RFID SECURITY MODULE

20TH DECEMBER 2017

PEPE VILA

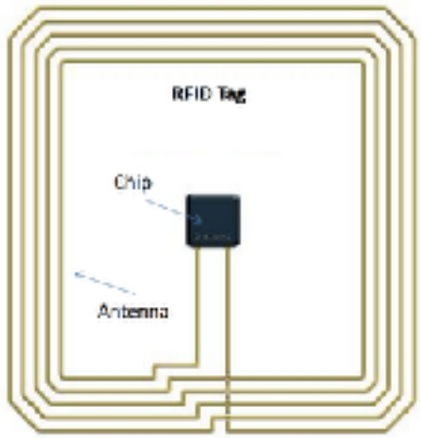
@CGVWZQ PEPE.VILA@IMDEA.ORG VWZQ.NET

- Introduction
- Readers: PM3, ACR122U, SmartPhones
- Tags: Specs + Examples
  - HID, MIFARE Ultralight, Classic, Desfire EV1
- Relay Attacks

What is RFID?

Radio-frequency identification (RFID)

"method of uniquely identifying items using radio waves"
(Origin: distinguish enemy aircraft during WWII)



Passive
vs.
Active Tags

- LowFrequency (LF): 125-134kHz
- HighFrequency (HF): 13.56mHz
- UltraHighFrequency (UHF): 856-960mHz

Tons of Technologies

Keyless Cars

Authentication

Credit Cards/Payments

Vending Machines

identification

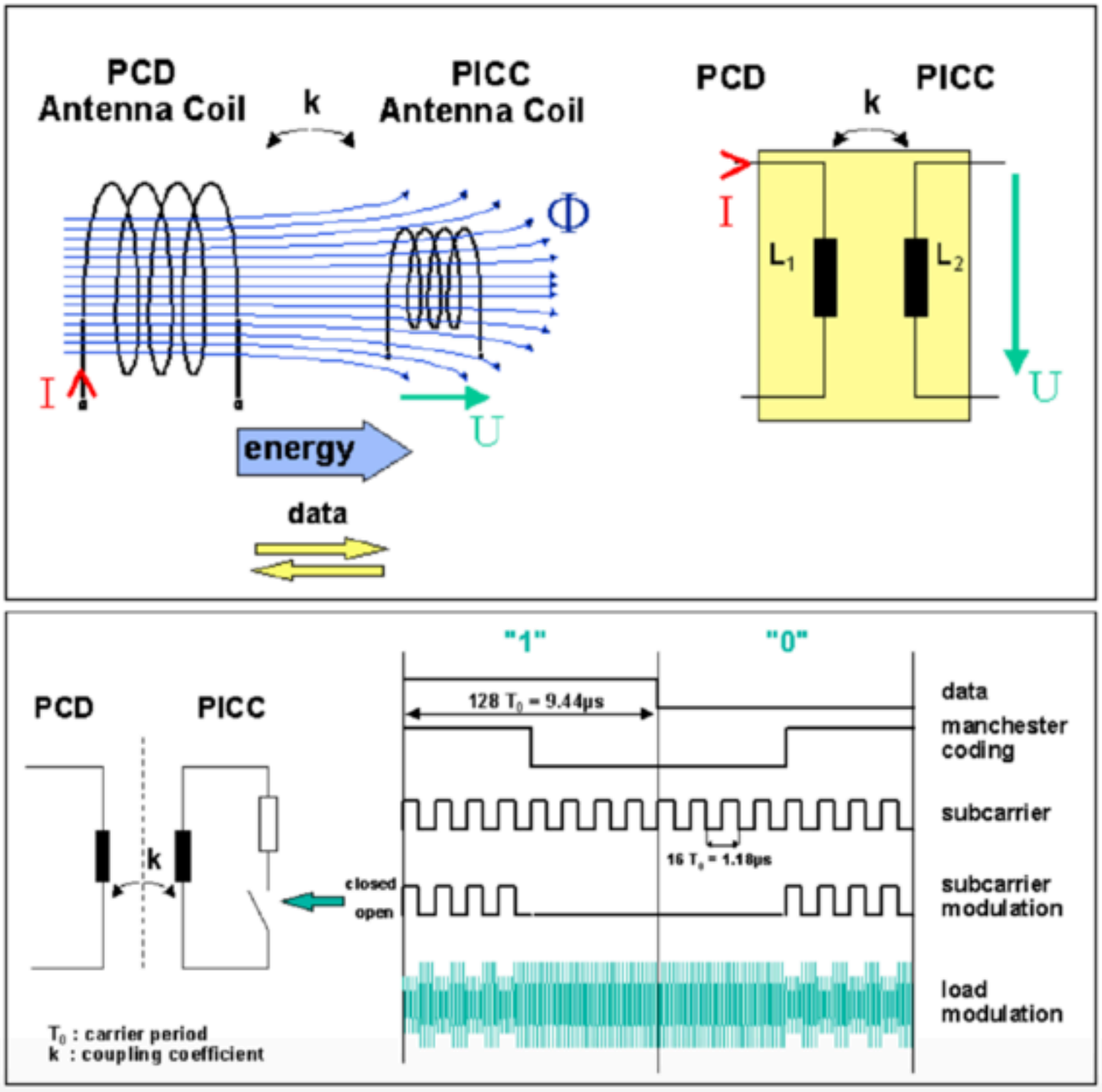
Tracking/Logistics

Ticketing systems

Biodevices

How It Works?

