Physically “Unclonable” Functions or Physically hard for yoU to clone Functions PUFs Part I

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Book

- These notes are based on the following book
  - Physically Unclonable Functions
  - *Constructions, Properties and Applications*
  - by Roel Maes
  - Springer-Verlag
  - 2013
  - ISBN 978-3-642-41394-0
  - ISBN 978-3-642-41395-7 (eBook)
- These notes also have a substantial basis derived from research & papers by Professor James Plusquellic of the University of New Mexico

Quote from Page 21 of Maes

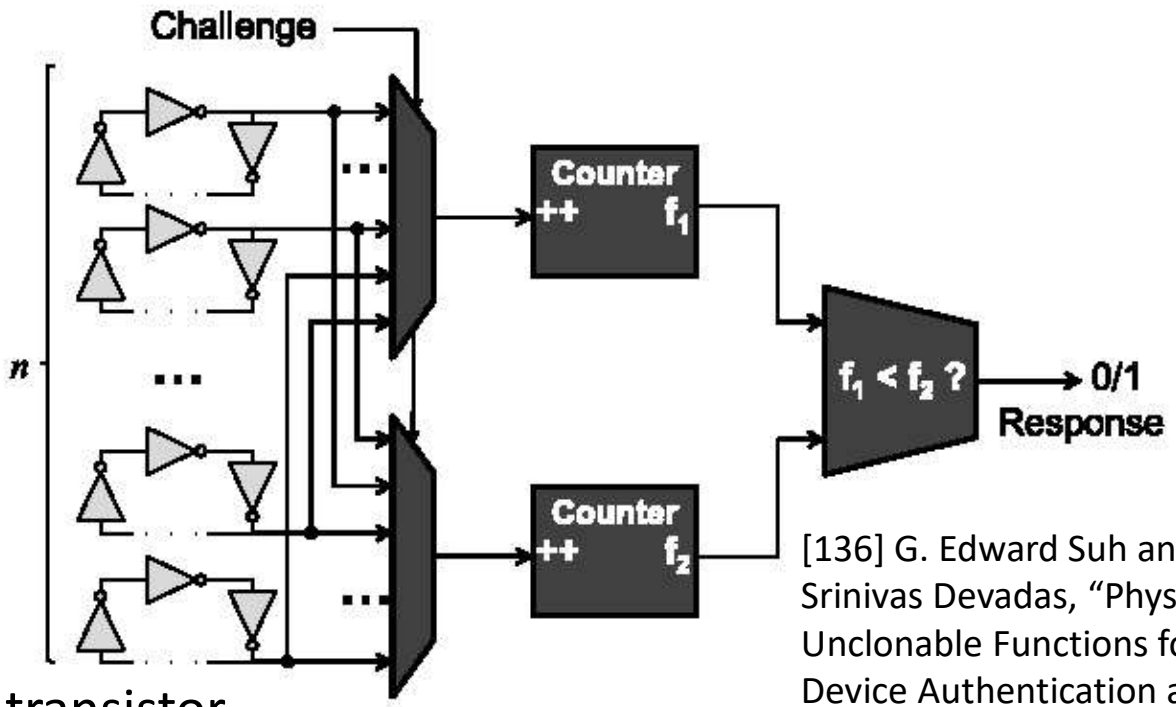
PUF having been used as a label for many different constructions, the literal semantic meaning of the acronym as “physical unclonable function” has been partially lost, up to the point where some consider it a misnomer. Moreover, slight variations in the actual wording were introduced over time, as expressed in the title of this section. In this book the acronym PUF does not generally refer to its literal meaning. Instead, it is used as the collective noun for the variety of proposed constructions sharing a number of interesting properties.

Notation

- $\mathcal{P}$ is a PUF class
  - A class is a complete description regarding how to construct this particular kind of PUF
- $\mathbf{r}^C$ is a randomized input
  - The superscript ^{C} indicates that fair coin tosses are used where a fair coin toss has an exact 50-50 probability distribution of heads versus tails (1 vs. 0)
  - Famous NFL coin toss moment on Thanksgiving day in 1998
    - https://www.youtube.com/watch?v=pmxb9FhiMaA
- PUF instantiation
  - A particular physical device, e.g., a silicon chip, can be manufactured to instantiate or "create" a specific PUF instance
  - $\mathcal{P}.Create()$

Ring Oscillators: Example of a Physically hard for yoU to clone Function (PUF)

Fig. 2.3 Construction of a comparison-based ring oscillator PUF as proposed by Suh and Devadas [136]



- Page 32 of Maes
- Each microchip will have transistor variations resulting in distinct timing characteristics for the ring oscillators

[136] G. Edward Suh and Srinivas Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," Design Automation Conference (DAC), 2007, pp. 9-14.

