

RFID Penetration Tests

when the truth is stranger than fiction

Dr. Tomáš Rosa, tomas.rosa@rb.cz
Raiffeisenbank, a.s.

SmartCard Forum 2009

- Technology overview
- Physical layer of LF and HF bands
- The „Unique ID “ phenomenon
- Penetration tests – selected aspects
 - Where the security of transponders comes from
 - The LF band – Q5 takes it all
 - The HF band – MIFARE: two ways to use, both of them bad
- Conclusion

Radio Classification of Transponders

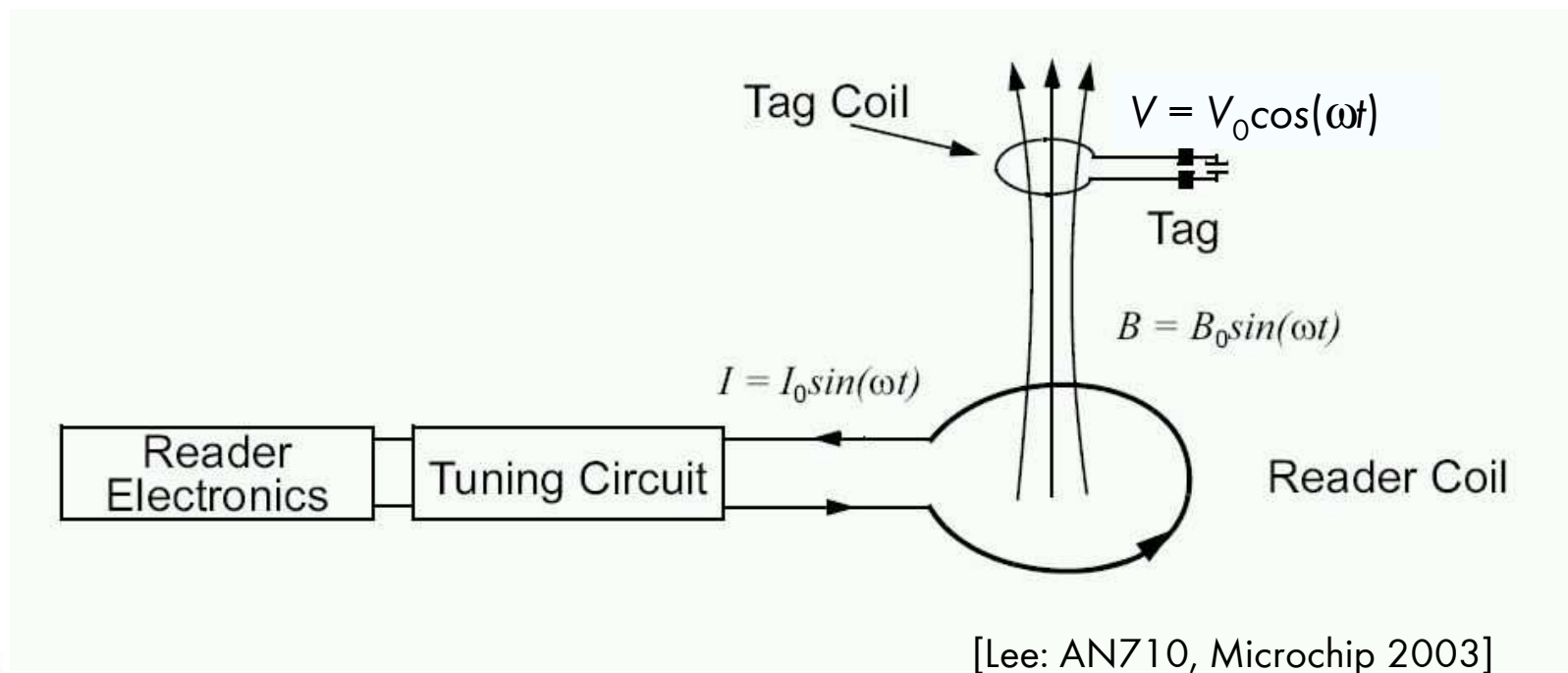
Frequency band	Sub-class	Typical sort	Typical deployment	Operation Distance (order)
LF (100 to 150 kHz)	-	Memory card	Access system, immobilizer, implant, loyalty card	cm to m(*)
HF (13.56 MHz)	Vicinity card	Memory card	Access system, skipass, loyalty card	cm to m
	Proximity card	Contact-less smartcard	Access system, payment card, e-passport	cm
UHF (430- 2450 MHz)	-	Memory card	Stock control	cm to 10s m

(*) rare configurations with low consumption read-only cards and high power, high dimension readers

LF and HF Band Physical Layer

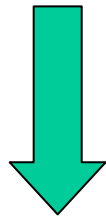
- Employs the behavior of so-called near field of the transmitter
 - Threshold is approx. $\lambda/2\pi$, $\lambda = 300/f$ [m, -, MHz]
 - Uses the well known effect of inductive coupling
 - Arrangement „terminal antenna – chip antenna“ can be viewed as a high frequency transformer

Feeding Up a LF/HF Transponder



Near Field Illustration

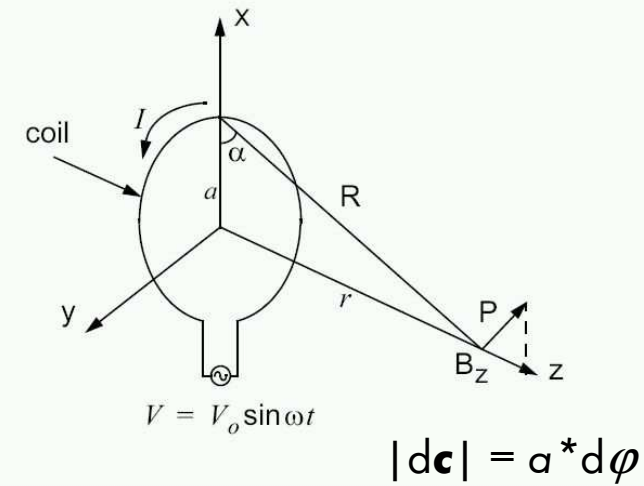
Biot-Savart: $d\mathbf{B} = \mu_0 N I (\mathbf{R} \times d\mathbf{c}) / (4\pi |\mathbf{R}|^3)$



