Analysis of Side-Channel Attacks on RFID/NFC Devices

Adel Qasem
Dr. Hervé Pelletier (Nagra) & Prof. Serge Vaudenay (LASEC)

Master Thesis - ISSS Berner Tagung

January 2023

Goal

Goal

Analyze the feasibility of **remote** electromagnetic side-channel attacks against RFID/NFC tags.

RFID Side-Channel Attacks

RFID

Radio Frequency IDentification

Wireless communication technology that uses a powered reader that provides energy, information, and a communication channel to a passive (i.e., powerless) tag using an EM field.

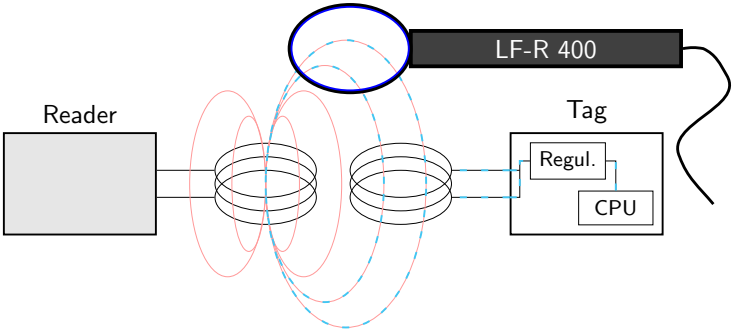
RFID Side-Channel Attack

We could use a microscopic electromagnetic probe, but we want a remote attack.

RFID Side-Channel Attack

We could use a microscopic electromagnetic probe, but we want a remote attack.

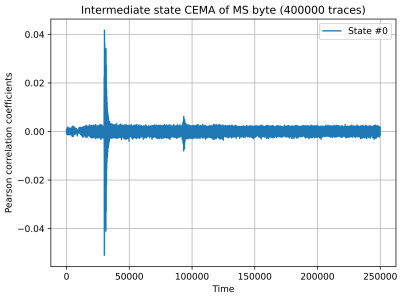
To do so, we measure the field of the EM coupling:



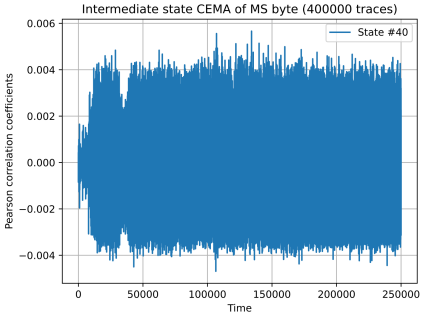
Attacks

Input and Output Correlation

We run a correlation analysis with the input and output:



(a) Input



(b) Output

Figure: Input and Output CEMA (20M traces).

Intermediate State Correlation

Similarly with an appropriate intermediate state:

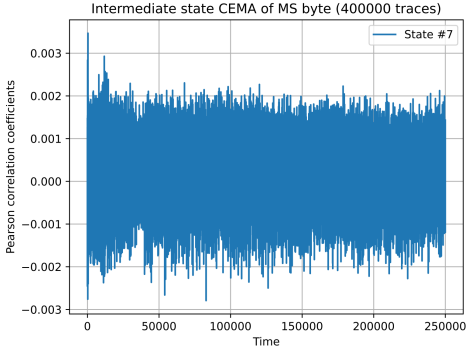


Figure: Intermediate state CEMA (20M traces)

Lack of Correlation

Why?

Lack of Correlation

Why? Could be a countermeasure such as desynchronization.

Lack of Correlation

Why? Could be a countermeasure such as desynchronization.
$\rightarrow$ Best way to find out: study the bare electromagnetic signal using analog demodulation.

