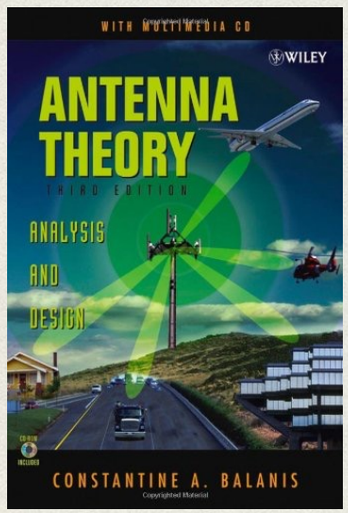
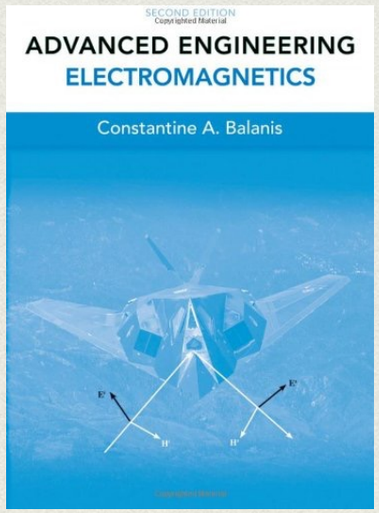
RADIO ASPECTS OF NFC SECURITY

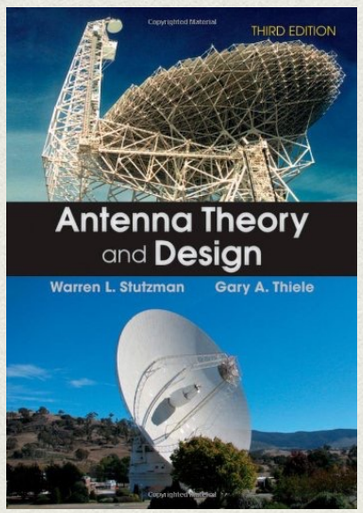
Tomáš Rosa

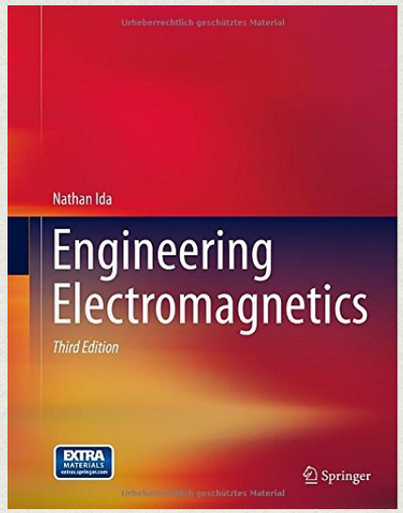
http://crypto.hyperlink.cz

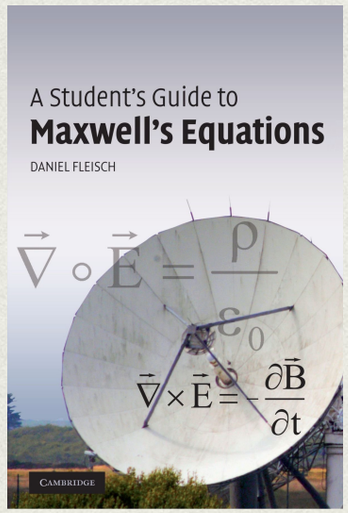
ANTENNA ESSENTIALS WITH NEAR AND FAR FIELDS DISCUSSION

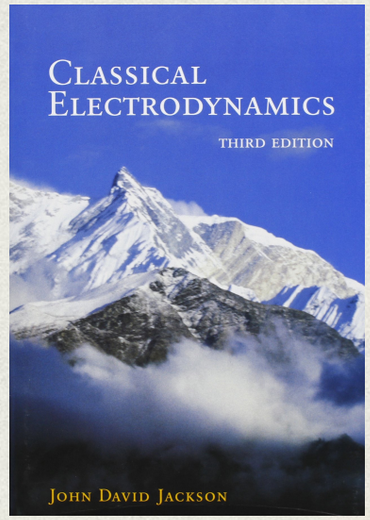












START WITH SOMETHING FAMILIAR

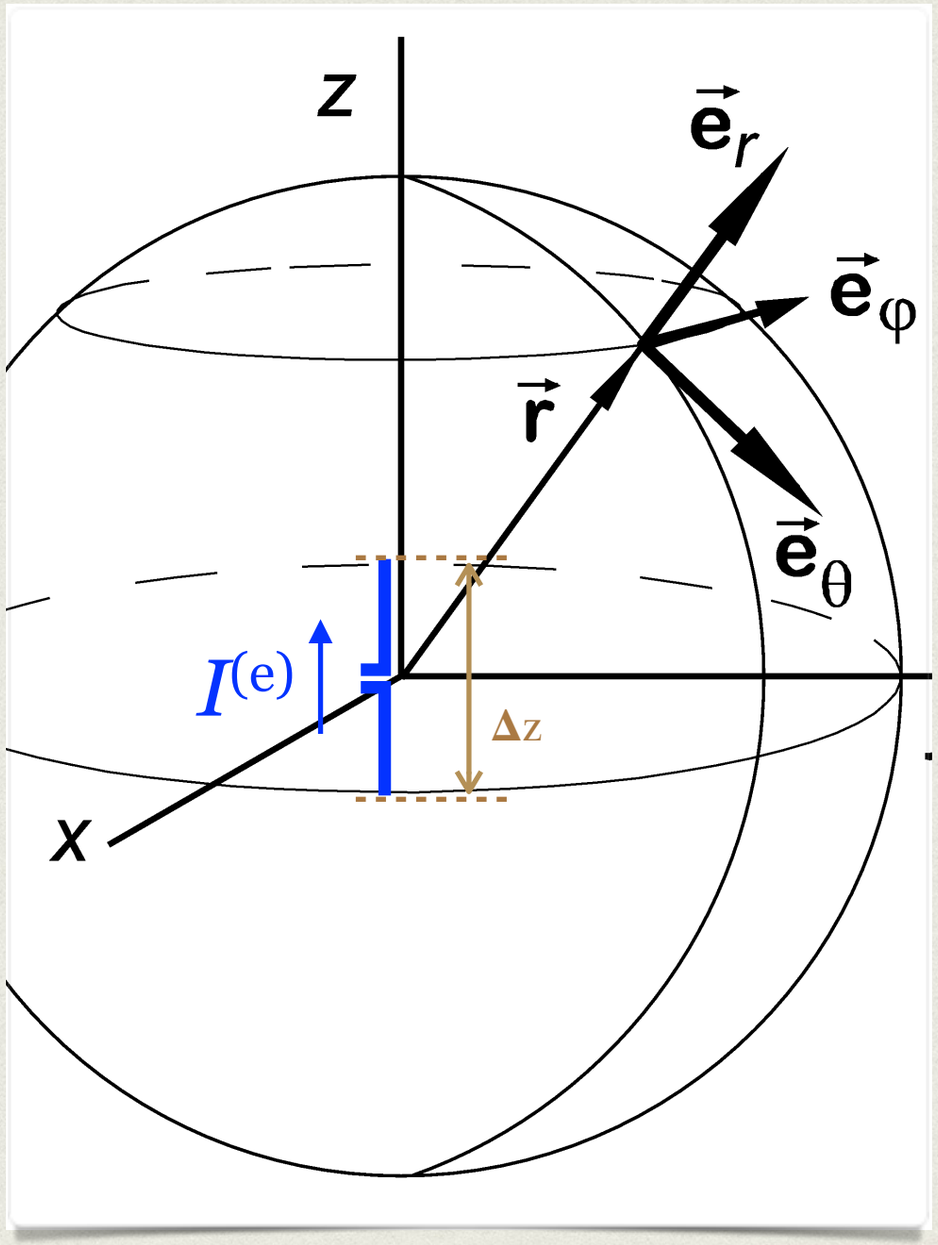
[Buddipole QRV by 5B8AP]

THE IDEAL ELECTRIC DIPOLE

- Electrically small, i.e. $\Delta z << \lambda$, uniform amplitude current element.
  - Ordinary dipole is covered by integration over these elements.
- In the far field, a donut-like pattern bearing the vertical polarisation is produced.
- In general, its field has the following components.