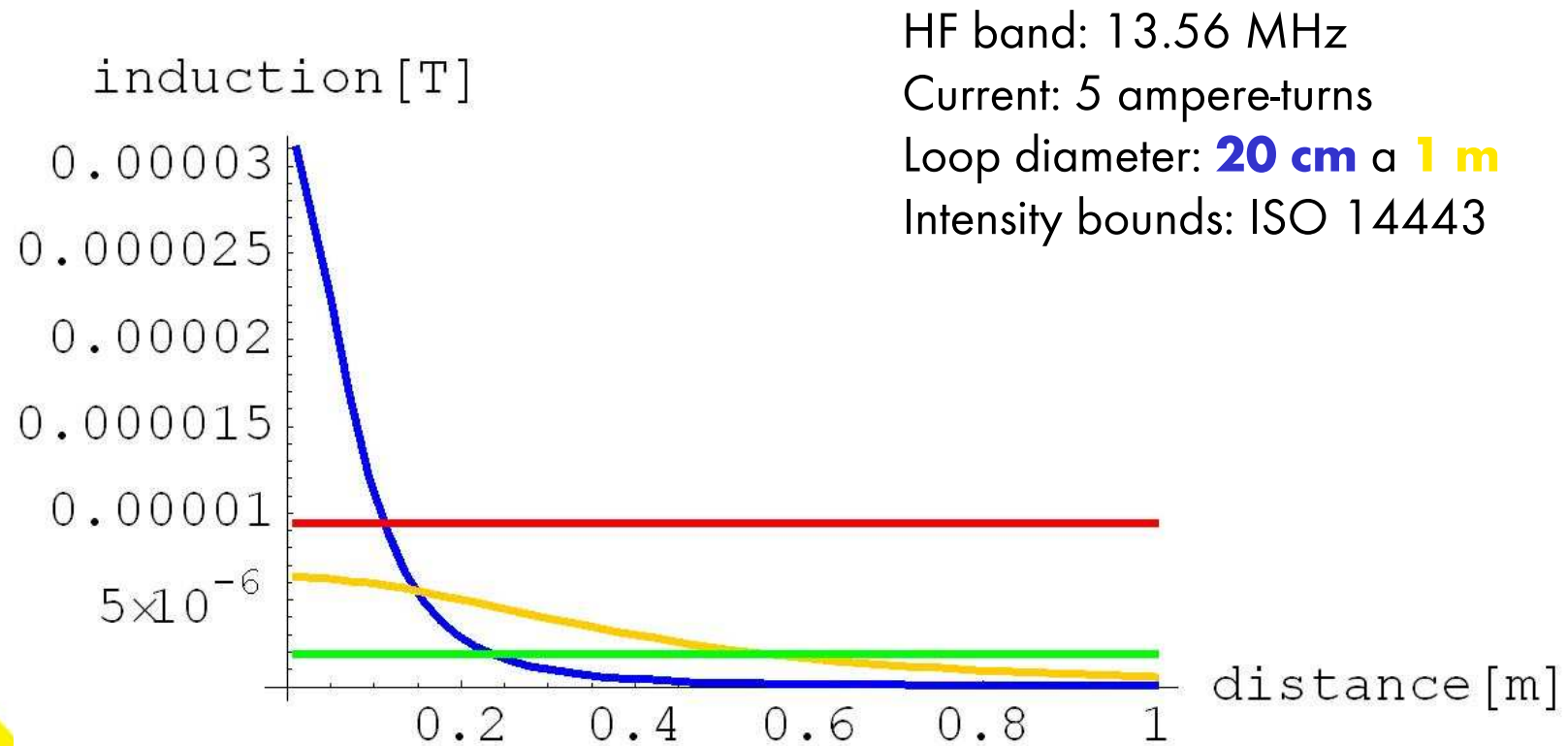
Solution for an ideal
circular loop antenna.

$$B_z = \frac{\mu_0 I N a^2}{2(a^2 + r^2)^{3/2}}$$

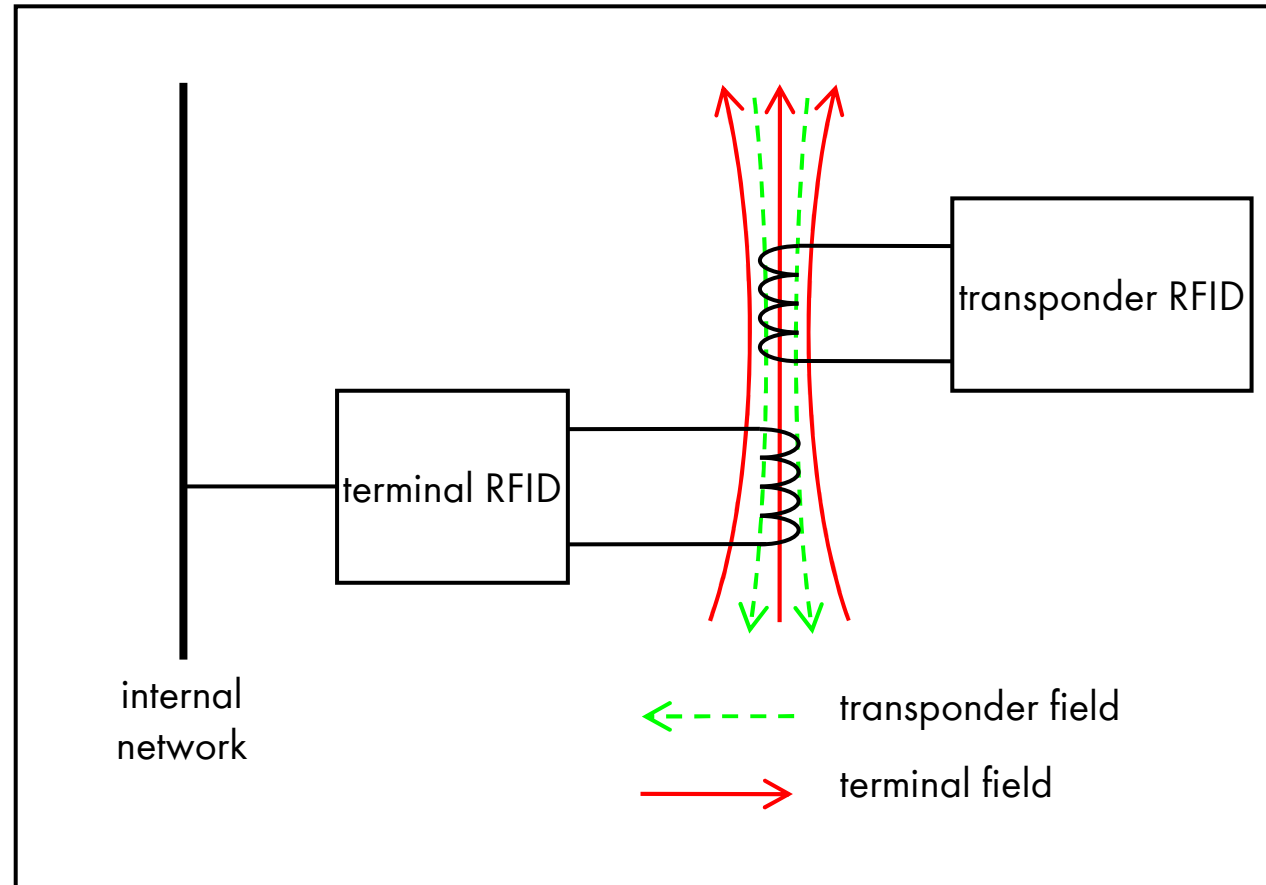
$$= \frac{\mu_0 I N a^2}{2} \left(\frac{1}{r^3} \right) \quad \text{for } r^2 \gg a^2$$



B_z vs. Distance vs. Loop Diameter



Talking with the LF/HF Transponder



Terminal: direct amplitude modulation of the basic carrier
Chip: load modulation resulting in indirect amplitude/phase modulation of the basic carrier

When the Distance Matters

Method	Distance
Active communication with the chip	dozens of cm
Passive reception – chip and terminal	units of m
Passive reception – terminal only	dozens of m
Active communication with the terminal	dozens of m

RFID in Access Control Systems

- A huge majority of access control systems in Czech Republic uses:
 - either so called Unique ID transponders in LF band,
 - or MIFARE (Classic) chips in HF band.

