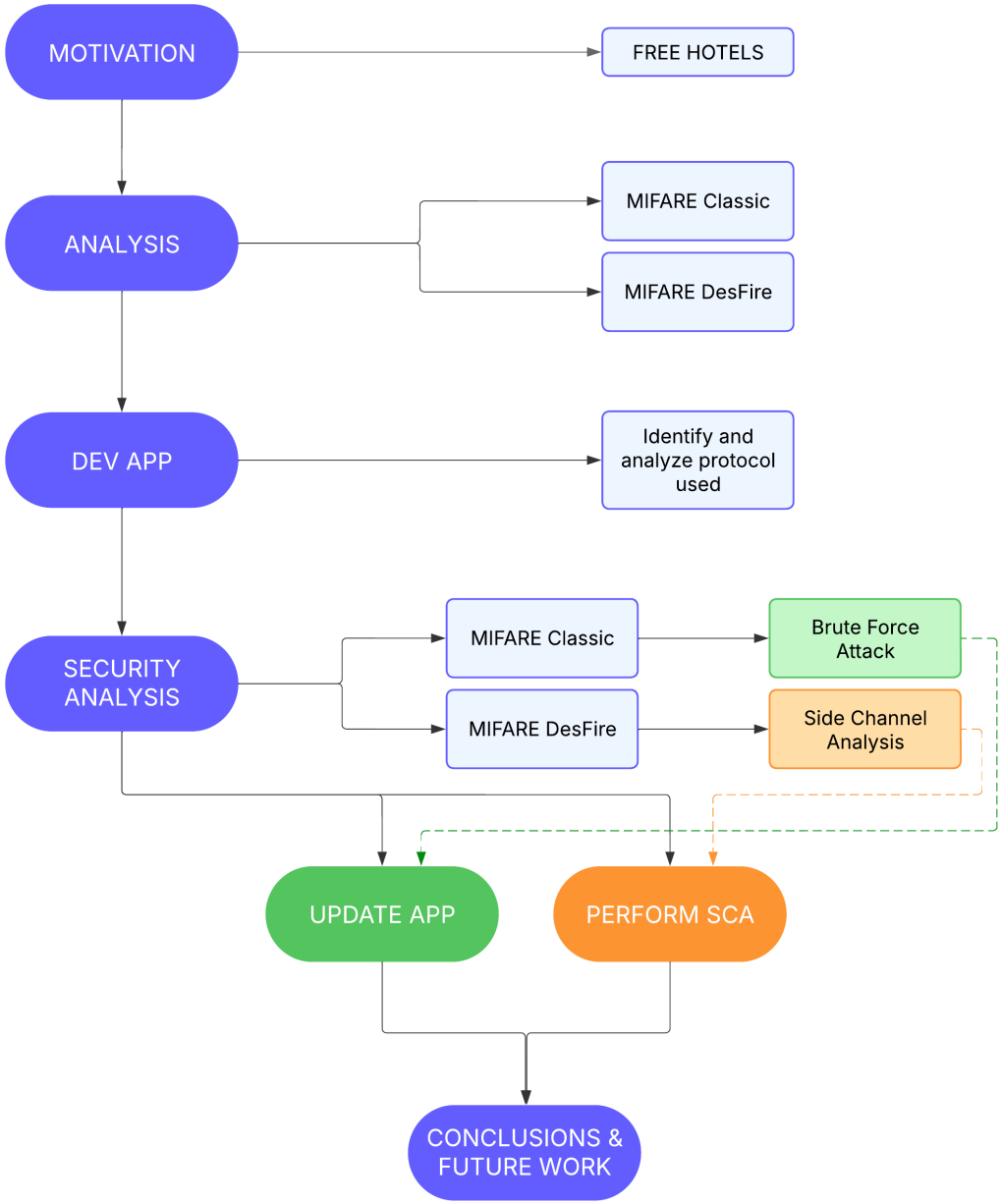
Development of Software for Identifying, Reading, and Cracking RFID Cards Using Side-Channel Analysis Techniques

