Empirical Evaluation of the Resilience of Novel Non-Algebraic AES S-Boxes to Power Side-Channel Attacks

Samuele Yves CERINI
samueleyves.cerini@studenti.polito.it

CYBERSECURITY NATIONAL LABORATORY

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Acknowledgments

The work has been supported by:

- CINI – Cybersecurity National Lab

  cybersecnatlab.it

CYBERSECURITY
NATIONAL
LABORATORY

CYBERSECURITY
NATIONAL
LABORATORY

Outline

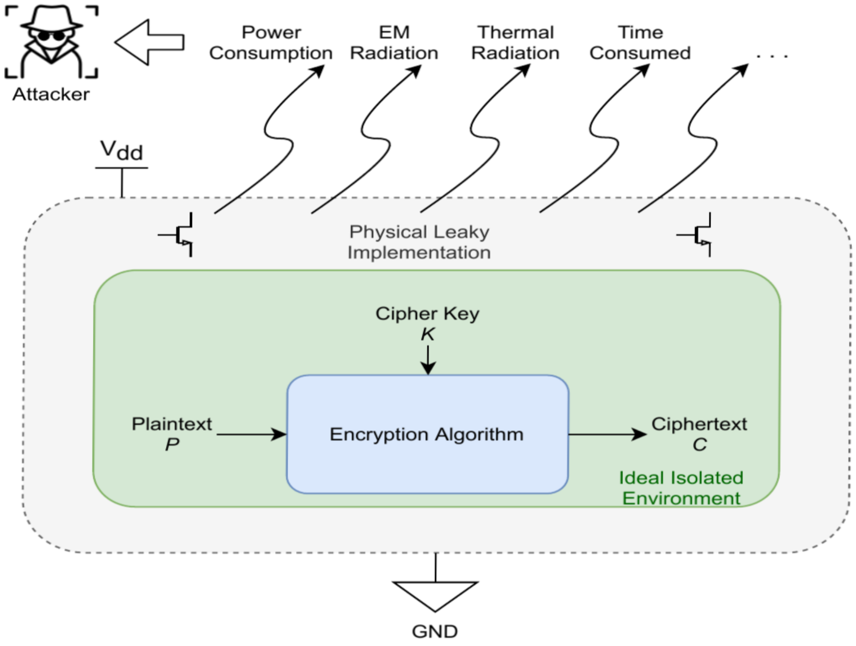
- (Power) Side-Channel Analysis
  - Definition and goals of the attack
- Countermeasures against SCA
  - Main rationale, issues of existing solutions
  - Why S-Boxes?
- Our contribution
  - Objectives and methodology
  - Results and conclusions

Outline

- (Power) Side-Channel Analysis
  - Definition and goals of the attack
- Countermeasures against SCA
  - Main rationale, issues of existing solutions
  - Why S-Boxes?
- Our contribution
  - Objectives and methodology
  - Results and conclusions

Side-Channel Analysis

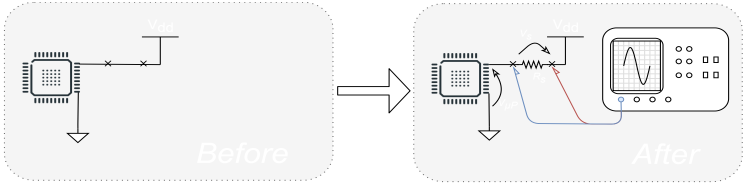
- **Goal:**
  - Retrieve sensitive data (secret keys)
- **Targets every operating device:**
  - IoT devices, embedded systems
- **Highly effective:**
  - Breaking AES-128:
    - Brute force: 2^{128} → SCA: $2^8 * 2^4 = 2^{12}$
  - Breaking AES-256:
    - Brute force: 2^{256} → SCA: $2^8 * 2^5 = 2^{13}$