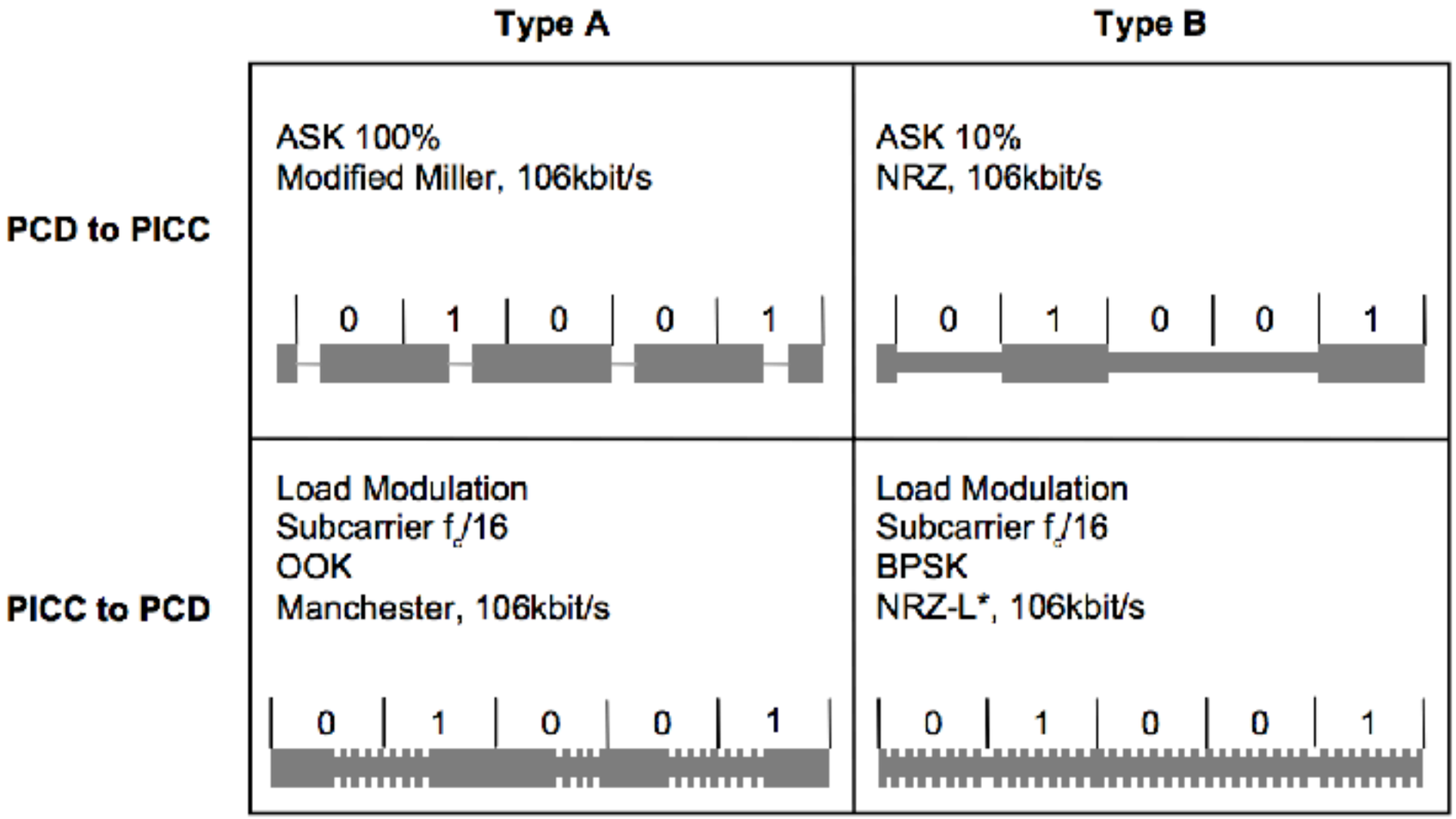
Proximity Coupling Device



Proximity Inductive Coupling Card

[Taken from 13.56 MHz RFID Proximity Antennas (http://www.nxp.com/documents/application_note/AN78010.pdf)]

How It Works?



(MODULATION FOR ISO-14443-2)

We will abstract from all these details, but if you are interested here is a recent and nice introduction to RF and SDR:
https://www.elttam.com.au/blog/intro-sdr-and-rf-analysis/

VS

Near Field Communication is a RFID technology

"NFC standards cover communications protocols and data exchange formats and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa."

Builds upon HF RFID (13.56mHz)

Usually restricted to ~10cm range (closeness = inherent security?)

Some NFC devices can operate in P2P mode or be emulated

Readers

PROXMARK 3

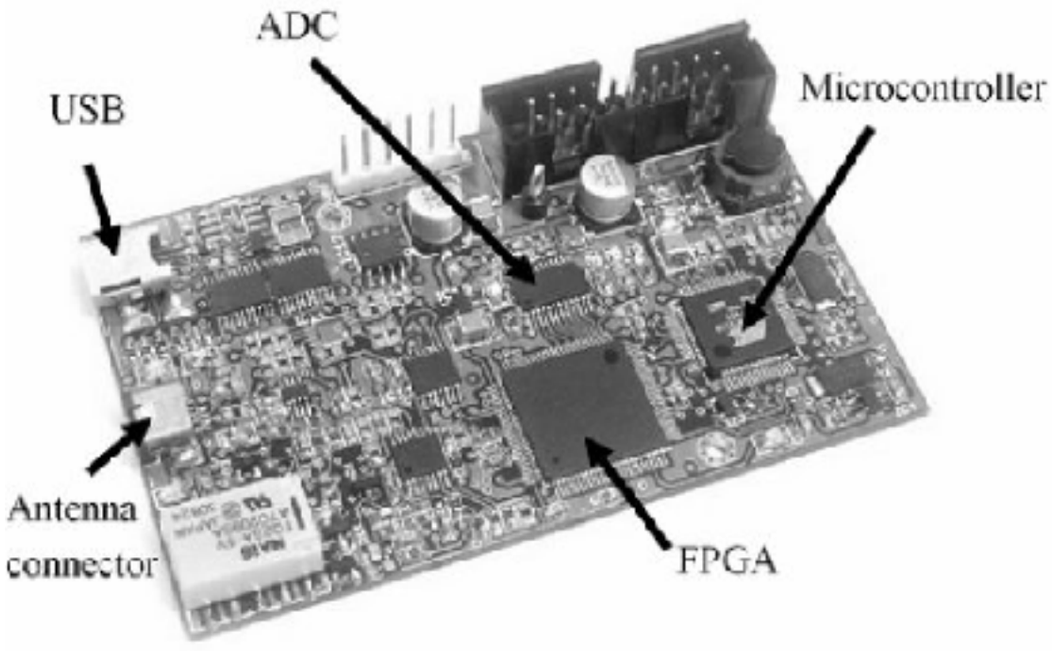
ACR122U

Android SmartPhones

Proxmark 3

Fully OpenSource: https://github.com/Proxmark/proxmark3

Support for LF and HF



FPGA + ARM for modulation/demodulation and coding/decoding

Active Community: http://www.proxmark.org/forum/index.php

Costs 200-300eur

ACR122U

NFC Tools: http://nfc-tools.org/index.php?title=ACR122

Basic NFC USB READER

Only HF (13.56mHz)

Support for a few specs (iso 14443 a/b, MIFARE, FeliCa...)