ADRIÁN BELLO CANDEL
adrianbeca7@gmail.com

UNIVERSITAT AUTÒNOMA DE BARCELONA
ESCOLA D'ENGINYERIA
ENGINYERIA INFORMÀTICA

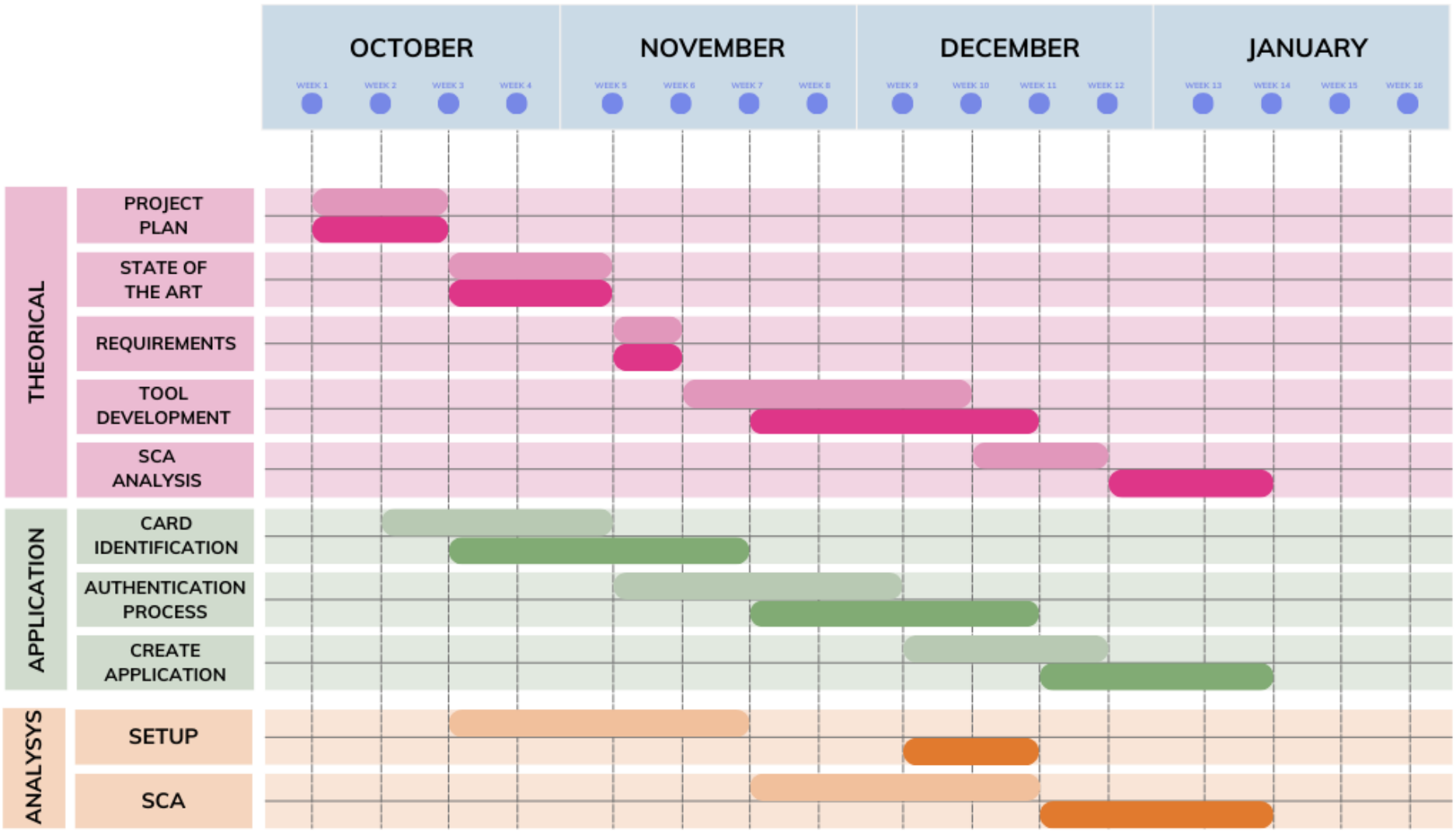
4 de febrero de 2025

Motivation and Objectives



Contents

Planning

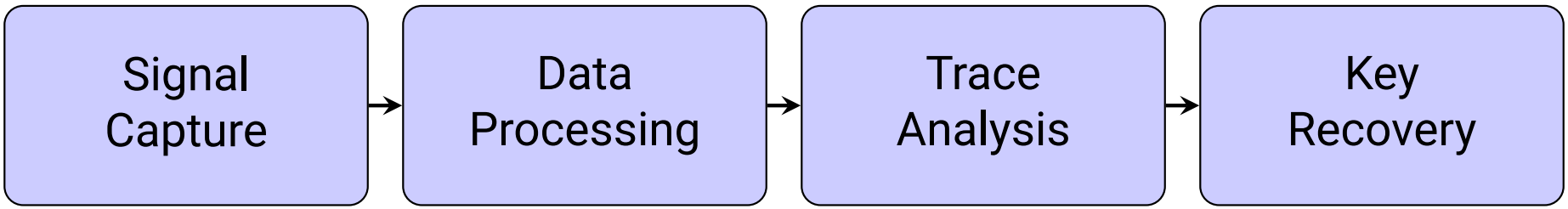

OCTOBER
NOVEMBER
DECEMBER
JANUARY
WEEK 1
WEEK 2
WEEK 3
WEEK 4
WEEK 5
WEEK 6
WEEK 7
WEEK 8
WEEK 9
WEEK 10
WEEK 11
WEEK 12
WEEK 13
WEEK 14
WEEK 15
WEEK 16
THEORICAL
PROJECT PLAN
STATE OF THE ART