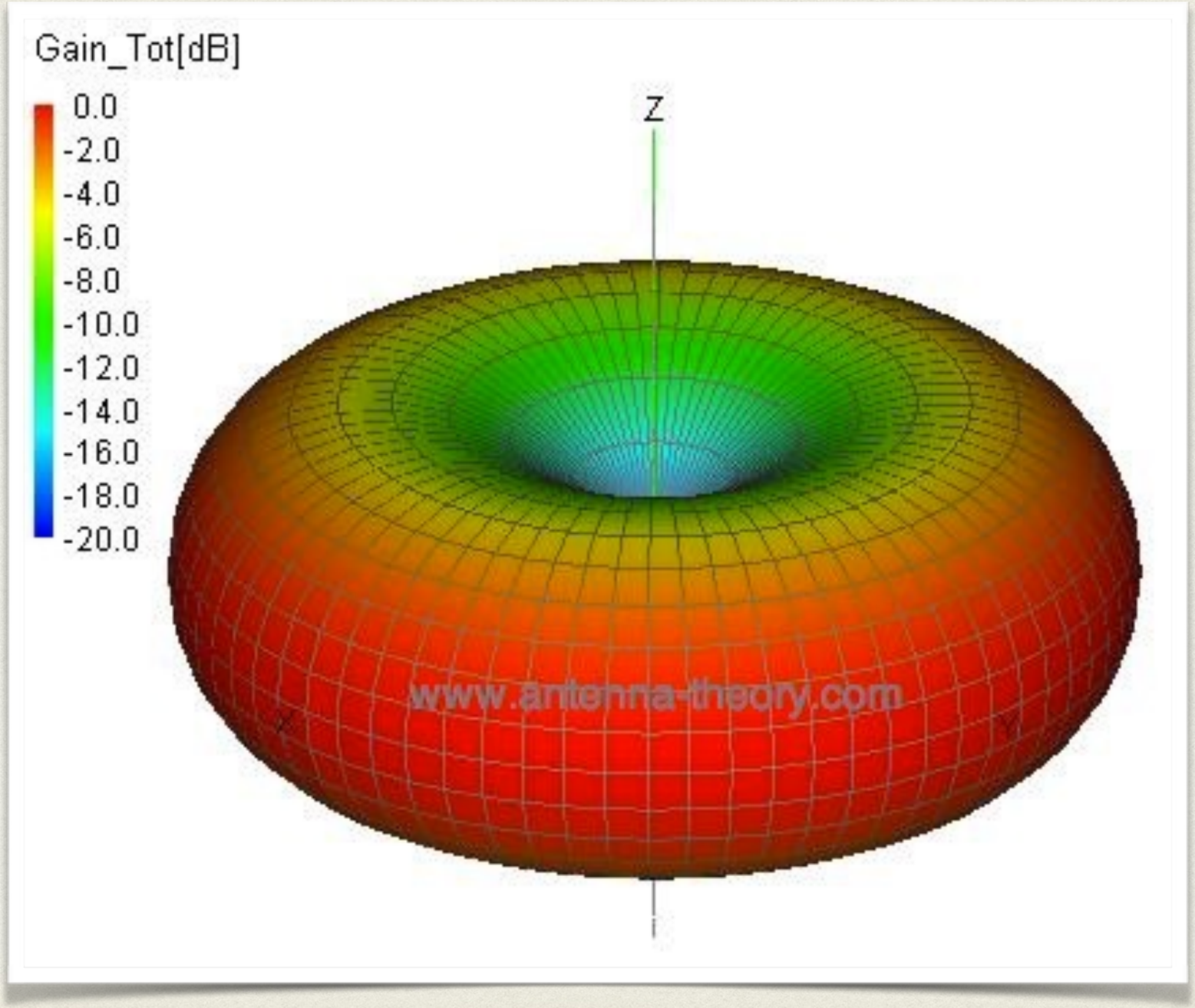
$$\vec{E}_{edp}(I^{(e)}) = E_{edp,\theta}(I^{(e)}) \cdot \hat{e}_\theta + E_{edp,r}(I^{(e)}) \cdot \hat{e}_r$$

$$\vec{H}_{edp}(I^{(e)}) = H_{edp,\phi}(I^{(e)}) \cdot \hat{e}_\phi$$



(illustration purpose only)

HAVE YOU SAID DONUT?



TOWARDS SOMETHING APPEALING

[AlexLoop by Alex, PY1AHD]

THE SMALL LOOP

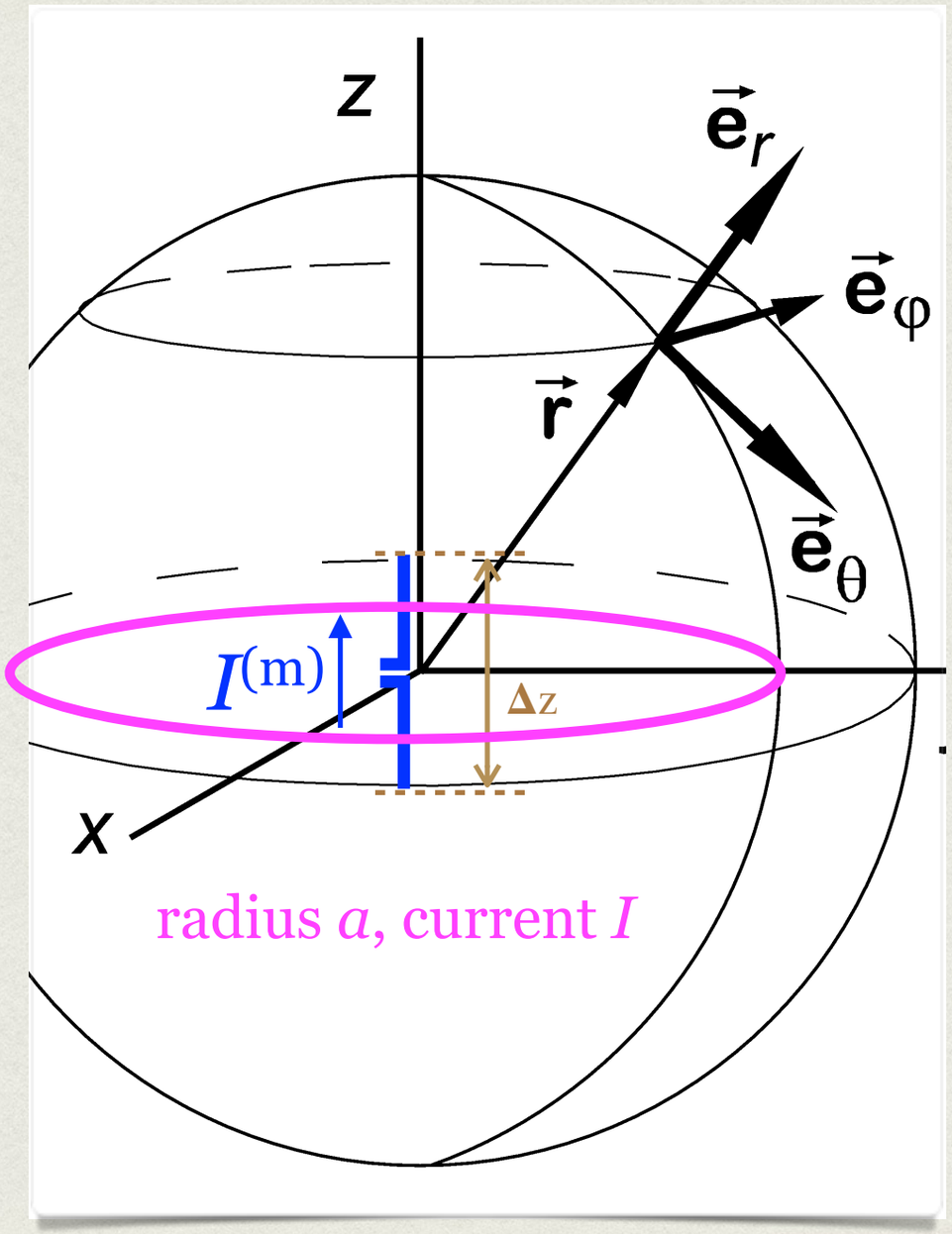
- Electrically small, i.e. $2\pi a < \lambda/10$, uniform amplitude current loop.
- Can be modelled as an ideal *magnetic* dipole which is the theoretical dual of the ideal electric dipole.
- The duality equations follow.

$$\vec{E}_{mdp}(I^{(m)}) \equiv -\vec{H}_{edp}(I^{(m)}),\ \vec{H}_{mdp}(I^{(m)}) \equiv \vec{E}_{edp}(I^{(m)})$$

$$\mu_{mdp} \equiv \varepsilon_{edp},\ \varepsilon_{mdp} \equiv \mu_{edp}$$

$$\beta_{mdp} = \omega\sqrt{\mu_{mpd}\varepsilon_{mdp}} = \omega\sqrt{\varepsilon_{edp}\mu_{edp}} = \beta_{edp}$$

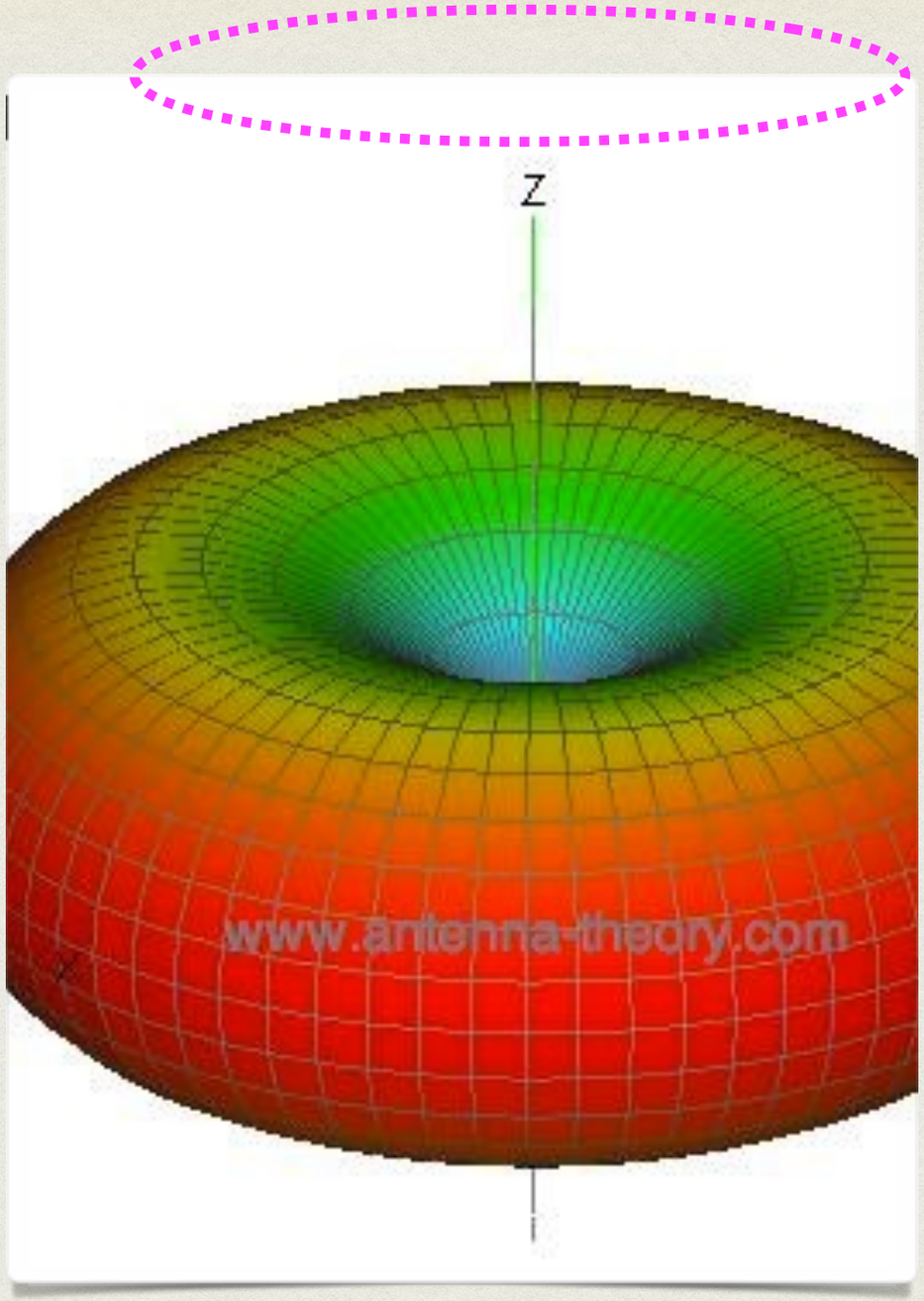
note also $\beta = \dfrac{2\pi}{\lambda}$, $v = \lambda f$



