# A holló meg a róka... meg a garázs

Veres-Szentkirályi András
vsza@silentsignal.hu

Silent Signal
szakmai délután
2012-06-21

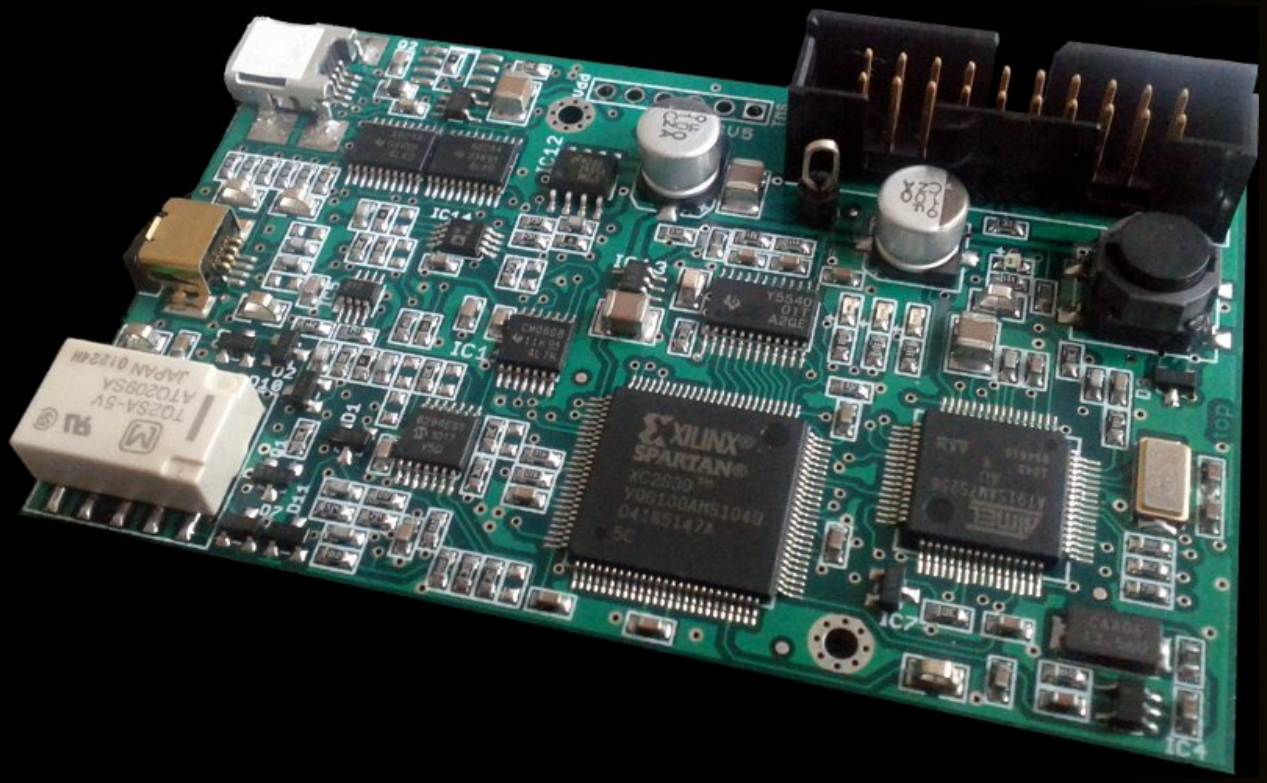
# Rendhagyó bemutatkozás

**Committed Changes** 555 - 531 of 555 Older ›

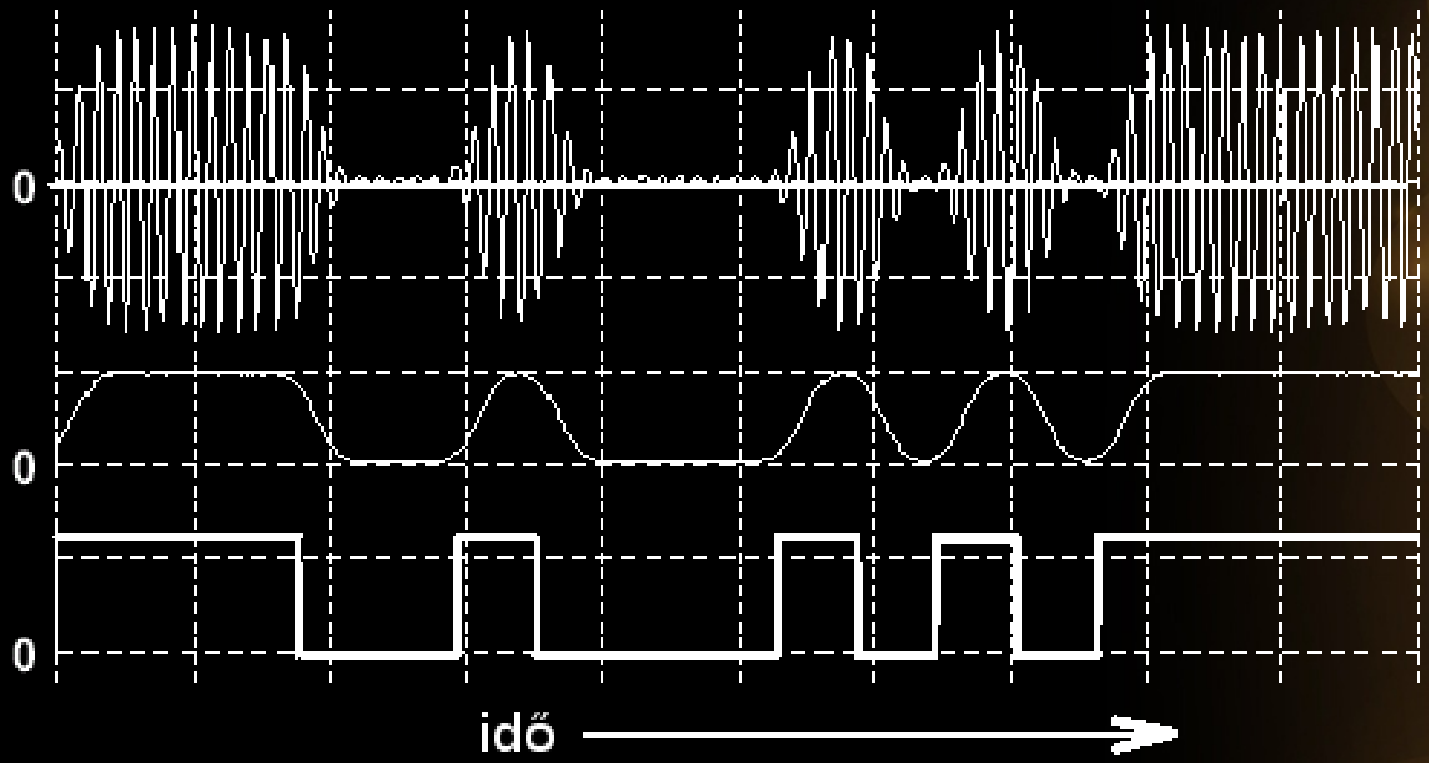
| Rev | Scores | Commit log message | Date | Author |
|---|---|---|---|---|
| r555 | | Commented out unused, set but never read variables (cause build to fail if warnings treated as errors) | Jun 12 (5 days ago) | GooglePlus@YoungJul... |
| r554 | | initialize graph cursors to avoid crashing (issue 21) | Jun 7, 2012 | dn337t@gmail.com |
| r553 | | Fixed markup (missing }}}) on wiki page Antennas | Jun 7, 2012 | dn337t@gmail.com |
| r552 | | Updated commands to reflect current ones on wiki page RunningPM3 | Jun 7, 2012 | dn337t@gmail.com |
| r551 | | Updated commands and udev entry on wiki page RunningPM3 | Jun 7, 2012 | dn337t@gmail.com |
| r550 | | Updated commands to reflect current ones on wiki page TagOps | Jun 7, 2012 | dn337t@gmail.com |
| r549 | | use downloaded keyring directly to avoid polluting the user's | Jun 7, 2012 | dn337t@gmail.com |
| r548 | | use char instead of uint8_t to avoid warnings/casting | Jun 7, 2012 | dn337t@gmail.com |
| r547 | | replaced the getline which doesn't support by minGW on windows | May 31, 2012 | douniwan5788 |
| r546 | | Enhanced hf mf chk , add default key,support dic file and so on. modify hf mf mifare to automatically use an invalid key'nt try again. make some ... | May 29, 2012 | douniwan5788 |
| r545 | | removed redundant Dbprintfs from SnoopIso1443a (issue 25) | May 29, 2012 | dn337t@gmail.com |
