ULB CYBERSECURITY RESEARCH CENTER

An introduction to Physically Unclonable Functions (PUFs)

by Cédrick De Pauw

on May 22, 2023

CyberExcellence
By CyberWal

Introduction

Physically Unclonable Functions

Fuzzy Extractors

Applications

Research

CyberExcellence
By CyberWal

» Context

IoT Technology

* Growth in popularity.
* Many IoT applications: smart health monitoring, smart homes, smart grids, smart cities.
* Many types of devices: sensors, actuators, terminals.
* Many types of data: health data, location, messages, passwords.

Problems

* Data transmission through the air or over the Internet.
* No encryption.
* Initialization of communication channels without trust.
* Limited computational resources and battery autonomy.

» Why PUFs?

Advantages

* Secure key storage.
  → Interesting for encryption.
* Challenge-response functions.
  → Intesting for authentication.

Drawbacks

* Still vulnerable to some attacks.
* Aging effects.

Introduction

Physically Unclonable Functions

Fuzzy Extractors

Applications

Research

CyberExcellence

By CyberWal

Physically Unclonable Functions

* Description
* PUF Properties
* Security Levels
* Example of PUF Architectures

CyberExcellence
By CyberWal

» Description

Physically Unclonable Function (PUF)

* black-box function,
* based on physical variations caused by the manufacturing process of ICs,
* one or many Challenge-Response Pairs (CRPs),
* not totally reliable without a fuzzy extractor.

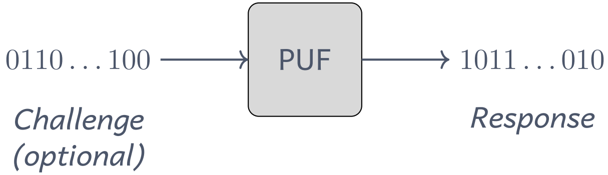

Figure: PUF challenge-response pair.

Physically Unclonable Functions

* Description
* PUF Properties
* Security Levels
* Example of PUF Architectures

CyberExcellence
By CyberWal

» PUF Reproducibility

Definition (Reproducibility)

A PUF circuit reproduces, with a high probability, the same response for a given challenge.

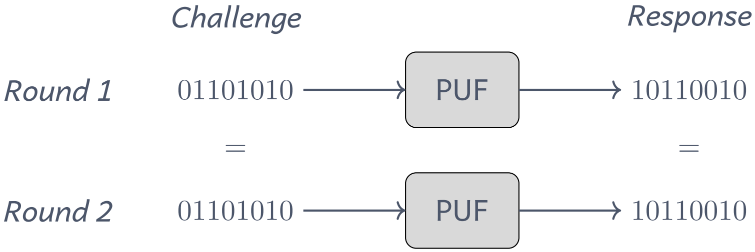

Figure: Illustration: PUF reproducibility.

» PUF Uniqueness

Definition (Uniqueness)

Two PUF circuits generate, with a high probability, distinct responses for a common challenge.

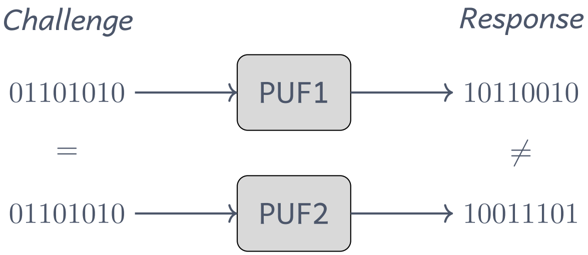

Figure: Illustration: PUF uniqueness.

Physically Unclonable Functions

* Description
* PUF Properties
* Security Levels
* Example of PUF Architectures

CyberExcellence
By CyberWal

SCIENTIA VINCERE TENEBRAS

» Security Levels

Definition (Strong PUFs)

PUF is *strong* if it satisfies two conditions:

- its CRPs space is very large,
- it is impossible to predict the response to an unknown challenge.

Definition (Weak PUFs)

A PUF is *weak* if its CRPs space is small, at worst of size one.