Cost ~20eur

OpenSource libraries (like LibNFC [https://github.com/nfc-tools/libnfc])

Compatible with Android

Android SmartPhones

No Cost if you already have one…

NXP PN5xx vs. BCM2079x Chips

Play Store Recommended Apps:

NFC Tag Info

https://play.google.com/store/apps/details?id=at.mroland.android.apps.nfctaginfo&hl=en

UltraManager Lite

https://play.google.com/store/apps/details?id=io.github.darkjoker.ultramanagerlite&hl=en

MIFARE DESFire EV1 NFC Tool

https://play.google.com/store/apps/details?id=com.skjolberg.mifare.desfiretool&hl=en

Credit Card Reader NFC (EMV)

https://play.google.com/store/apps/details?id=com.github.devnied.emvnfccard&hl=en

Real ID

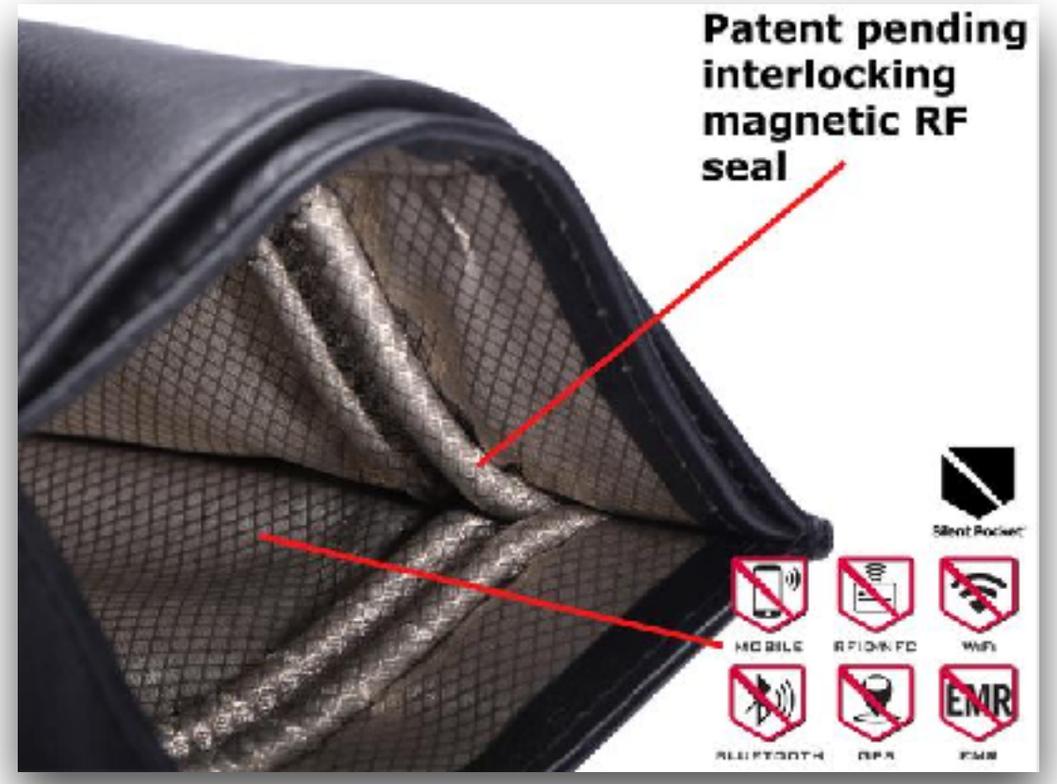
https://play.google.com/store/apps/details?id=nl.innovalor.nfciddocshowcase&hl=en

“Arrimar Cebolleta” Attack

https://www.trustwave.com/Resources/SpiderLabs-Blog/Proxmark-3,-now-with-more-Android/

