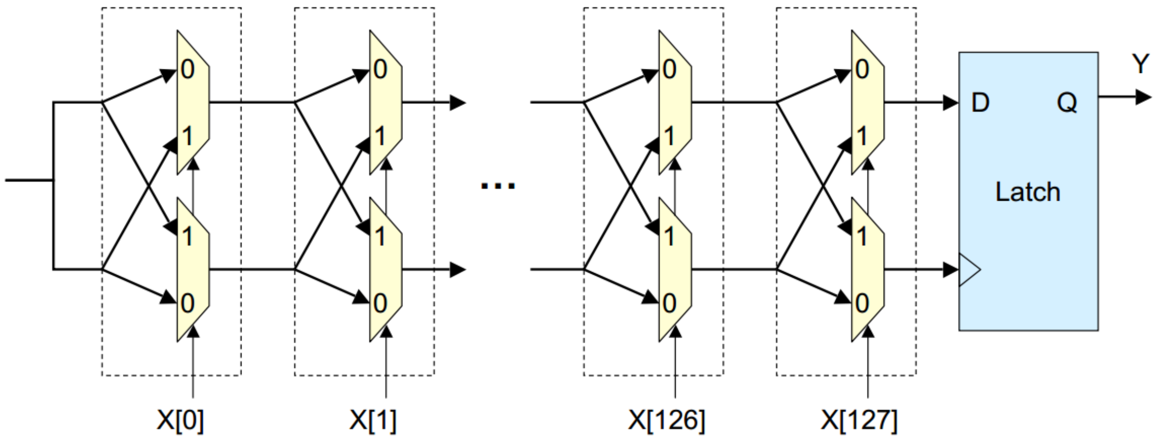


Fig. 1. Arbiter PUF

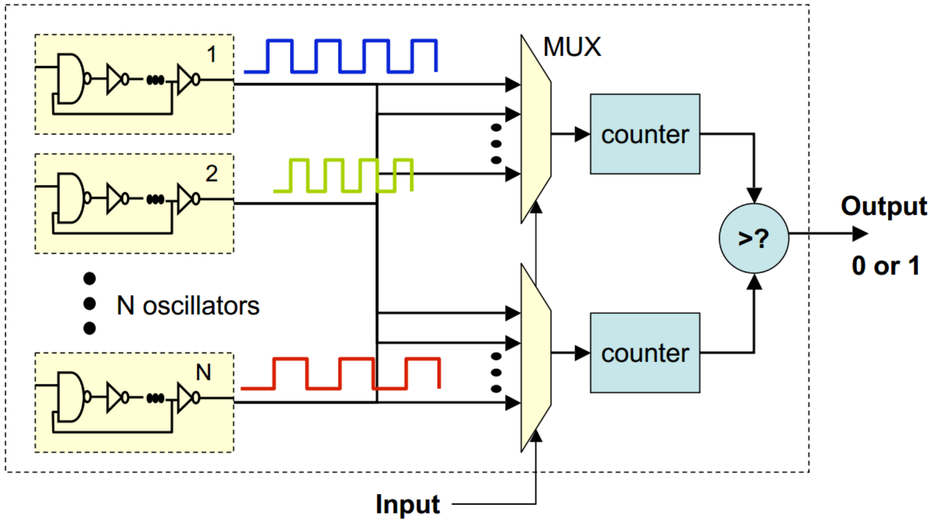


Fig. 2. Ring Oscillator PUF

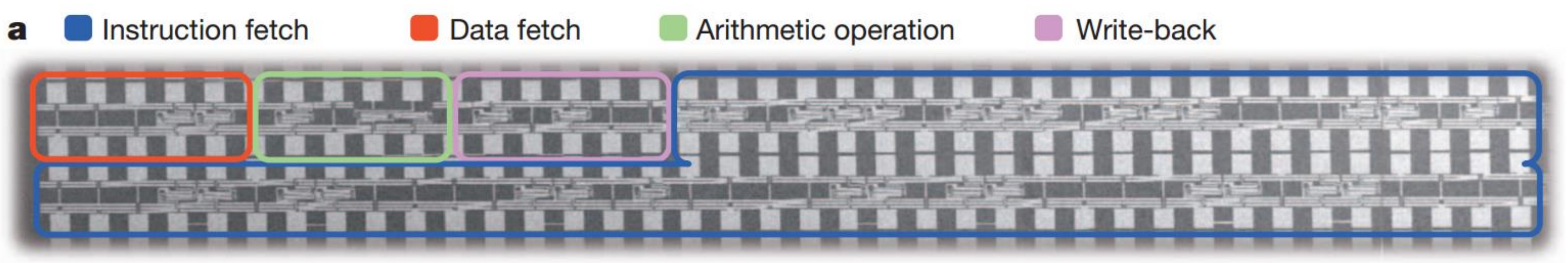
Source: G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. *44th DAC 2007.*