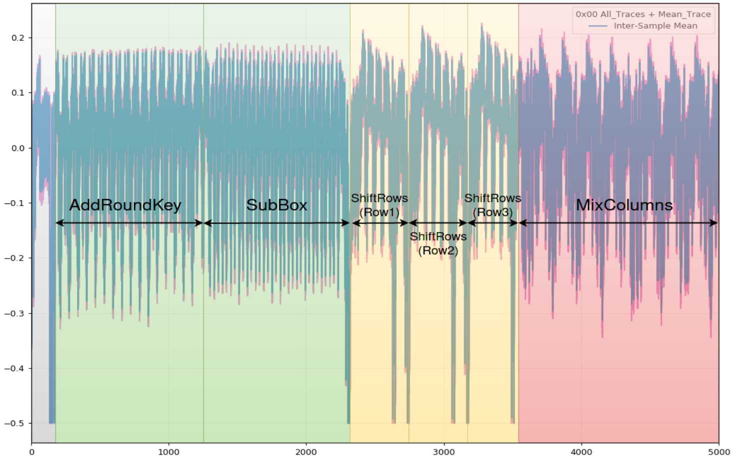


CYBERSECURITY NATIONAL LABORATORY

Power Analysis

- **Simple Power Analysis (SPA)**
  - A single power trace may suffice
  - Human visual analysis
  - Reverse Engineering and Timing Attacks
- **Differential/Correlation Power Analysis (DPA/CPA)**
  - Multiple power traces are needed
  - Based on automated statistical computations
  - Correlates the power consumption of the device to the (intermediate) encrypted data (plaintext XOR key)





CYBERSECURITY NATIONAL LABORATORY

Outline

- (Power) Side-Channel Analysis
  - Definition and goals of the attack
- Countermeasures against SCA
  - Main rationale, issues of existing solutions
  - Why S-Boxes?
- Our contribution
  - Objectives and methodology
  - Results and conclusions

SCA Countermeasures

- **Physical emissions cannot be prevented, but…**
  1) Leakage can be reduced
  2) What cannot be prevented can be made “unreadable”
- **Countermeasures can be inserted at different levels:**
  - Device-level
    - Balanced transitions, masking, noise circuitry
    - High impact on area, power consumption and performance
  - Cryptographic-level
    - Device-independent
    - **New S-Boxes, designed from the ground up to be (hopefully) SCA-resistant**

SCA Countermeasures - Why S-Boxes?

- **Why target Substition Boxes?**
  - Crucial component for many block ciphers (AES)
    - **SW implementations:**
      - Look-Up-Tables (LUTs)
      - No memory impact (just replace the original S-Box)
      - Device-independence (one design to rule them all?)
      - Automated heuristic design is possible
  - **Issues:**
    - Difficult to apply on HW implementations
      - Algebraic representation instead of LUTs
    - Adoption
      - Re-standardization, can take years

```
sbox = [
    # 0     1     2     3     4     5     6     7     8     9     a     b     c     d     e     f
    0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76, # 0
    0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0, # 1
    0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15, # 2
    0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75, # 3
    0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84, # 4
    0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf, # 5
    0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8, # 6
    0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2, # 7
    0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73, # 8
    0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb, # 9
    0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79, # a
    0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08, # b
    0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a, # c
    0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e, # d
    0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf, # e
    0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16  # f
]
```

Outline

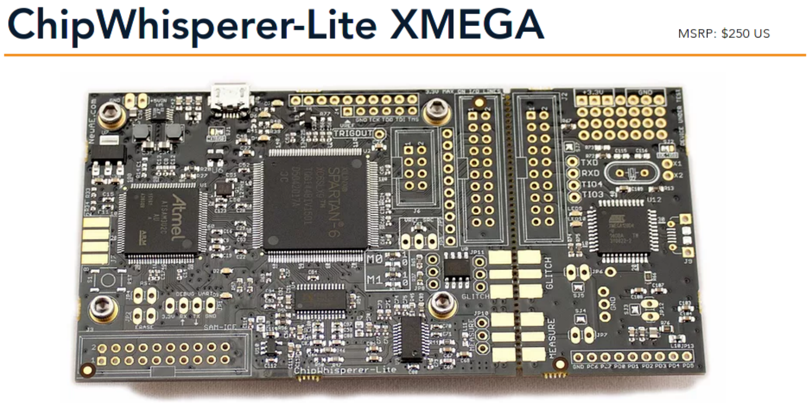
- (Power) Side-Channel Analysis
  - Definition and goals of the attack
- Countermeasures against SCA
  - Main rationale, issues of existing solutions
  - Why S-Boxes?
- Our contribution
  - Objectives and methodology
  - Results and conclusions

Our contribution - Rationale

- **What we observed?**
  - **A plethora of new S-Box designs based on:**
    - Chaotic systems and Heuritic methods
    - (Only) theoretical claims of improved SCA resistance
  - **Lack of emprirical tests on real world microcontrollers**
  - **Poor results and hard-to-verify benchmarks**
    - Synchronous or asynchronous sampling?
    - Sampling rate?
    - How many traces were collected?
    - Do I have the same microcontroller?