https://eternal-todo.com/es/blog/give-me-credit-card-nfc-way

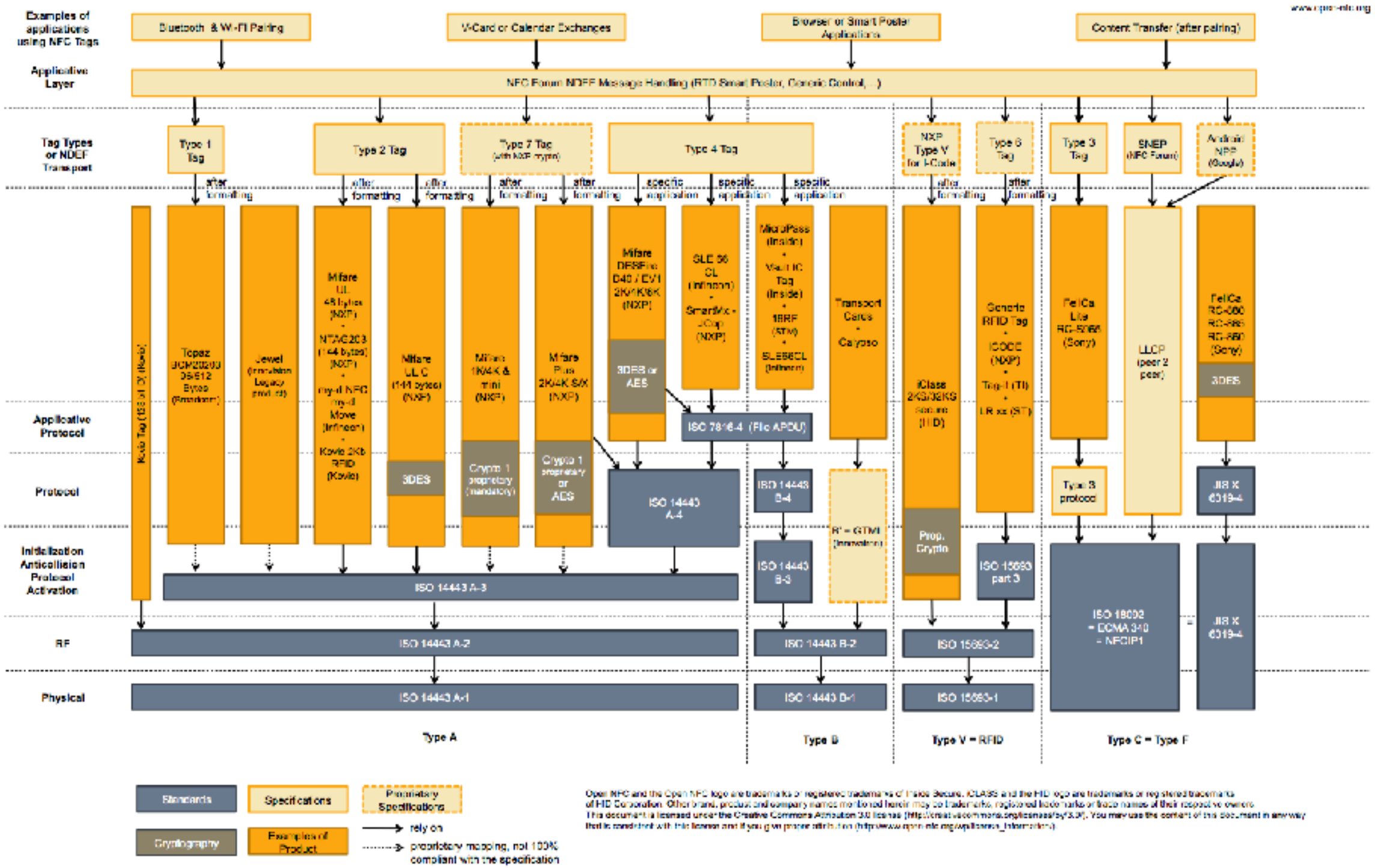
Faraday Cage Wallets



Level 1

Level 9999

The NFC zoo



Mirror: http://vwzq.net/download/nfczoo.pdf

ISO/IEC-14443 A/B Specification

(most common in Europe and USA)

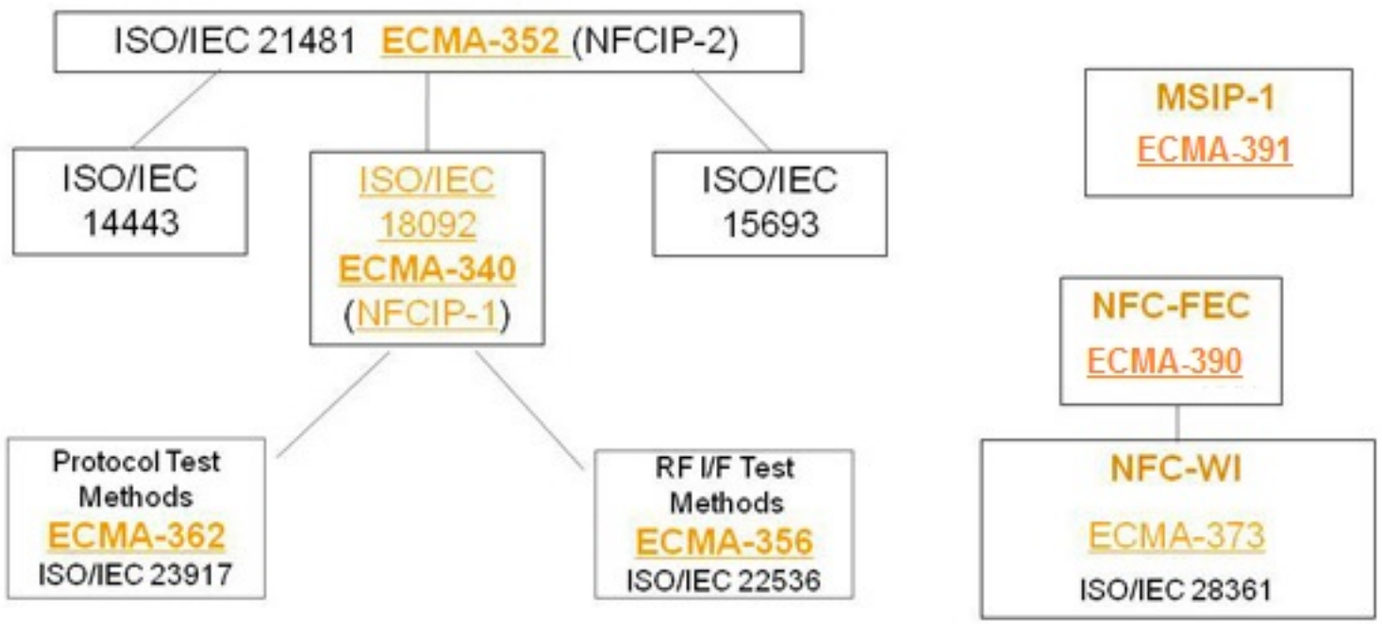
- ISO/IEC 14443-1:2016 Part 1: Physical characteristics
- ISO/IEC 14443-2:2016 Part 2: Radio frequency power and signal interface
- ISO/IEC 14443-3:2016 Part 3: Initialization and anticollision
- ISO/IEC 14443-4:2016 Part 4: Transmission protocol

ISO specs are not free, by default…

A FEW MORE...

- ISO/IEC 15693 (VICINITY CARDS)
- FELICA (BY SONY WAS PROPOSED FOR ISO-14443 TYPE C)
- LOTS OF PROPRIETARY PROTOCOLS (LIKE NXPS)

NFCIP (OR ECMA 352 & 340)



NFC protocol arrangement

OSINT

(Open Source Intelligence)

First step of an investigation is data gathering:

- DataSheets (http://www.datasheetcatalog.com/)
- Specifications
- Patents (https://www.google.com/patents)
- News (photos)
- …

Google Dorks (e.g.: filetype:pdf) can help a lot!

You would be surprised of how much info there is exposed on manufacturers web pages (DataSheets, internal docs, screenshots of internal tools, software…)

Let's see some tags

- HID Prox
- MIFARE Ultralight
- MIFARE Classic
- MIFARE Desfire EV1

LF Tags

predominant in identification and access control

Lower read range and communication speed

Low-cost and low-security with simple UIDs or KEYs

Some Examples:

- EM4x
- ATA55xx/T55xx
- HID Prox
- HiTag2 (used by cars: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf)

Interesting: t5577 have multiple parameters allowing to emulate/simulate other tags

RFID hacking with the Proxmark 3:

https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/

Tag Example: HID Prox

HID Prox TAG ID: 020f58dd777

HID cards store 44 bits (11 hex digits) (start always with "02" for Customer Code)

Support for many data formats. The only question is which one…
This seems to be Quadrakey (by Honeywell), which is equivalent to Wiegand 34-bit (N10002):

Wiegand Data (34-bit output from reader)

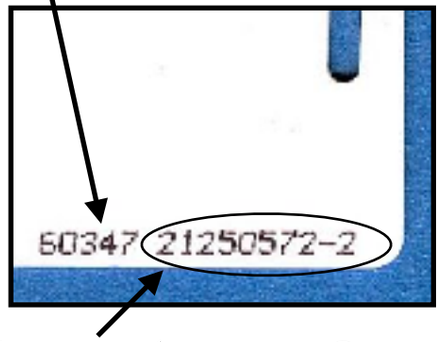
34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
OP	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	OP
OP	Facility Code (0-65535)																Card Number (0-65535)																OP