Introduction (4)

- PUF Applications
  - Device identification
  - Device authentication
  - Random Number Generator
  - Secret Key Generator
  - Hardware Trojan Detection
- Properties
  - Volatile: Tampering results in wrong behavior
  - Reliability: Measured in Intra-Chip Hamming Distance
  - Uniqueness: Measured in Inter-Chip Hamming Distance
- Various Silicon PUFs exist:
  - Delay, Frequency, Current, Subthreshold, …
  - Explore emerging technologies for new variation sources

Background

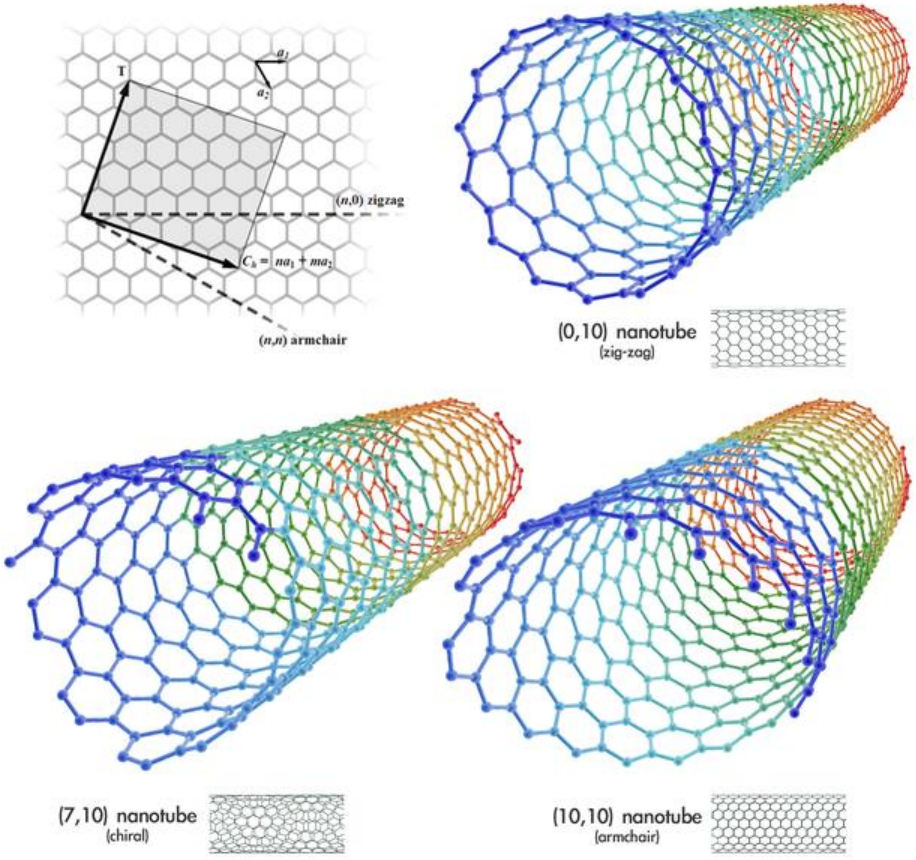
- Carbon Nanotubes (CNTs) promising candidate for future electronics
  - Desirable properties (strong, high conductivity, …)
- CNTs are technology of the future, but very fast paced development
  - First computer (1kHz) consisting of CNTs exclusively



Carbon nanotube computer, Shulaker et al., Nature 2013

Background (2)

- Can be thought of as a rolled Graphene sheet
  - Chirality of the CNT describes the way it is rolled
  - Determines band gap and type as metallic CNT (m-CNT) or semiconducting CNT (s-CNT)



[4]

Background (3)

