An RFID skimming gate using higher harmonics

René Habraken, Peter Dolron, Erik Poll, Joeri de Ruiter

June 2015

Radboud University

Welcome!

RFID System Attacks:

An RFID skimming gate using higher harmonics

René Habraken

Electrical engineering
Techno Centre | High Energy Physics
Nijmegen, the Netherlands
r.habraken@science.ru.nl

Outline of the presentation

Case

- It is possible to communicate with an RFID card in the middle of 100 cm gate.

Goal

- Method
- Show skimming results

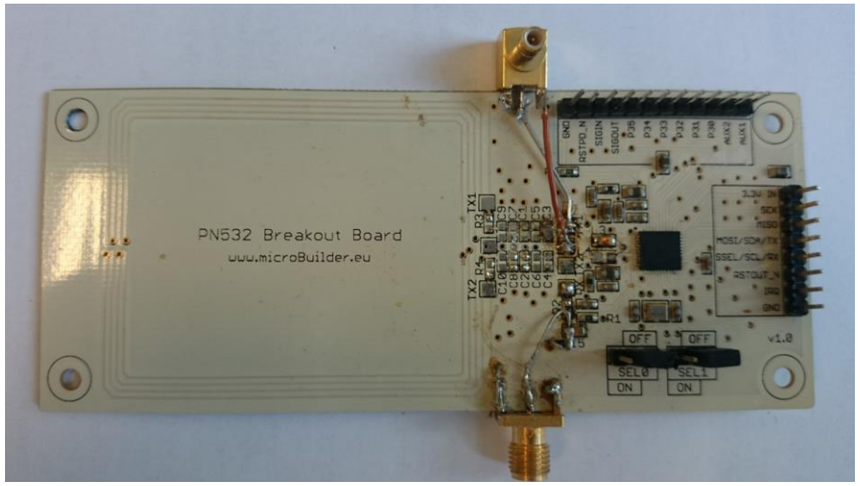
Terminology

- Reader
- Tag or card
- Communication
- Quality factor (q-factor)

Project boundaries

- ISO/IEC 14443, Type A and B
- Results are obtained without the use of digital signal processing