Physically Unclonable Functions

* Description
* PUF Properties
* Security Levels
* Example of PUF Architectures

» SRAM PUF

Description

* Based on a Static Random-Access Memory.
* Source of randomness: variations between inverters from SRAM cells.
* No input or memory offset used as challenge.
* Response obtained on power-up from SRAM cell values.
* Small number of CRPs (weak PUF).

» SRAM PUF

Illustration

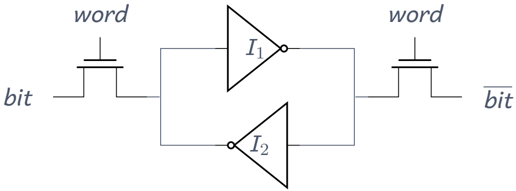

Figure: SRAM cell logic circuit.

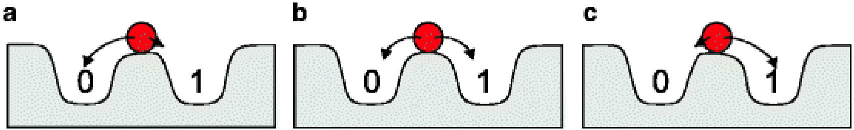

Figure: SRAM cell as a bistable system[1]: (**a**) and (**c**) illustrate the two stable states; (**b**) illustrates the metastable state.

[1] C. Böhm and M. Hofer. *Physical Unclonable Functions in Theory and Practice.* Springer New York, 2013. DOI: 10.1007/978-1-4614-5040-5.

Fuzzy Extractors

- Purpose
- Description

CyberExcellence
By CyberWal

» PUF Problem: Noise Sources

Description

PUFs are subject to noise

- silicon aging,
- environment conditions,
- physical variations not being significant enough,
- etc.

Fuzzy extractors are necessary

- *information reconciliation*: guarantees PUF reproduciblity,
- *privacy amplification*: guarantees uniformly distributed key.

Fuzzy Extractors

- Purpose
- Description

Usage

1. **Enrollment**: take reference PUF response, generate key, release helper data.
2. **Reconstruction**: take noisy PUF response, reproduce associated key thanks to helper data.

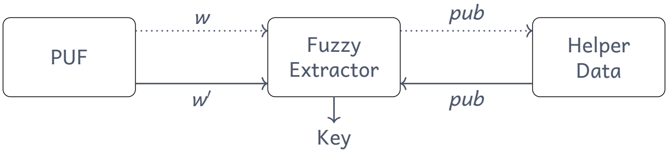

Figure: Fuzzy extractor procedures[2]. Dotted arrows: enrollment; plain arrows: reconstruction. Notation: w and w' respectively are the reference PUF response and a noisy PUF response, *pub* is the helper data.

[2] G. J. Schrijen. *Physical Unclonable Functions to the Rescue A New Way to Establish Trust in Silicon*. 2018.

» Construction

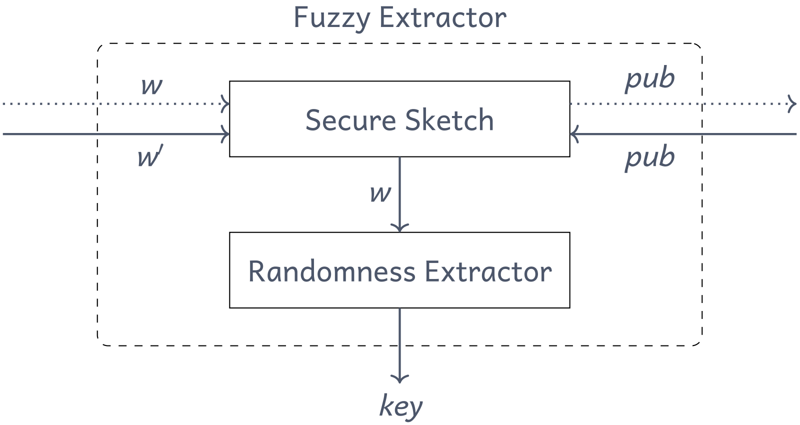

Figure: Generic fuzzy extractor construction.