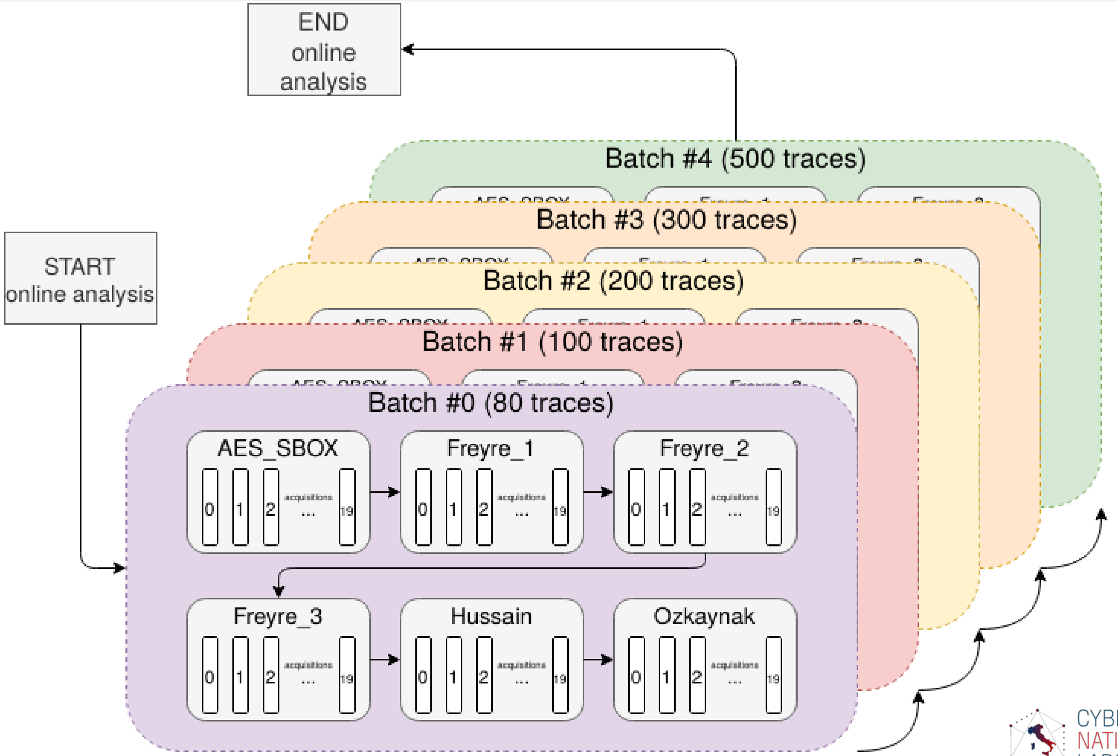
Our contribution – Methodology

- **What we did?**
  - **Select a subset of the latest S-Box proposals:**
    - #2 LUTs with no resistance to SCA
    - #4 LUTs with (claimed) theoretical resistance to SCA
  - **Empirical analysis leveraging a ChipWhisperer board**
    - 8-bit XMEGA AVR Microcontroller (SW AES-128)
    - Default probe configuration, synchronous sampling
    - Open-source code, completely reproducible
  - **CPA attack, with a Hamming Weight leakage model**