Notation (continued)

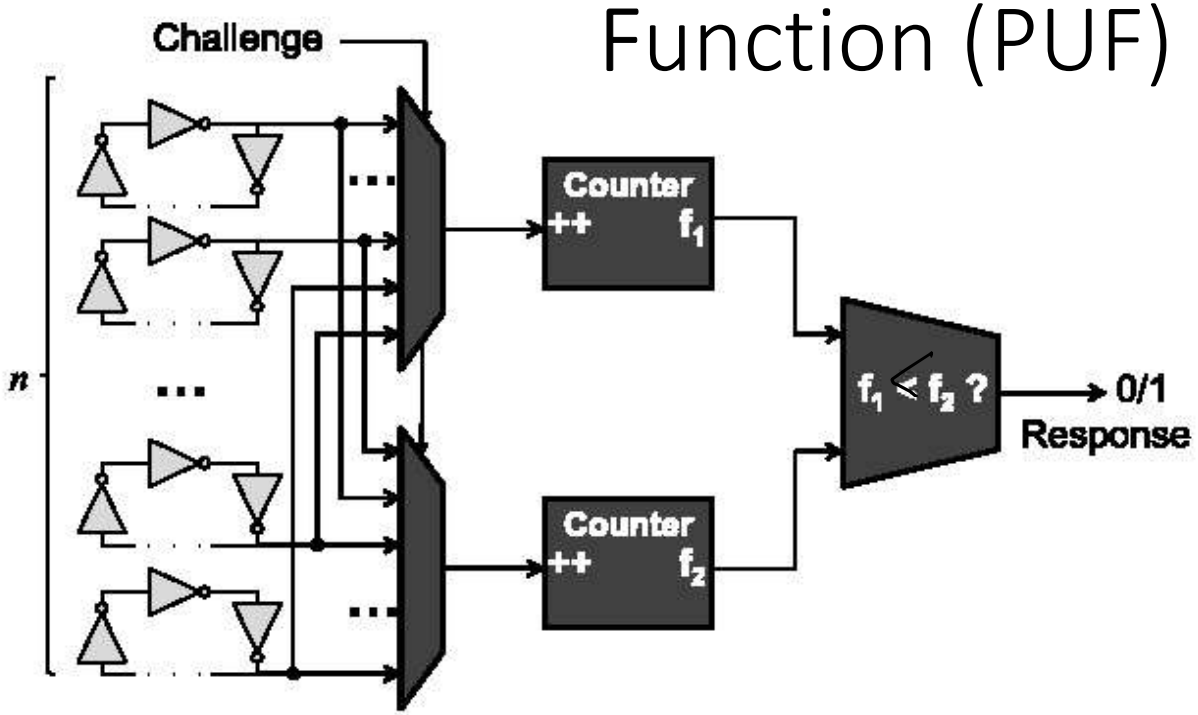
- Given a PUF class $\mathcal{P}$ is (e.g., a ring oscillator design), a specific instance (chip) will be referred to as a *puf*
- The input to a *puf* is referred to as a *challenge*
  - Let the challenge be *x*, then *puf*(*x*) refers to the application of *x* to the *puf*
  - The set of all possible challenges for PUF class $\mathcal{P}$ is {*x*} = $\mathcal{X}_{\mathcal{P}}$
- Traditionally the process of applying an input challenge to a *puf* is distinguished from the output
  - The output is referred to as a *response*
  - *puf*(*x*).*Eval* refers to the response
  - The set of all possible responses is $\mathcal{Y}_{\mathcal{P}}$

Hamming Distance

- Language note (from Merriam Webster online, www.merriam-webster.com)
  - intra- = within (e.g., intragalactic) or between the layers of (e.g., intradermal)
  - inter- = between (e.g., interstellar or interglacial) different instances
- Hamming distance is simply the number of bit entries with different values
  - E.g., 1010010110 and 1010110110 differ by one bit
  - For this example, the Hamming distance is one
  - To normalize the distance measurement to range between 0 and 1 (i.e., to use percentages), divide the Hamming distance by the number of bits compared
    - For this example, the result is 1/10 = 10%

Ring Oscillator Physically hard for yoU to clone Function (PUF)

Fig. 2.3 Construction of a comparison-based ring oscillator PUF as proposed by Suh and Devadas [136]



- Environmental conditions (voltage & temperature) affect oscillation
- Intra-chip Hamming Distance refers to comparisons of the same PUF instance and input challenge at different times
- Inter-chip Hamming Distance refers to comparisons of the same PUF design or structure but different instances
  - Same input challenge

