CPA Attack to Embedded AES Algorithm

Lourdes Bruna
Òscar Pérez
Albert Vilardell

HSES
Master in Cybersecurity

2022/2023 Q2

Contents

Contents

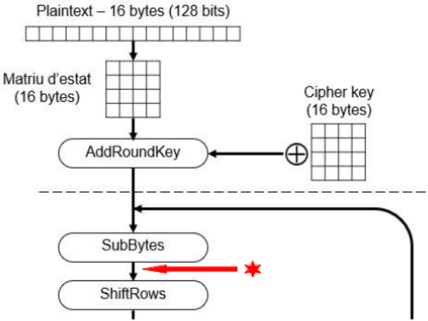
1. Introduction
2. Dataset 1
3. Dataset 2
4. Improvement
5. Comparison
6. Conclusions

Introduction

Correlation Power Analysis

- Dataset 1 (well clocked)
- Dataset 2 (not well clocked)

- HW model
- Calculate correlation



Motivation

We made some assumptions before starting the project, which we resolved by the end of it:

Motivation

We made some assumptions before starting the project, which we resolved by the end of it:

- We will get correlations either very close to 1 or to 0

Motivation

We made some assumptions before starting the project, which we resolved by the end of it:

- We will get correlations either very close to 1 or to 0
- We will get high correlations on almost every time instant of using the right key byte

Motivation

We made some assumptions before starting the project, which we resolved by the end of it:

- We will get correlations either very close to 1 or to 0
- We will get high correlations on almost every time instant of using the right key byte
- In dataset 2, we will realign all the 50.000 traces

Motivation

We made some assumptions before starting the project, which we resolved by the end of it:

- We will get correlations either very close to 1 or to 0
- We will get high correlations on almost every time instant of using the right key byte
- In dataset 2, we will realign all the 50.000 traces
- Dataset 2 is safer than dataset 1 (i.e. it is harder to hack)

Motivation

We made some assumptions before starting the project, which we resolved by the end of it:

- We will get correlations either very close to 1 or to 0
- We will get high correlations on almost every time instant of using the right key byte
- In dataset 2, we will realign all the 50.000 traces
- Dataset 2 is safer than dataset 1 (i.e. it is harder to hack)
- Dataset 2 is not 100% resistant to CPA

Contents

1. Introduction
2. Dataset 1
3. Dataset 2
4. Improvement
5. Comparison
6. Conclusions

Dataset 1

```
sbox = [0x63, ... , 0x16]
```

- Python implementation
- POWER α HW(**SBOX**(P $\oplus$ K))
- Correlation between the consumption and the model

Dataset 1

```
sbox = [0x63, ... , 0x16]

...

xor = (cleartext[x][z])^(y)
HW = bin(sbox[xor]).count('1')
```

- Python implementation
- POWER α **HW**(SBOX(P $\oplus$ K))
- Correlation between the consumption and the model

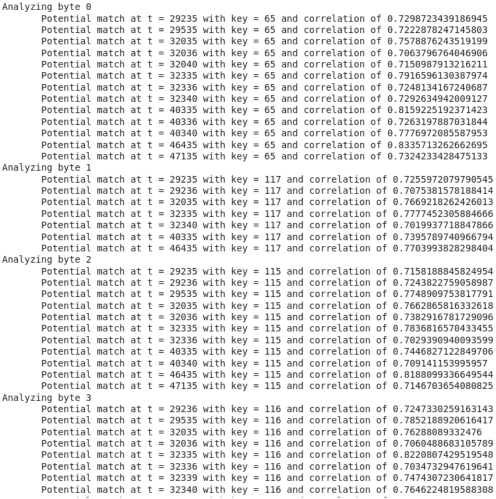
Dataset 1

- Python implementation
- POWER α HW(SBOX(P $\oplus$ K))
- **Correlation between the consumption and the model**

```
sbox = [0x63, ... , 0x16]

...

xor = (cleartext[x][z])^(y)
HW = bin(sbox[xor]).count('1')

...

corr0 = np.corrcoef(trace_i,
    model_transposed[i])

value = abs(corr0[0][1])
if (value >= 0.7):

...
```