REQUIREMENTS
TOOL DEVELOPMENT
SCA ANALYSIS
APPLICATION
CARD IDENTIFICATION
AUTHENTICATION PROCESS
CREATE APPLICATION
ANALYSYS
SETUP
SCA

State of the Art

Comparison of RFID Cards

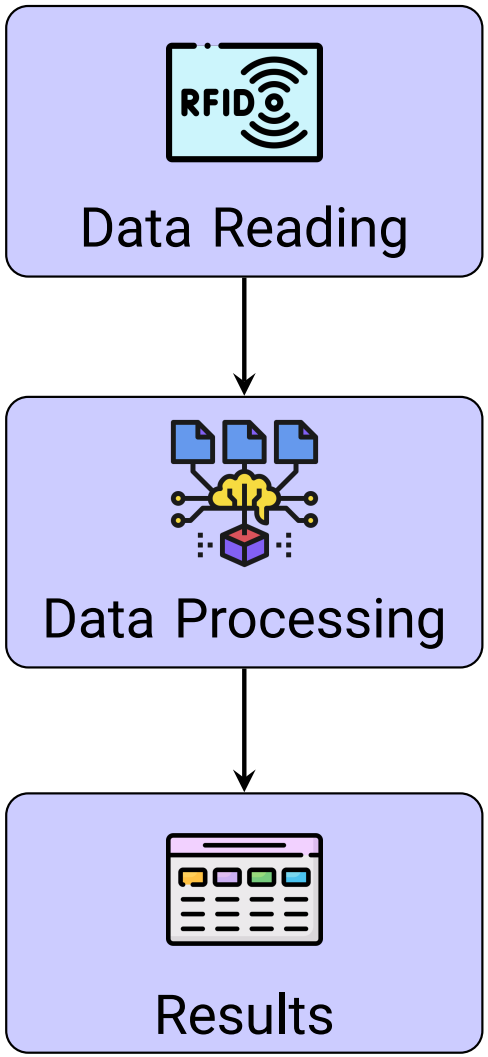
Card	Year	Algorithm	Security	Applications
MIFARE Classic	1994	CRYPTO1	Low	Public Transportation
MIFARE DESFire	2002	DES/AES/3DES	High	Access Control
MIFARE Ultralight	2001	None	Low	Single-Use Tickets
NTAG	2012	AES	Medium	NFC Applications