Modified reader, more power and a bigger antenna

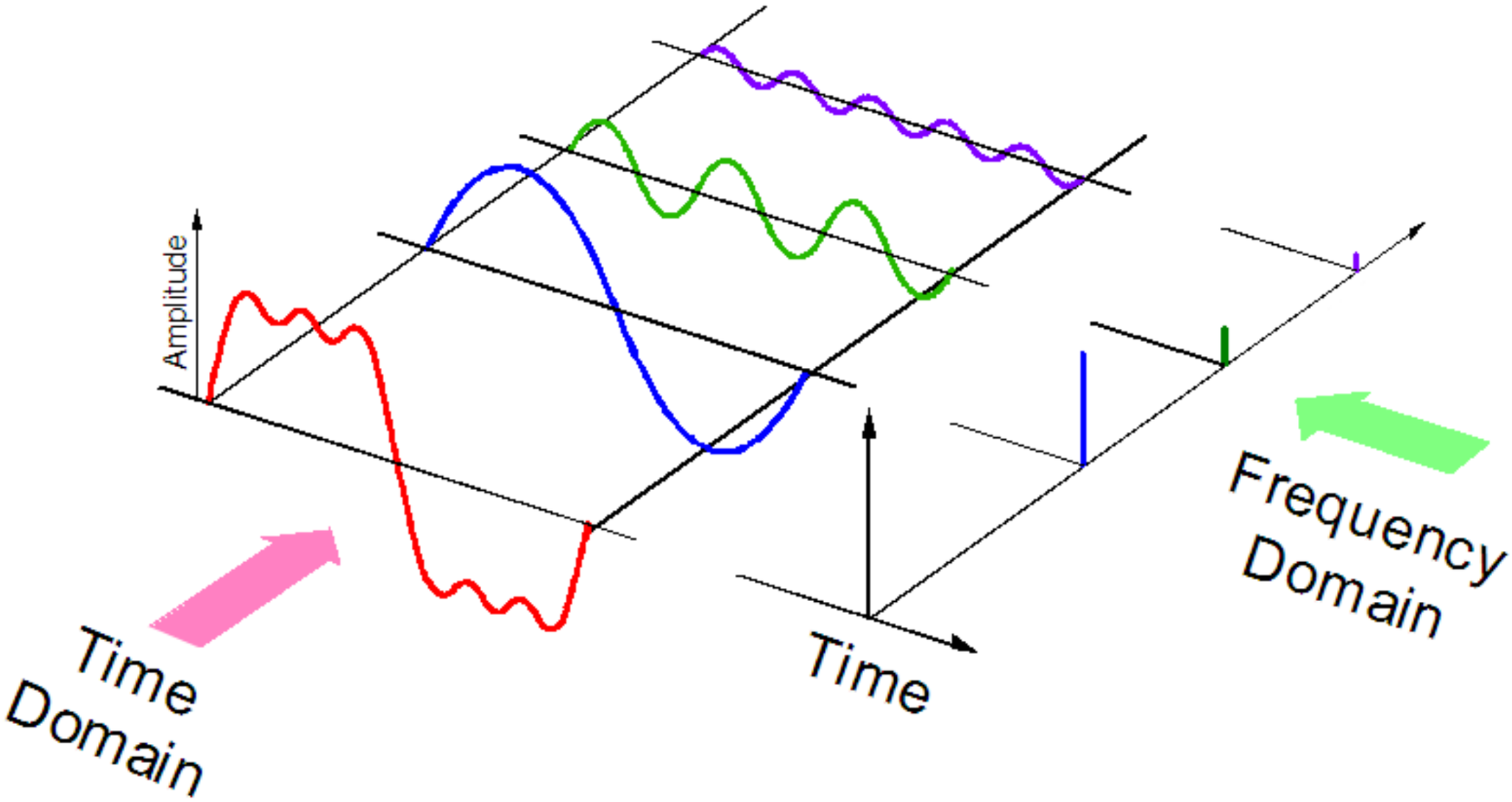


Reader

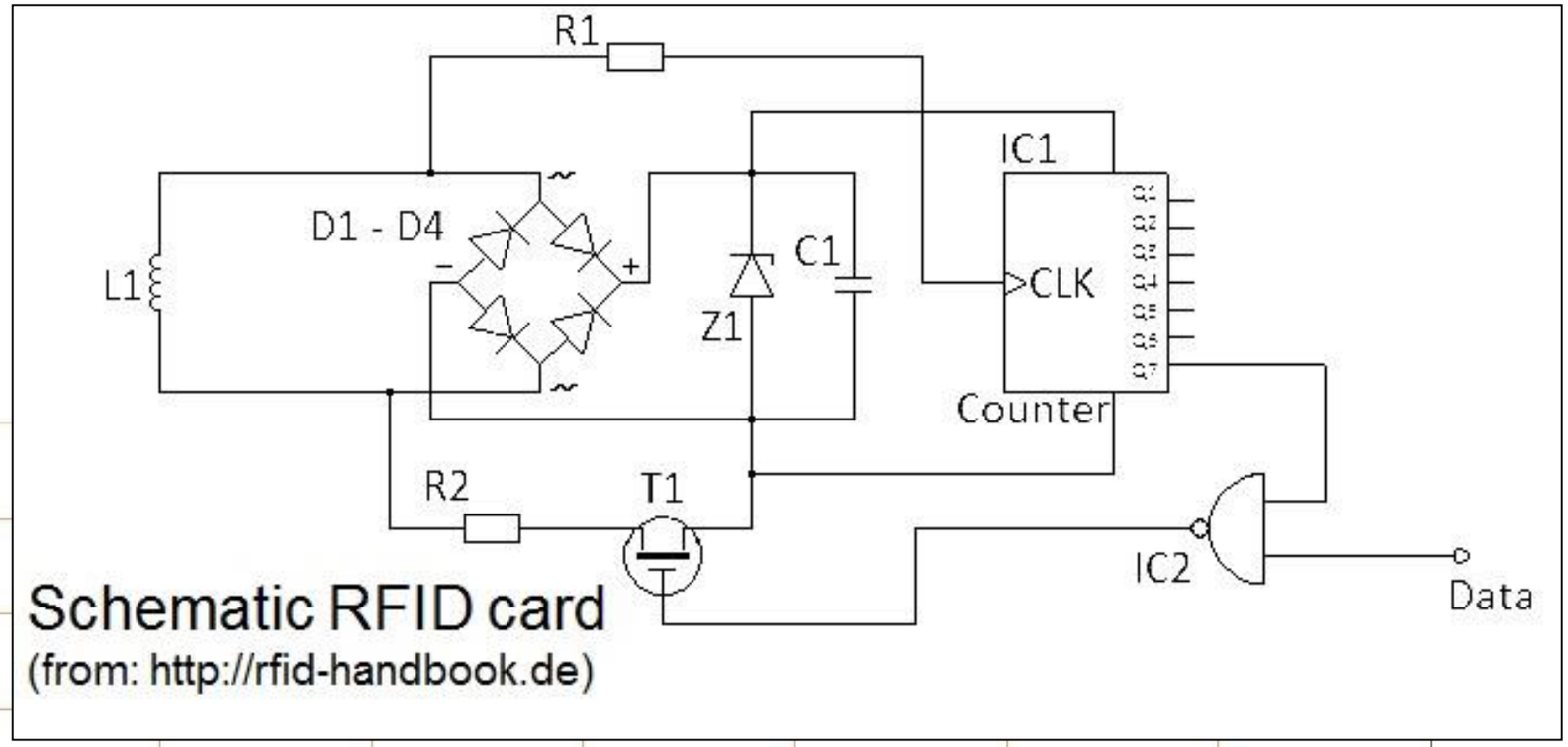
Max 100 W,