(illustration purpose only)

DONUT PATTERN AGAIN

- The duality with the ideal electric dipole tells us the *far field* has the donut-like form.
- The polarisation is reversed (!) - i.e. horizontal in place of vertical, now.
- In the *near field*, however, there is a significant radial component (cf. below).



(rough illustration purpose only)

LONG STORY SHORT

$$\vec{E}_{mdp}(I^{(m)}) = -\frac{I^{(m)}\Delta z}{4\pi} j\beta(\frac{1}{r} + \frac{1}{j\beta r^2})e^{-j\beta r}\sin\theta\cdot\hat{e}_\phi$$

$$\vec{H}_{mpd}(I^{(m)}) = \frac{I^{(m)}\Delta z}{4\pi} j\omega\varepsilon(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\sin\theta\cdot\hat{e}_\theta$$

$$+\frac{I^{(m)}\Delta z}{2\pi} j\omega\varepsilon(\frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\cos\theta\cdot\hat{e}_r$$

MAGNETIC CURRENT OF THE SMALL LOOP

$$I^{(m)}\Delta z = j\omega\mu IS$$

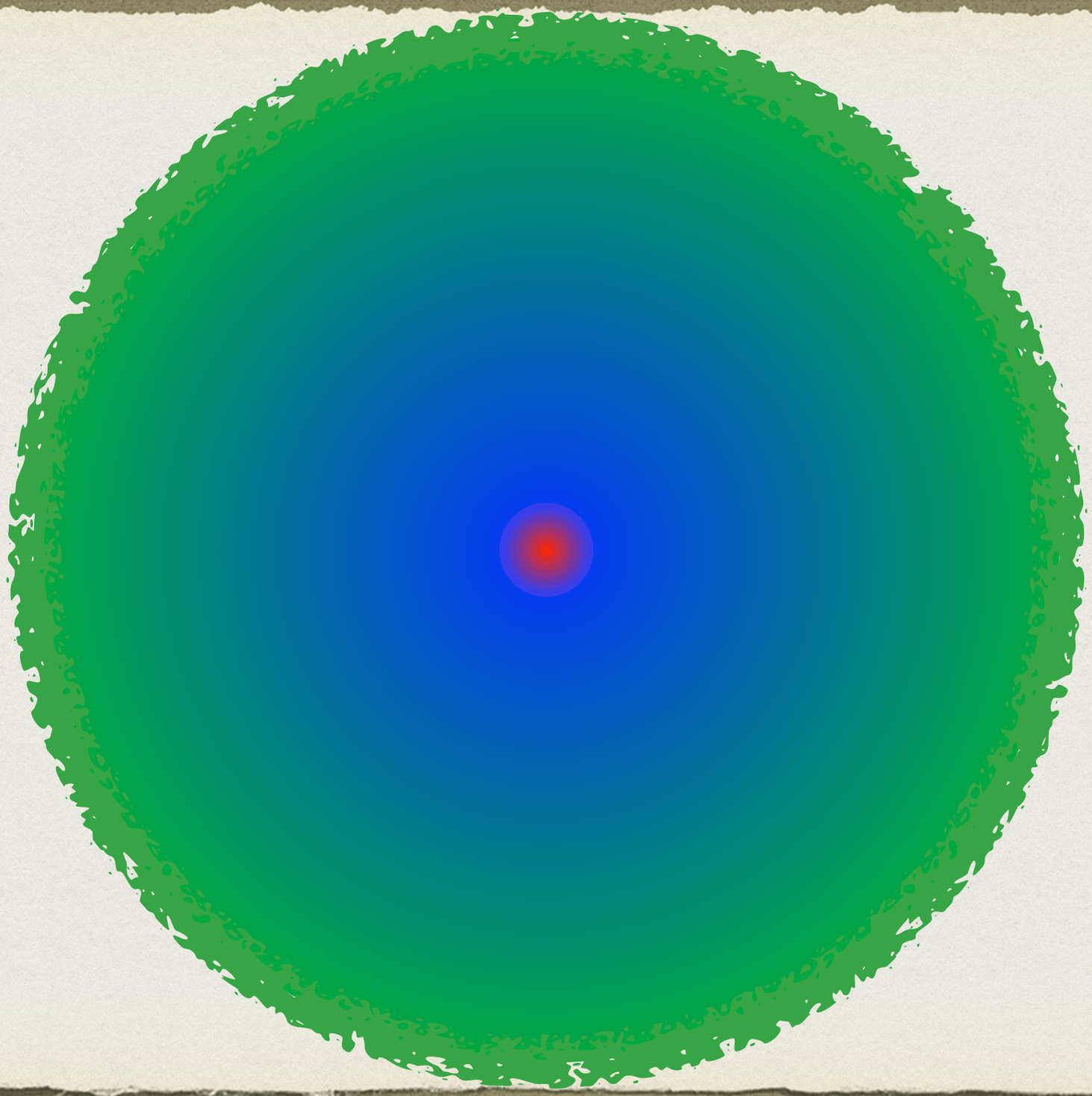
$$S = \pi a^2$$

(based on far field equivalence)

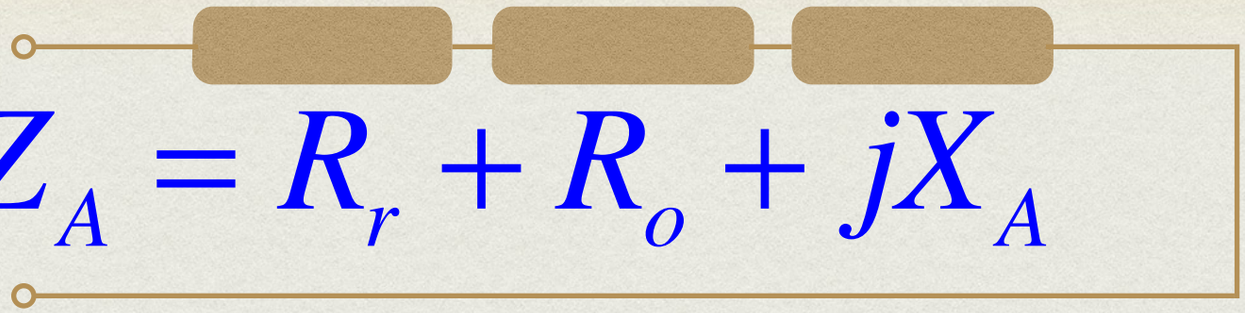
NEAR, FAR

- Basing on the dominating *E*, *H* field terms, it is useful to distinguish:
  - *Reactive near field* (XNF), where the terms with $1/r^2$ and $1/r^3$ dominate. Energy is mainly stored and exchanged between *E* and *H*.
  - *Radiating near field* (Fresnel region), where the $1/r^2$ terms start to dominate, i.e. $r > \lambda/2\pi$. Energy is mainly radiated with unstable patterns, however.
  - *Far field* (Fraunhofer region), where the $1/r$ terms remain to dominate and the plane wave model can be used. Several conditions shall be met: $r > 2D^2/\lambda$, $r > 5D$, $r > 1.6\lambda$, where *D* is the largest antenna dimension. Energy is radiated with a distance-independent field pattern.

WHEREVER YOU ARE



ANTENNA IMPEDANCE



$$Z_A = R_r + R_o + jX_A$$

- The input impedance Z_A describes the antenna from the lumped circuit parameters viewpoint.
  - R_r is the equivalent radiation resistance representing the energy emanated through the radio waves
  - R_o describes the dissipative energy loss
  - X_A reflects the energy exchanged back-and-forth with the reactive near field

RADIATION OF THE SMALL LOOP

$$P = 10I^2(\beta^2 S)^2$$

$$R_r = \frac{2P}{I^2} = 20(\beta^2 S)^2 \approx 31171(\frac{S}{\lambda^2})^2$$

$$\approx 31171(\frac{NS}{\lambda^2})^2 \text{, for a small } N\text{-turn loop}$$

DAMPING RESISTOR

- For the radiation efficiency analysis, R_o shall also cover any damping resistor R_q used.

- Especially for NFC, a nonzero R_q is often inserted serially to lower the antenna Q to achieve the required bandwidth.

- Finally, we can expect a very small radiation efficiency for a typical NFC antenna.

- Interestingly, we may investigate on how to design a yet-usable NFC antenna that is, however, a very poor radiator anyway.

- *Nevertheless, it does not mean the radiation is zero.*

EFFICIENCY ANALYSIS

- To get a better overview, we can compute the radiation efficiency e_r that can be further used for e.g. gain estimation, etc.

