AN INTRODUCTION TO PHYSICAL UNCLONABLE FUNCTIONS AND THEIR APPLICATIONS

Cédrick De Pauw
Université Libre de Bruxelles

ULB

Motivations

Many problems with the security of IoT devices:

- **Initialization** of communication channels **without trust**
- Limited computational resources and battery autonomy: **no encryption**
- ...

⇒ **Hardware-intrinsic security**

Physical Unclonable Function

Overview:

- **Hardware-based** black-box **function**
- Based on **physical variations** caused by manufacturing processes
- **Unique, unpredictable and hard to clone**
- Input (optional): **challenge**, output: **response**
- **One or many CRPs** (challenge-response pairs)
- Require a **fuzzy extractor to provide reliable responses**

Advantages:

- Secure key storage → encryption
- Challenge-response function → authentication

PUF Classication

Intrinsic and Non-Intrinsic PUF

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

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

Otherwise, it is ***non-intrinsic***.

Implementation Technologies

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.

Security Levels

A 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.

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

Silicon PUF Examples

SRAM PUF

- Based on a Static Random-Access Memory (**memory-based** PUF)
- Source of randomness: variations between **inverters from SRAM cells**
- Challenge bits (optional): SRAM cells to select
- Response bits: (selected) SRAM cells **start-up values**
- **Weak PUF**

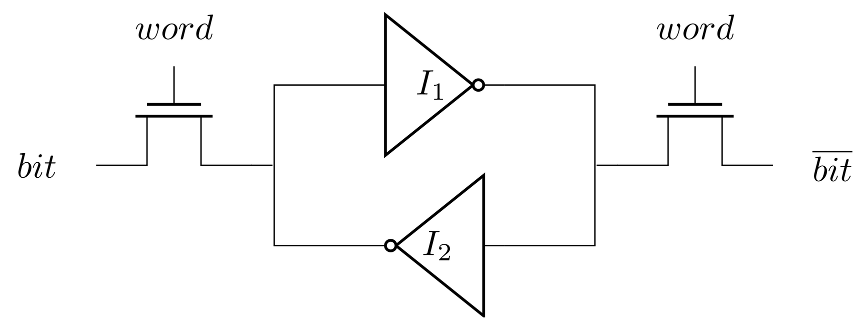

Fig. 1: SRAM cell logic circuit.

Arbiter PUF

- Based on gate propagation delay in arbiter PUF circuits (**delay-based** PUF)
- Arbiter PUF circuit: circuit built with multiplexers and a latch (arbiter)
- Source of randomness: variations between **multiplexers**
- Challenge bits: input to multiplexers
- Response bits: **fastest paths** pointed by arbiters
- **Strong PUF**

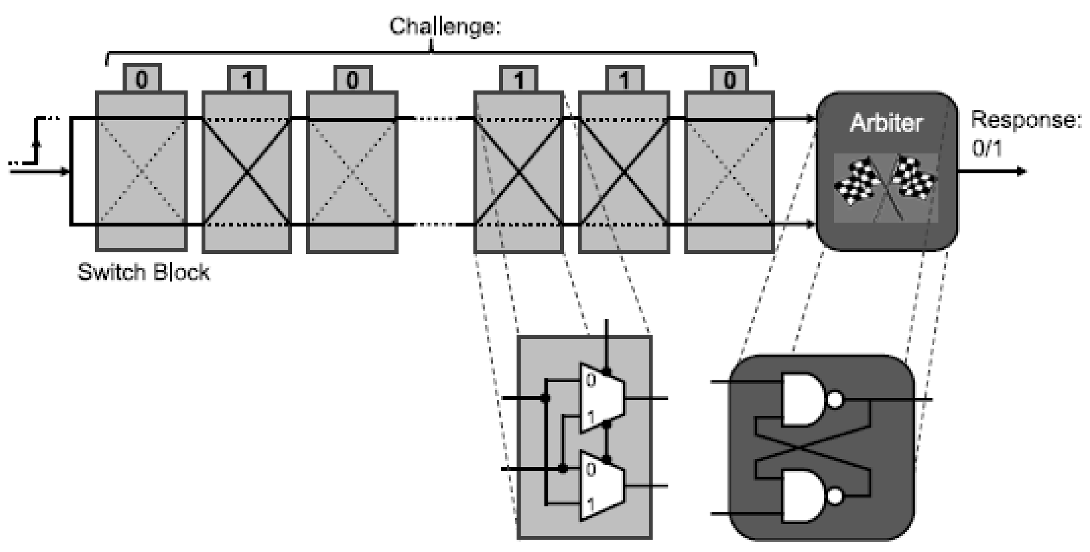

Fig. 2: Arbiter PUF circuit [1].