Dataset 1

- Computation time: 9 hours



```
Analyzing byte 0
        Potential match at t = 29235 with key = 65 and correlation of 0.7298723439186945
        Potential match at t = 29535 with key = 65 and correlation of 0.7222878247145803
        Potential match at t = 32035 with key = 65 and correlation of 0.7578876243519199
        Potential match at t = 32036 with key = 65 and correlation of 0.7063796764046906
        Potential match at t = 32040 with key = 65 and correlation of 0.7150987913216211
        Potential match at t = 32335 with key = 65 and correlation of 0.7916596130387974
        Potential match at t = 32336 with key = 65 and correlation of 0.7248134167240687
        Potential match at t = 32340 with key = 65 and correlation of 0.7292634942009127
        Potential match at t = 40335 with key = 65 and correlation of 0.8159225192371423
        Potential match at t = 40336 with key = 65 and correlation of 0.7263197887031844
        Potential match at t = 40340 with key = 65 and correlation of 0.7776972085587953
        Potential match at t = 46435 with key = 65 and correlation of 0.8335713262662695
        Potential match at t = 47135 with key = 65 and correlation of 0.7324233428475133
Analyzing byte 1
        Potential match at t = 29235 with key = 117 and correlation of 0.7255972079790545
        Potential match at t = 29236 with key = 117 and correlation of 0.7075381578188414
        Potential match at t = 32035 with key = 117 and correlation of 0.7669218262426013
        Potential match at t = 32335 with key = 117 and correlation of 0.7777452305884666
        Potential match at t = 32340 with key = 117 and correlation of 0.7019937718847866
        Potential match at t = 40335 with key = 117 and correlation of 0.7395789740966794
        Potential match at t = 46435 with key = 117 and correlation of 0.7703993828298404
Analyzing byte 2
        Potential match at t = 29235 with key = 115 and correlation of 0.7158188845824954
        Potential match at t = 29236 with key = 115 and correlation of 0.7243822759058987
        Potential match at t = 29535 with key = 115 and correlation of 0.7748909753817791
        Potential match at t = 32035 with key = 115 and correlation of 0.7662865816332618
        Potential match at t = 32036 with key = 115 and correlation of 0.7382916781729096
        Potential match at t = 32335 with key = 115 and correlation of 0.7836816570433455
        Potential match at t = 32336 with key = 115 and correlation of 0.7029390940093599
        Potential match at t = 40335 with key = 115 and correlation of 0.7446827122849706
        Potential match at t = 40340 with key = 115 and correlation of 0.709141153995957
        Potential match at t = 46435 with key = 115 and correlation of 0.8188099336649544
        Potential match at t = 47135 with key = 115 and correlation of 0.7146703654080825
Analyzing byte 3
        Potential match at t = 29236 with key = 116 and correlation of 0.7247330259163143
        Potential match at t = 29535 with key = 116 and correlation of 0.7852188920616417
        Potential match at t = 32035 with key = 116 and correlation of 0.76288089332476
        Potential match at t = 32036 with key = 116 and correlation of 0.7060488683105789
        Potential match at t = 32335 with key = 116 and correlation of 0.8220807429519548
        Potential match at t = 32336 with key = 116 and correlation of 0.7034732947619641
        Potential match at t = 32339 with key = 116 and correlation of 0.7474307230641817
        Potential match at t = 32340 with key = 116 and correlation of 0.7646224819588308
```

Key for dataset 1

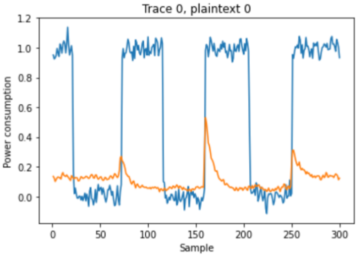
[65, 117, 115, 116, 114, 97, 108, 111, 112, 105, 116, 104, 101, 99, 117, 115]

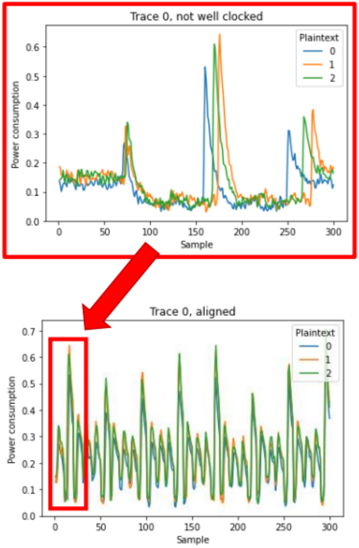
Whose values add to the checksum, 1712.

Contents

1. Introduction
2. Dataset 1
3. Dataset 2
4. Improvement
5. Comparison
6. Conclusions

Dataset 2





- Computation time: 1 hour

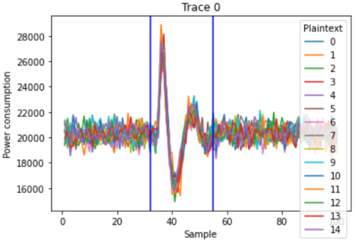
Key for dataset 2

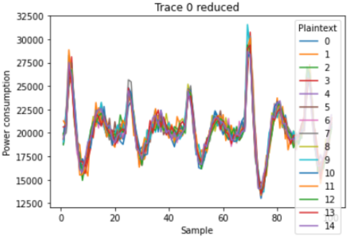
[84, 104, 97, 116, 115, 32, 109, 121, 32, 75, 117, 110, 103, 32, 70, 117]

Whose values add to the checksum, 1434.