- We do that by comparing the equivalent real resistances from the circuit model of Z_A.

$$R_s = \sqrt{\frac{\omega\mu}{2\sigma}}$$

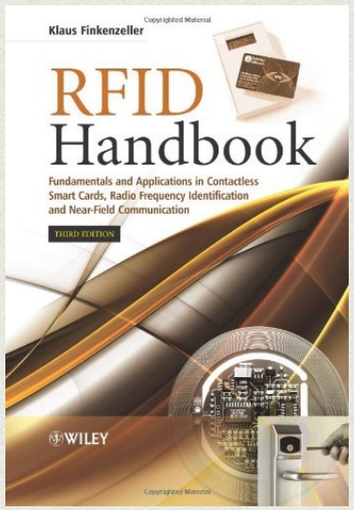
$$R_o = \frac{a}{c} R_s, \text{ a } \sim \text{ loop radius, c } \sim \text{wire radius}$$

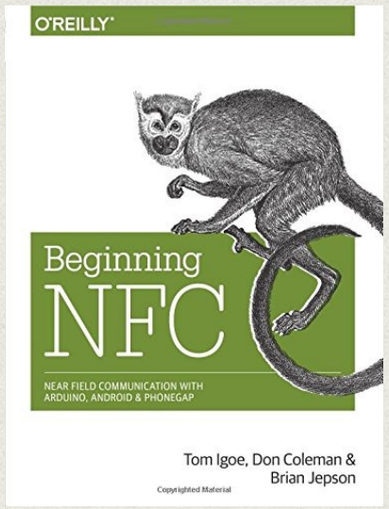
$$e_r = \frac{R_r}{R_q + R_o + R_r}$$

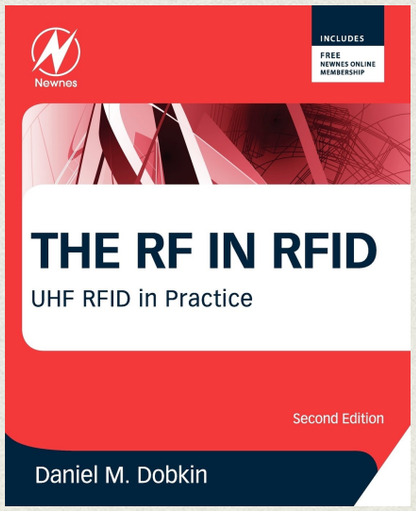
PARASITIC ANTENNAS

- From the security viewpoint, we shall recognise it may not be the *primary* antenna only that can radiate sensitive data.
- In general, any spatial distribution of a time-varying current modulated (or sensed!) by the internal processing unit is a potential backdoor.
- We are getting to the well-known phenomenon of the electromagnetic side-channels.
- Here, we have an extremely high chance this mechanism is exploitable by attackers.
- In principle, applying anti-RFI techniques for all those patch cables and power lines is a good idea to start with.