| r544 | | typofix in install-gnuarm4 script | May 29, 2012 | dn337t@gmail.com |
| r543 | | optimized loop in MifareNested (issue 36) | May 29, 2012 | dn337t@gmail.com |
| r542 | | fixed assignment vs. equals operator (issue 35) | May 29, 2012 | dn337t@gmail.com |
| r541 | | added CmdHF15CmdReadmulti using Adrian's second patch from issue 20 | May 29, 2012 | dn337t@gmail.com |
| r540 | | textual changes: error messages and comments by Andrian + attribution | May 29, 2012 | dn337t@gmail.com |
| r539 | | added head comments on CmdHF15Cmd{Read,Write} using Adrian's second patch from issue 20 | May 29, 2012 | dn337t@gmail.com |
| r538 | | clarification in 'hf 15 cmd write' message using Adrian's second patch from issue 20 | May 29, 2012 | dn337t@gmail.com |
| r537 | | implemented output of received octets in 'hf 15 cmd raw' | May 18, 2012 | dn337t@gmail.com |
| r536 | | added 'hf 15 cmd sysinfo' using Adrian's second patch from issue 20 | May 18, 2012 | dn337t@gmail.com |
| r535 | | typofix in prepareHF15Cmd comment based on Adrian's second patch from issue 20 | May 18, 2012 | dn337t@gmail.com |
| r534 | | fixed offset in 'hf 15 cmd read' to avoid losing the first octet/byte | May 18, 2012 | dn337t@gmail.com |
| r533 | | boolean fix in 'hf 15 cmd read' using Adrian's second patch from issue 20 | May 18, 2012 | dn337t@gmail.com |
| r532 | | typofixes in ISO15693 getUID head comment | May 18, 2012 | dn337t@gmail.com |
| r531 | | extended ISO 15693 UID map using Adrian's second patch from issue 20 | May 17, 2012 | dn337t@gmail.com |

