Permission to Use Conditions

ECE 448/548 Cyber-System Security

Physically Unclonable Function (PUF)

F. Gebali

EOW 433

Office Phone: 250-721-6509

https://ece.engr.uvic.ca/~fayez/

Outline

Background: Cybersecurity Labeling of Smart Devices

1. Create a cyber trust mark: strong default passwords, data protection, software updates, incident detection
2. Manufacturers will increase cybersecurity on smart devices
3. Smart devices: TV, fridge, μwave, fitness tracker, climate control
4. Attacks on privacy, data theft, hidden junk fees
5. Target routers, smart meters, power inverters
6. Root-of-trust (RoT) is essential for connected devices [**?**]

Motivation

1. Rapid increase in IoT-connected devices requires using authentication and cryptography at very large scale
2. There is shift from software-only to to hardware-based security solutions
3. Physically Unclonable Functions (PUFs) now protect 500,000,000 devices from just one supplier: Intrinsic ID [**?**]

Introduction

Traditional Security

1. Protecting information relies on user ID, password, usually combined with use of smart card
2. Multifactor authentication relies on:
   1. What you know (e.g. password or pass phrase)
   2. What you have (e.g. smart card)
   3. What you are (e.g. biometrics)
   4. Context (e.g. location, time, velocity)

Elements of Security

1. Encryption/Decryption for information confidentiality
2. Digital Signature for nonrepudiation
3. Authentication to verify identity of a party and integrity/source of message
4. Availability/Reliability for service continuity (no DoS or DDoS)

Other Security Requirments

1. Random number generation (PRNG or TRNG)
2. Key generation and exchange
3. Supply chain security/integrity

Traditional Blackbox Secrecy

1. Traditional encryption and authentication rely on a secret key
2. A difficulty of secret key is key generation and key exchange or distribution
3. Traditionally public key infrastructure (PKI) is relied upon for key generation and distribution
4. Traditionally also, secret keys are assumed to be securely stored.
5. Key security assumption is no longer valid in IoT age

Motivation for Using PUFs

1. Horizontal IC business model introduces threats to ICs security and authenticity:
    1. Intellectual property (IP) piracy
    2. IC overproduction
    3. IC counterfeiting
2. Key-based cryptography is usually used for IP protection & licensing (DRM, metering)
3. Key storage is not secure against physical attacks and tampering
4. We must provide tamper-proof ICs that generate keys on demand

IoT System Prevalence

1. Profusion of unsecured hardware devices (e.g. IoT)
2. IoT edge devices are vulnerable to attacks
3. System security could be compromized by edge devices
4. Security is usually based on secret key (vulnerable)
5. PUF provides measure of HRoT plus secure secret key

Advantages of PUF

1. PUF gives each device a unique ID similar to biometrics
2. PUF protects devices form
   1. Reverse engineering
   2. Tampering
3. PUF allows for multifactor authentication
4. PUF facilitates cryptography through
   1. Generation of secret keys on-demand (no NVRAM)
   2. Secure exchange of secret key
5. Secure: no power implies no response or stored state values

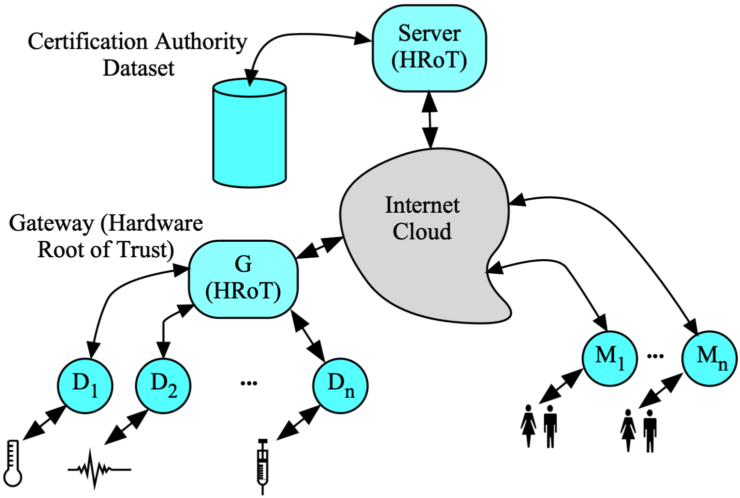
Authenticating Physical Objects

1. Multifactor authentication was used to authenticate individuals
2. Authenticating physical devices is based on their physical properties
3. Physical properties give each device a unique ID similar to biometrics
4. Physical properties are inherently noisy and means have to be found to remove this noise
5. We must ensure secure storage of secret device biometrics