Unique ID Transponders

- Serial memory programmed during the chip manufacturing or personalization phase
- When in the terminal (reader) field, they transmit the memory content automatically in a cycle
- There is no communication origin authentication
 - The transponder talks to anybody
 - The terminal listens to anybody
- Examples: EM Unique, HID Prox, INDALA

- Two basic ways of usage:
 - So-called „UID only“ mode which is functionally equivalent to the unique-ID transponders.
 - Easy to break using a transponder emulator.
 - So-called “cryptographic” mode that uses i.a. mutual authentication of transponder and terminal.
 - Broken totally in 2007-2009. At present, there are dozens of practically feasible devastating attacks.

- Known weaknesses
 - Insufficient key length of Crypto1 alg. (48 bits)
 - Possibility to stabilize the PRNG state
 - Non-linear filter tap symmetry in LFSR of Crypto1
 - Conditional multidifferential property of Crypto1
 - Fault side channel in the authentication protocol
 - Inappropriate order of encryption and error control codes
 - ...

- Implications
 - **Secret key recovery** basing on an interaction with the terminal (reader) only
 - **Secret key recovery** from an intercepted terminal-transponder relation (it is enough to hear the terminal part only – feasible dozens of meters away)
 - **Secret key recovery** basing on an interaction with the transponder only
 - Totally devastating for a huge amount of micro-payment and public transportation applications.

MIFARE Classic – What next?

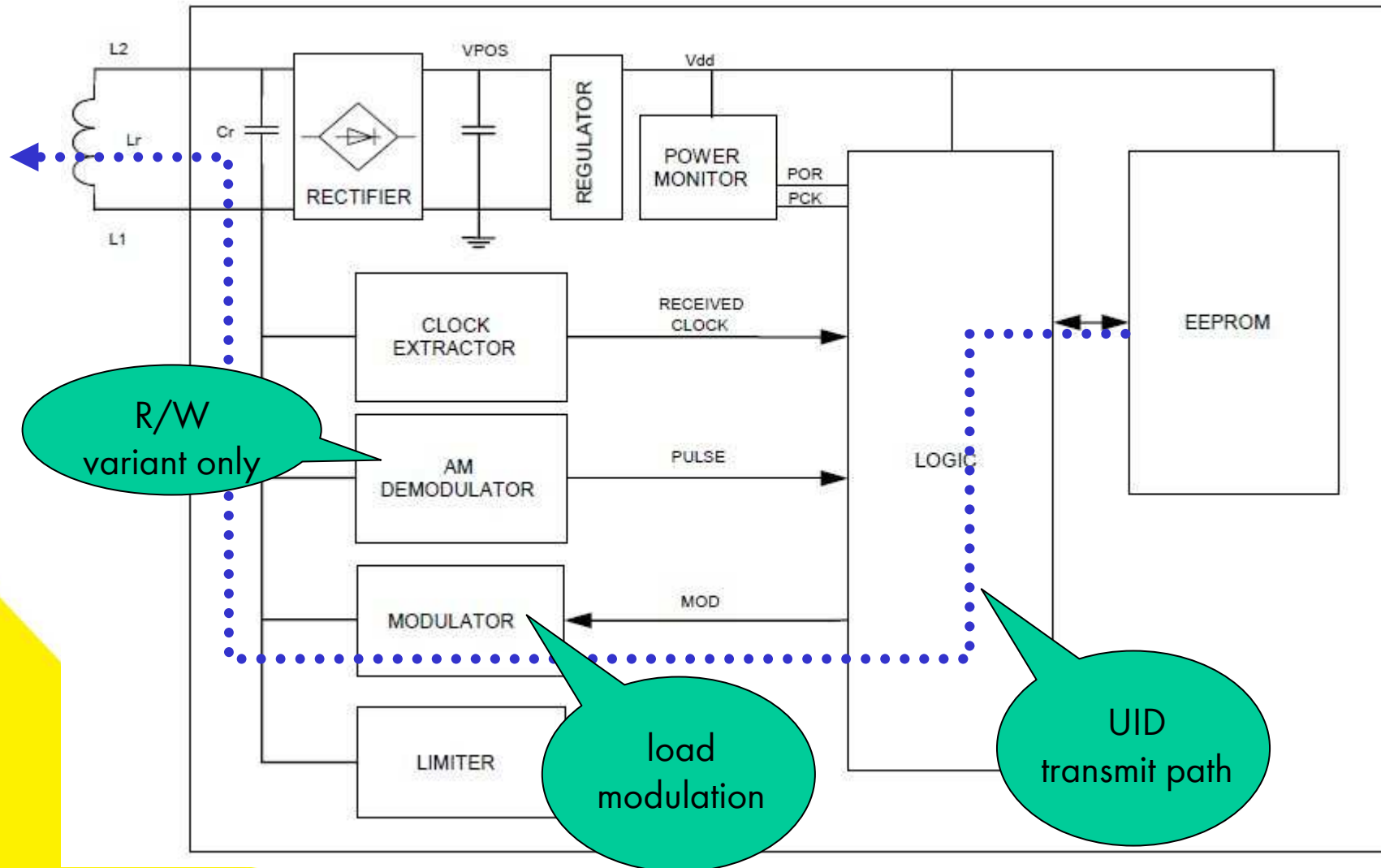
- MIFARE DESFire
 - Defeats number of attacks while (!) introducing large amount of another possible weaknesses.
 - Obviously spoiled interconnection in between cryptography and the application protocol.
 - There is a threat of attacks based on erred configurations (the architecture encourages them)...
- MIFARE Plus
 - Up to now (spring 2009) there is no technical documentation nor engineering samples available (should have been available in Q3 of 2008).

- Despite no necessary dependence, the majority of applications offer the MF Classic profile only.
 - Thus sharing a number of original weaknesses as well.
- It is a question whether these profiles eliminate at least those weakness, that are possible to fix without a compatibility loss.
 - Weak PRNG and the fault side channel in the authentication procedure.

Penetration Test Scope

- The aim was to try to make a functionally equivalent duplicate of an existing access control card.
 - That is a theft of identity of some employee or temporary worker or an external supplier, etc.