OP=Even Parity (bits 18-33) OP=Odd Parity (bits 2-17)

(Online Calculator: https://www.brivo.com/support/card-calculator)

00000010	00	0011110101100 0110	1110101110111011	1
Customer	Padding	Facility	Card Number	P
02		31430	60347	

Only secret



Sales Order Number (next to Card Number)

Data formats: http://www.proxmark.org/files/proxclone.com/iCLASS%20Wiegand%20Data%20Formats_26-37.pdf

Tag Example: Ultralight

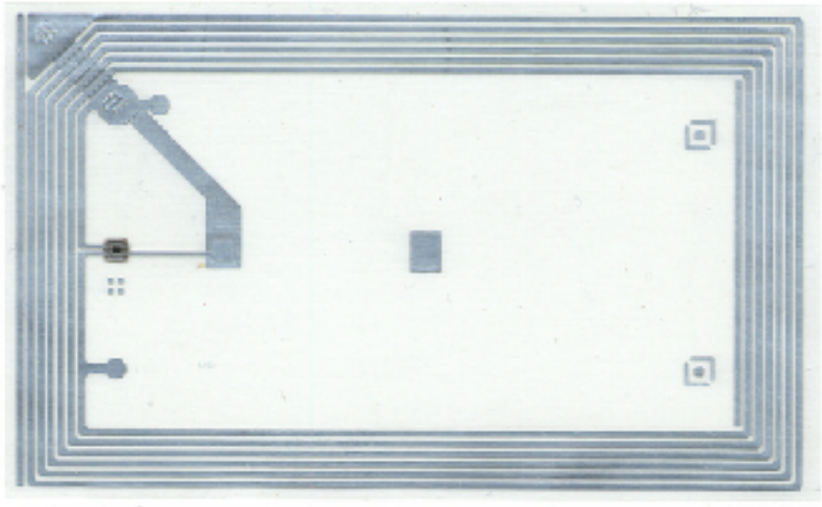
HF Low-Cost

No crypto

Built in top of ISO-14443-3A

512 bits of memory (16 pages x 4 bytes):

- 80 bits manufacturer + 16 bits config
- 32 OTP bits + 384 bits for r/w data



Exercise: Read MIFARE Ultralight Specification

MF0ICU1

MIFARE Ultralight contactless single-ticket IC

Rev. 3.9 — 23 July 2014 Product data sheet
028639 COMPANY PUBLIC

1. General description

The MIFARE MF0ICU1 has been developed by NXP Semiconductors to be used in a contactless smart ticket or smart card in combination with a Proximity Coupling Devices (PCD) in accordance with ISO/IEC 14443 A (see Ref. 1). It is intended for use as single trip or limited use tickets in public transportation networks, loyalty cards or day passes for events as a replacement for conventional ticketing solutions such as paper tickets, magnetic stripe tickets or coins.

Tag Example: Ultralight

Online vs. Offline systems:

- on: Higher control and security
- off: More expensive installation, not always possible

No data stored -> no need to reverse engineer

Possible to clone UID by using special tags (~10 EUR)

also possible to emulate (and brute force)…

Tag Example: Ultralight

2001: MIFARE Ultralight introduced
https://www.nxp.com/docs/en/data-sheet/MF0ICU1.pdf

2008: MIFARE Ultralight C (support for Triple DES Authentication)
https://www.nxp.com/docs/en/data-sheet/MF0ICU2.pdf

2012: MIFARE Ultralight EV1 (backwards compatible with extra security)
https://www.nxp.com/docs/en/data-sheet/MF0ULX1.pdf

Tag Example: Classic

Introduced in 1994 (NXP previously known as Philips)

Communication layer based on ISO 14443

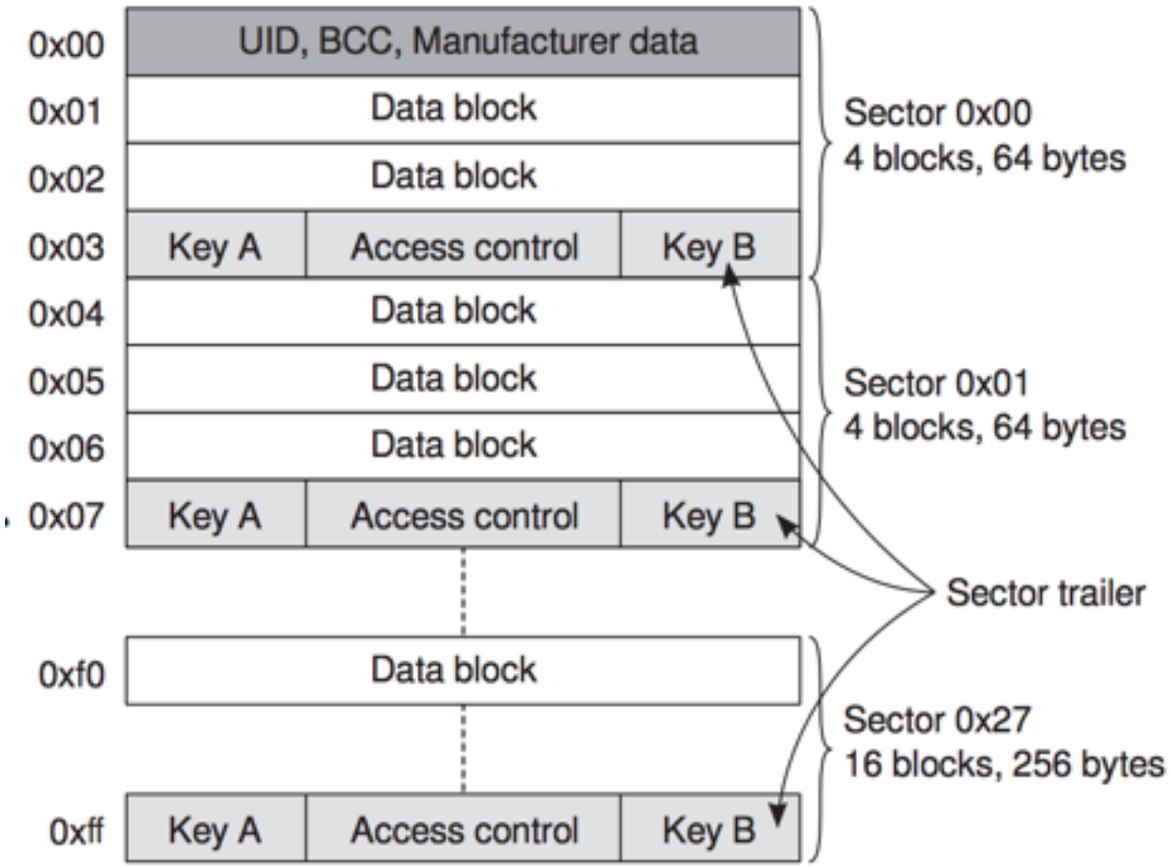
Proprietary crypto (security by obscurity always ends badly...)