Unique Identity for Authentication

1. Use random physical features to identify objects
2. Biometrics for humans: finger prints, retina, etc.
3. Watermarking for documents and artwork
4. Use PUFs for IoT devices

Example of IoT for Telehealth



Advantages of PUFs

1. Protects secret keys through silicon one-way functions
2. Simple to implement PUFs
3. Can simultaneously provide low-entropy bits as well as high-entropy bits
4. These two types of bits help generate secret keys as well as true random number generation

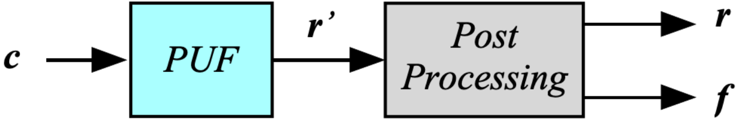
Definition

Silicon PUF Definition [1, 2, 3, 4, 5, 6]

Definition

Hardware that maps a digital input (challenge *c*) to a digital output (response *r*) for use as a unique identity of a given IC

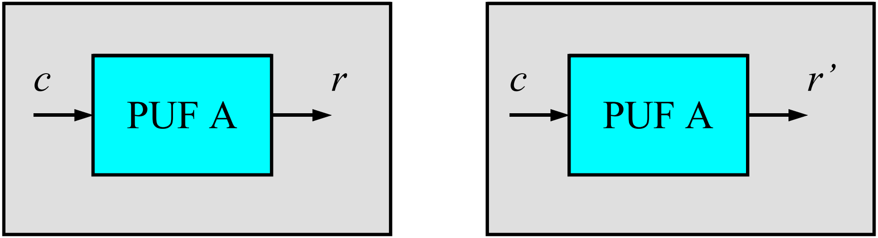
$$F : \mathcal{C} \rightarrow \mathcal{R} : [\mathbf{r},\ \mathbf{f}] = F(\mathbf{c})$$