Unique ID Transponder Overview



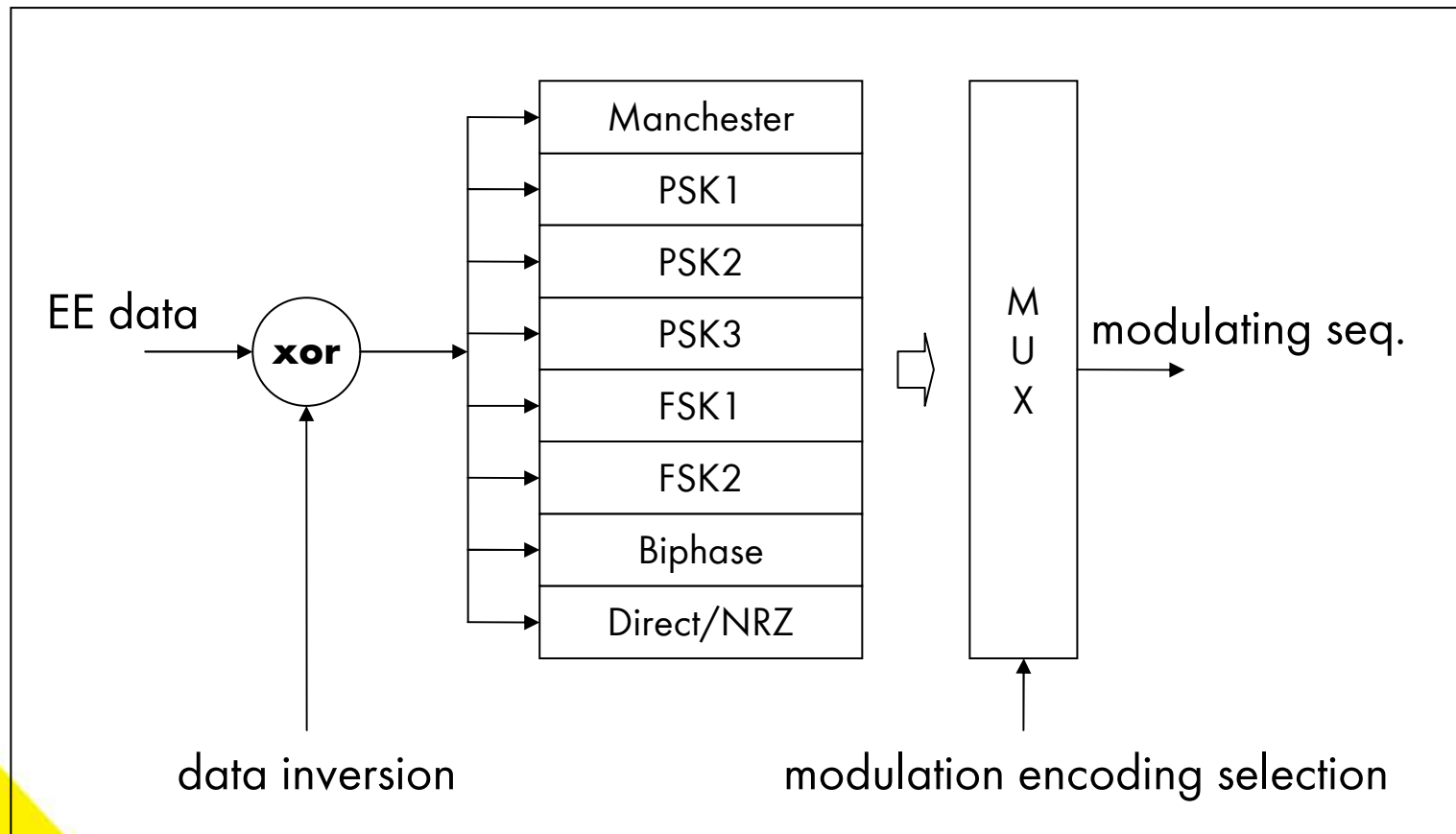
Where the Security Comes From

- It is important to note what the attacker really does **not** have to do:
 - To understand the meaning of the data stored in the transponder memory. The data can even be encrypted (and it still does not matter here).
- Necessary and sufficient condition to make the duplicate of the transponder is:
 - To effectively describe the control sequence driving the load modulator and to repeat this action in the terminal (reader) field later on.

Q5 – Queen of the LF Band

- Programmable LF transponder called “Q5”
 - 224 user defined EEPROM bits (330 b in total)
 - wide support of modulation and encoding schemes
- Variable chip packing – key fob, ISO card, etc.
- It was able to emulate all those LF “Unique ID” transponders tested, so far
- Widely available on the market 😊
 - E.g. http://www.therfidshop.com/product_info.php?products_id=373