555 - 531 of 555 Older ›

# Proxmark3 – „A Radio Frequency IDentification Tool”



# 1. kitérő: Amplitude-shift keying (ASK)




Forrás: University of Rhode Island
Department Of Electrical and Computer Engineering

`http://www.ele.uri.edu/Courses/ele436/`

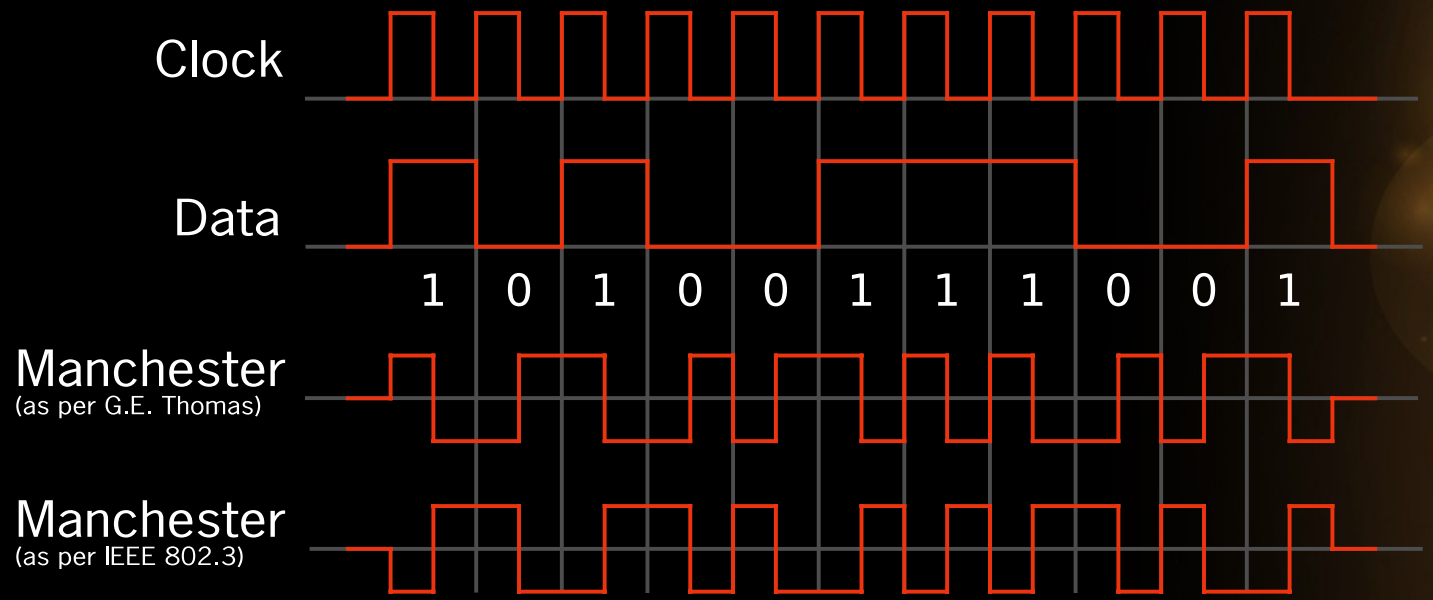
# 1. demo: egyszerű forgalomvisszajátszás