Flow of an SCA Attack

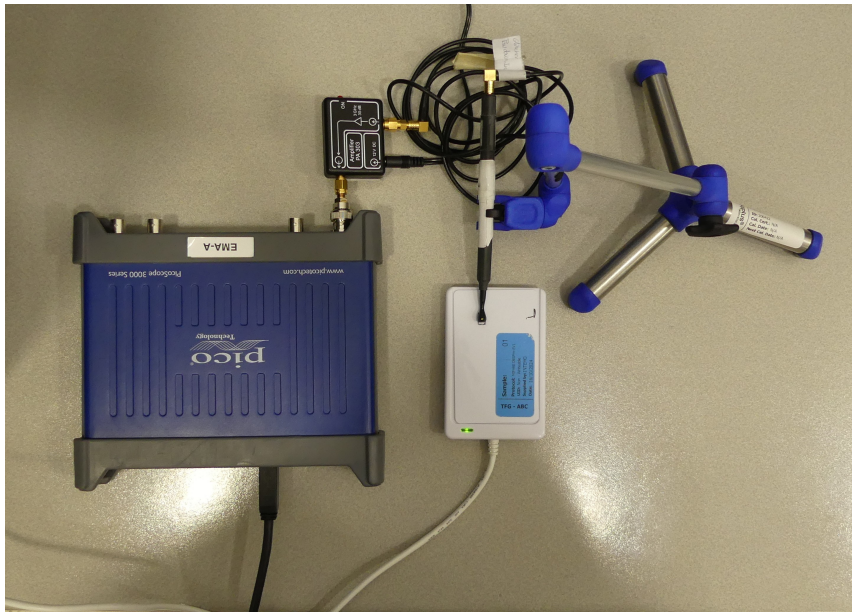


Methodology

Application Development Flow

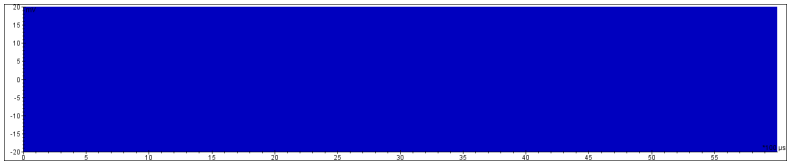


Experimental Setup for SCA Analysis

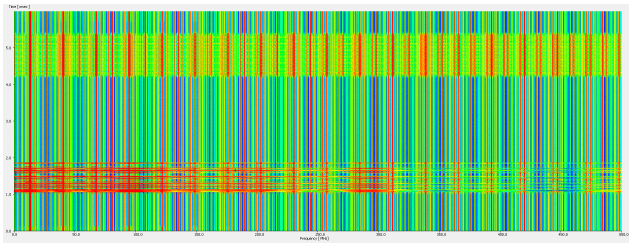


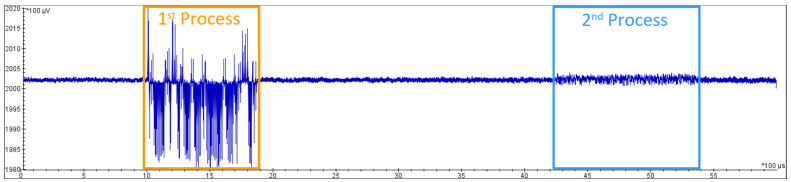
Side Channel Analysis: SPA