Intra- Versus Inter-chip HD

Intra-chip HD

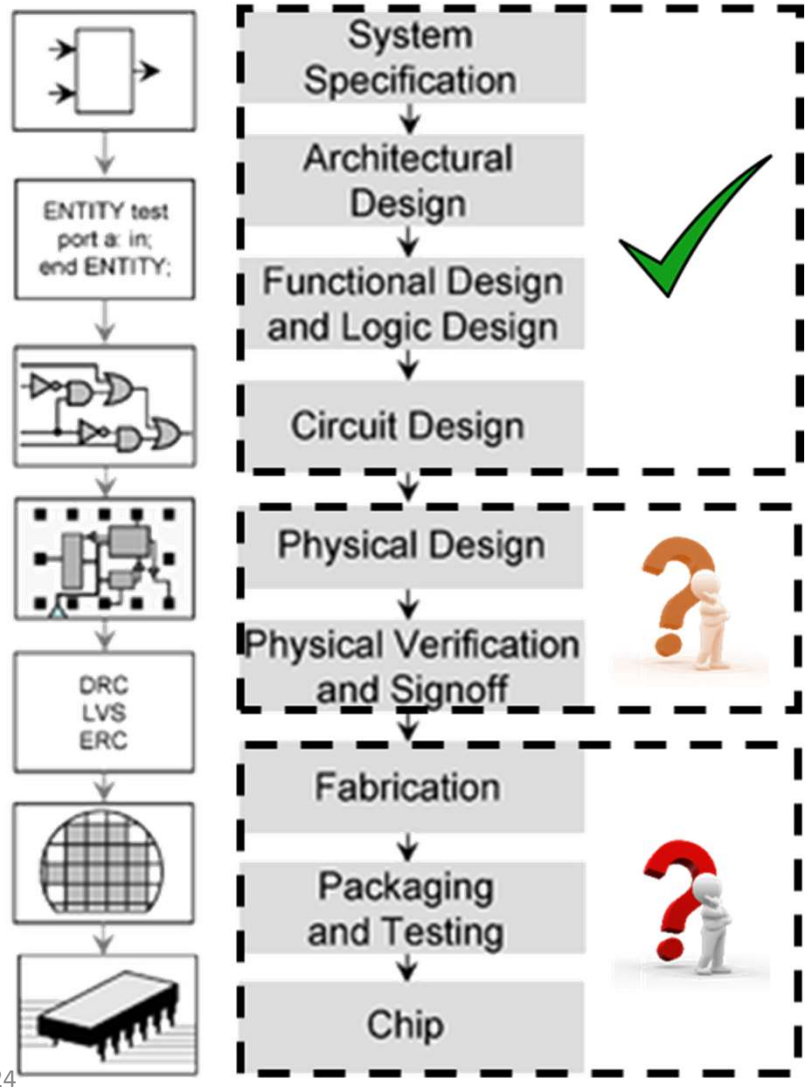
- Same PUF class
- Same PUF instance
  - E.g., same # inverters
- Same chip
- Same challenge
- Different environment
  - Vdd, temperature

Inter-chip HD

- Same PUF class
- Different PUF instance
  - E.g., different # inverters
- Same or different chip
- Same challenge
- Same environment
  - Vdd, temperature

Typical Scenario for PUF Usage

- Identification
  - Authentication
    - *challenge-response*
  - Unique per chip
- Encryption
  - Symmetric key (typical)
  - Note PUF response never transmitted
- Design process
- Supply chain



Supply Chain

- Modern business efficiencies typically result in no one company and, indeed, no one country as the only location where a product is designed, manufactured, tested and configured for sale
  - Configuration includes hardware, software and more (e.g., labels)
- Recall the traditional four levels of an adversary
  - Hacker without a technical degree
  - Hacker with a technical bachelor's degree, e.g., ECE or CS
  - Industrial company
  - Country
- Security and trust will be non-uniform through the supply chain

Traditional (non-PUF-based) Approaches

- Labels which are very difficult to erase
  - Requires physical access
- Black box design (versus white box)
- Tamper resistance
- Non-Volatile Memory (NVM)
  - ROM
  - Flash (both NOR and NAND)
  - Hard Disk Drive (HDD)
  - …
- Patents
- Trade Secrets

PUF Benefits

- Replace a more expensive alternative
  - Authentication easier to replace
  - Key generation requires higher level of assurance of randomness
- Remove key value from memory
  - Reverse engineering of memory contents does not reveal the key
  - Key (re-)generation done only during use (with power supplied to the chip)

PUF Attacks

- Model building
- Machine learning
- Brute force
- Replay