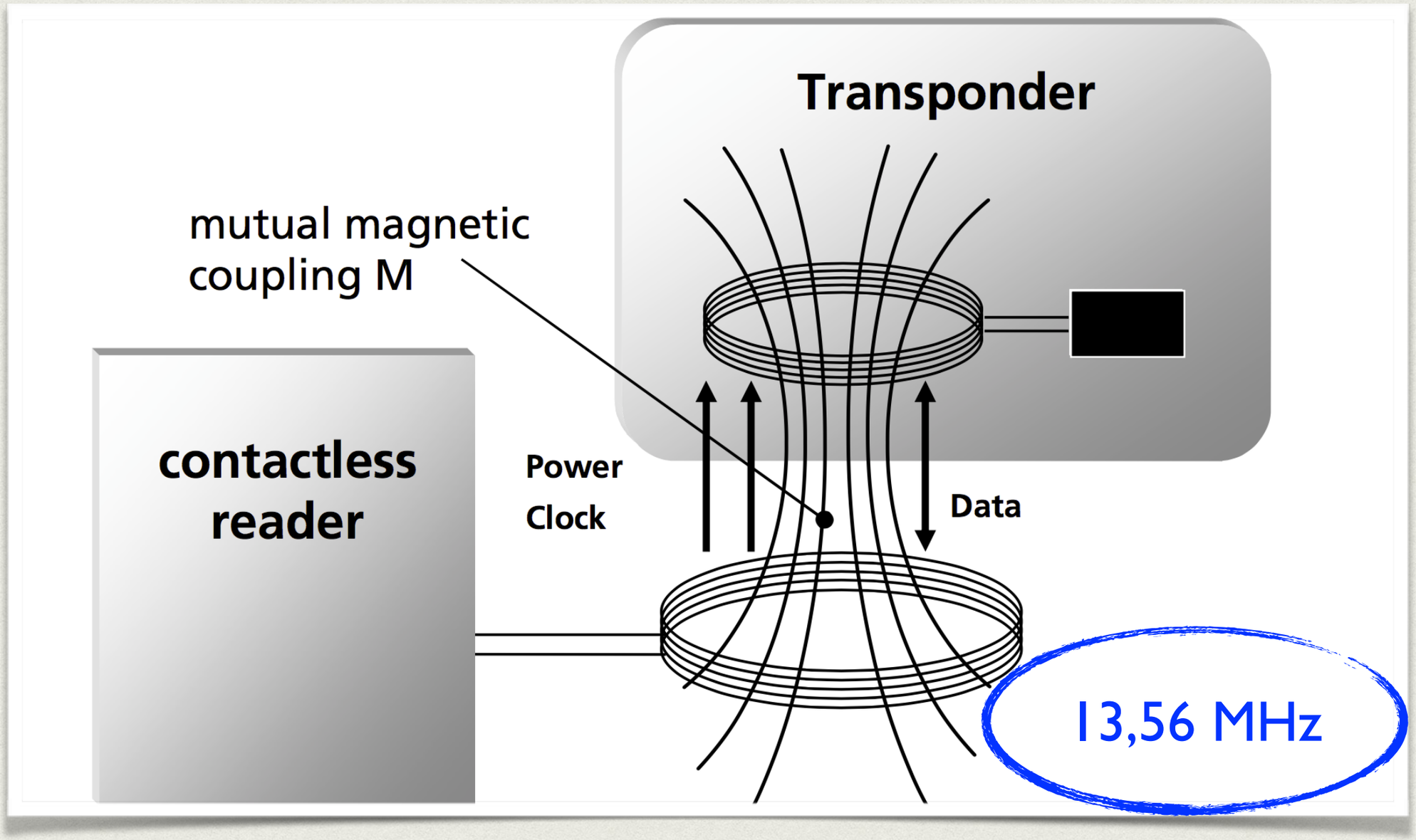
NEAR FIELD COMMUNICATION





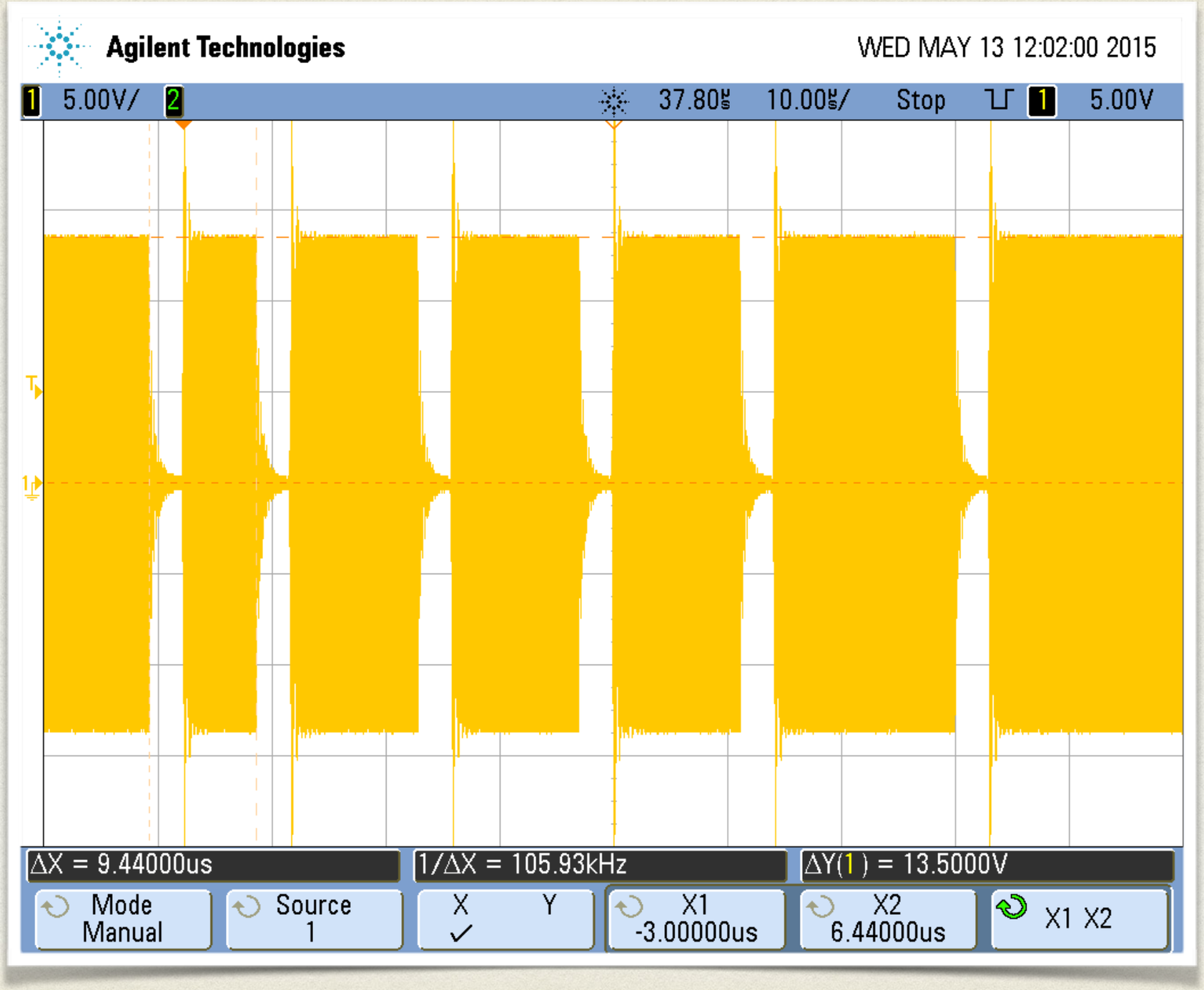


PASSIVE NFC COUPLING

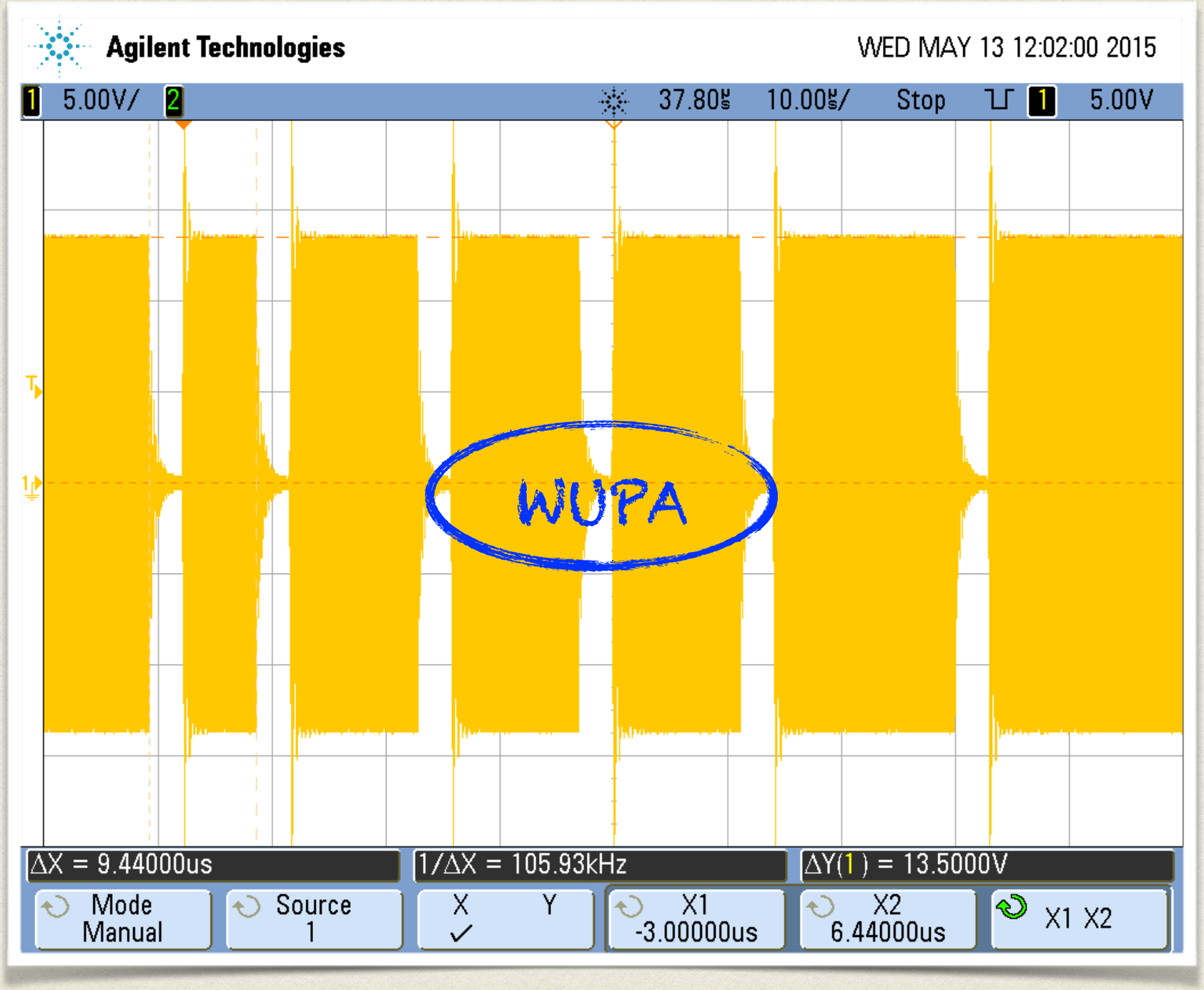


[Finkenzeller, K., 2011]