c: Challenge vector
r′: Raw response vector
f: Confidence vector

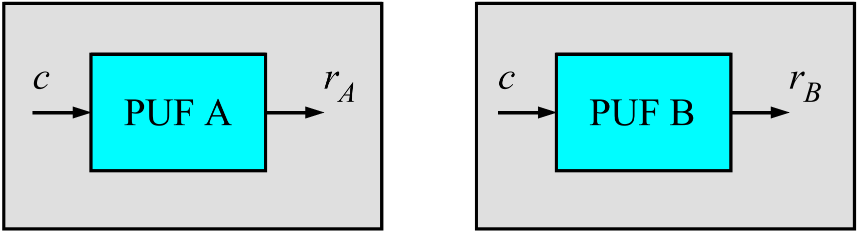
r: Response vector

PUF Response: Intra Hamming-Distnace



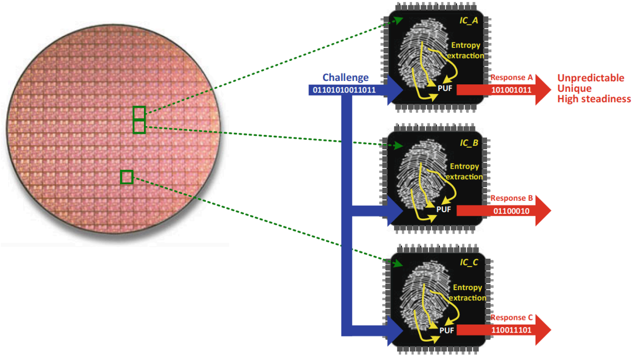
$$r \approx r'$$

PUF Response: Inter Hamming-Distnace

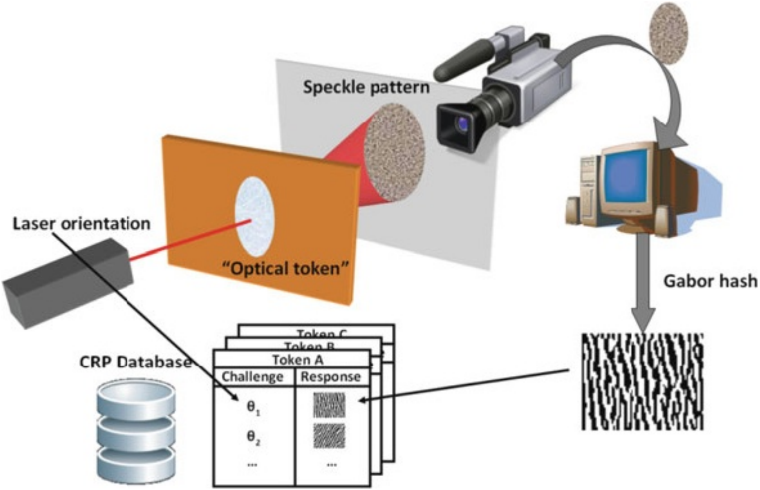


$$r_A \neq r_B$$

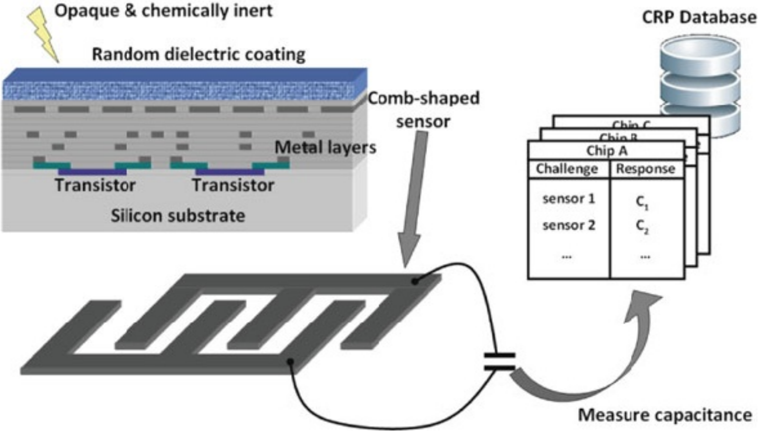
PUF Unique ID (Inter Hamming-Distnace)



Optical PUF: Used for diamonds long time ago



Electrical PUF



Silicon PUFs

1. PUFs can be delay-based or memory-based
2. Temperature and supply voltage could introduce unwanted noise
3. Delay-based PUFs require extra hardware to measure delay
4. Memory-based PUF relies on random value in register after power-up
5. IC variations is due to manufacturing or environmental variations (static or slowly-varying variations)

Silicon PUF Types

1. SRAM PUF
2. DRAM PUF
3. Arbiter PUF
4. Ring Oscillator (RO) PUF
5. Coating PUF
6. Bistable PUF

Desired PUF Properties

Desired PUF Properties

1. Tamper resistance to counteract attempts at counterfeiting and reverse engineering and cloning
2. Knowing the structure of the PUF circuit, it is impossible to predict the I/O response
3. Knowing the challenge c, it is impossible to predict the response r
4. Knowing the response r, it is impossible to predict the challenge c
5. Observation of challenge-response pairs (CRP) does not lead to modelling the PUF

Desired PUF Properties

1. Reliability/Reproducibility: Produce same response for same challenge. This changes due to CMOS noise
2. Uniqueness: Distinguishability among devices. Device produces unique response different from other PUFs.
3. Randomness: for a given challenge, it is hard to predict the response. Must guard response to reuse it again.
4. Tamper Resistance: Tampering with an IC changes F to G and for any c

$$F(c) \neq G(c)$$

Intra Hamming Distance to Quantify: Reliability [7]

$$\text{Reliability} = \frac{1}{k}\sum_{i=1}^{k}\frac{HD(R_{i,1}, R_{i,2})}{B}$$

1. Apply k challenges to a given PUF
2. Checks effect to temp, voltage and aging
3. Obtain two responses $R_{i,1}$ and $R_{i,2}$ at different times
4. Ideal normalized value should be 0

Inter Hamming Distance to Quantify: Uniqueness [7]

$$\text{Uniqueness} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \left[\sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{B} \right]$$

1. Apply k challenges to k different PUFs
2. B is number of bits of a response
3. Total tries is $\binom{k}{2} = k(k-1)/2$
4. Uniqueness should ideally be 0.5

Intera Hamming Distance to Quantify: Uniformity [7]