Signal without any filter

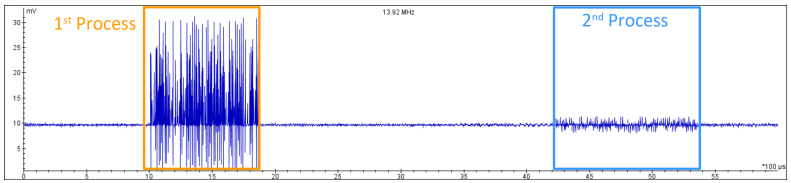


Spectrogram

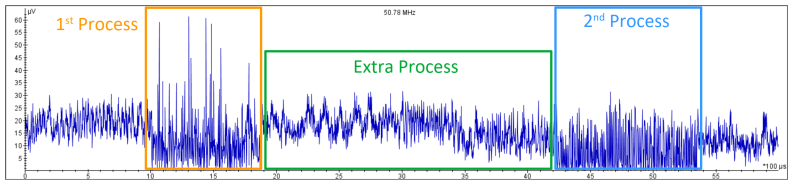




Signal after LowPass and Absolute



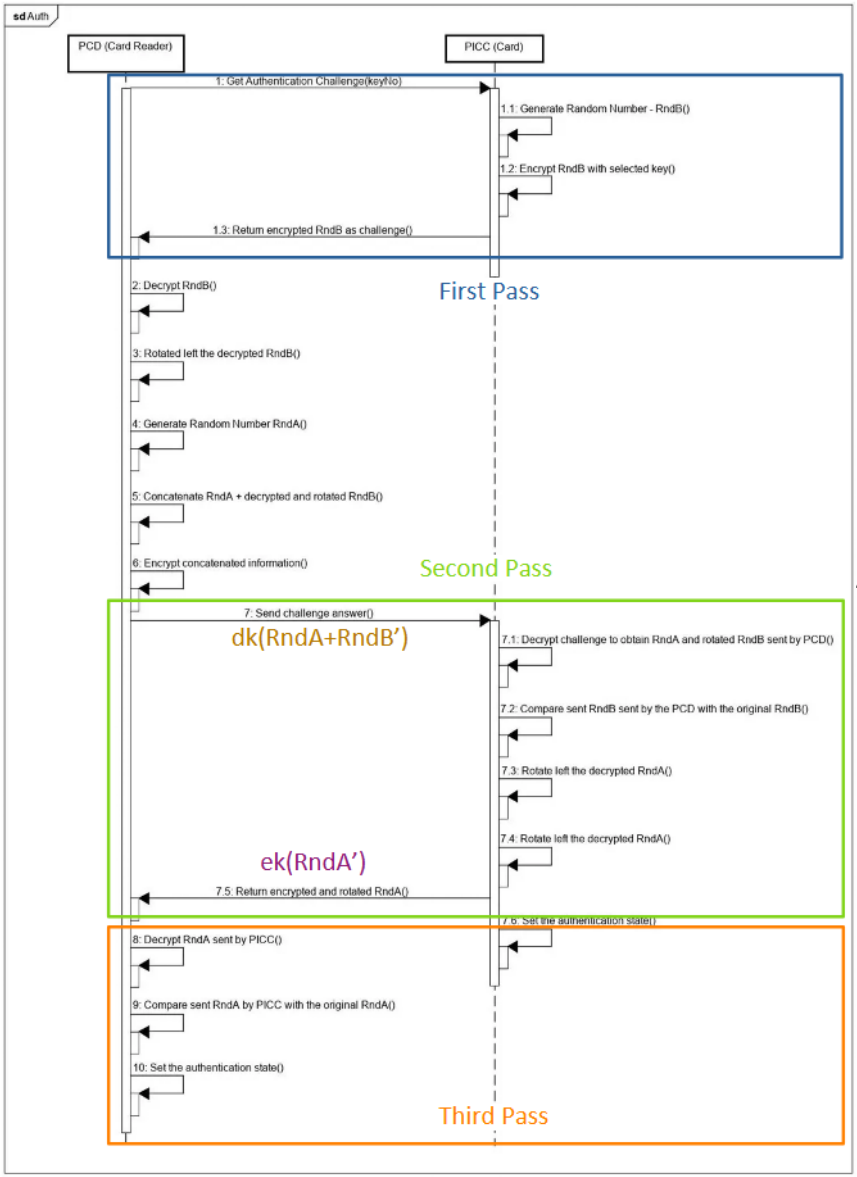
Filtered in 13.92 MHz



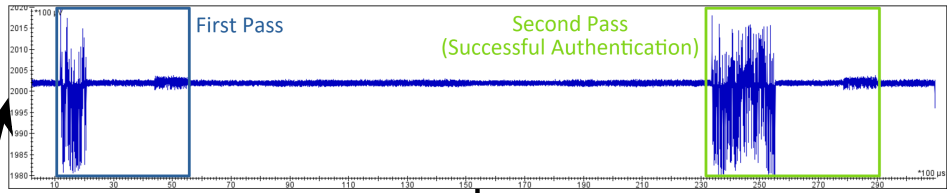
Filtered in 50.78 MHz

Side Channel Analysis: SPA