CRYPTO1 by NXP Semiconductors

More than 3.5 billion cards produced

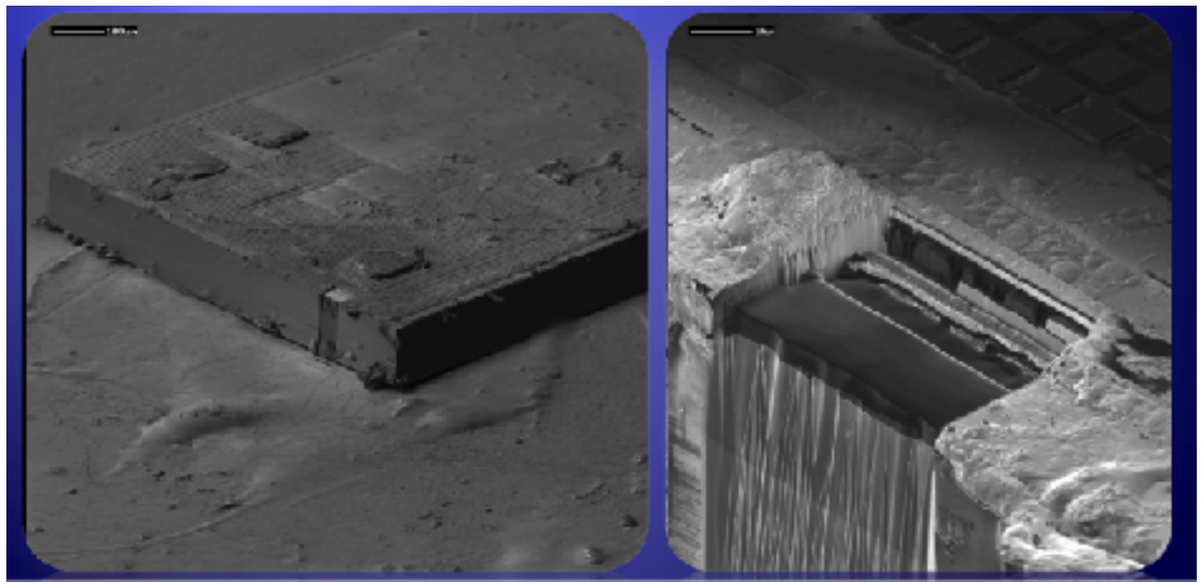
1K version: 1024 bytes split into 16 sectors
4K version: 4096 bytes split into 40 sectors

Keys: 6 bytes
Access control: 3 bits
Data block: 16 bytes



Tag Example: Classic

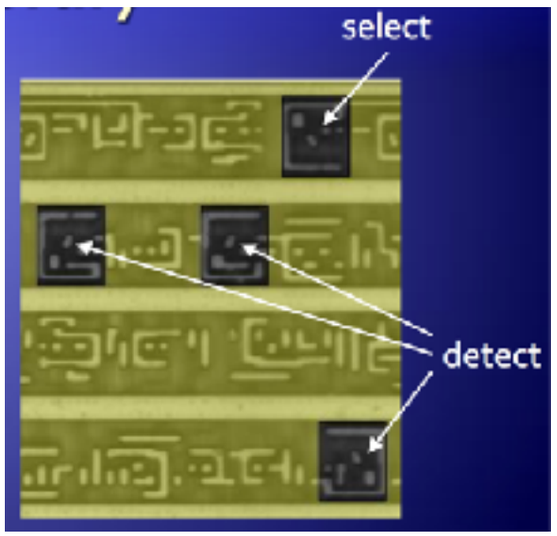
Dec 2007 - Nohl et al. partial RE in CCC (https://www.youtube.com/watch?v=QJyxUvMGLro)

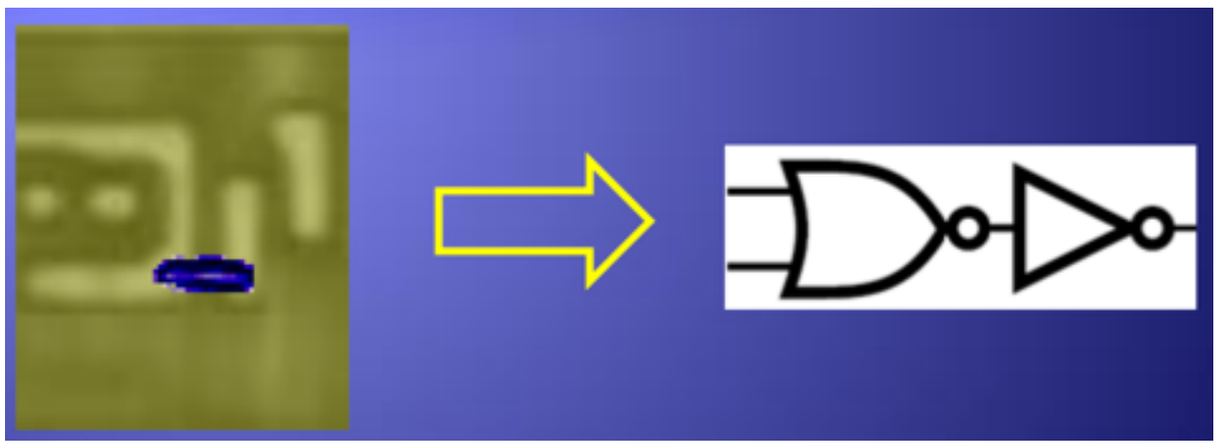


Crypto 1: Stream Cipher

weakness on pseudorandom generator, the 32-bit nonces used for authentication have only 16 bits of entropy

More: http://www.cs.ru.nl/~flaviog/publications/Attack.MIFARE.pdf





(from: https://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html)

Tag Example: Classic

March 2008 - Research group from Radbond University completely Reverse Engineered the Crypto-1 cipher

Paper: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.437.2501&rep=rep1&type=pdf
Slides: http://www.sos.cs.ru.nl/applications/rfid/2008-esorics-slides.pdf

Card only attack! (critical)