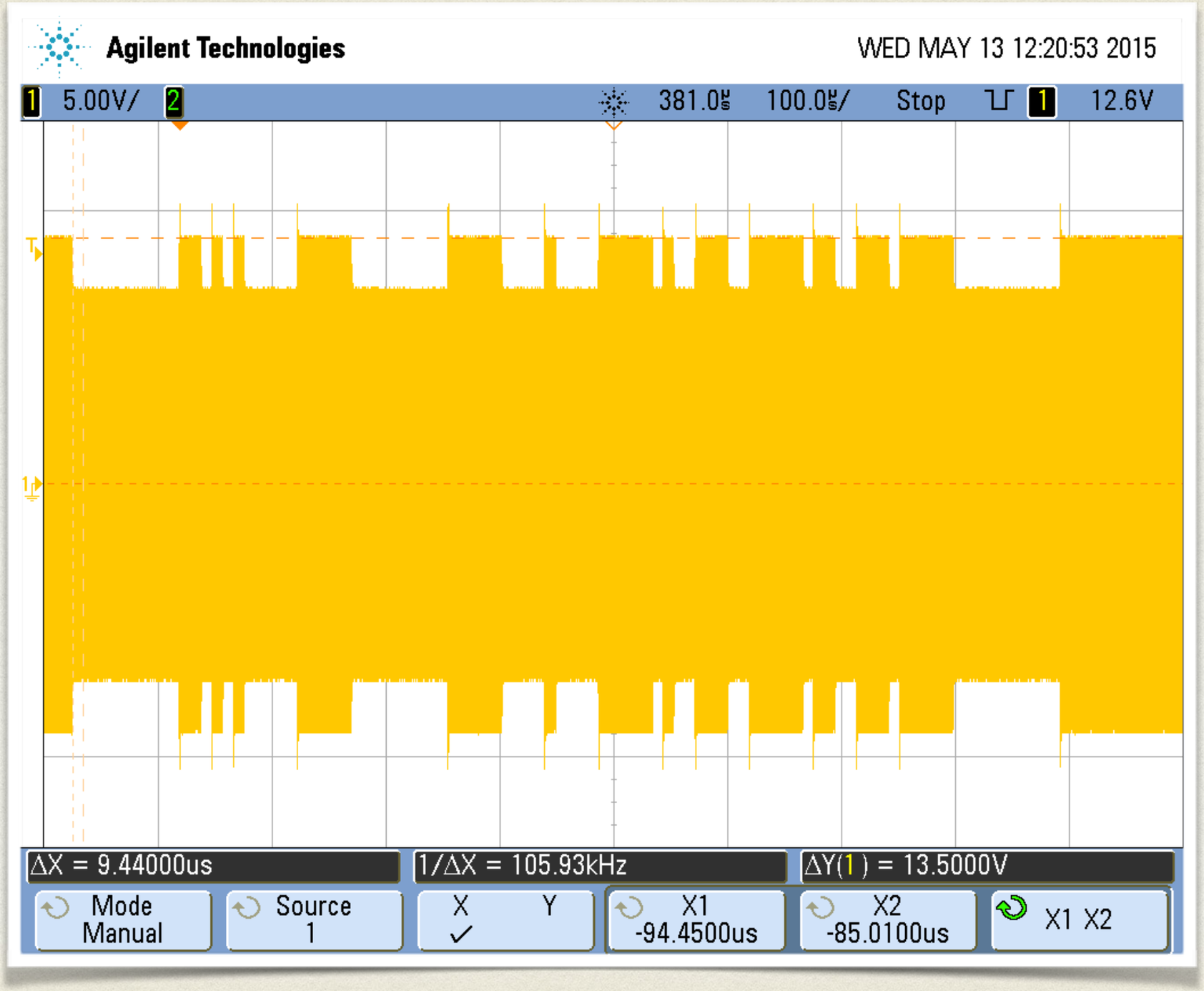
INITIATOR SPEAKING NFC-A



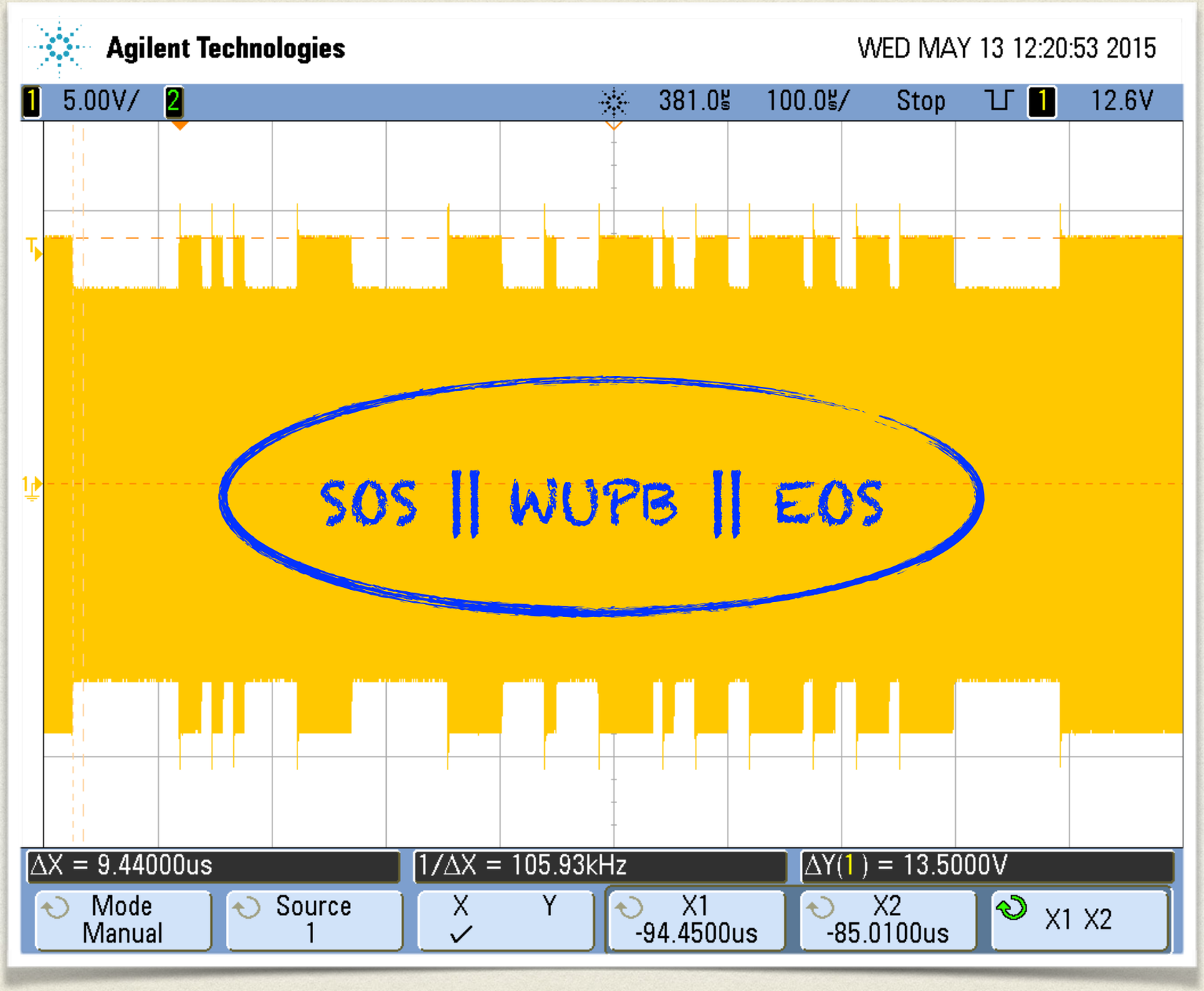
INITIATOR SPEAKING NFC-A



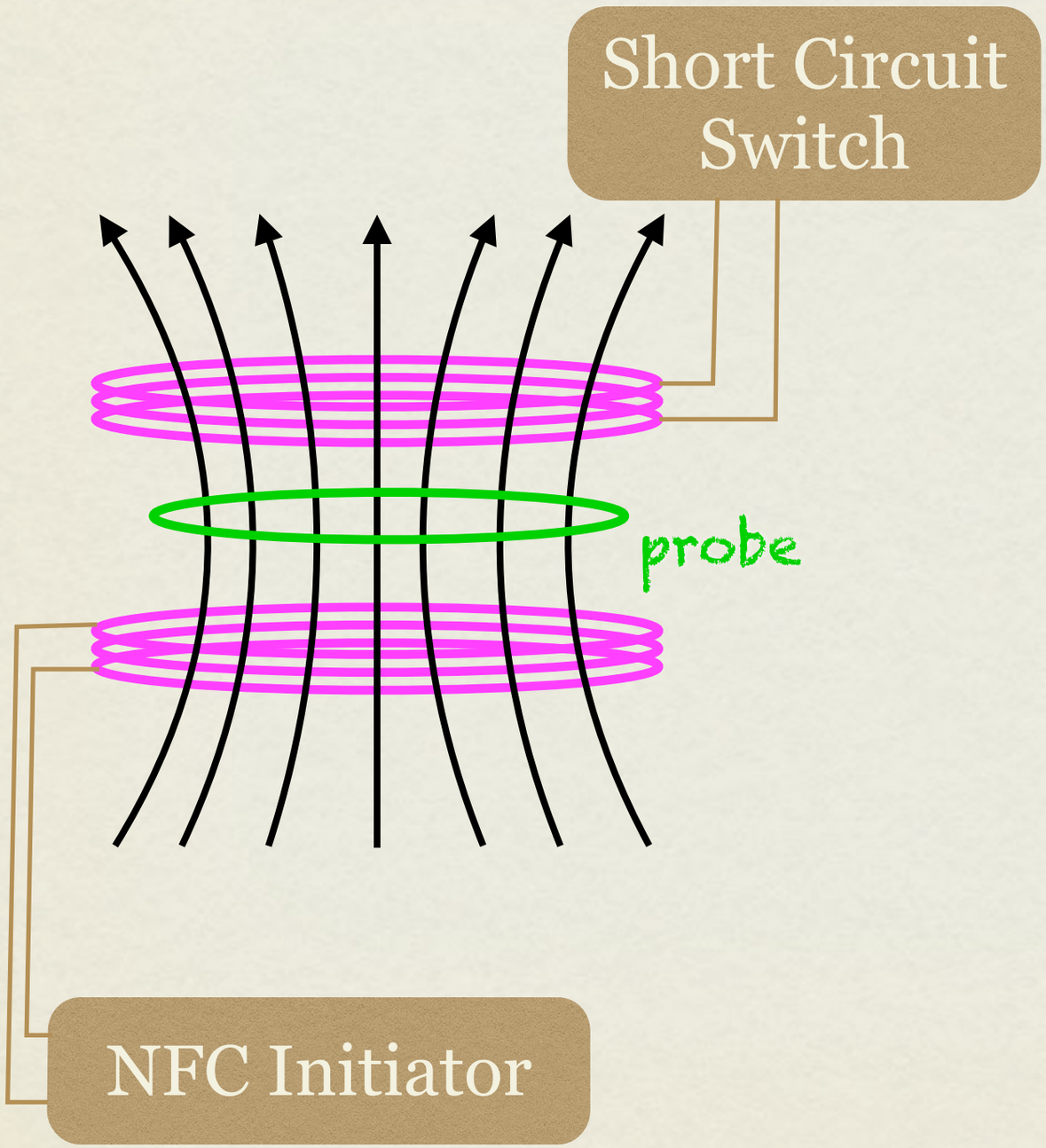
INITIATOR SPEAKING NFC-B