delivered by
two amplifiers

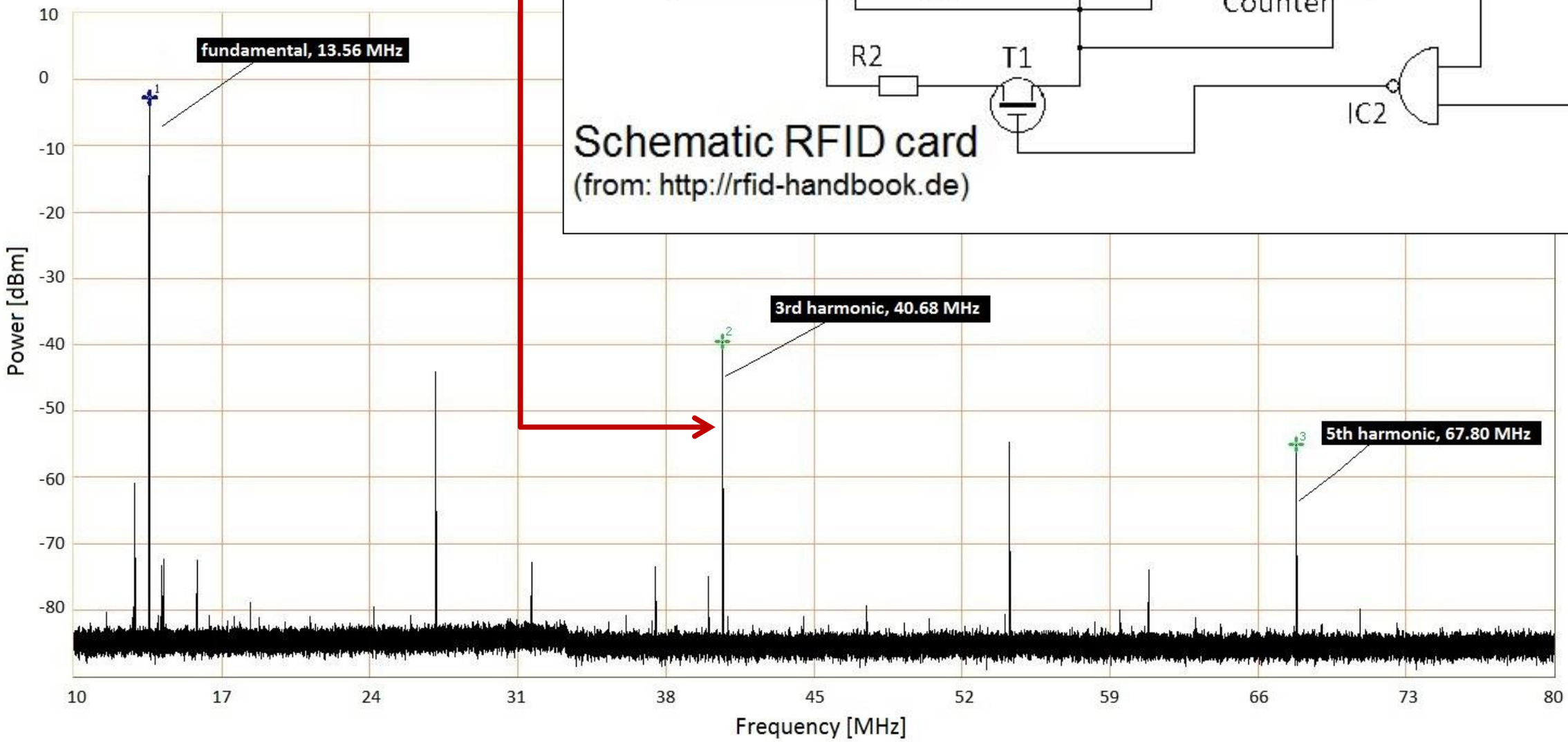
50 cm loop antenna

Time and frequency domain

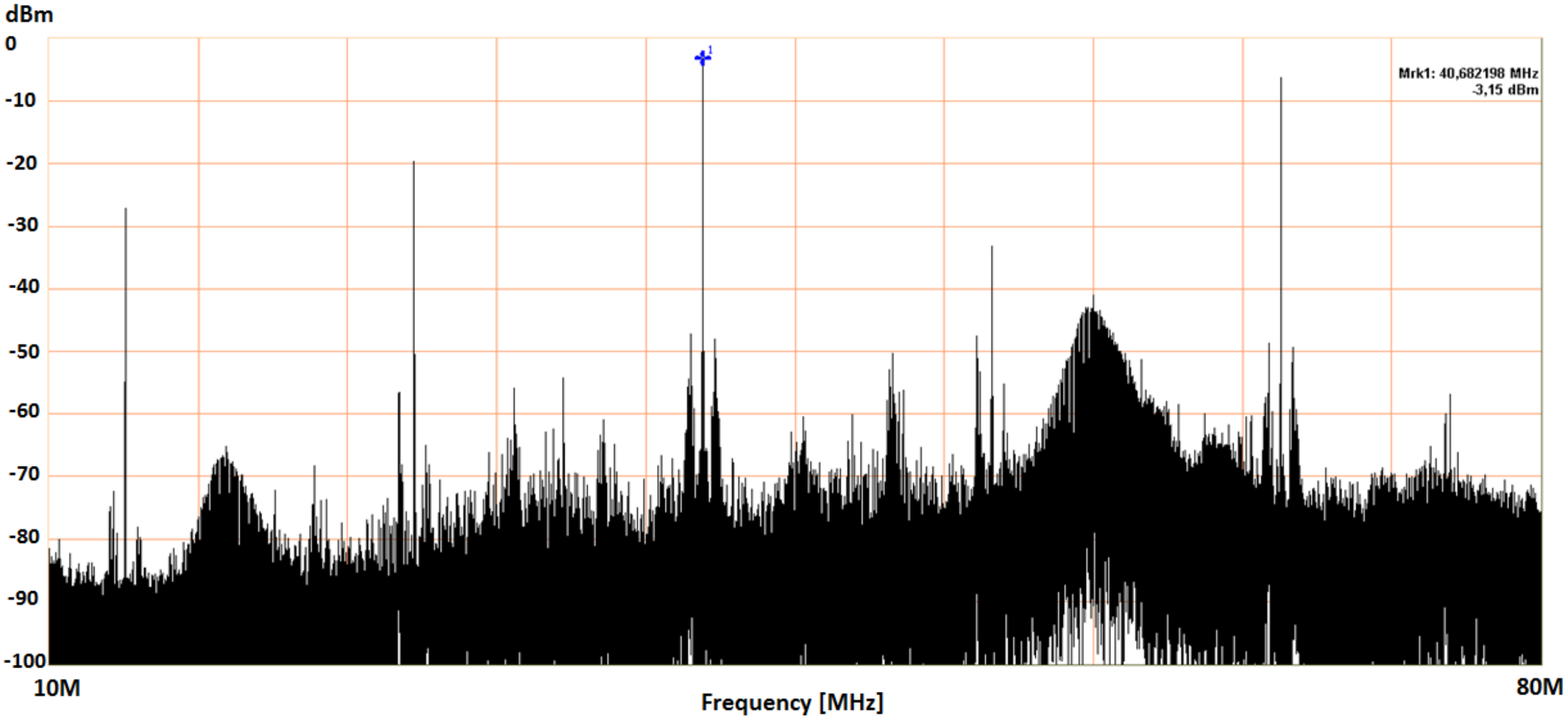