Secure Sketch Construction: Example

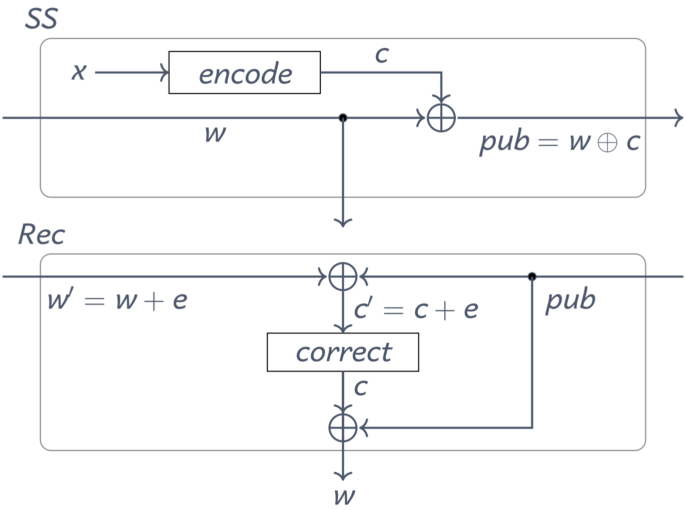

Figure: Secure sketch example: code-offset construction.

Introduction

Physically Unclonable Functions

Fuzzy Extractors

Applications

Research

CyberExcellence

By CyberWal

SCIENTIA VINCERE TENEBRAS

Applications

* Application 1: Mutual Authentication and Session Key Establishment Protocols
* Application 2: Privacy-preserving Tag Tracking Protocol

CyberExcellence
By CyberWal

» Protocols & Setup

Mostafa et al.[3] proposed two protocols:

* two-factor mutual authentication protocol,
* session key establishment protocol.

IoT device setup:

* two PUFs: SRAM PUF, Arbiter PUF,
* device enrollment:
  - → the device identifier,
  - → a secret key extracted from its SRAM PUF,
  - → a CRP generated by its Arbiter PUF.

[3] A. Mostafa, S. J. Lee, and Y. K. Peker. "Physical Unclonable Function and Hashing Are All You Need to Mutually Authenticate IoT Devices". In: *Sensors* 20.16 (2020). ISSN: 1424-8220. DOI: 10.3390/s20164361. URL: https://www.mdpi.com/1424-8220/20/16/4361.

Two-Factor Mutual Authenticaton Protocol

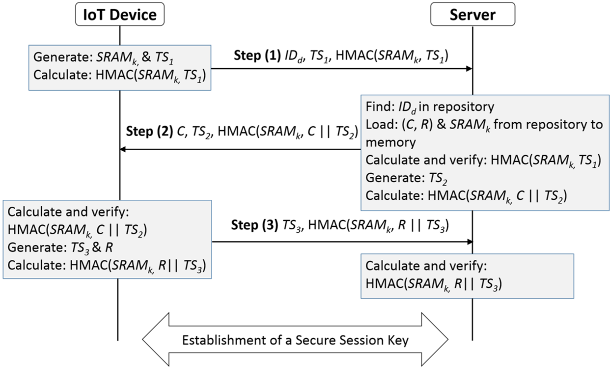

Figure: Two-factor mutual authentication protocol[4].

[4] A. Mostafa, S. J. Lee, and Y. K. Peker. "Physical Unclonable Function and Hashing Are All You Need to Mutually Authenticate IoT Devices". In: *Sensors* 20.16 (2020). ISSN: 1424-8220. DOI: 10.3390/s20164361. URL: https://www.mdpi.com/1424-8220/20/16/4361.