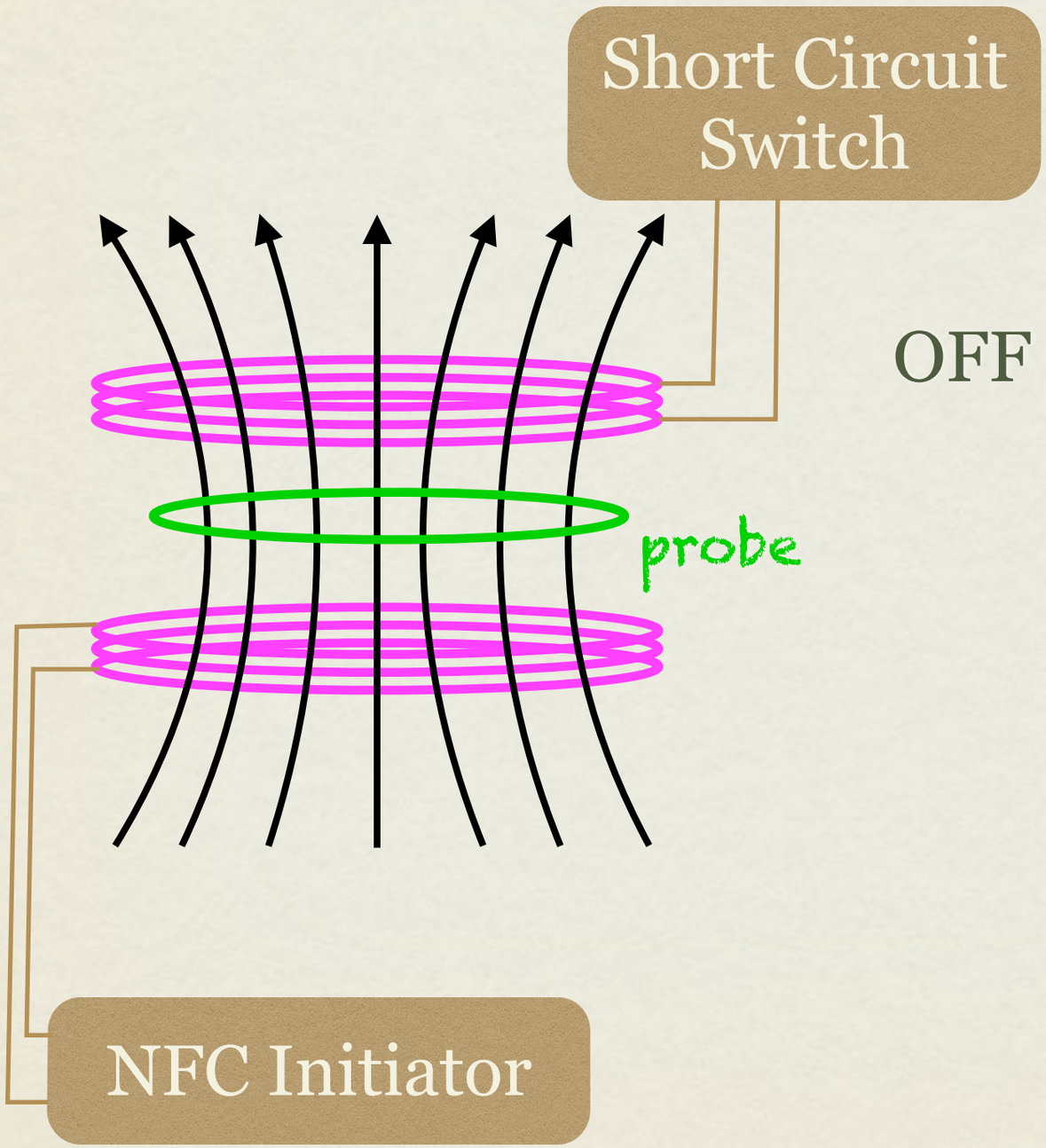
INITIATOR SPEAKING
NFC-B

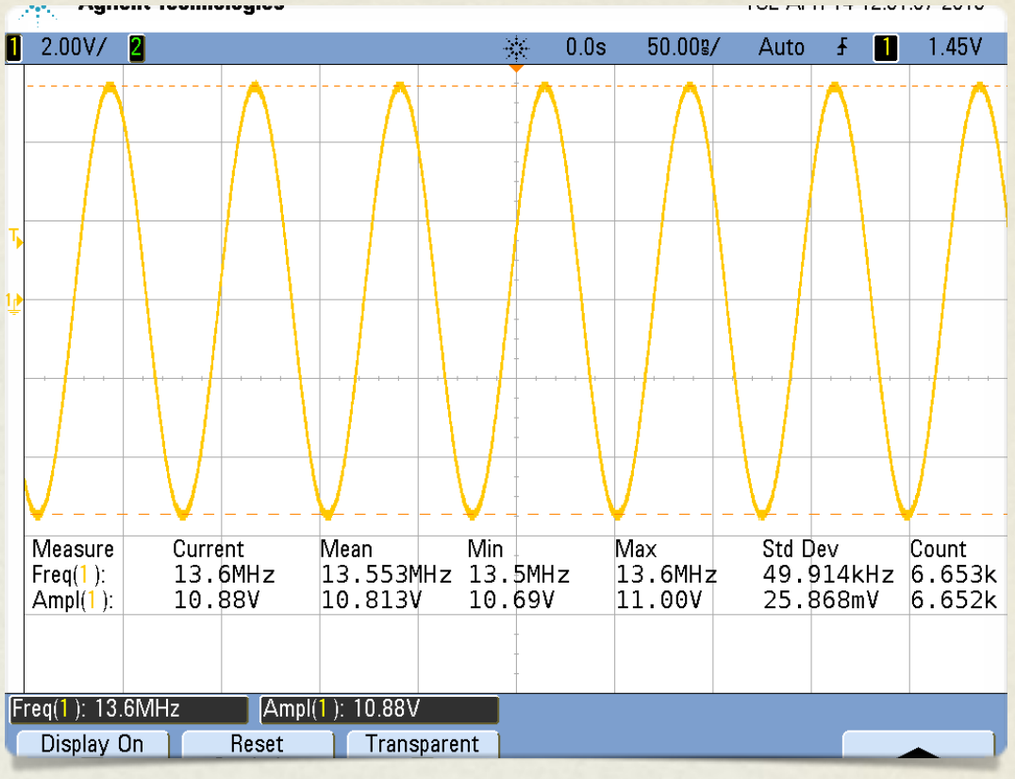


Lenz's Law Illustrated

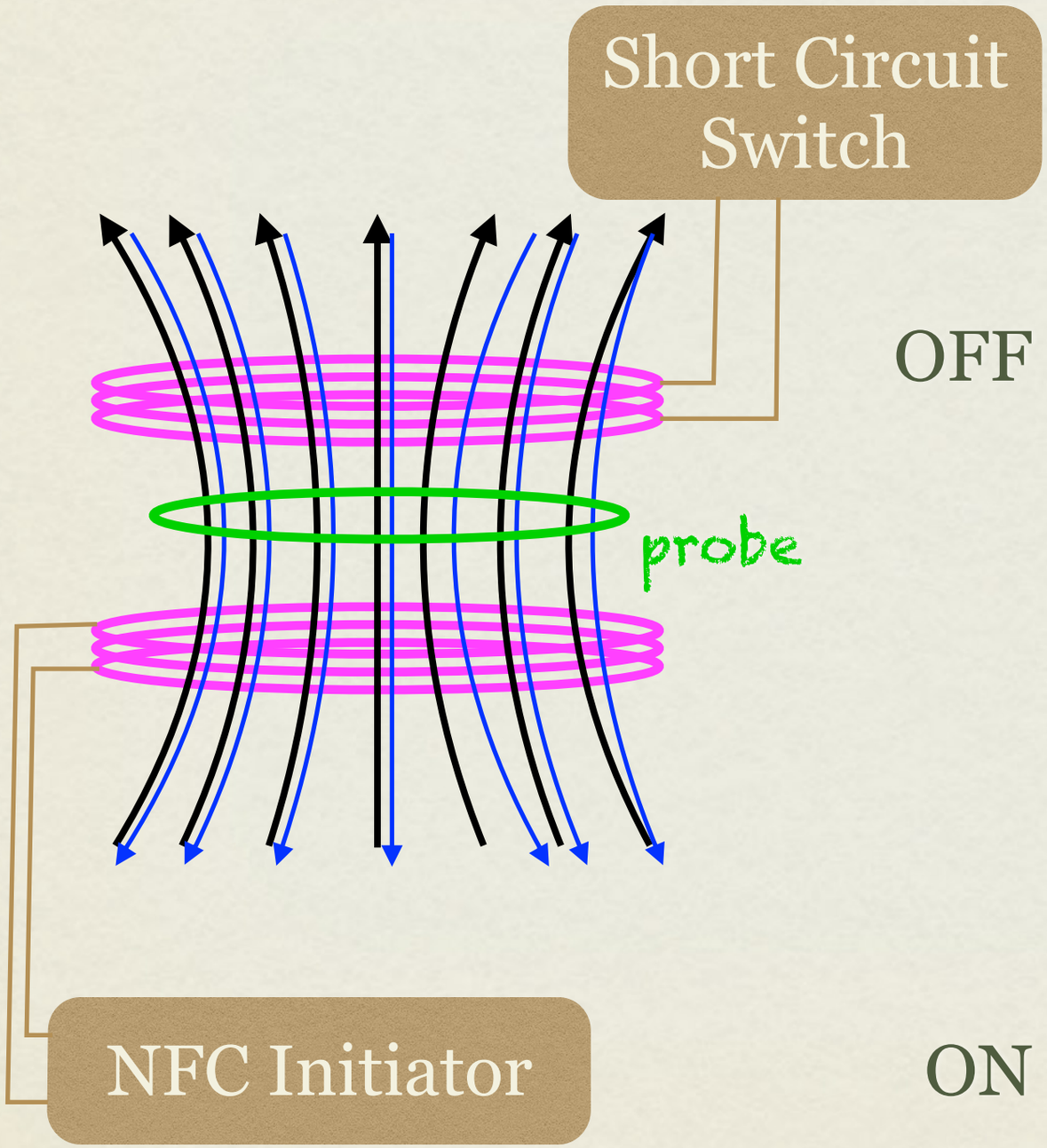


Lenz's Law Illustrated