3rd harmonic
40.68 MHz

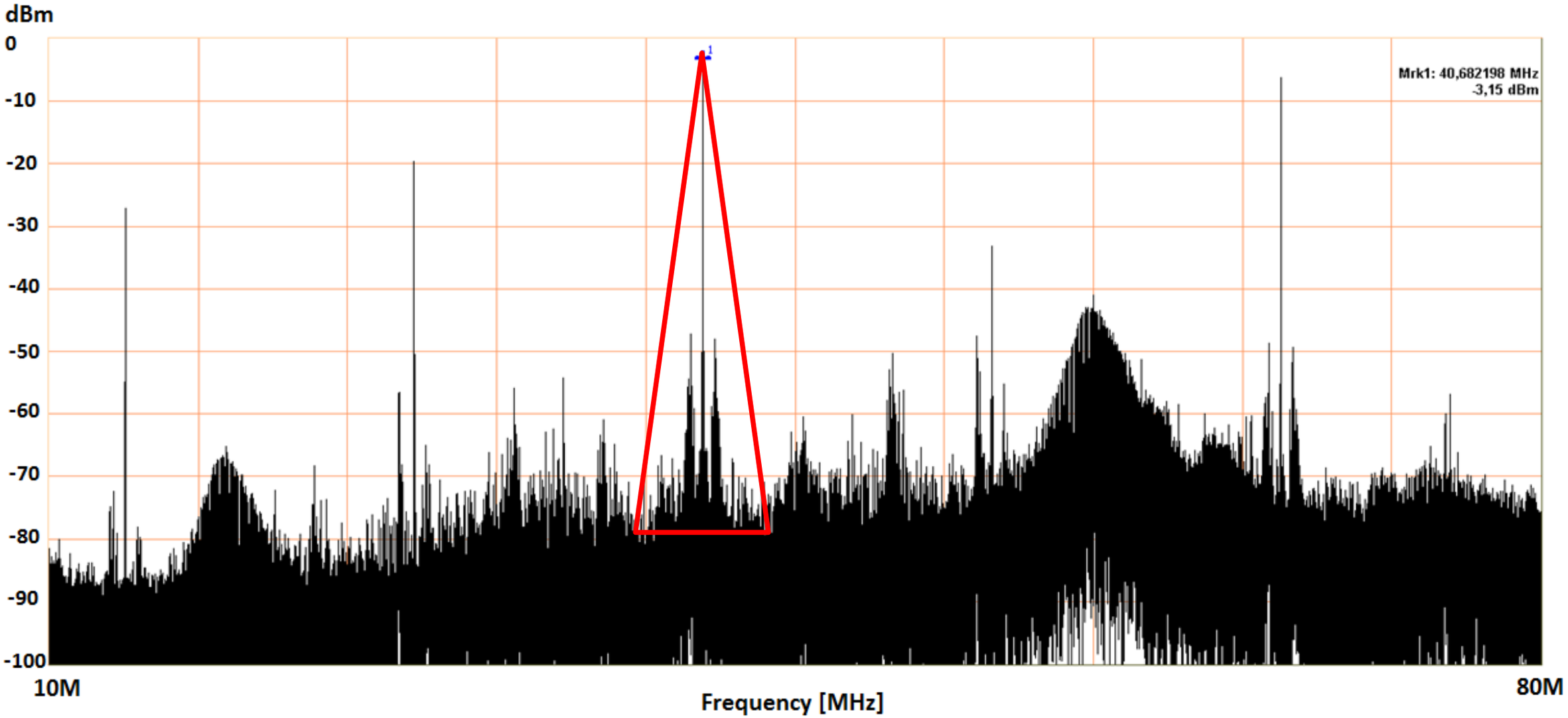




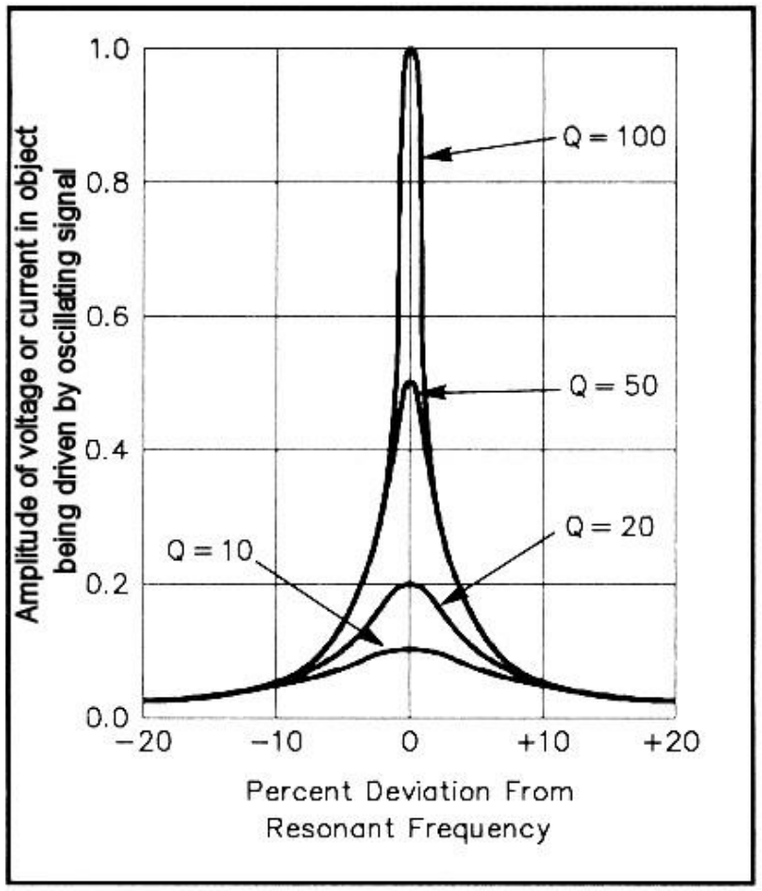
RFID Spectrum (13.56 MHz filtered)