Q5 – Output Encoder Part

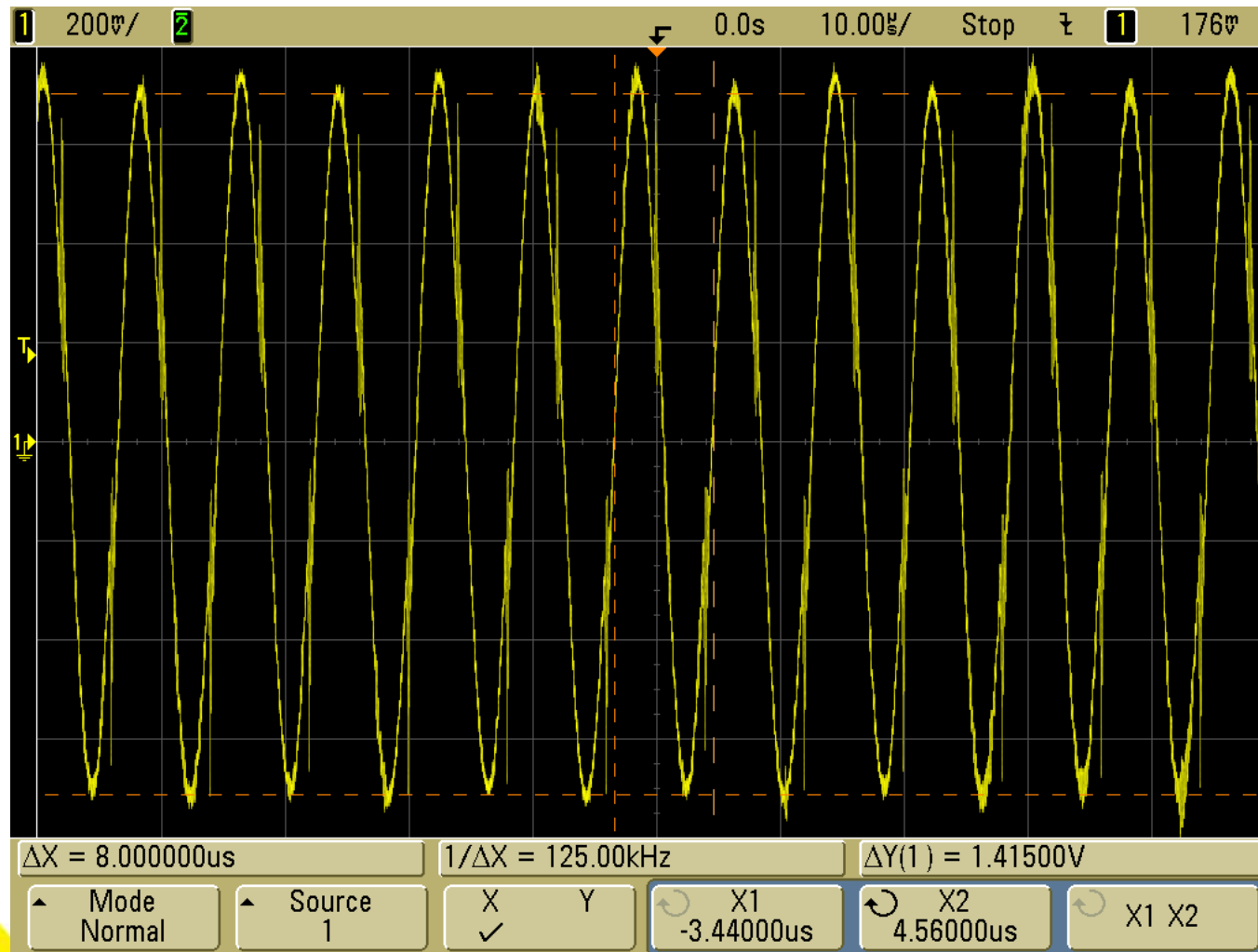


Using Q5 for an Attack

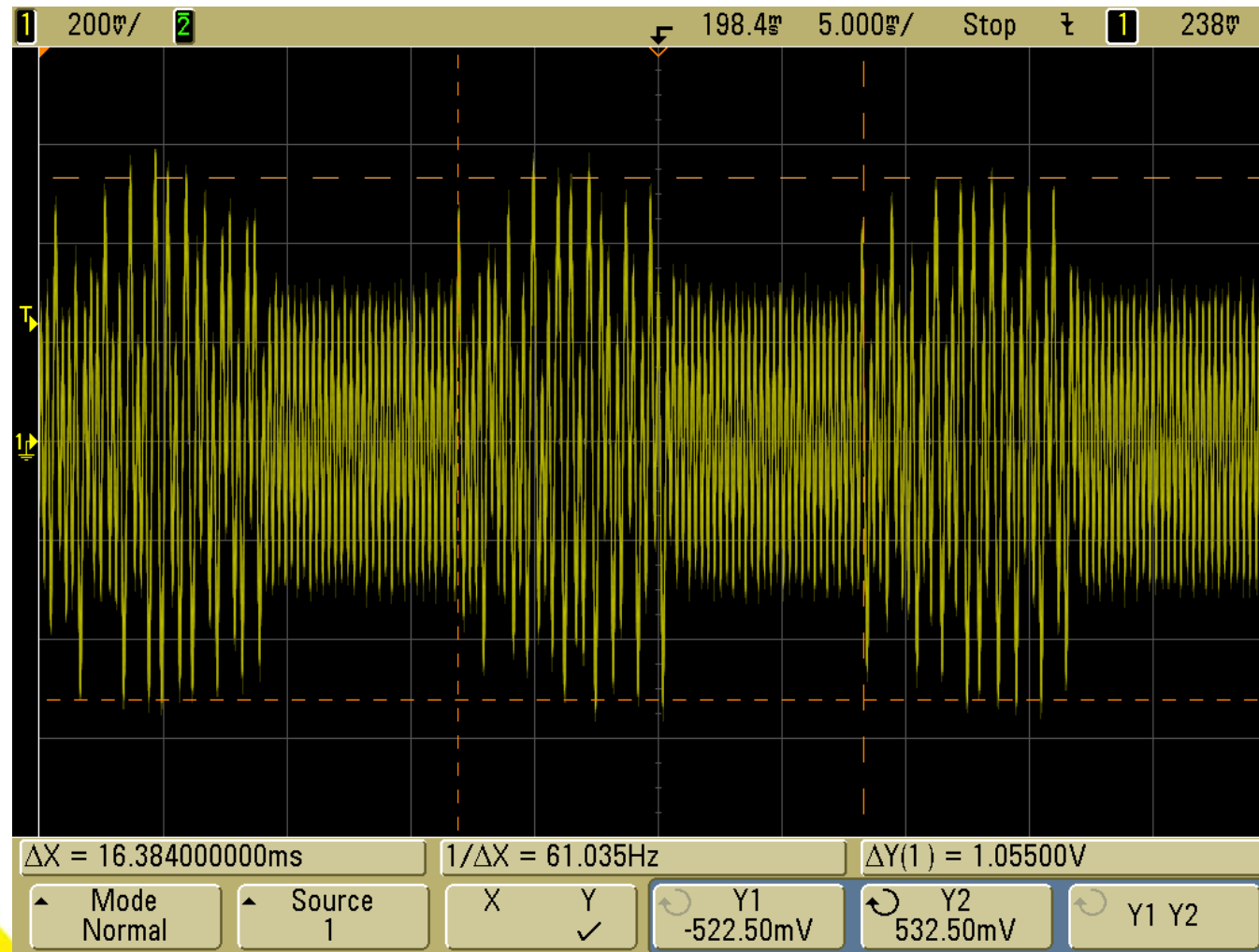
- Phase I – describing the modulating seq. of the original transponder
 - In theory, this can be a very hard problem, but...
 - ... in practice, we seldom meet something “unique”.
 - Let us be led by all those possible Q5 configurations!
- Phase II – making the duplicate
 - We store the modulating seq. into Q5 memory and program its output encoder/modulator...

Examples of the Phase I follow...

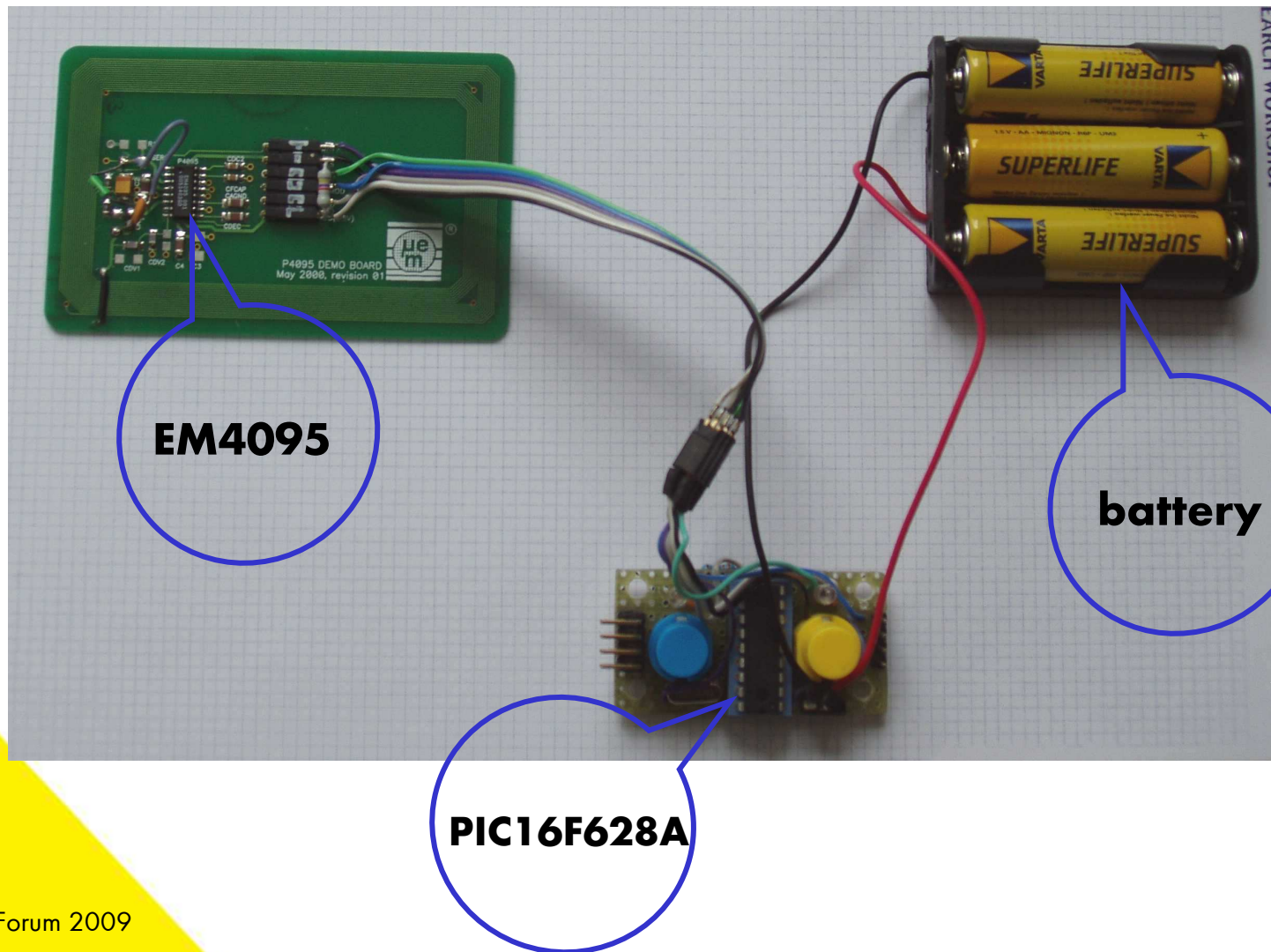
LAB Example: The Effect of Using a Subcarrier Frequency