» Session Key Establishment Protocol

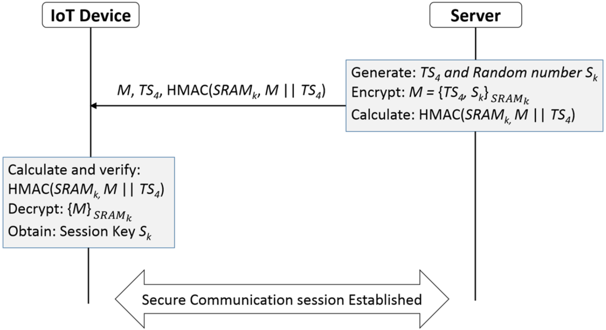

Figure: Key establishment protocol[5].

[5] A. Mostafa, S. J. Lee, and Y. K. Peker. "Physical Unclonable Function and Hashing Are All You Need to Mutually Authenticate IoT Devices". In: *Sensors* 20.16 (2020). ISSN: 1424-8220. DOI: 10.3390/s20164361. URL: https://www.mdpi.com/1424-8220/20/16/4361.

Applications

* Application 1: Mutual Authentication and Session Key Establishment Protocols
* Application 2: Privacy-preserving Tag Tracking Protocol

Context

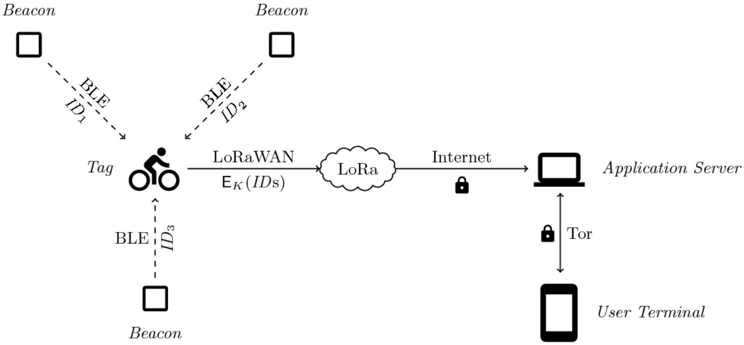

Figure: Privacy-preserving tag tracking system[6].

[6] T. Ashur et al. "A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network". In: *Cryptology and Network Security*. Ed. by S. Capkun and S. S. M. Chow. Cham: Springer International Publishing, 2018, pp. 347–369. ISBN: 978-3-030-02641-7.

Setup

- SRAM PUF partitioned into m segments.
- Each segment is used to generate a master key k_{tag}.
- Master keys are shared using a QR code.
- After deployment, every segment is used once.

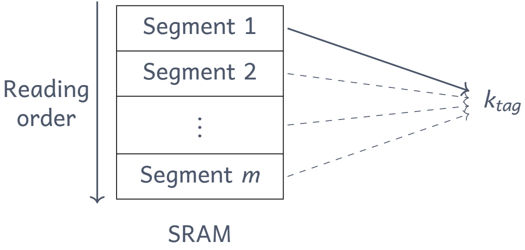

Figure: Memory segments used in turn to produce master key k_{tag}.

» Session key generation

- Hash chain used to derive session keys.
- Session key and domain separator provided to a KDF:
  - → one-time pseudonym,
  - → one-time authenticated encryption key.

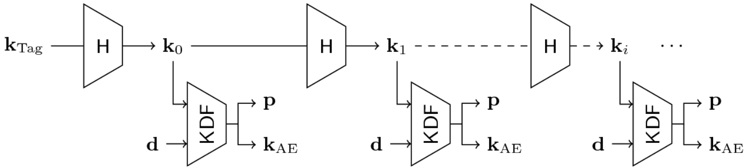

Figure: Generation of one-time encryption keys k_{AE} and corresponding pseudonyms p using a master key k_{tag}, a hash function H, a key derivation function KDF and a domain separator d [7].

[7] T. Ashur et al. "A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network". In: *Cryptology and Network Security*. Ed. by S. Capkun and S. S. M. Chow. Cham: Springer International Publishing, 2018, pp. 347–369. ISBN: 978-3-030-02641-7.