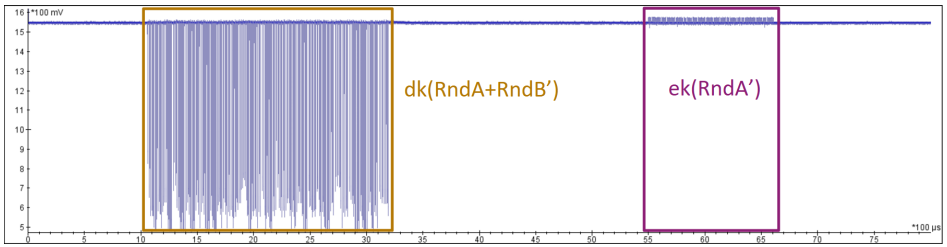
Three-pass authentication



First and Second Pass

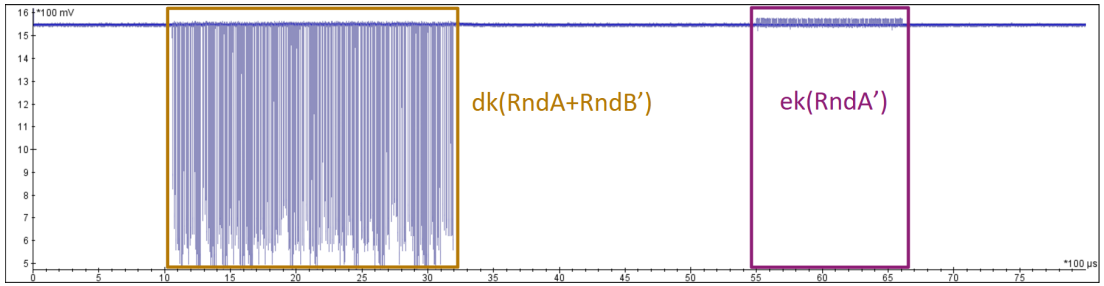


Second Pass

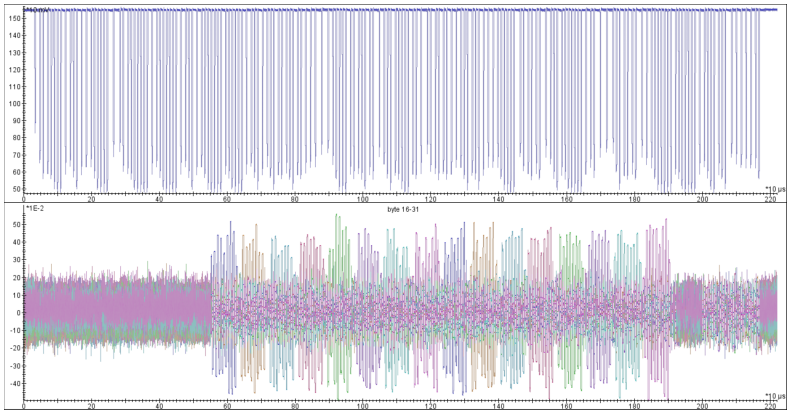


Side Channel Analysis: SPA

Second Pass

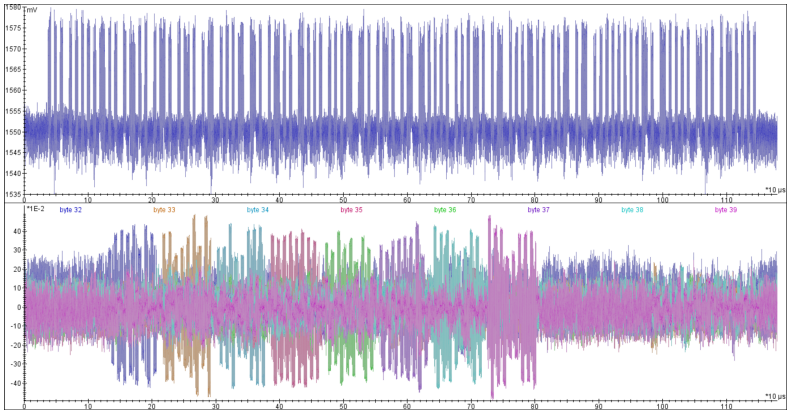


Correlations dk(RndA+RndB')



