Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions

Leah Lathrop*, Simon Liebl*, Ulrich Raithel†, Matthias Söllner*, Andreas Aßmuth*

*Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany
†SIPOS Aktorik GmbH, Altdorf, Germany

Presented by Leah Lathrop <l.lathrop@oth-aw.de>

October 2020

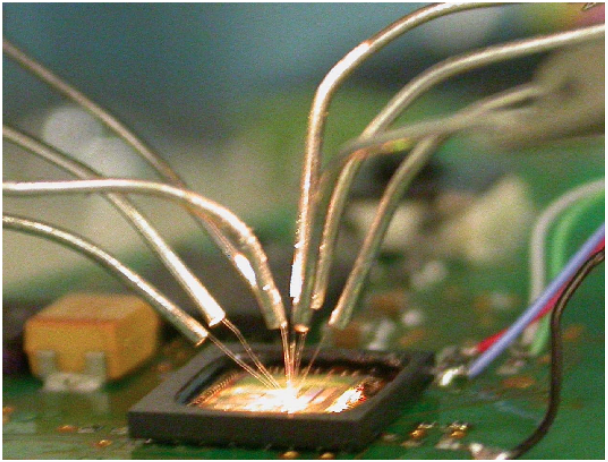
About the Author

Leah Lathrop, B. Eng.:

- Project Engineer and Master's Student at OTH Amberg-Weiden, Germany
- Fields of Research:
  - Physical Unclonable Functions
  - Side-channel Attacks

Outline

Motivation



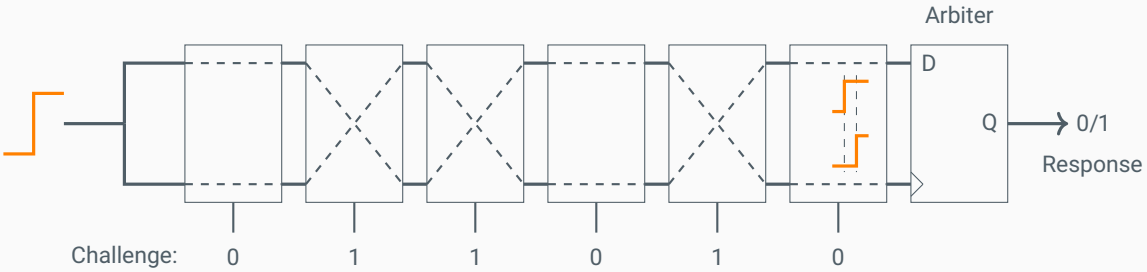
S. Skorobogatov, “How microprobing can attack encrypted memory,” in *2017 Euromicro Conference on Digital System Design (DSD)*. IEEE, August 2017, pp. 244-251.

Physical Unclonable Functions

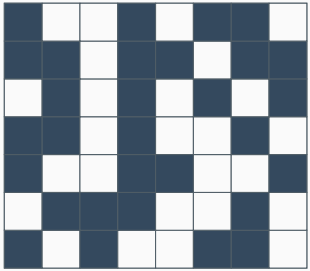
- Like biometrics for physical objects
- Use of an intrinsic random physical feature
- Challenge-Response Behavior

Outline

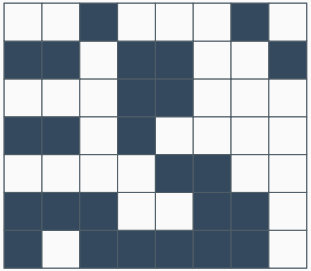
Arbiter PUF



SRAM PUF



SRAM 1

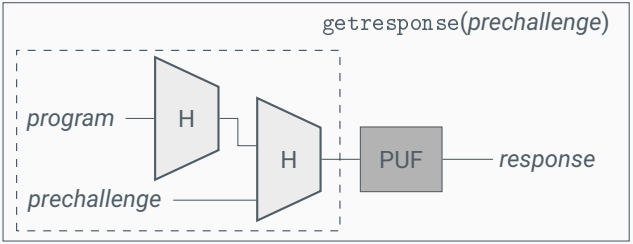


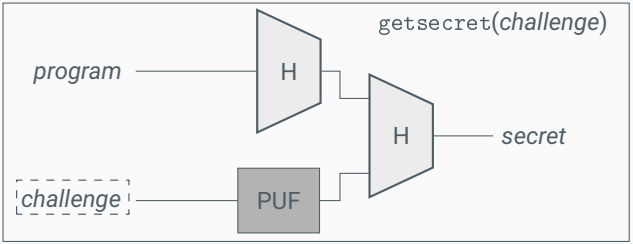
SRAM 2

PUF Characteristics

	Arbiter PUF	SRAM PUF
Number of Challenges	Strong PUF	Physically Obfuscated Key
Probabilistic Behavior	Delay-Based	Memory-Based

PUF Applications

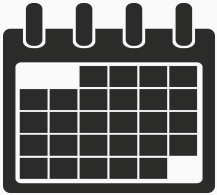




B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled physical random functions," in *18th Annual Computer Security Applications Conference*. IEEE, January 2002, pp. 149-160.