Selective narrowband antenna



Quality factor antennas

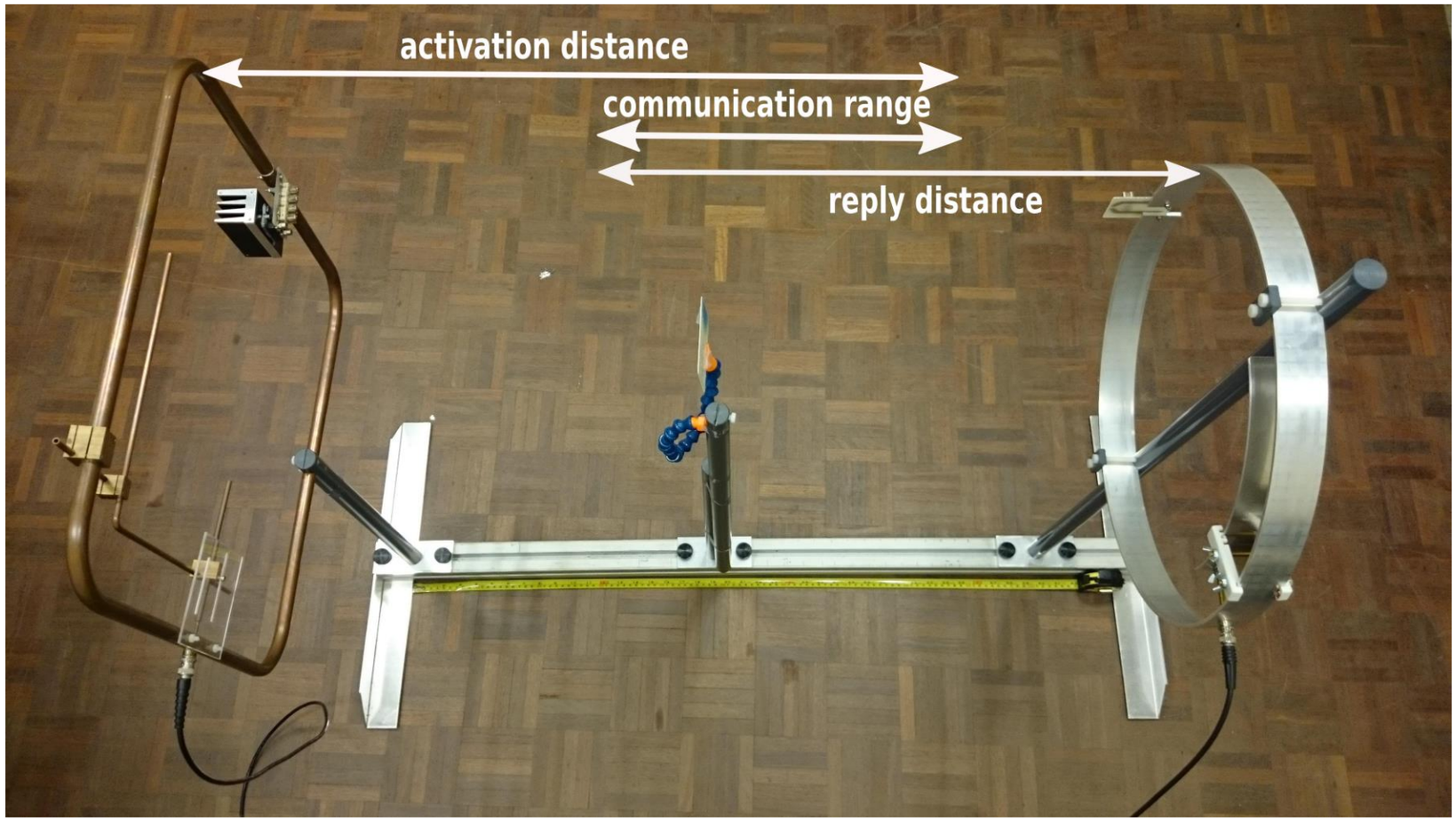


Specs receive antenna:

- Resonant at 40.68 MHz
- Inductance ≈ 1.3 uH
- Diameter = 46 cm
- Undamped, no damping resistor
- Gamma matching network

Q-factor
Activation antenna = 22
Receive antenna = 78

RFID skimming gate - results



Gate width [cm]	Power [W]	Activation distance [cm]	Range [cm]	Reply distance [cm]
100	80	50	< 5	50
90	18	75	< 5	20
70	18	60	50	60

Related work

- Kirschenbaum and Wool - How to Build a Low-Cost, Extended-Range RFID Skimmer, 2006.
  Using: a single 40 cm loop antenna.

- Hancke - Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens, 2011.
  Using: a 50 cm loop antenna for activation and an active magnetic field antenna for reception.

Comparison with related work

Kirschenbaum and Wool (2006)				
Gate width [cm]	**Power [W]**	**Activation distance [cm]**	**Range [cm]**	**Reply distance [cm]**
1 antenna	2.5	25	unknown	25

Hancke (2011)				
Gate width [cm]	**Power [W]**	**Activation distance [cm]**	**Range [cm]**	**Reply distance [cm]**
40	4	20	unknown	20
215	1	15	unknown	200

Our results (2015)				
Gate width [cm]	**Power [W]**	**Activation distance [cm]**	**Range [cm]**	**Reply distance [cm]**
100	80	50	< 5	50
90	18	75	< 5	20
70	18	60	50	60

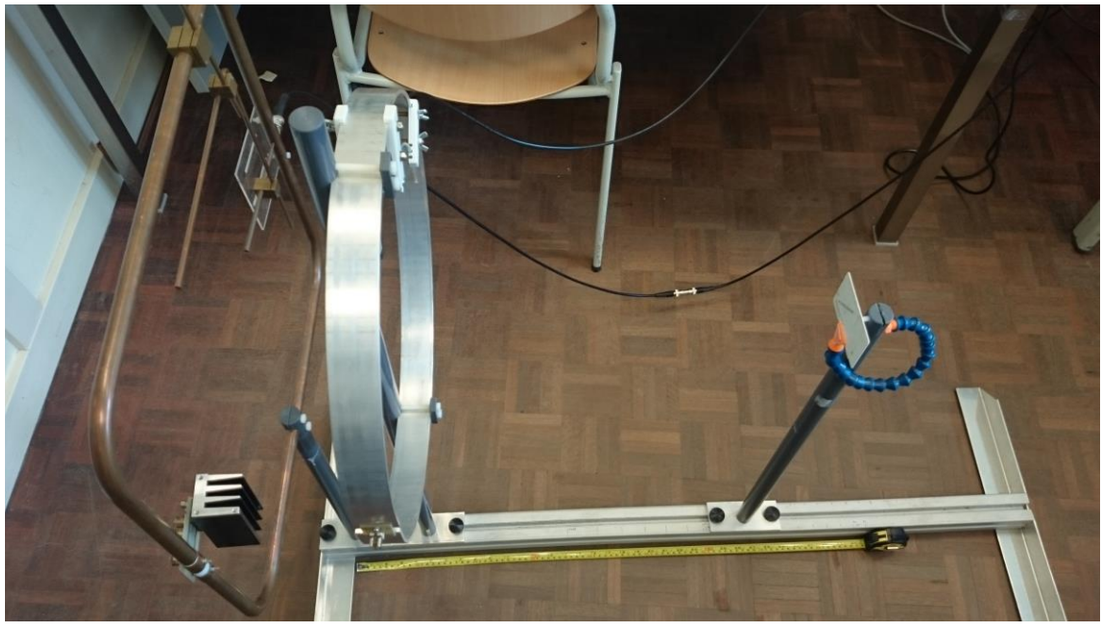
Other antenna arrangements

Add a resonant antenna (at 13.56MHz) behind the receive antenna.

- Gate width = 93 cm
- Receive antenna on 77 cm
- Communication range ≈ 60 cm

More compact solution

- Communication range ≈ 50 cm (from reception antenna)



Increased distance for ISO / IEC 14443 RFID communication

How?