0x90, 0xAF, 0x00, 0x00, 0x10 + [16 bytes] + 0x00

Correlations ek(RndA')

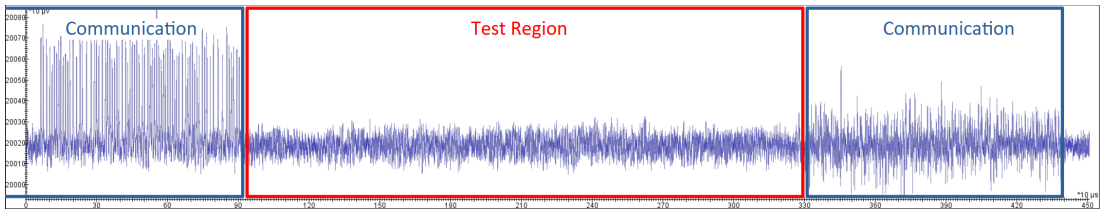


0x91, 0x00 + [8 bytes]

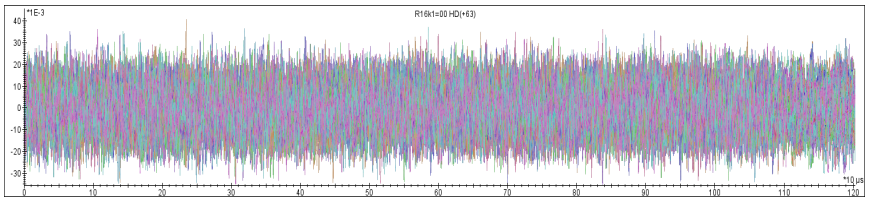
- 16 random bytes from the reader and 8 random bytes from the card.

Side Channel Analysis: CPA

Test Region

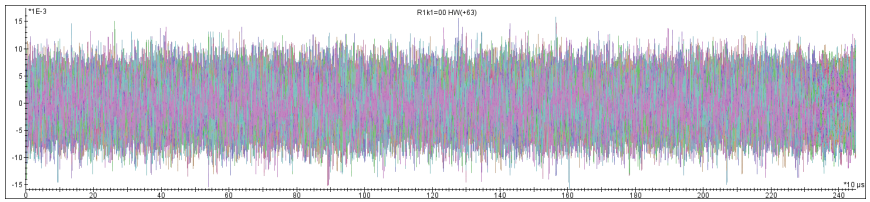


Correlations 20.000 traces



Key Byte	Rank	Candidate	Confidence	Sample Position
Byte 1	55	0x00	0.0299	15618
Byte 2	45	0x00	0.0310	107811
Byte 3	20	0x00	0.0346	39393
Byte 4	14	0x00	0.0354	55246
Byte 5	18	0x00	0.0337	53771
Byte 6	44	0x00	0.0319	264280
Byte 7	2	0x00	0.0386	65061
Byte 8	49	0x00	0.0311	166721