NXP tried to stop the disclosure... Court decides to allow publication

Oct 2008 - Crypto-1 implementation is open sourced

MIFARE Plus announced as a drop-in replacement based on 128-bit AES

new "hardened" cards have been released in and around 2011 (MIFARE Classic EV1), not susceptible to previous known card-only attacks

2015: Card Only attacks against hardened MIFARE Classic: http://cs.ru.nl/~rverdult/Ciphertext-only_Cryptanalysis_on_Hardened_Mifare_Classic_Cards-CCS_2015.pdf

Tag Example: Classic

Public Attack Implementations:

- Nested Attack: mfoc

  Src: https://github.com/nfc-tools/mfoc
  Slides: https://nethemba.com/resources/mifare-classic-slides.pdf

- Dark-side Attack: mfcuk

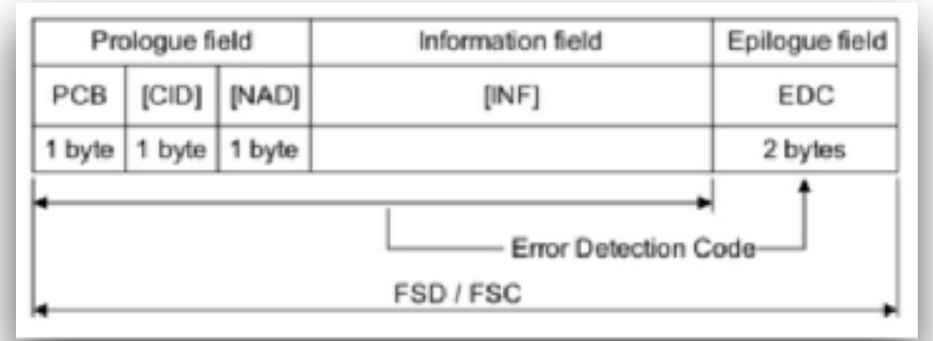
  Src: https://github.com/nfc-tools/mfcuk
  Paper: https://eprint.iacr.org/2009/137.pdf

Tag Example: DESFire

Introduced in 2002

- 3DES with 4KB of storage
- AES (2, 4 or 8KB; see MIFARE DESFire EV1)

Protocol compliant with ISO-14443-4



Supports "native commands" AND ISO-7816 APDUs
(Smart Card Application Protocol Data Unit)

Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

Response APDU	
Body (optional)	Trailer (required)
Data Field	SW1 SW2

Tag Example: DESFire

Wide Set of Commands: `SELECT, READ/WRITE BINARY, GET DATA, GET CHALLENGE, GENERATE APP CRYPTOGRAM...`

Used to interact with Smart Card Applications and the FileSystem

Name	Definition
Application	28 in each card. Distinguish by 3-byte AID.
File	16 files each application.
Key	14 keys each application. For access control purpose.

Select Application (or Directory File) by its AID (3 bytes)

List File IDs and Key Settings

3 access levels: PICC or Card level, application level and file level

Keys also used for establishing a session key and encrypt communication

More details: https://brage.bibsys.no/xmlui/bitstream/handle/11250/262988/742061_FULLTEXT01.pdf (section 3)

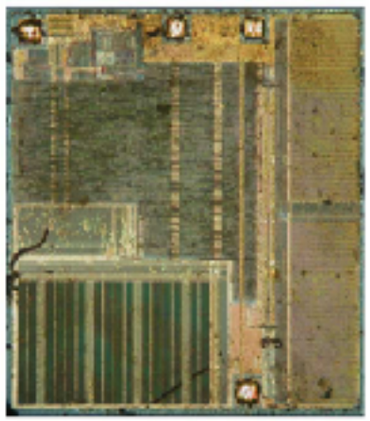
Tag Example: DESFire

2011 - MIFARE DESFire (MF3ICD40) vulnerable to Correlation Power Analysis side-channel attack

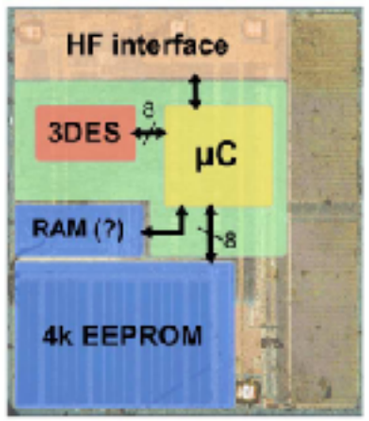
Breaking mifare DESFire MF3ICD40: power analysis and templates in the real world
http://www.emsec.rub.de/media/crypto/veroeffentlichungen/2011/10/10/desfire_2011_extended_1.pdf

"The full key recovery attack takes ~250,000 traces, which require about 7 hours to collect."

NXP's response: https://www.mifare.net/update-on-mifare-desfire-mf3icd40/

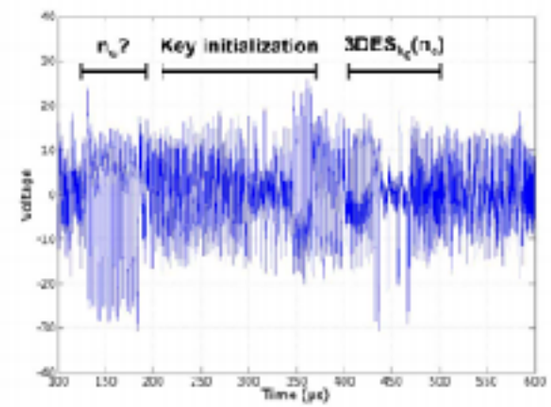


(a) IC photo

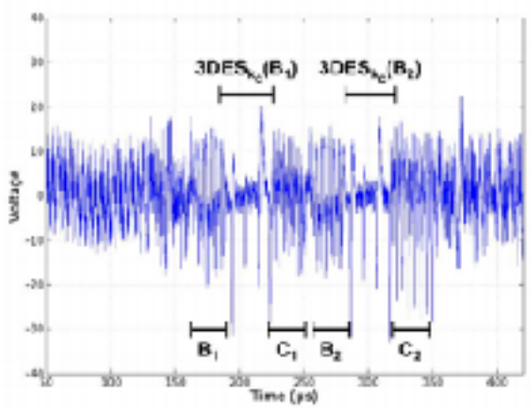


(b) Hypothetical structure

Fig. 4: The DESFire MF3ICD40 IC



(a) Step 1



(b) Step 2

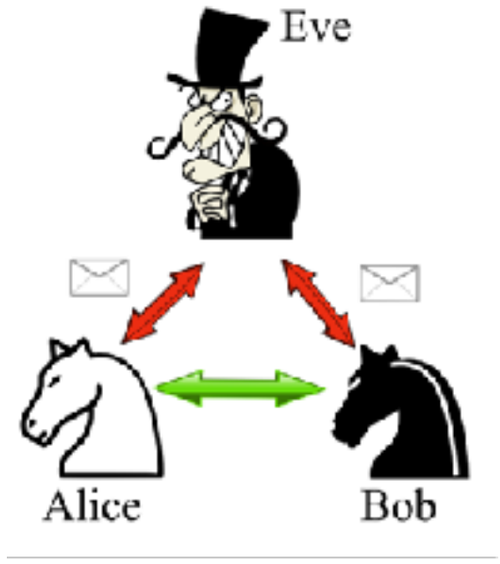
Fig. 5: Annotated traces during the authentication protocol (after analog processing)