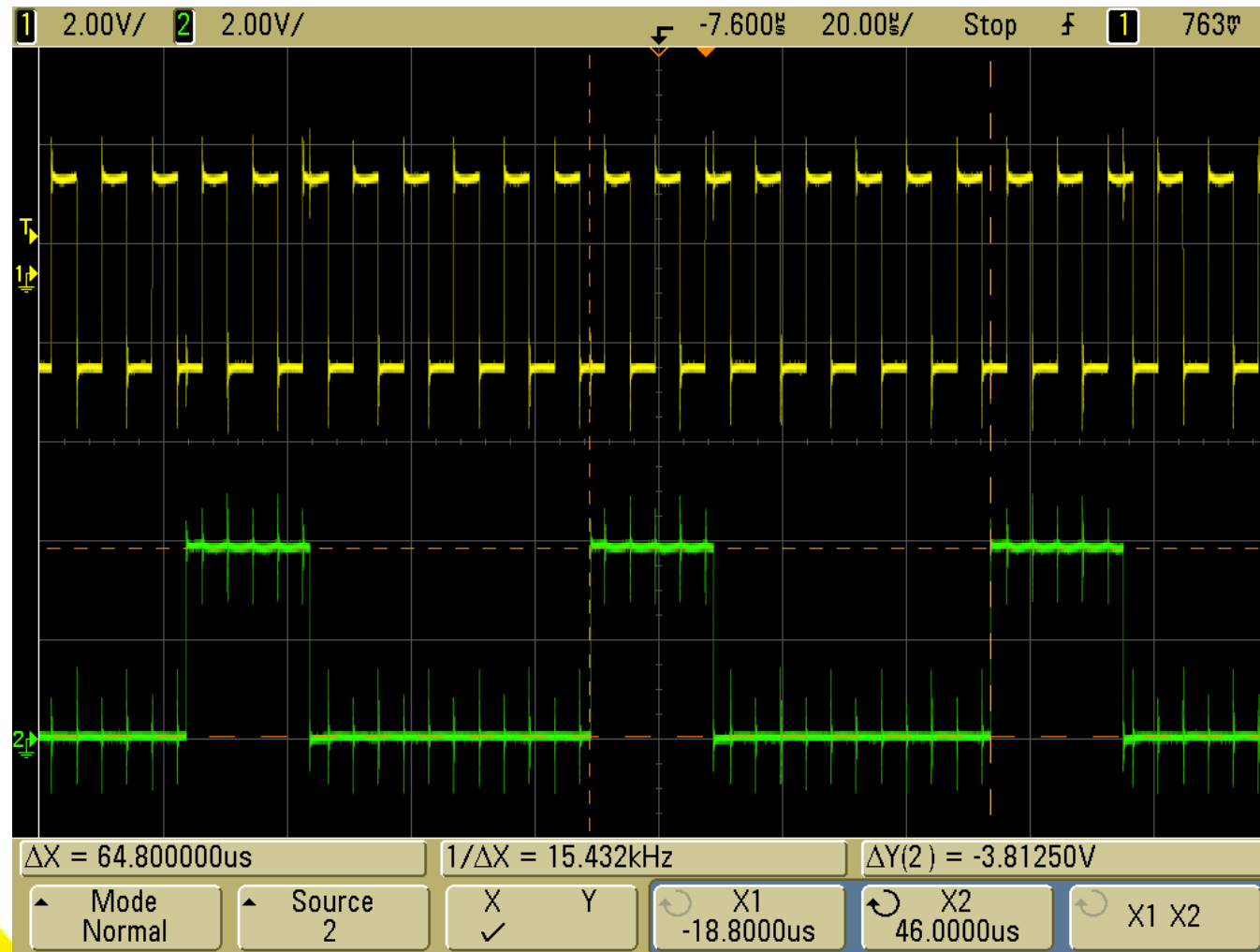
LAB Example: Subcarrier with Phase Modulation



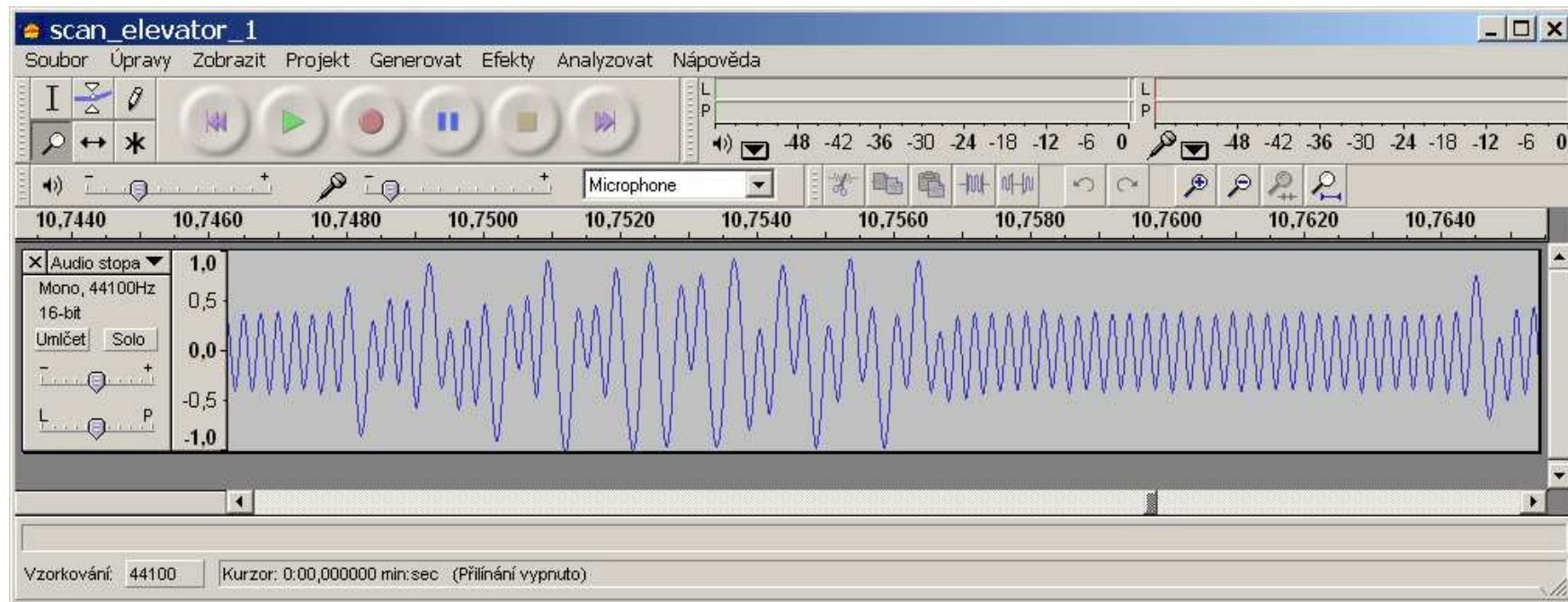
LAB Example: Ad Hoc Spyware



LAB Example: Frequency Modulation Disclosed by EM4095 (green)



Another Practical Scenario: Eavesdropping in Elevator...