- CNT Field Effect Transistors (CNFETs) are very difficult to control
  - Chirality, Diameter
  - Growth / Density
  - Alignment
  - Doping concentration
- Naturally 1/3 of CNTs are metallic
  - Improved processes available, but cannot achieve 100% s-CNT required for digital logic applications

Background (4)

- Metallic CNTs can lead to undesired effects
  - Drain-to-Source shorting
  - Low Ion/Ioff ratio
- Metallic CNT removal can also be complicated
  - Residue of metallic CNTs
  - Damaged semiconducting CNTs
  - There is a possibility that not all of the m-CNTS are removed

Carbon Nanotube PUF

- Observation in CNFET:
  - m-CNTs dominate off-behavior
  - m-CNTs and s-CNTS determine on-behavior together
  - Number of s-CNTs significantly larger than m-CNTs
- Constellation of m-CNTs and s-CNTs as dominant source of static variation
  - m-CNT burning not required
- Current as metric to take advantage of all the different process variations

Carbon Nanotube PUF (2)

- Exploit unique CNT characteristic to achieve simple and efficient design
  - Problematic m-CNTs provide main source of variation

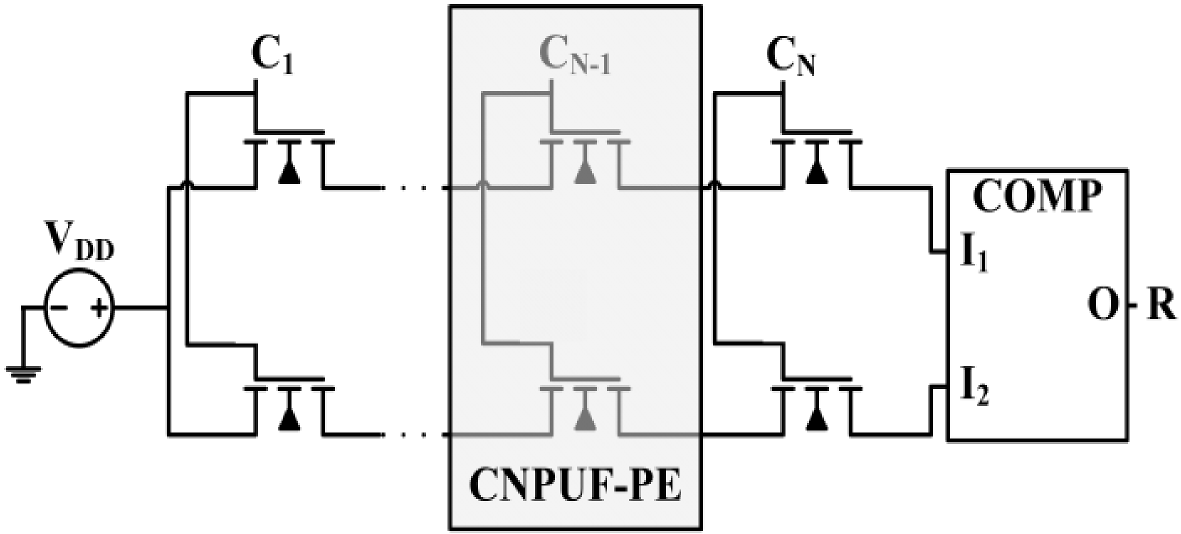
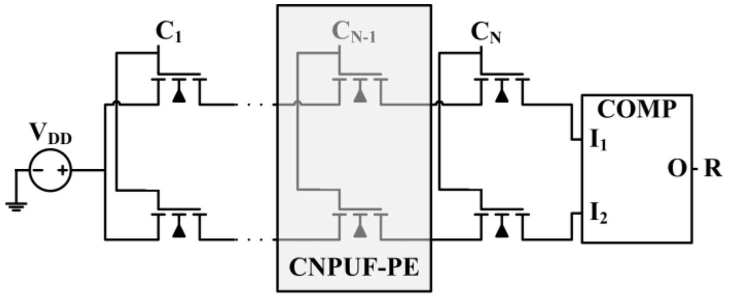


Fig. 3. CNPUF consists of CNPUF Parallel Elements

Carbon Nanotube PUF (3)