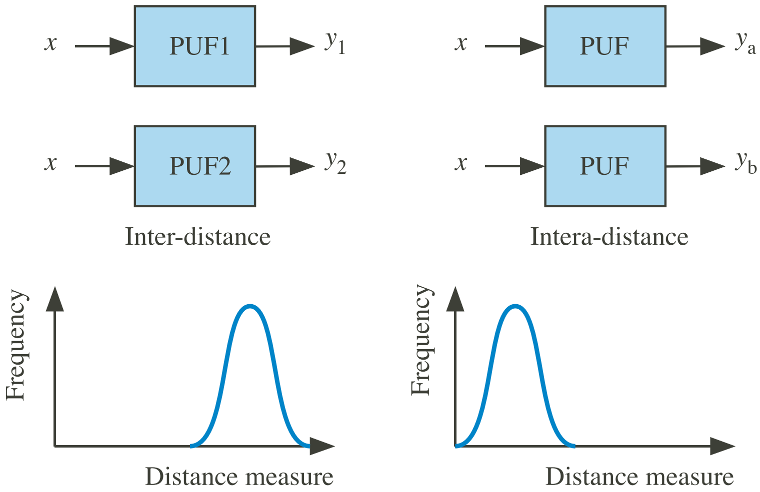
$$\text{Uniformity} = \frac{1}{B}\sum_{i=1}^{B} b_i$$

1. Ideally should be 0.5
2. Indicates randomness of each response

More PUF Properties

1. Evaluatable: Given c, it easy to evaluate $F(c)$
2. Unclonable: Given F, it is hard to find G such that $G(c) = F(c)$
3. Unpredictable: Hard to predict r_i if c_i is given without evaluating $F(c_i)$
4. One-Way: Given F and r, it is hard to find c such that $r = F(c)$

PUF Inter and Intra Hamming Distances



IDeal PUF Inter and Intra Hamming Distances

Ideally it is desired that:

1. Inter Hamming distance $\approx$ 50% of bits in the response

2. Intra Hamming distance $\approx$ 0% of bits in the response

Strong PUF Properties

Definition

1. Number of CRP must be large
2. Stable against environmental variations
3. Stable against aging
4. Unpredictability by attacker, user, or fabricator
5. Hard to read, predict or derive response to a challenge

Weak PUF

Definition

1. Has small number of challenges
2. Not meant to be publicly divulged
3. A special form of nonvolatile key storage but hard to read out compared to RAM, NVRAM or EEPROM
4. Stable secret key

Reconfigurable PUF

Definition

Ability to reconfigure challenge-response space after deployment using some external control.

1. Adds control logic around the PUF
2. Control incoming challenges
3. Hides direct access to the PUF responses

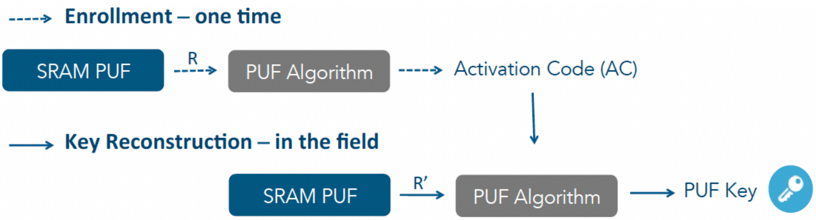
PUF Important Properties

1. Unclonability: A device fabricator can not duplicate the device. A mathematical model can not be constructed by observing device CRP samples.

2. Unpredictability: CRP can not be predicted by observing many CRP samples.

Removing Response Noise: Stable Key

1. Few of the response bits are very noisy
2. Helper data *w* or activation code remove this noise
3. Publishing *w* does not reveal the key
4. *w* is customized for one PUF and one challenge only



PUF-Based Authentication

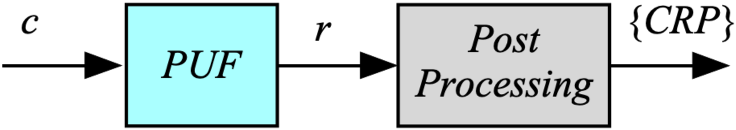
Authentication using PUF

1. We are talking about hardware authentication (not data or human authentication)
2. Gives unique ID to an IC
3. PUF maps challenges to responses
4. Responses are stored in silicon circuits, not memory
5. Challenge/Response mapping is unique to each device
6. PUF can not be replicated or tampered with
7. PUF properties are known only after fabrication