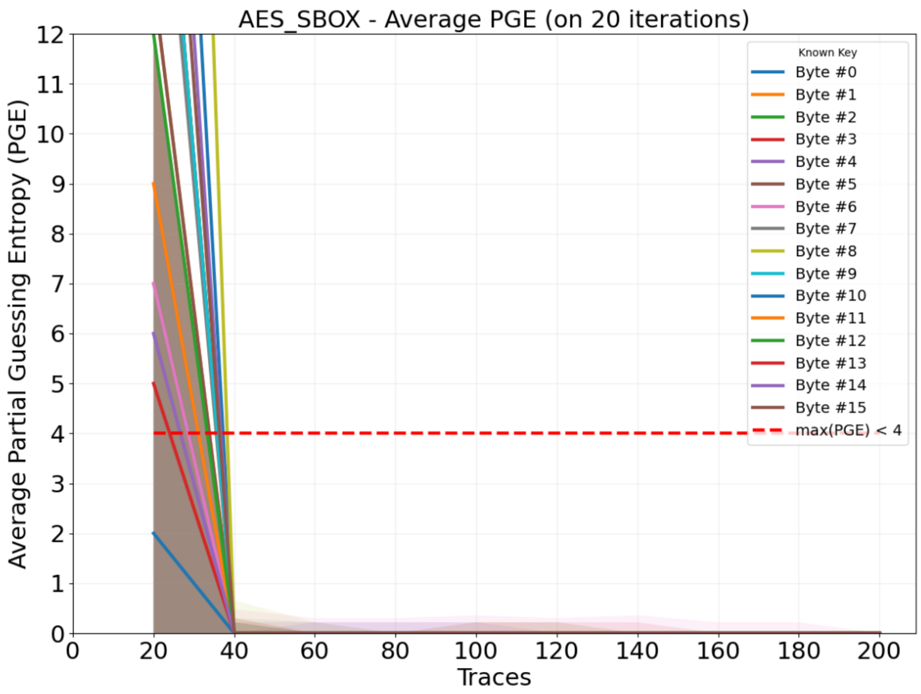
Our contribution – Methodology

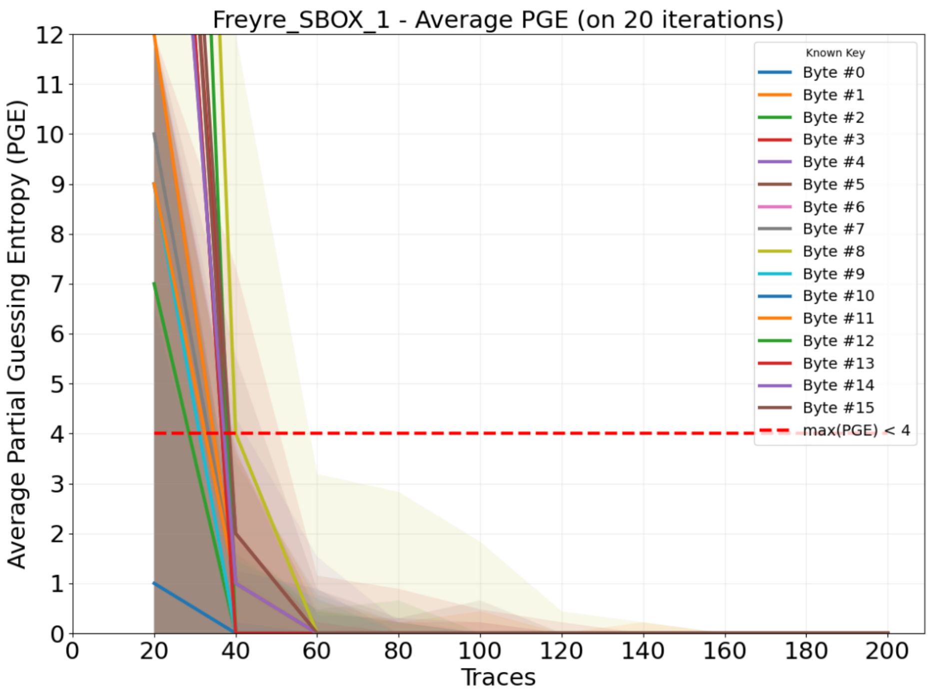
- **Extensive data collection**
  - 20 different datasets are collected for each structure
- **For each S-Box:**
  - 20 CPA attacks are performed
  - Average of the results



CYBERSECURITY NATIONAL LABORATORY

Our contribution – Results





Our contribution – Observations

- **What we observed?**
  - **AES, Hussain's and Özkaynak's S-Boxes**
    - Can be breaked in less than 50 traces
  - **Freyre's S-Boxes (heuristic methods)**
    - Can be breaked, in the best case scenario, within 100 traces
- **Results:**
  - Up to a 2x improvement in the case of Freyre's S-Boxes, seems promising…
  - … but is it really?

Our contribution – Conclusions

- **Problem:**
  - **ChipWhisperer-Lite acquires 40 traces per second**
    - Collecting 100 traces only requires 2 seconds!
  - **Sadly, a 2x improvement is not sufficient**
    - Trace capture can be done on-site → time constraints
    - An attack can be carried away later, off-site → no time constraints
- **Conclusions:**
  - Standard benchmarks and reproducible attacks are needed
  - Further improvements on SCA resistance are needed

Thanks for your attention!

CYBERSECURITY NATIONAL LABORATORY