- Use a bigger antenna and more power
- Add a second antenna with a high Q-factor resulting in narrowband reception

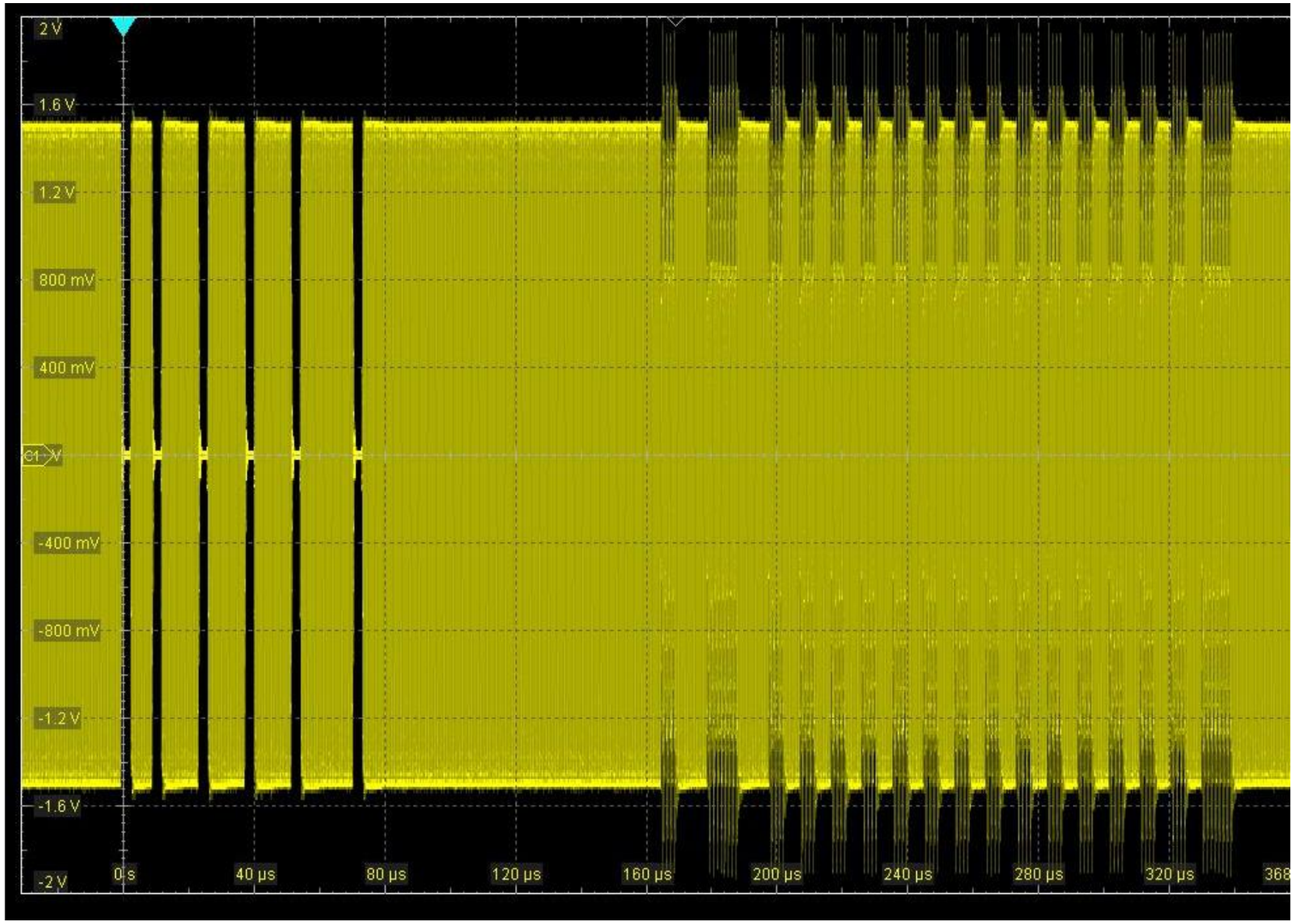
Resulting in:

- Separation of activation and reception signals in frequency domain

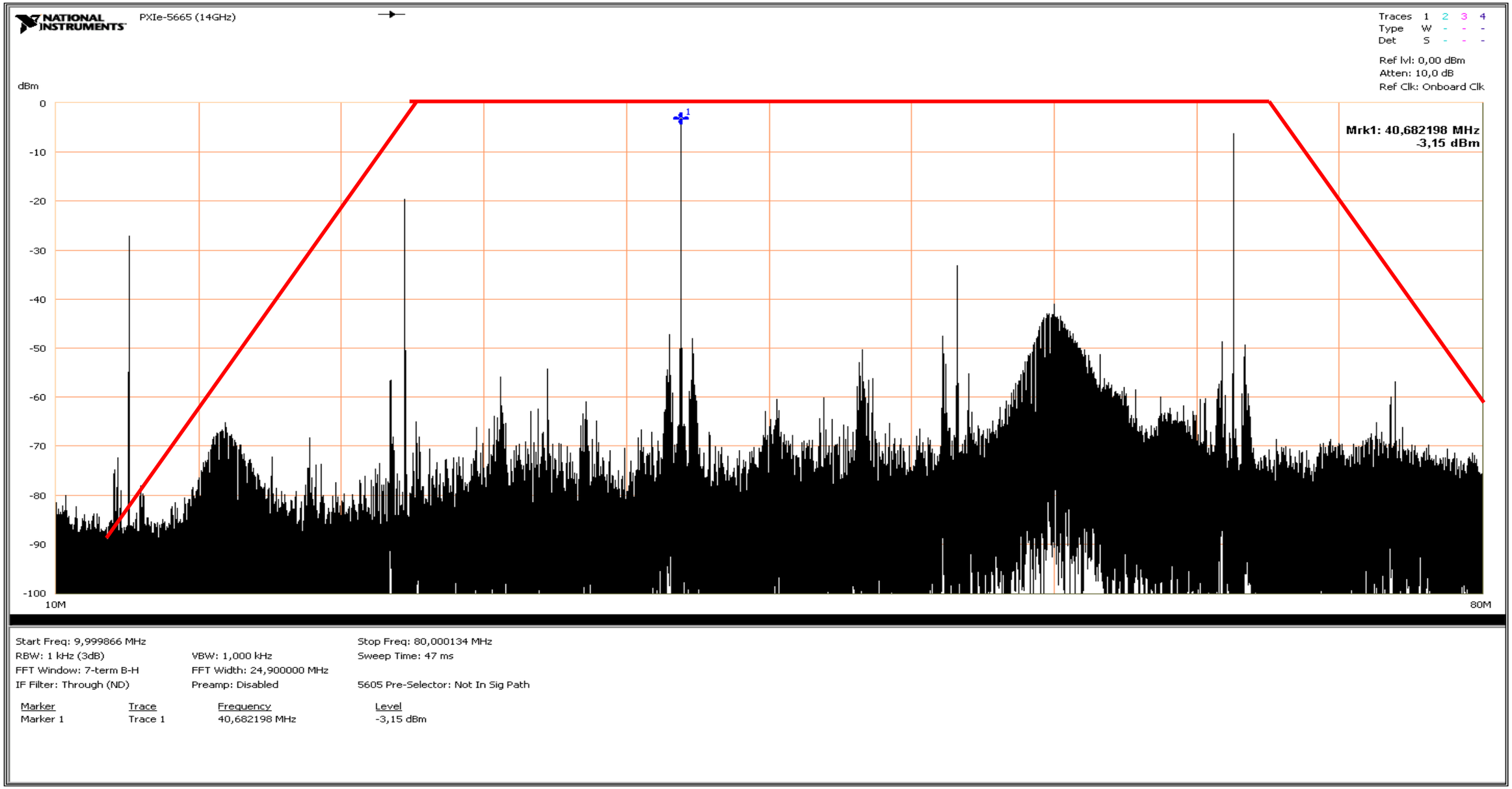
Questions / discussion

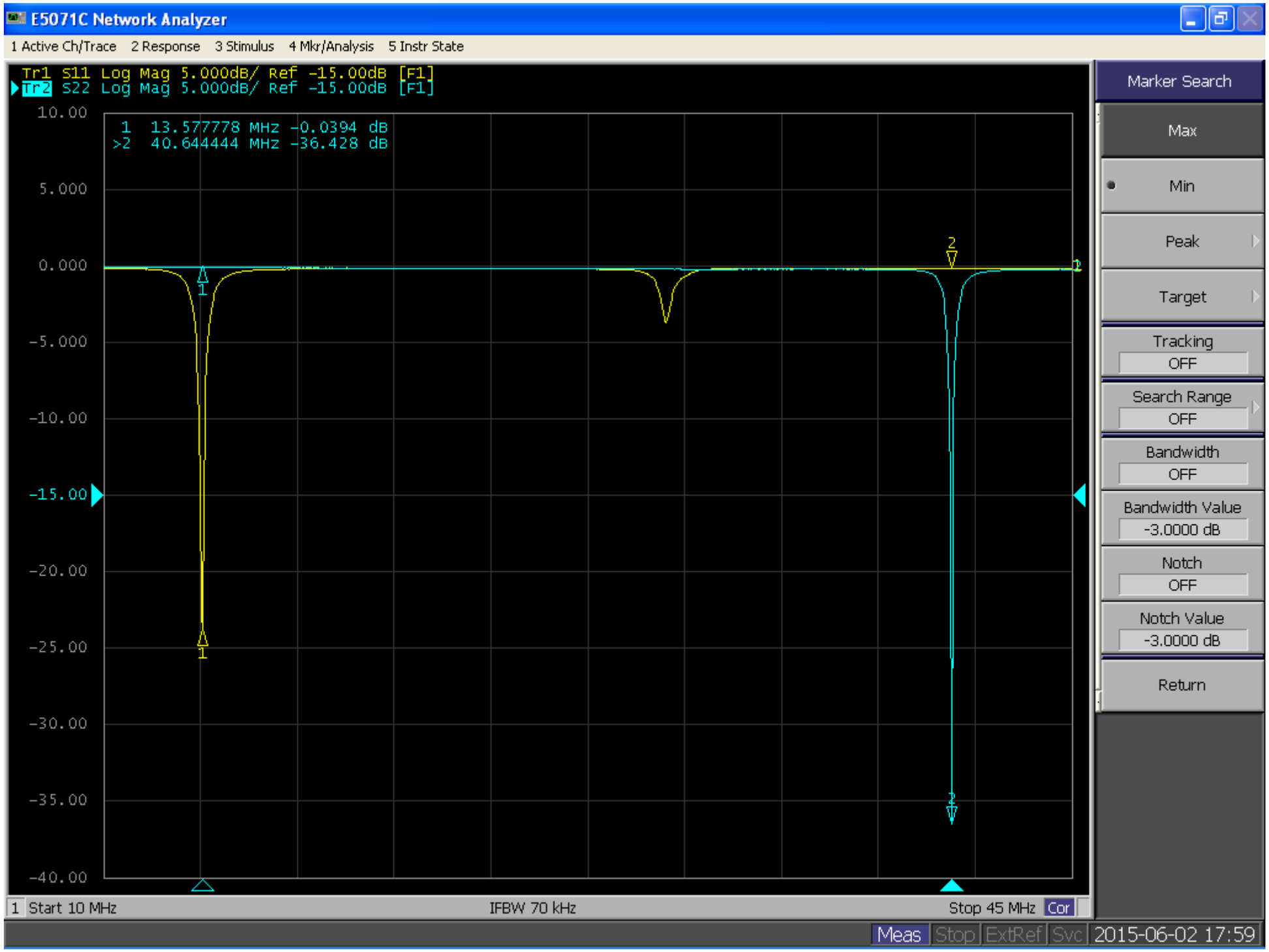
Radboud University

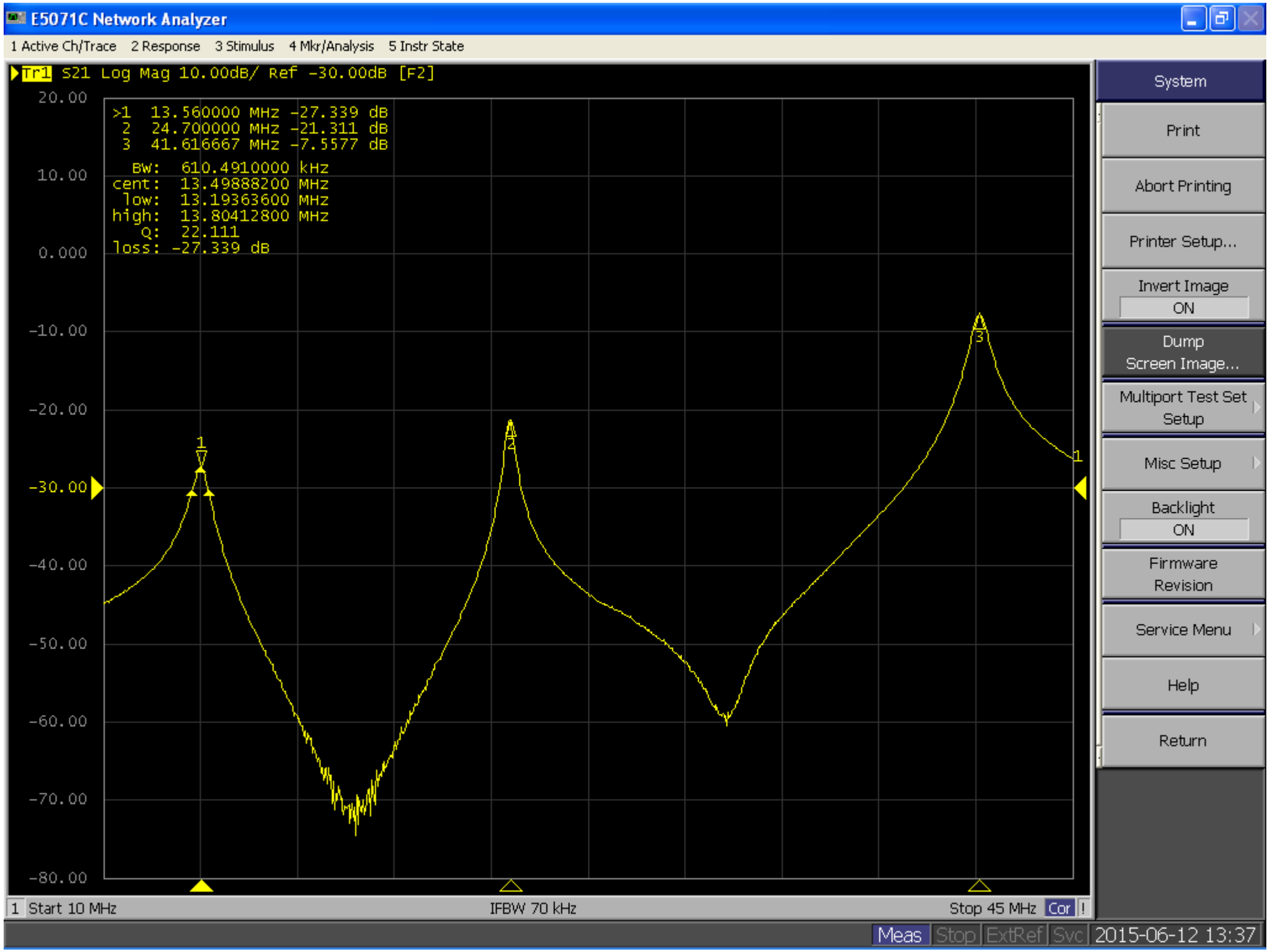
Activation distance and reply distance for skimming attacks



Sensitive broadband antenna




E5071C Network Analyzer
1 Active Ch/Trace 2 Response 3 Stimulus 4 Mkr/Analysis 5 Instr State
Tr1 S11 Log Mag 5.000dB/ Ref -15.00dB [F1]
Tr2 S22 Log Mag 5.000dB/ Ref -15.00dB [F1]
1 13.577778 MHz -0.0394 dB
>2 40.644444 MHz -36.428 dB
10.00
5.000
0.000
-5.000
-10.00
-15.00
-20.00
-25.00
-30.00
-35.00
-40.00
1 Start 10 MHz
IFBW 70 kHz
Stop 45 MHz
Cor
Marker Search
Max
Min
Peak
Target
Tracking
OFF
Search Range
OFF
Bandwidth
OFF
Bandwidth Value
-3.0000 dB
Notch
OFF
Notch Value
-3.0000 dB
Return
Meas
Stop
ExtRef
Svc
2015-06-02 17:59


E5071C Network Analyzer
1 Active Ch/Trace 2 Response 3 Stimulus 4 Mkr/Analysis 5 Instr State
Tr1 S21 Log Mag 10.00dB/ Ref -30.00dB [F2]
>1 13.560000 MHz -27.339 dB
2 24.700000 MHz -21.311 dB
3 41.616667 MHz -7.5577 dB
BW: 610.4910000 kHz
cent: 13.49888200 MHz