PUF-Based Authentication

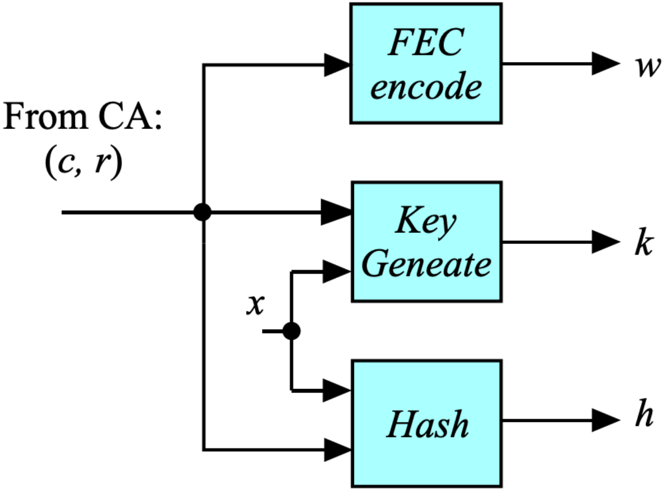
1. Authenticate ICs without using cryptographic primitives
2. Used in IoT edge devices such as RFID, etc.
3. Economical on silicon area & power consumption
4. Secret key or ID depends on random physical properties not NVRAM content
5. Can not be duplicated by manufacturer or adversary

PUF-Based Authentication: at Fab House



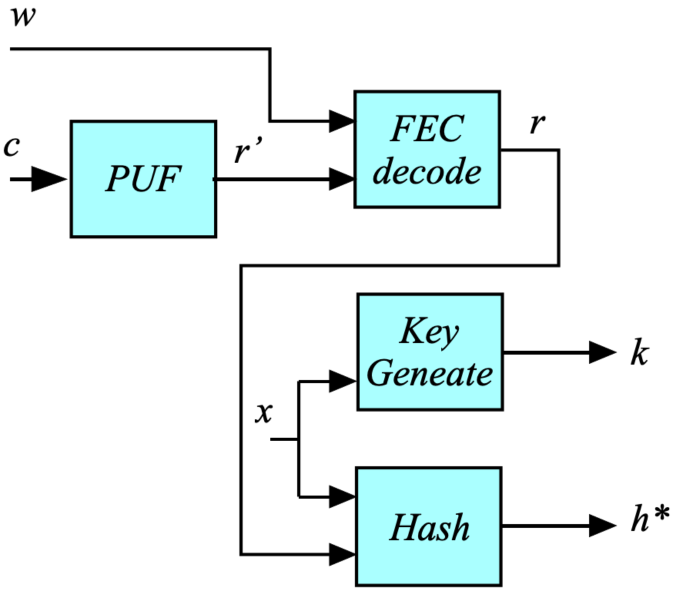
Store $\{CRP\}$ at trusted certification authority (CA)

PUF-Based Authentication: at Server



Send c, w and x to client

PUF-Based Authentication: at Server



Simple PUF-Based Authentication Protocols

	Hardware		Server		CA
1	Req (ID)	$\rightarrow$			
2			Req(ID)	$\rightarrow$	
3				$\leftarrow$	$\{c, r\}$
4			select c		
5			$w = \text{FEC}(r)$		
6			$h = \text{HASH}(r)$		
7		$\leftarrow$	$m = \{c,\ w\}$		
8	$r_1 = \text{PUF}(c)$				
9	$r_2 = \text{Decode}(r_1,\ w)$				
10	$h_2 = \text{HASH}(r_2)$	$\rightarrow$			
11			Compare h & h_2		

n is a nonce

Limitation of PUF-Based Authentication Protocols

1. Naive approach subject to machine learning attacks
2. Challenge and associated response are exchanged on unsecured channel
3. CRP pair can not be used again
4. Reason for wanting to use strong PUFs
5. Similar to logging and using a readable password!

Attacks on PUFs

PUF Attack Taxonomy

1. Mathematical model clone
2. Machine learning clone
3. physical clone
4. Aim is to either expose secret key or deny service

[1] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Design Automation Conference*, 2007, pp. 9–14.

[2] T. Machida, D. Yamamoto, M. Iwamoto, , and K. Sakiyama, “A new arbiter PUF for enhancing unpredictability on FPGA,” *The Scientific World Journal*, 2015.

[3] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, “Silicon physical random functions,” in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.

[4] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Springer, 2013.

[5] S. S. Mansouri and E. Dubrova, “Ring oscillator physical unclonable function with multi level supply voltages,” in *IEEE 30th International Conference on Computer Design (ICCD)*, 2012.

[6] D. Mukhopadhyay and R. S. Chakraborty, *Hardware Security Design, Threats and Safeguards*. Roca Baton, Florida: CRC Press, 2015.

[7] M. Tehranipoor, N. Pundir, N. Vashistha, and F. Farahmandi, *Hardware Security Primitives*. Springer, 2023.