- alacsonyfrekvenciás RFID kulcstartó „megvilágítása”
- vivőfrekvencia mintavételezése (`lf read`)
- adatok PC-re vitele (`data samples 2000`)
- adatok vizualizálása (`data plot`)
- ASK demoduláció (`data askdemod 1`)
- kapott jel visszajátszása (`lf sim`)

# 1. demo tanulságai

- az alacsonyfrekvenciás RFID kulcstartók „buták”
- elegendő egy másodperc az adatgyűjtéshez
- nem szükséges a (teljes) protokoll ismerete

# 2. kitérő: Manchester-kódolás




Forrás: Wikipedia

https://en.wikipedia.org/wiki/Manchester_code

# 2. demo: forgalomelemzés

- alacsonyfrekvenciás RFID kulcstartó „megvilágítása”
- vivőfrekvencia mintavételezése (`lf read`)
- adatok PC-re vitele (`data samples 4000`)
- adatok vizualizálása (`data plot`)
- korrelációkeresés (`data autocorr 4000`)
- üzenet- és bithossz meghatározása (kurzorvonalak)
- ASK demoduláció (`data askdemod 1`)
- Manchester-demoduláció (`data mandemod`)
- nyomtatott azonosító „kibányászása”

# 2. demo tanulságai

- a protokollok „nem túl összetettek”
- árulkodók a feliratok – elég egy fénykép?

# 3. demo: Manchester-modulált jel visszajátszása

- alacsonyfrekvenciás RFID kulcstartó „megvilágítása”
- vivőfrekvencia mintavételezése (`lf read`)
- adatok PC-re vitele (`data samples 2600`)
- ASK demoduláció (`data askdemod 1`)
- Manchester-demoduláció (`data mandemod`)
- Ismétlődő jelsorozat formázása (`tr -d ' '`)
- Manchester-modulált jel visszajátszása (`lf simman`)

# 3. demo tanulságai

- analízist követően a tartalom módosítható
- a módosított adat visszajátszható
  - hardveres fuzzing
  - megszemélyesítés

# 3. kitérő: EM410x káryák

- Gyártó: EM Microeletronic
  - Swatch Group Electronics Systems
- Frekvencia: alacsony (125 vagy 134 kHz)
- Kapacitás: 64 bit
  - 9 bit fejléc
  - 4 bitenként sorparitás
  - 4 bit oszlopparitás
  - 1 stopbit
  - Hasznos adat: 8 + 32 bit

# 4. demo: EM410x kártya klónozása

- EM410x kártya „megvilágítása”
- vivőfrekvencia mintavételezése (`lf read h`)
- adatok PC-re vitele (`data samples 4000`)
- EM410x ID dekódolása (`lf em4x em410xread`)
- EM410x szimulátor indítása (`lf em4x em410xsim`)

# 4. demo tanulságai

- teljes protokoll stack visszafejthető
- bármilyen ID megszemélyesíthető
  - ha rá van nyomtatva, fényképről is
  - mekkora az entrópia? nyers erőnek ellenáll?

# Összefoglalás

- „kedvenc vesszőparipák”
  - nincs silver bullet (se ingyen ebéd)
  - biztonság vs. használhatóság
- Újdonság ez egyáltalán?
- biztonság a TCP/IP-n túl
  - GSM
  - TETRA
- Soha ne higgy a security by obscurity-ban!


Köszönöm a figyelmet!
Facebook
vsza@silentsignal.hu
web
e-mail
SILENT SIGNAL
VÉSZJELZÉS HELYETT...
WWW.SILENTSIGNAL.HU