- Parallel CNFETs with manufacturing variations
  - CNT count, alignment, etc. can be different
  - m-CNT to s-CNT ratio can be different
- Each input bit controls one CNPUF-PE (parallel elements)
  - 10% to 33% m-CNTs -> Each CNPUF-PE has a different state for on and off operation
  - Input bits (challenge) determine which transistors are on, which are off
  - Current comparator determines output bit



Carbon Nanotube PUF (4)

- Motivation achieved: High area efficiency
  - 2 transistors per challenge bit
  - Compared to: $8\frac{T}{bit}$ for Arbiter PUF and $\frac{2^{N}-1}{N}6\frac{T}{bit}$ for RO-PUF
  - In addition to the area reduction that CNT-technology promises for the future
- Motivation achieved: Power efficiency
  - Less transistors
  - Less power / transistor despite m-CNTs

Extended CNPUF

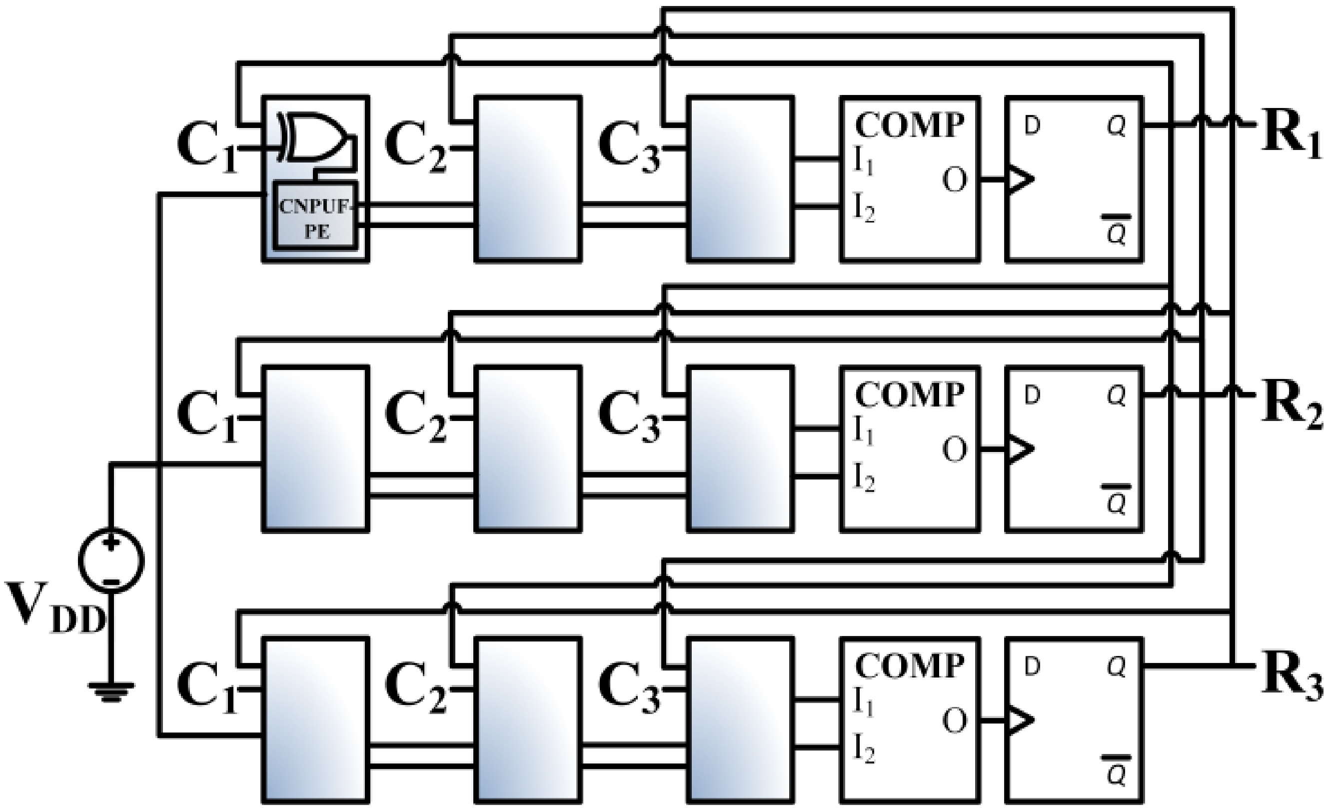


Fig. 4. Extended CNPUF for dynamic configuration

Extended CNPUF (2)