Envelope Detector Implementation

We tried multiple solutions to implement an envelope detector:

Envelope Detector Implementation

We tried multiple solutions to implement an envelope detector:

- Software Defined Radio
  $\rightarrow$ Complex demodulation is hard to implement

Envelope Detector Implementation

We tried multiple solutions to implement an envelope detector:

- Software Defined Radio
  $\rightarrow$ Complex demodulation is hard to implement
- Analog circuitry
  $\rightarrow$ Careful implementation and optimization is required

Envelope Detector Implementation

We tried multiple solutions to implement an envelope detector:

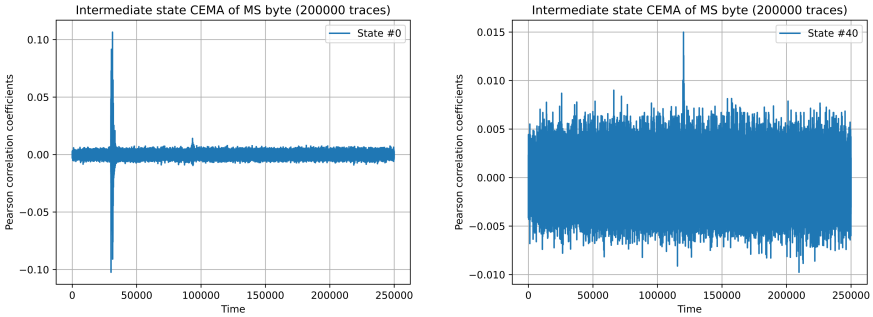
- Software Defined Radio
  → Complex demodulation is hard to implement
- Analog circuitry
  → Careful implementation and optimization is required
- RFID Reader
  → Only ASK (de)modulation is done by the frontend

Vertical Peak Focus

Zoom to focus on the variations of the carrier signal caused by modulation.

Vertical Peak Focus

Zoom to focus on the variations of the carrier signal caused by modulation.



(a) Input

(b) Output

Figure: Input and output CEMA (12.5M traces).

Vertical Peak Focus

For the intermediate state CEMA on the traces with vertical peak focus.

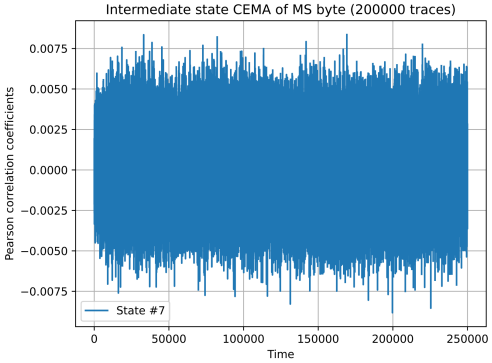


Figure: Intermediate State CEMA (12.5M traces).

Machine-Learning Side-Channel Attack

Machine learning is commonly used for side-channel attacks as it show good result. The goal is to build a classifier to recover the subkeys.

Fix vs Random Classifier

We used multiple classifiers to determine if a trace is fixed or random. We get very good result:

74.9%	25.1%
27.5%	72.5%

(a) Logistic regression.

73.6%	26.4%
30.6%	69.4%

(b) Linear SVM.

87.7%	12.3%
12.3%	87.7%

(c) MLP.

This reinforces the idea that we might have key-related leakage.

Fix vs Fix Classifier

Similarly, we built a fix vs fix classifier. We again get very good result:

62.6%	37.4%
42.3%	57.7%

(a) Linear SVM.

79.9%	20.3%
21.4%	78.6%

(b) MLP.

We do have full-key leakage!

Sub-Key Classifier

We need to be able to classify traces according to a subkey (e.g., 2^8 classes).
$\rightarrow$ The byte key classifiers did not however show good results...

Sub-Key Classifier

We need to be able to classify traces according to a subkey (e.g., 2^8 classes).
$\rightarrow$ The byte key classifiers did not however show good results...

Possibly a key-dependent mask preventing byte-level analysis.
$\rightarrow$ Key-dependent leakage, but no sub-key dependent leakage

Future Works

- Higher-order side-channel attack
  $\rightarrow$ Requires insight and much smaller time frames

Future Works

- Higher-order side-channel attack
  $\rightarrow$ Requires insight and much smaller time frames
- Microscopic probe insight
  $\rightarrow$ An attacker could use it to do the whole attack

Thank you!