Contents

Dataset 1 improvement





- Computation time: 1 hour

Improvement using Rust

- Python version was really slow (hours)
- Port python version to rust
- Computation time decreased to seconds
- **157x** on dataset1
- **210x** on dataset2

Contents

1 Introduction

2 Dataset 1

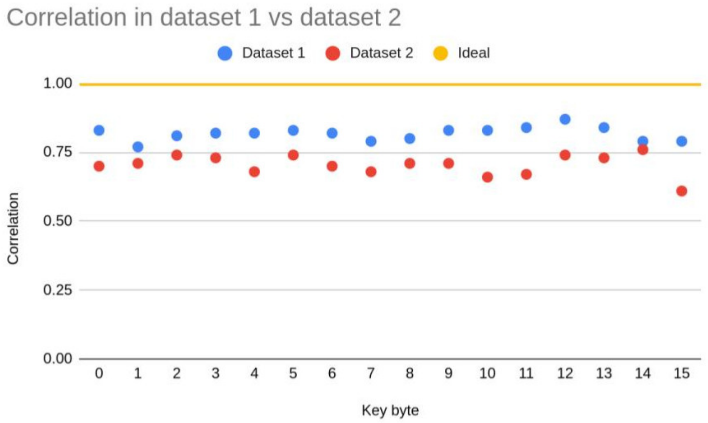
3 Dataset 2

4 Improvement

5 Comparison

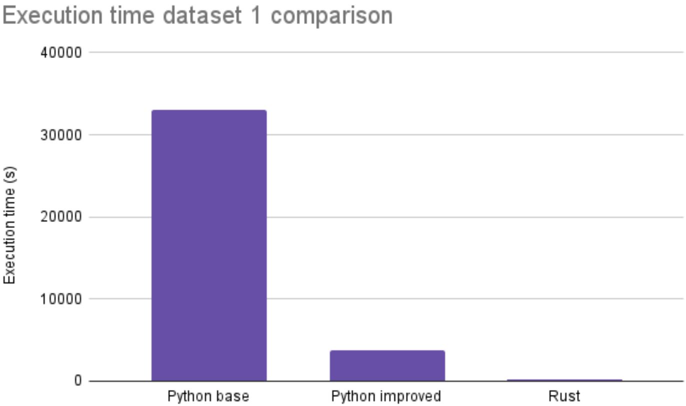
6 Conclusions

Correlation between the datasets

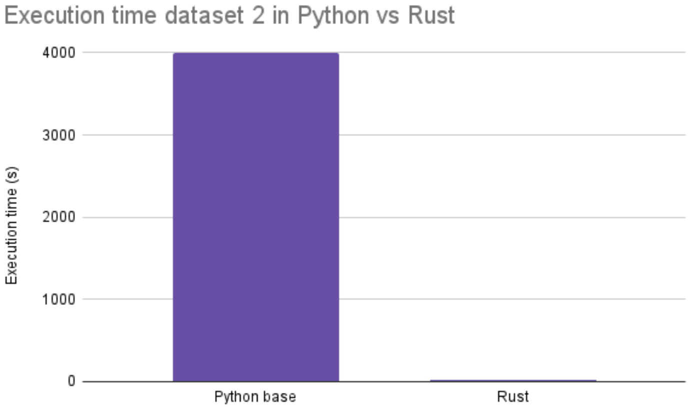


- Dataset 2 obtains correlations that are **smaller** than in dataset 1.

Performance: Dataset 1



Performance: Dataset 2



Contents

1 Introduction

2 Dataset 1

3 Dataset 2

4 Improvement

5 Comparison

6 Conclusions

Conclusions

We have obtained the keys. We have improved the performance by a factor of **157x** and **210x** by using Rust instead of Python.

Conclusions

We have obtained the keys. We have improved the performance by a factor of **157x** and **210x** by using Rust instead of Python.

- ✗ We will get correlations either very close to 1 or to 0
- ✗ We will get high correlations on almost every time instant of using the right key byte

- ✗ In dataset 2, we will realign all the 50.000 traces
- ✓ Dataset 2 is safer than dataset 1 (i.e. it is harder to hack)
- ✓ Dataset 2 is not 100% resistant to CPA

CPA Attack to Embedded AES Algorithm

Lourdes Bruna
Òscar Pérez
Albert Vilardell

HSES
Master in Cybersecurity

2022/2023 Q2