Correlations 100.000 traces

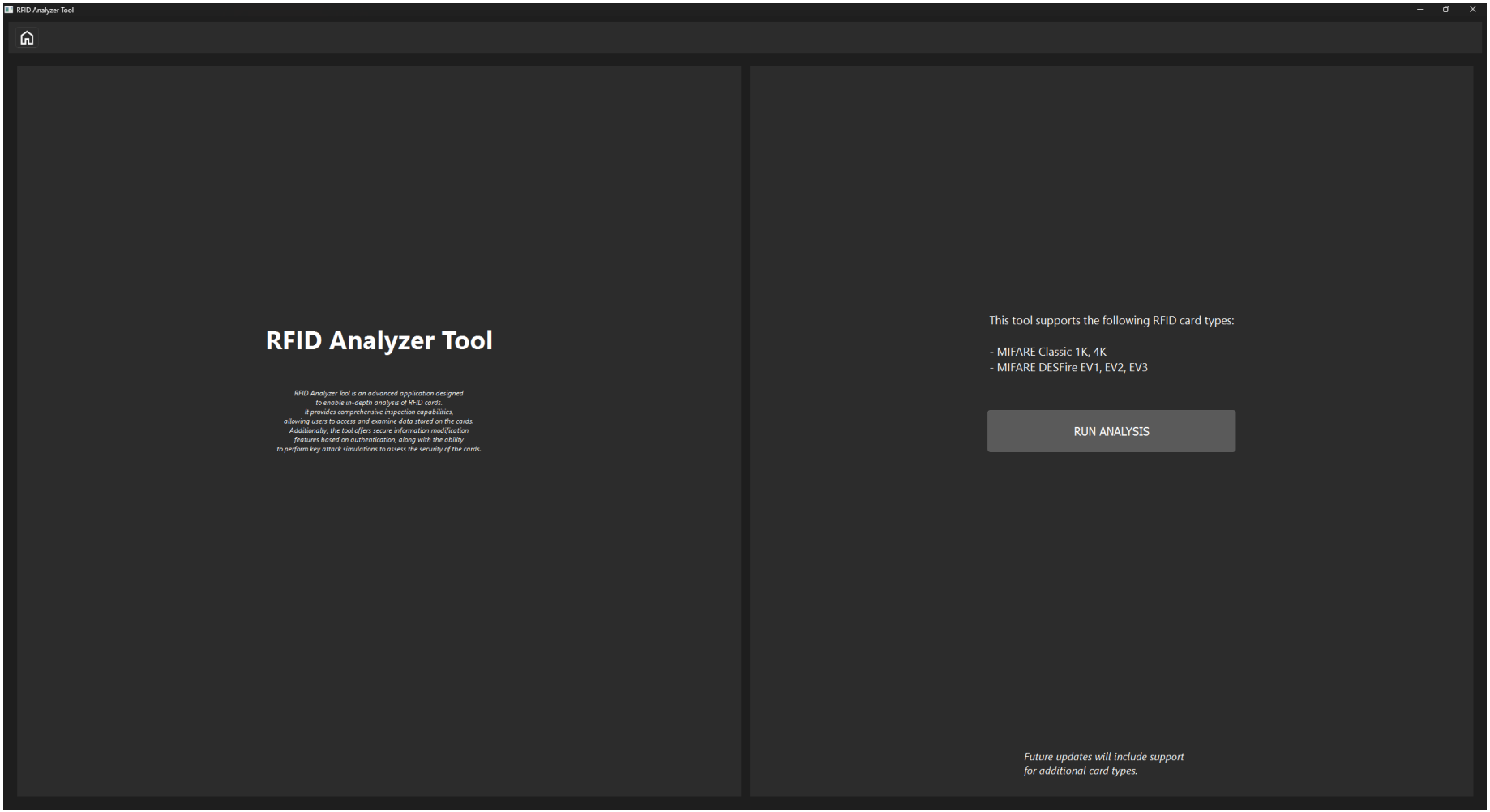


Key Byte	Rank	Candidate	Confidence	Sample Position
Byte 1	20	0x00	0.0137	512442
Byte 2	64	0x00	0.0114	138341
Byte 3	12	0x00	0.0142	108886
Byte 4	11	0x00	0.0144	261116
Byte 5	41	0x00	0.0131	162218
Byte 6	52	0x00	0.0124	184356
Byte 7	35	0x00	0.0132	342666
Byte 8	8	0x00	0.0150	418490

- The inherent noise in the chip's signal significantly increases its resistance to Side Channel Analysis, making it highly secure against correlation attacks.

Application Demo

Main Page



Conclusions and Future Work

A functional tool was developed to analyze RFID cards, and conduct a brute-force attack to MIFARE Classic cards.

SPA and CPA methods were used to investigate MIFARE DESFire cards.

Vulnerabilities could not be assessed as the chip's high level of noise effectively prevents successful CPA.

Understanding the structure of RFID cards and exploring cryptographic methods like DES, has been highly valuable to support my growth in my professional career.

Future Work

Further efforts will focus on improving the tool's functionality, refining signal processing, and exploring advanced methods to enhance security analysis.

Thanks for your attention

Special thanks to:

Applus+, INTEMO, and UOC

Josep Prieto, David Hernández, Sara Ribes, Natalia Mendo, Cristian Fernández, Josep Clopes, David Gañan and Joan Melià

All my family and friends who supported me throughout this challenging project.