Fuzzy Extractor

1. **Generation** procedure:
   reference PUF response → (*helper data*, *key*)
2. **Reconstruction** procedure:
   (*noisy PUF response*, *helper data*) → *key*

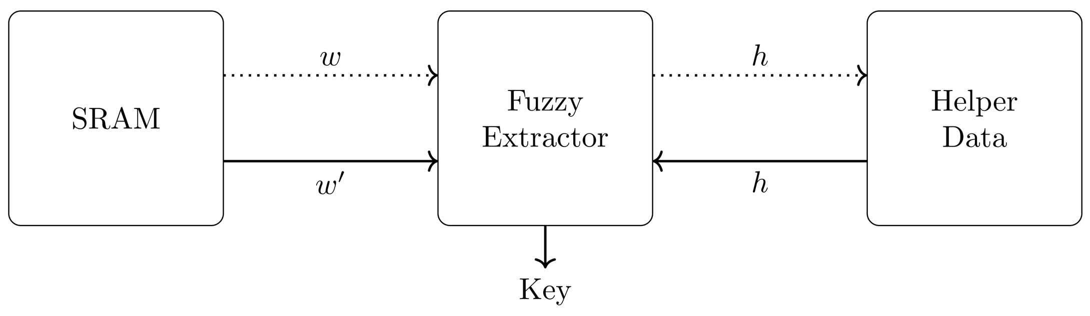

Fig. 3: Fuzzy extractor procedures [2]. Dotted arrows: generation procedure; plain arrows: reconstruction procedure. Notation: w and w' respectively are the reference PUF response and a noisy PUF response, h is the helper data.

Applications

Setup [3]:

- SRAM PUF and Arbiter PUF
- Device enrollement: $(\mathrm{ID}_d, \mathrm{SRAM}_k, (\mathrm{C}, \mathrm{R}))$

Two-factor mutual authentication protocol

- IoT device and server prove they know the SRAM key
- IoT device proves it knows the corresponding PUF response

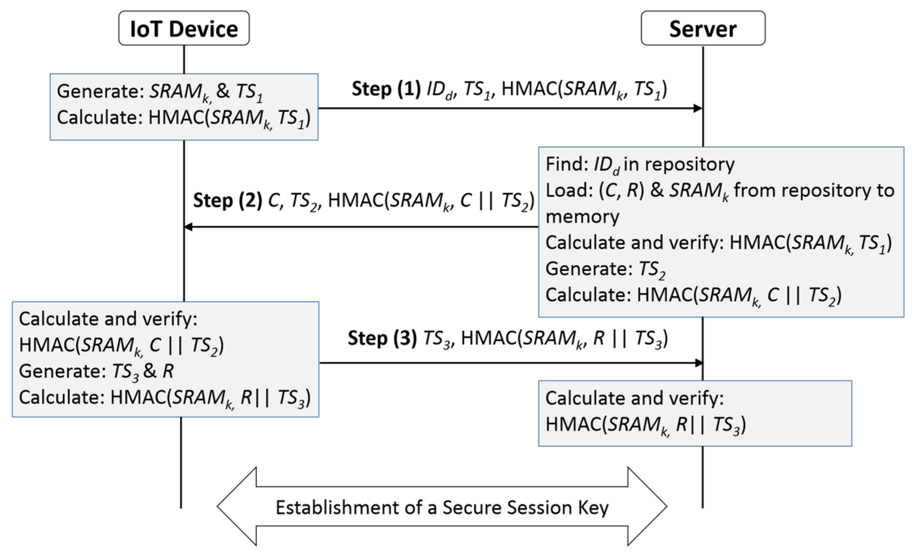

Fig. 4: Two-factor mutual authentication [3].

Session key establishment protocol

- Server sends a session key S_k encrypted with SRAM_k
- Future messages are encrypted with S_k

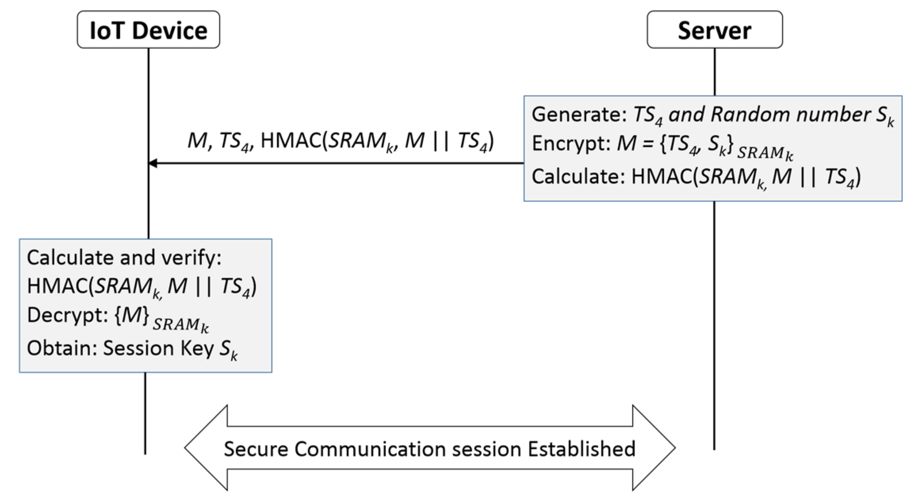

Fig. 5: Key establishment [3].

Acknowledgements

Funded through the CyberExcellence project from the Walloon Region. This research will cover the following workpackages:

- WP1: task 4
- WP5: tasks 1 and 3
- WP6: tasks 2 and 4

References

[1] 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.

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

[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.