LF band transponder data intercepted while its holder was
authenticating to the reader in an elevator
Distance: cca 0,5 m.
Receiver: Sangean ATS 909W.

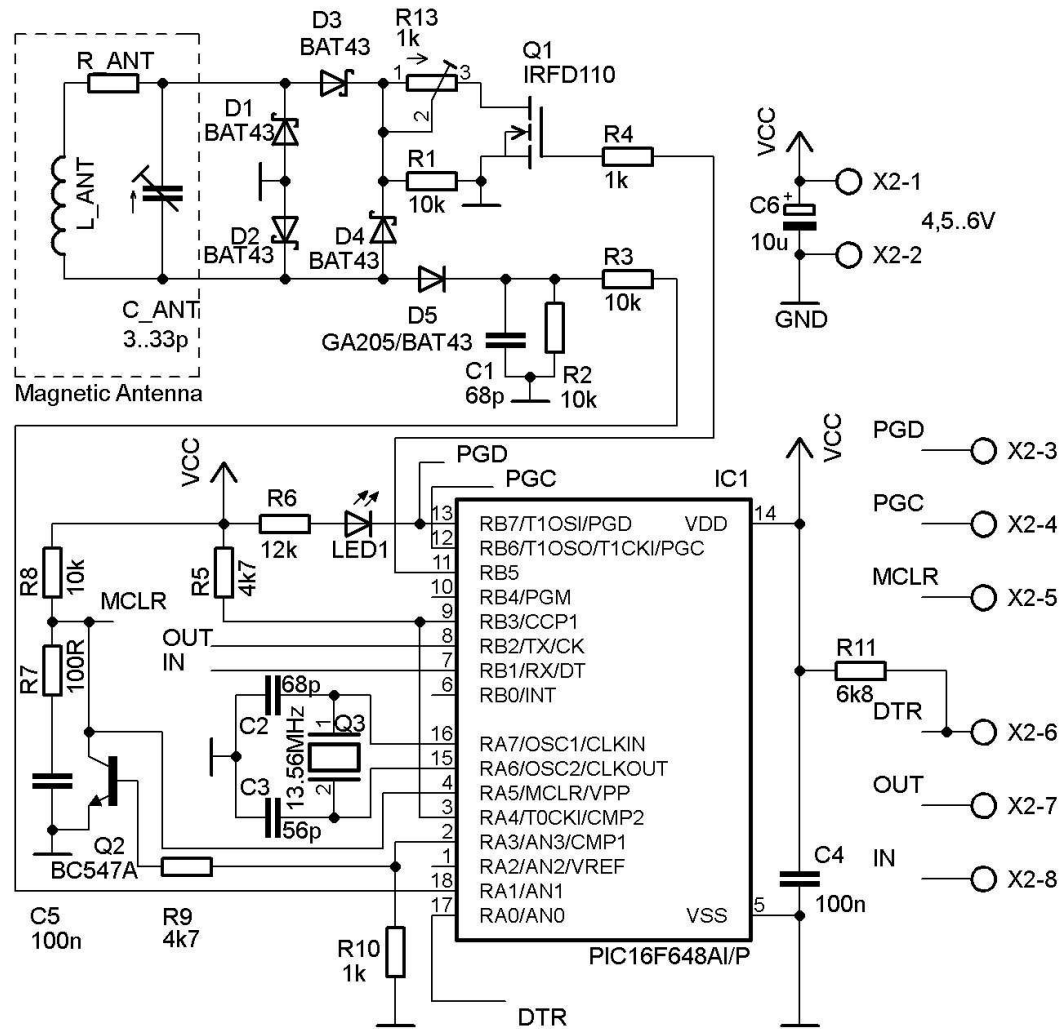
Disclosing “The Secret” ...

- EM Unique
 - direct manchester encoding, bitrate $f/64$, 64 bits in total
 - Q5 configuration word: 60 01 F0 04
- INDALA (1 particular setup)
 - subcarrier $f/2$ with phase shift keying, modulating sequence length of 64 bits
 - Q5 configuration word: 60 00 F0 A4
- HID Prox (1 particular setup)
 - 2 subcarriers $f/8$ and $f/10$ with frequency shift keying, modulating sequence length of 96 bits
 - Q5 configuration word: 60 01 80 56

MIFARE „UID only“

- In practice, huge amount of MF installations use this approach.
- In many aspects, the security of this approach is even worse than of the transponders in LF discussed before.
 - The communication protocol is standardized (ISO14443A)
 - UID interception is possible up to dozens of meters away
- Only one obstacle here – there is no Q5 analogue for the HF band...
 - We need to build our own emulator – e.g. PicNic.