Research

Supervision	Professor Jean-Michel Dricot (ULB).
Research area	Embedded systems design & security.
Current topic	Physically unclonable functions.
Current work	Off-the-shelf SRAM analysis for PUF usage. PUF-based protocol analysis and improvements.
Work packages	WP1: security by design. WP4: data protection. WP6: factory (TBC).

Thank you for your attention.

Any Question?

» Construction Properties

Definition (Intrinsic PUFs)

A PUF is *intrinsic* if its construction is such that:

- measurement of its characteristics is internal,
- introduction of its source of randomness is implicit.

Definition (Non-intrinsic PUFs)

A PUF is *non-intrinsic* if its construction is not intrinsic.

In general, intrinsic PUFs are preferred for security reasons.

» Implementation Technology

Non-electronic/hybrid PUFs

* random variations in non-electronic materials,
* conversion to electronic signals,
* example: Optical PUF.

Electronic PUFs

* random variations in electronic materials,
* example: Power Distribution PUF.

Silicon PUFs

* random variations in silicon chips,
* example: SRAM PUF.

» Arbiter PUF

* Based on gate propagation delay.
* Formed by multiple arbiter PUF circuits.
* Arbiter PUF circuit: circuit built with multiplexers and a latch.
* Source of randomness: variations between multiplexers.
* Challenge bits: input to multiplexers.
* Response bits: output from latches.
* Many CRPs (strong PUF).

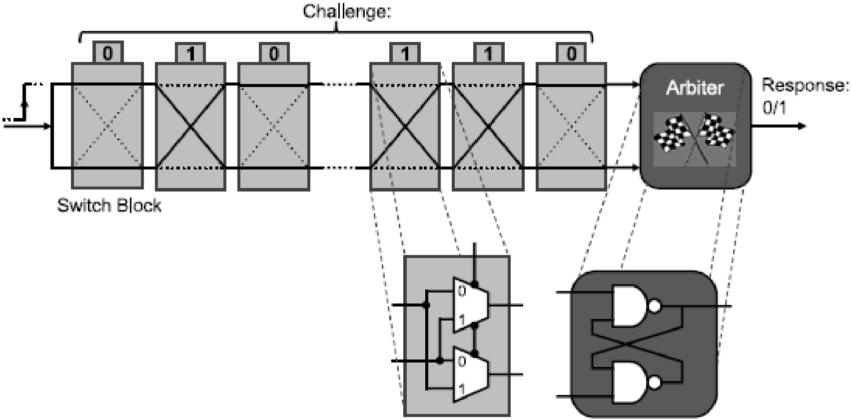

Figure: Arbiter PUF circuit[8].

[8] R. Maes. *Physically Unclonable Functions: Constructions, Properties and Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. ISBN: 978-3-642-41395-7. DOI: 10.1007/978-3-642-41395-7. URL: https://doi.org/10.1007/978-3-642-41395-7.

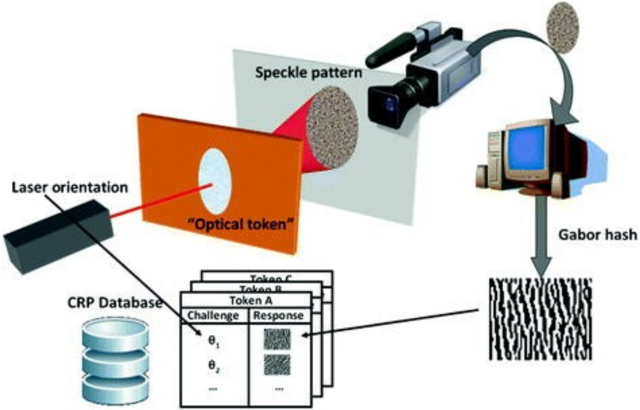

Figure: Optical PUF[9].

[9] R. Maes and I. Verbauwhede. "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions". In: Oct. 2010, pp. 3–37. ISBN: 978-3-642-14451-6. DOI: 10.1007/978-3-642-14452-3_1.