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
Leah Lathrop, B. Eng.:

► Project Engineer and Master’s Student at OTH Amberg-Weiden, Germany

► Fields of Research:
  ● Physical Unclonable Functions
  ● Side-channel Attacks
1 Introduction

2 Physical Unclonable Functions

3 Market Analysis

4 Conclusion
Physical Unclonable Functions

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

2. Physical Unclonable Functions

3. Market Analysis

4. Conclusion
Arbiter PUF

Challenge: 0 1 1 0 1 0

Response:

Arbiter

D

Q

0/1

Leah Lathrop: Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions
SRAM PUF

SRAM 1

SRAM 2
## PUF Characteristics

<table>
<thead>
<tr>
<th></th>
<th>Arbiter PUF</th>
<th>SRAM PUF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Challenges</strong></td>
<td>Strong PUF</td>
<td>Physically Obfuscated Key</td>
</tr>
<tr>
<td><strong>Probabilistic Behavior</strong></td>
<td>Delay-Based</td>
<td>Memory-Based</td>
</tr>
</tbody>
</table>

Leah Lathrop: Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions
PUF Applications


Leah Lathrop: Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions
Environmental Influences

Temperature  Aging  Supply Voltage
Outline

1. Introduction
2. Physical Unclonable Functions
3. Market Analysis
4. Conclusion

Leah Lathrop: Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions
Intellectual Properties by Intrinsic ID
- QuiddiKey (Hardware)
- BroadKey (Software)

Integrated into products by:
- NXP
- Microsemi
Current Mirror

Leah Lathrop: Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions
Current Mirror PUF

PUF by Invia

Comparator

\[ I_2 > I_1 \text{ (Bit = 1)} \]
\[ I_2 \leq I_1 \text{ (Bit = 0)} \]

Selector

ChipDNA by Maxim Integrated

PUF Element (1,1)

PUF Element (1,16)

PUF Element 1

PUF Element 2

Leah Lathrop: Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions
Ring Oscillator PUF

challenge

delay line

edge detector

counter

n(t)
Outline

1. Introduction
2. Physical Unclonable Functions
3. Market Analysis
4. 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”.

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