Discontinued in favour of DESFire EV1 (introduced in 2008 Common Criteria EAL 4+)

Tag Example: DESFire

No known attacks against DESFire EV1, only a recent study:
2017 - "Bias in the MIFARE DESFire EV1 TRNG" by D Hurley-Smith

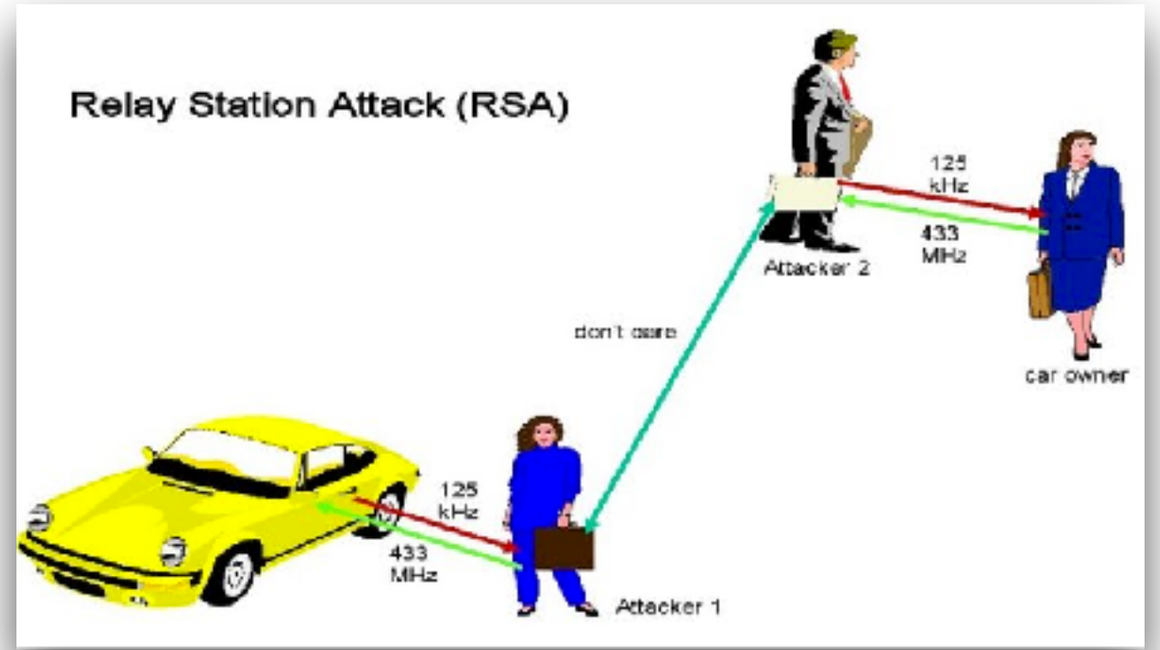
Relay Attack = violates the "closeness" assumption
(Masther thesis on DESFire Ev1 relay: https://brage.bibsys.no/xmlui/bitstream/handle/11250/262988/742061_FULLTEXT01.pdf)

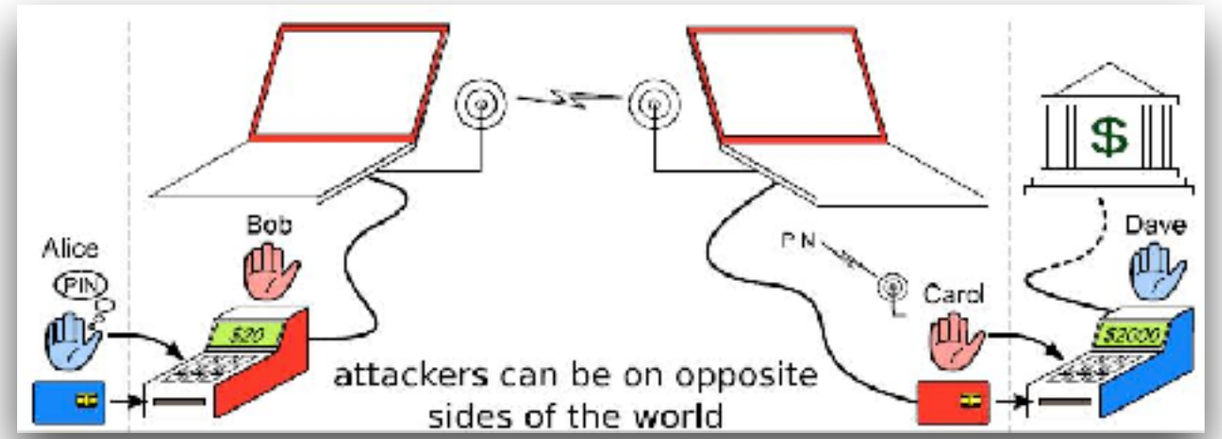


John Conway (1976) relay of a correspondence chess game

MIFARE DESFire EV2 introduced in 2016 with a proximity check

Relay Attacks





NFC relay attacks with Android mobile devices

http://vwzq.net/relaynfc/

(https://www.youtube.com/watch?v=qMQc_snB_yE)

Mitigation - Distance Bounding Protocols (establish bounds based on timing delays)

Interesting Links

NFC Glossary: https://www.nfc-research.at/index.php@id=40.html

RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication

Proxmark 3 forum: http://www.proxmark.org/forum/index.php

RFIDIDIOt (Python lib): http://rfidiot.org/

Chasing Cars: Keyless Entry System Attacks https://conference.hitb.org/hitbseconf2017ams/sessions/chasing-cars-keyless-entry-system-attacks/

A few more not so RFID...

OpenSesame: http://samy.pl/opensesame/

Injecting RDS-TMC Traffic Information Signals: https://github.com/abarisani/abarisani.github.io/tree/master/research/rds (video: https://www.youtube.com/watch?v=xgGgRKi1CGo)