- CNPUF is lightweight, but provides limited flexibility
- Extended CNPUF enables dynamic security
  - Feedback of intermediate responses
  - Flexible number of iterations determine robustness against modeling
- Tradeoff Power/Energy vs. Security/Complexity

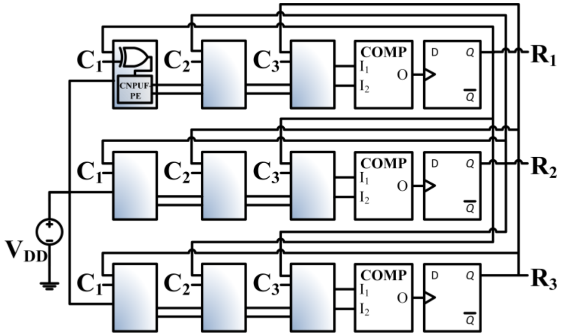


Fig. 4. Extended CNPUF for dynamic configuration

Experimental Evaluation

- HSPICE simulation with Stanford CNFET model
- 8-Bit implementation for large CRP-set in presence of long simulation times
  - 128-Bit as Proof of Concept

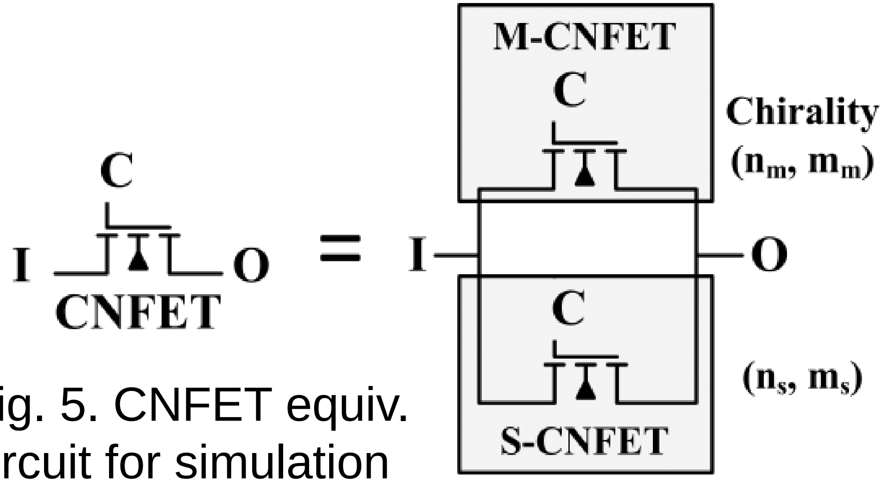


Fig. 5. CNFET equiv. circuit for simulation

Experimental Evaluation (2)

- Limited comparability for PUFs
  - Different authors use different types of variation
  - Using new technology means relying on simulations
- Experiments with different variation cases
  - Case 1: Static temperature and supply voltage variations
  - Case 2: Case 1 + Dynamic temperature and local voltage variations

Experimental Evaluation (3)

SIMULATION PARAMETERS FOR CNPUF

Parameter	Range
Temperature T	$-20° \; to \; 80°C$
Dyn. Temp. T_{rand}	$0° \; to \; 20°C$
Voltage variation	$\mu = 0.8V$ $3\sigma_{supply} = 22.5\%$ $3\sigma_{dynamic} = 7.5\%$
CNT ratio variation	$\mu_{ratio} = \{0.1, 0.2, 0.3\}$ $3\sigma_{phy} = 22.5\%$
Channel length variation	$\mu_{channel} = 14nm$ $\sigma_{channel} = 7.5\%$

Experimental Evaluation (4)