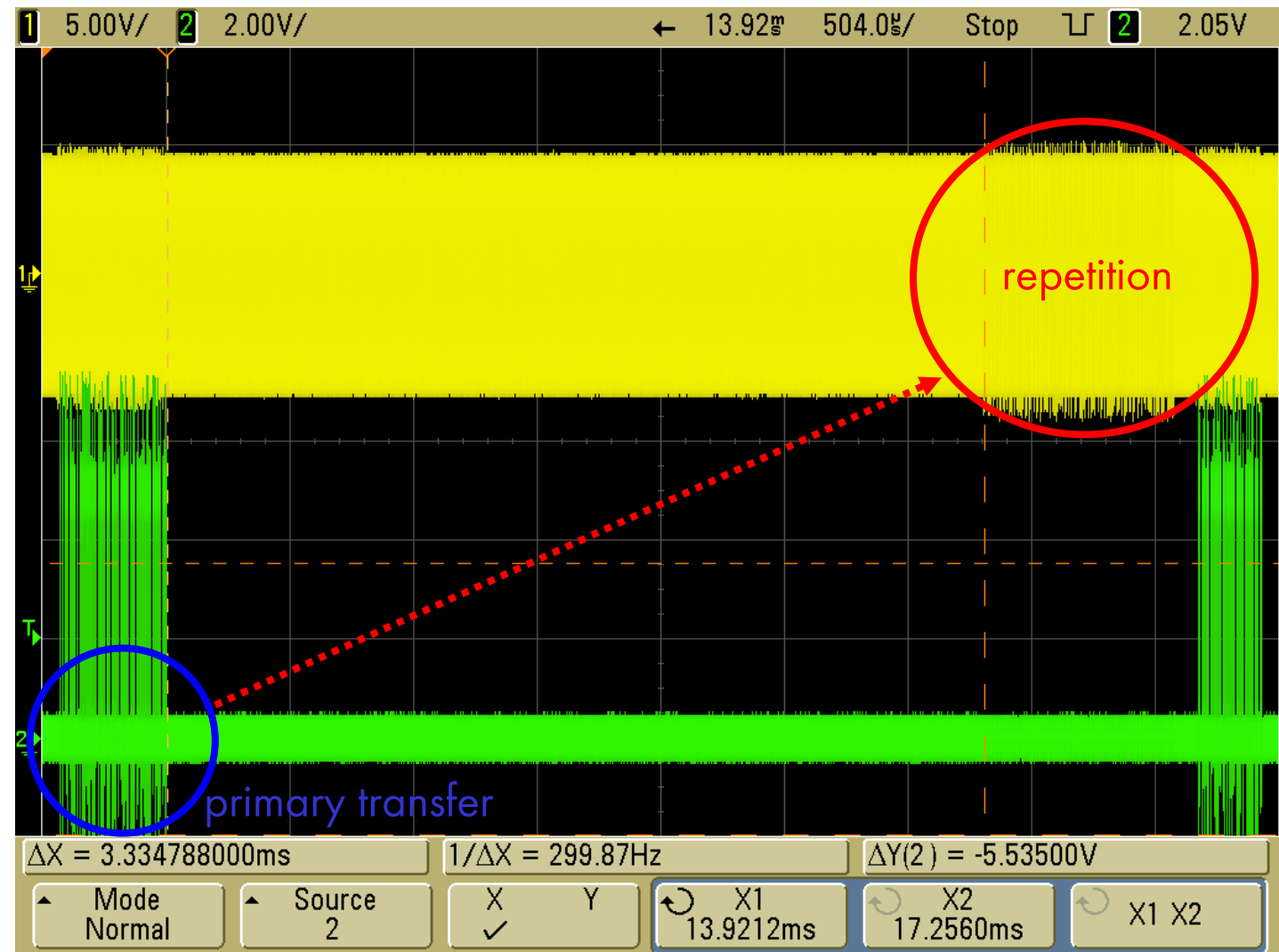
PicNic: HF Band Transponder Emulator



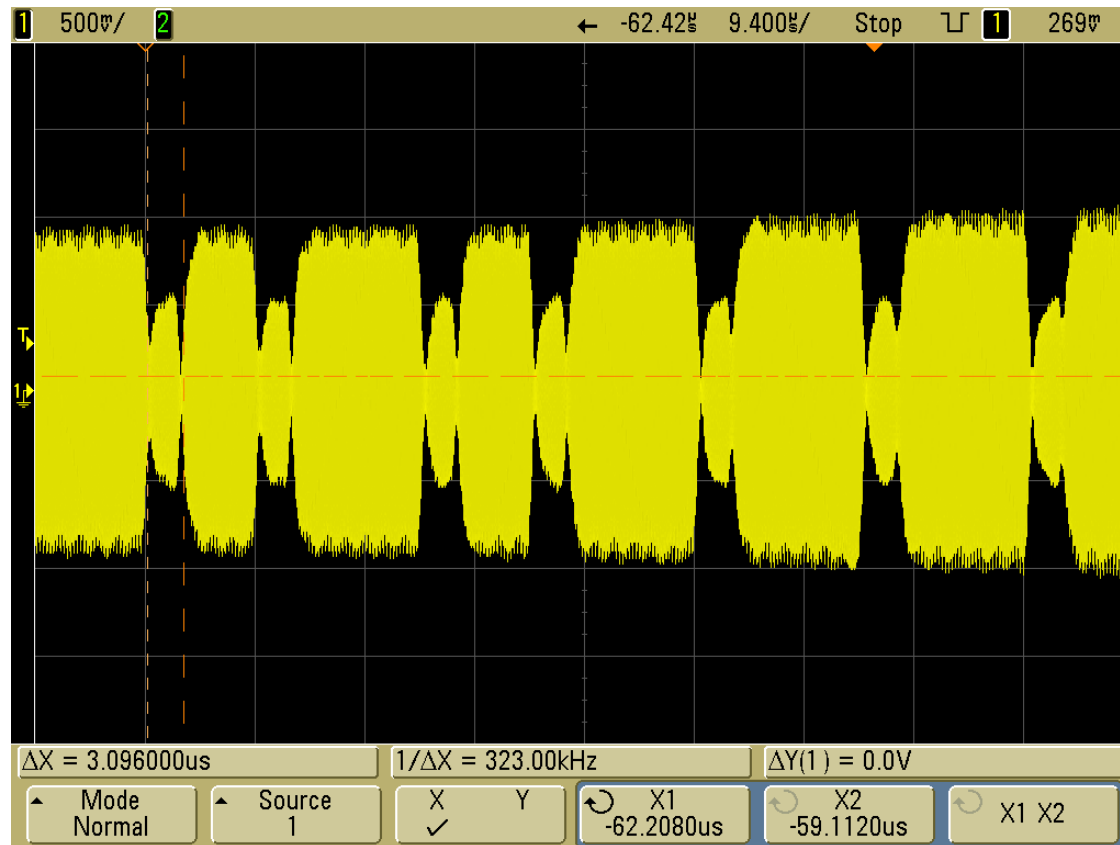
For details cf. crypto.hyperlink.cz/picnic.htm

On MF UID Interception

- Yellow
trace:
basic
carrier
- Green
trace:
AM
detector



Real Life Experiment



Receiver AOR AR8600MK2, HF output at i.f. 10,7 MHz.
Distance cca 2 m, at least two readers in the field.
UID can be read clearly, still without any preprocessing
(becomes necessary with increasing distance).

Another Real Life Scenario or “The whole chain is as weak as...”

Danovy doklad c.: PD-08-002-5396
DUZP: 1.12.08
[redacted], s.r.o.
PS-08-002-9080 [redacted] 1.12.08 11:07

1x Zampionova polevka	29,00	A
1x Cocka se sazenym vejcem	69,00	A
1x Bonaqua neperлива 0,5l	20,00	A
Sleva 5%	-6,00	
CELKEM	112,00	

3cf2e2da9000 15 ROSA TOMAS

Zam. Karta	112,00	
9% DPH/VAT 9,30	(102,70)	112,00 A

Puvodni zustatek: 395,00
Novy zustatek: 283,00

UID
here

Besides paying
in the canteen,
the same card
opens the office
door. Of
course...
So, lets feel the
power of
technology
convergence –
take a lunch
and go for a
walk around
the office... ☺

- Huge majority of contemporary access control systems is vulnerable to an identity theft attack.
 - Transponders serve the role of subject identification only.
 - They do not provide any reasonable subject authentication!
- Huge majority of physical security managers is not aware of such risk.
 - Seeing the risk requires noting that computer systems play a crucial role (even) in the area of physical security.
 - Material engineering is just not enough for physical security risk assessment any more.
 - Common principles of information security have to be applied as well.
 - Especially, RFID systems shall be subject to the penetration testing.

Thank you for your attention...

For more cf.: crypto.hyperlink.cz/cryptoprax.htm



Dr. Tomáš Rosa
Raiffeisenbank, a.s.
tomas.rosa@rb.cz