Environmental Influences

Temperature



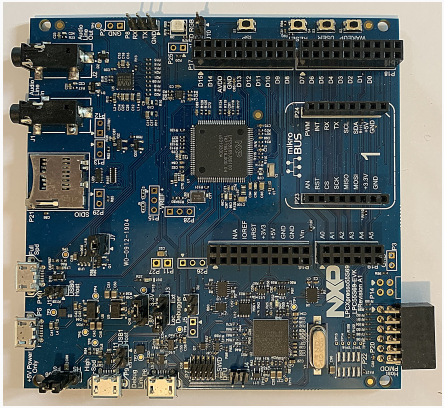
Aging

Supply Voltage

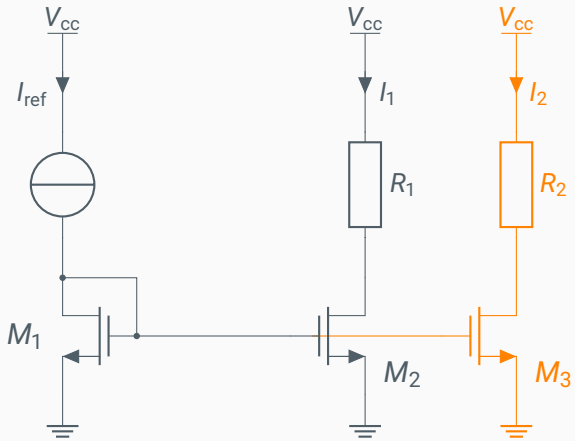
Outline

SRAM PUF

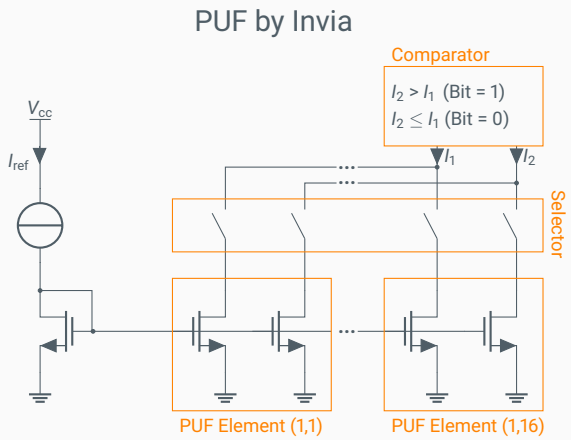
- Intellectual Properties by Intrinsic ID
  - QuiddiKey (Hardware)
  - BroadKey (Software)
- Integrated into products by:
  - NXP
  - Microsemi

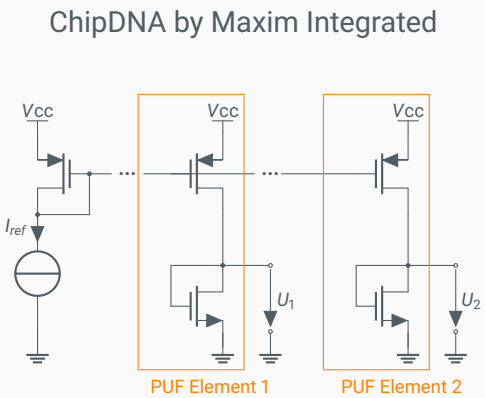


Current Mirror

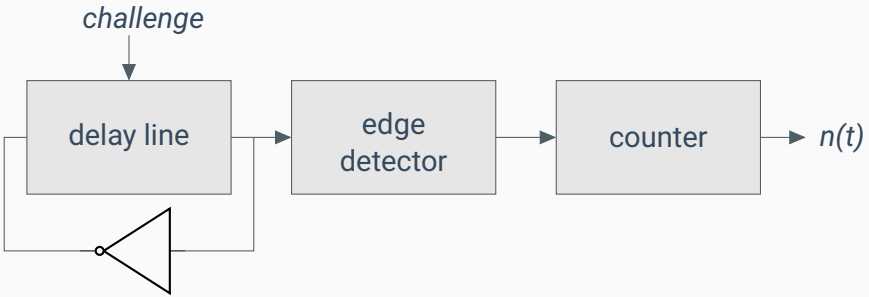


Current Mirror PUF





Ring Oscillator PUF

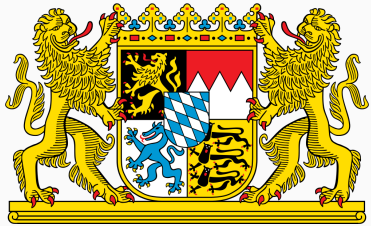


Outline

Conclusion

- Variety of different PUF types
- PUFs included in a many different types of devices
- Some of the PUFs used in basic ways
- All technologies were physically obfuscated keys

Thank You! Questions?



The project iSEC is funded by the Bavarian State Ministry for Economic Affairs, Regional Development and Energy within the framework of the Bavarian funding program for research and development “Information and Communication Technology”.