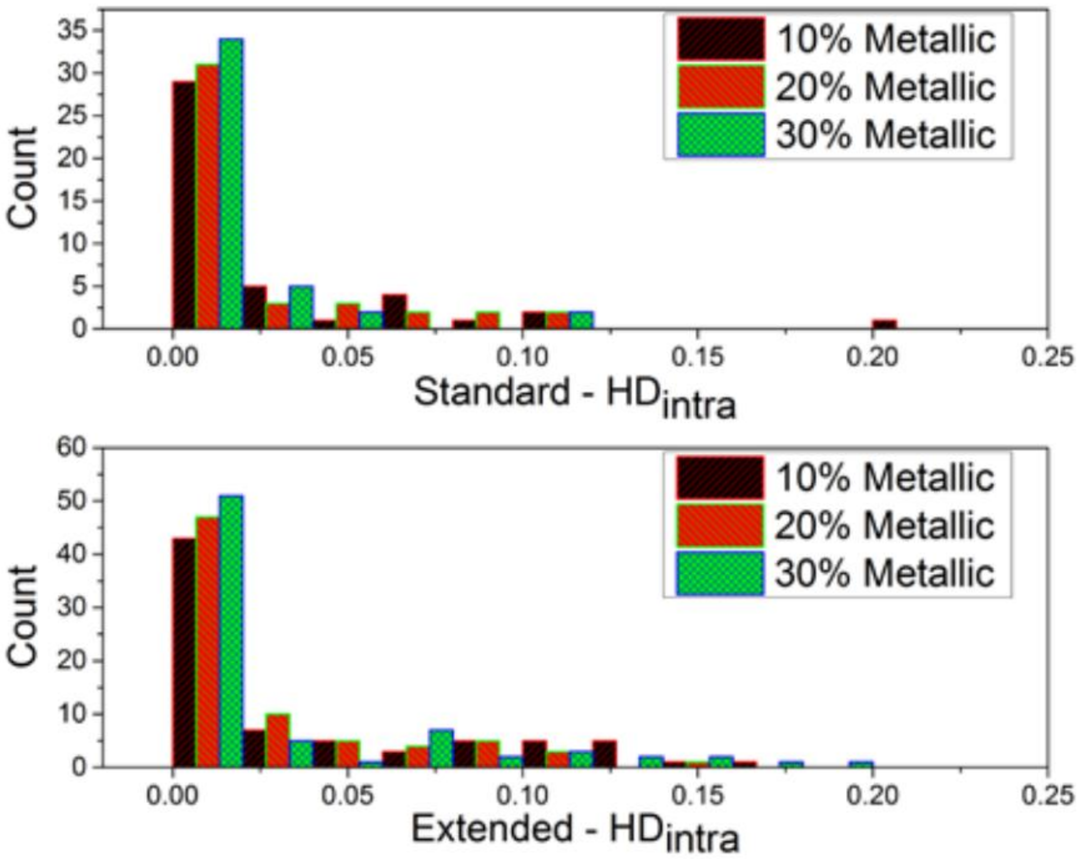
COMPARISON OF HD_{intra} IN DIFFERENT SIMULATED PUF DESIGNS. LOWER PERCENTAGES MEAN HIGHER ROBUSTNESS.

CNPUF	SCANPUF[24]	ROPUF[9]	CLOCKPUF[9]	CURRENT PUF[10]
1.9%	5%	9.51%	5.07%	~3%

COMPARISON OF HD_{intra} BETWEEN REAL PUF CIRCUITS AND CNPUF UNDER EXTENDED ENVIRONMENT SIMULATION.

CNPUF	BUTTERFLY PUF [8]	SRAM-PUF [25]
3.5%	6%	~8%-18%

Experimental Evaluation (5)



Experimental Evaluation (6)

POWER AND ENERGY COMPARISON BETWEEN CNPUF AND ULTRA -LOW POWER CURRENT-BASED PUF [10] AT 14NM AND 90NM.

Designs	CNPUF		Current based PUF [10]	
Technology	90nm, 1.2V	14nm, 0.8V	90nm	14nm, 0.8V
Power	15.6µW/bit	1.26µW/bit	150µW/bit	24µW/bit
Delay	43ps	26.5ps	250ps	~5ps
Energy	0.67fJ/bit	0.0334fJ/bit	37.5fJ/bit	0.12fJ/bit

For 90nm: 89.6% power and 98% energy reduction
For 14nm: 94.75% power and 72.16% energy reduction

Conclusion & Outlook

- Lightweight PUF designs for new applications
- Simple design based on CNT-unique "feature"
  - Turned CNT difficulty into advantage
- Introduced security as a new area that CNTs can contribute to
  - More than only good electrical properties
  - Various future possibilities based on CNPUF

Thank you.
Questions?

Pictures

- [1] http://www.tomas-sanchez.com
- [2] http://www.digitaltrends.com
- [3] http://www.cats.rwth-aachen.de
- [4] http://www.thenanoage.com