low: 13.19363600 MHz
high: 13.80412800 MHz
Q: 22.111
loss: -27.339 dB
20.00
10.00
0.000
-10.00
-20.00
-30.00
-40.00
-50.00
-60.00
-70.00
-80.00
1 Start 10 MHz
IFBW 70 kHz
Stop 45 MHz
Cor
System
Print
Abort Printing
Printer Setup...
Invert Image
ON
Dump Screen Image...
Multiport Test Set Setup
Misc Setup
Backlight
ON
Firmware Revision
Service Menu
Help
Return
Meas
Stop
ExtRef
Svc
2015-06-12 13:37

Comparison with related work

Kirschenbaum and Wool - How to Build a Low-Cost, Extended-Range RFID Skimmer, 2006 Using: single 40 cm antenna				
Gate width [cm]	**Power [W]**	**Activation distance [cm]**	**Range [cm]**	**Reply distance [cm]**
1 antenna	2.5	25	?	25

Hancke - Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens, 2011. Using: 50 cm loop antenna for activation and an active magnetic field antenna for reception.				
Gate width [cm]	**Power [W]**	**Activation distance [cm]**	**Range [cm]**	**Reply distance [cm]**
40	4	20	?	20
215	1	15	?	200

Our results:				
Gate width [cm]	**Power [W]**	**Activation distance [cm]**	**Range [cm]**	**Reply distance [cm]**
100	80	50	< 5	50
90	18	75	< 5	20
70	18	60	50	60