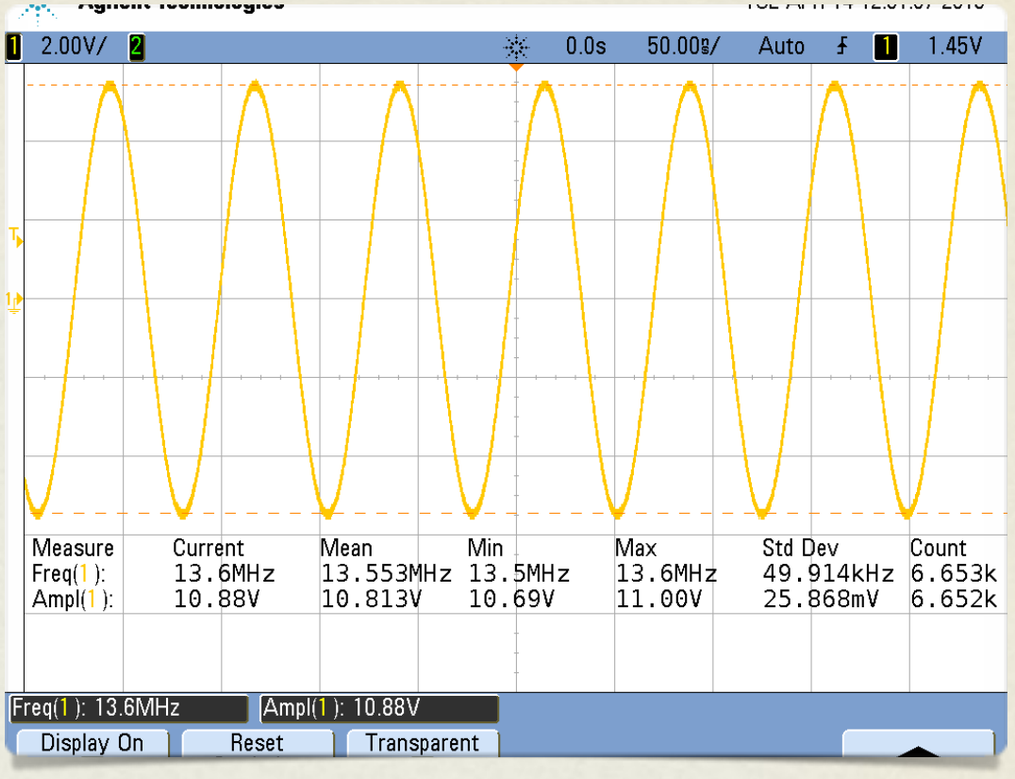




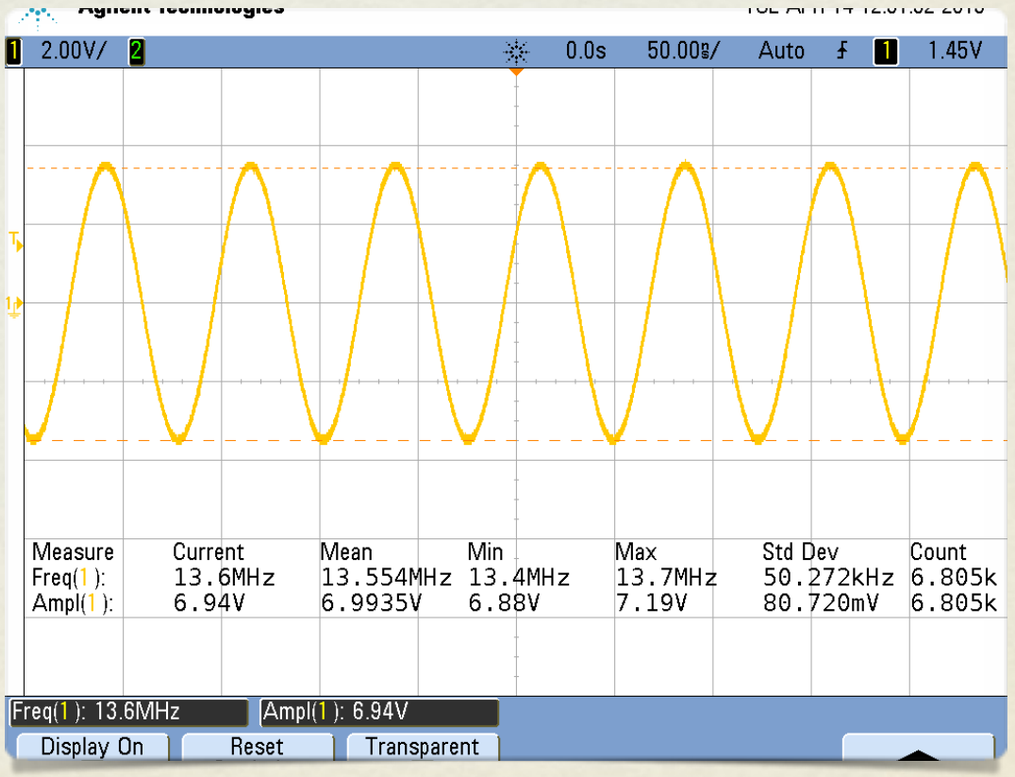
Lenz's Law Illustrated



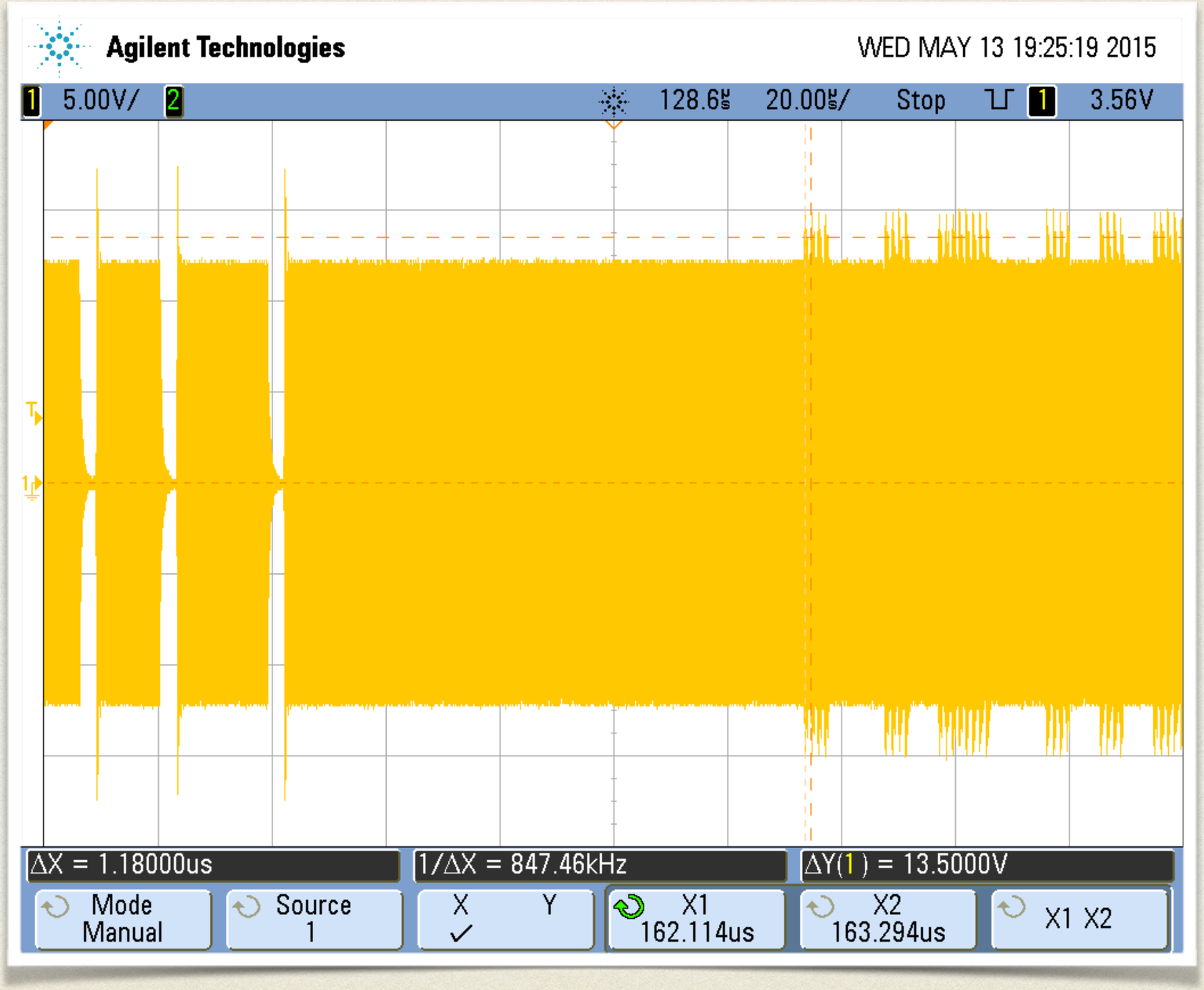
OFF



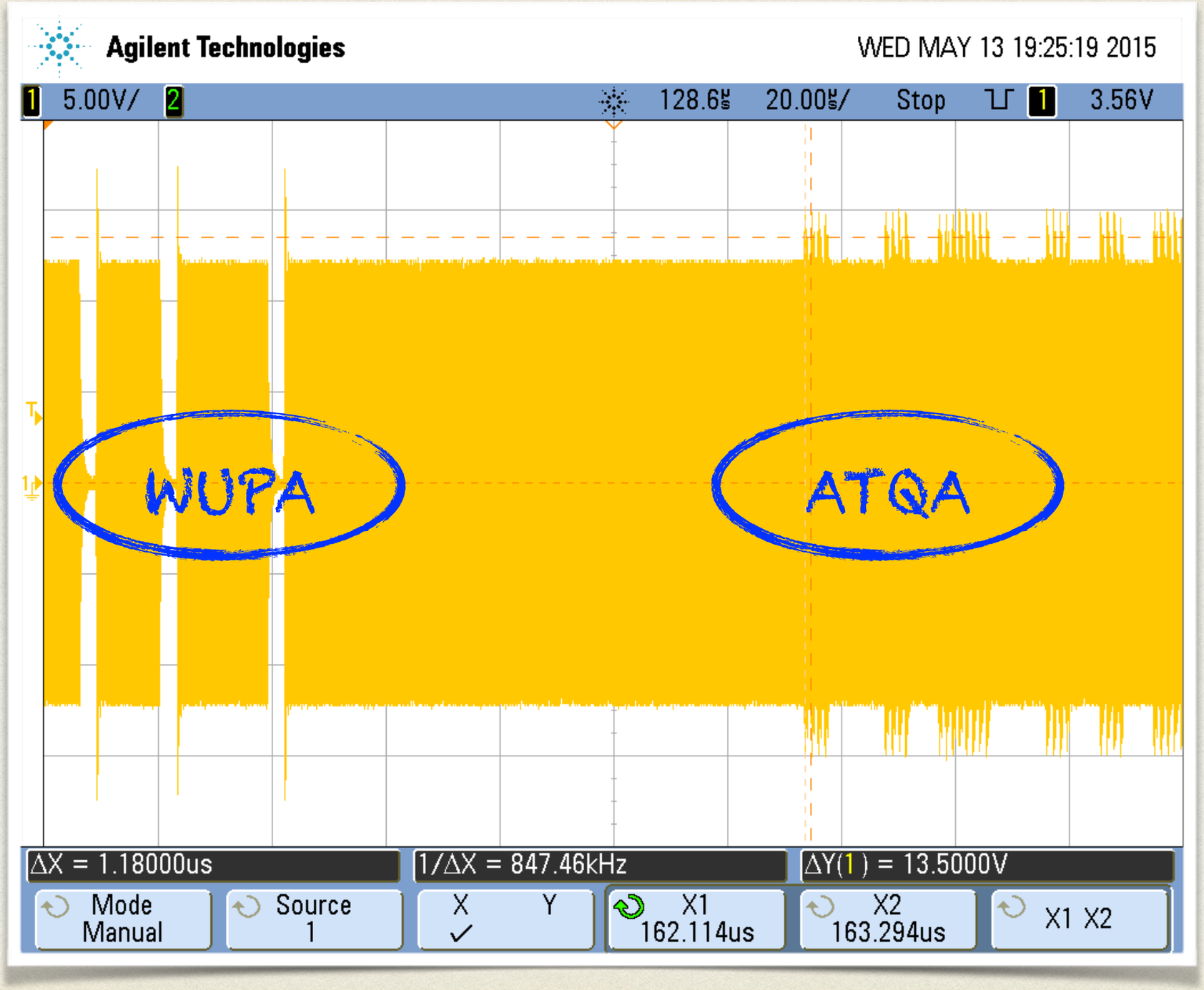
ON



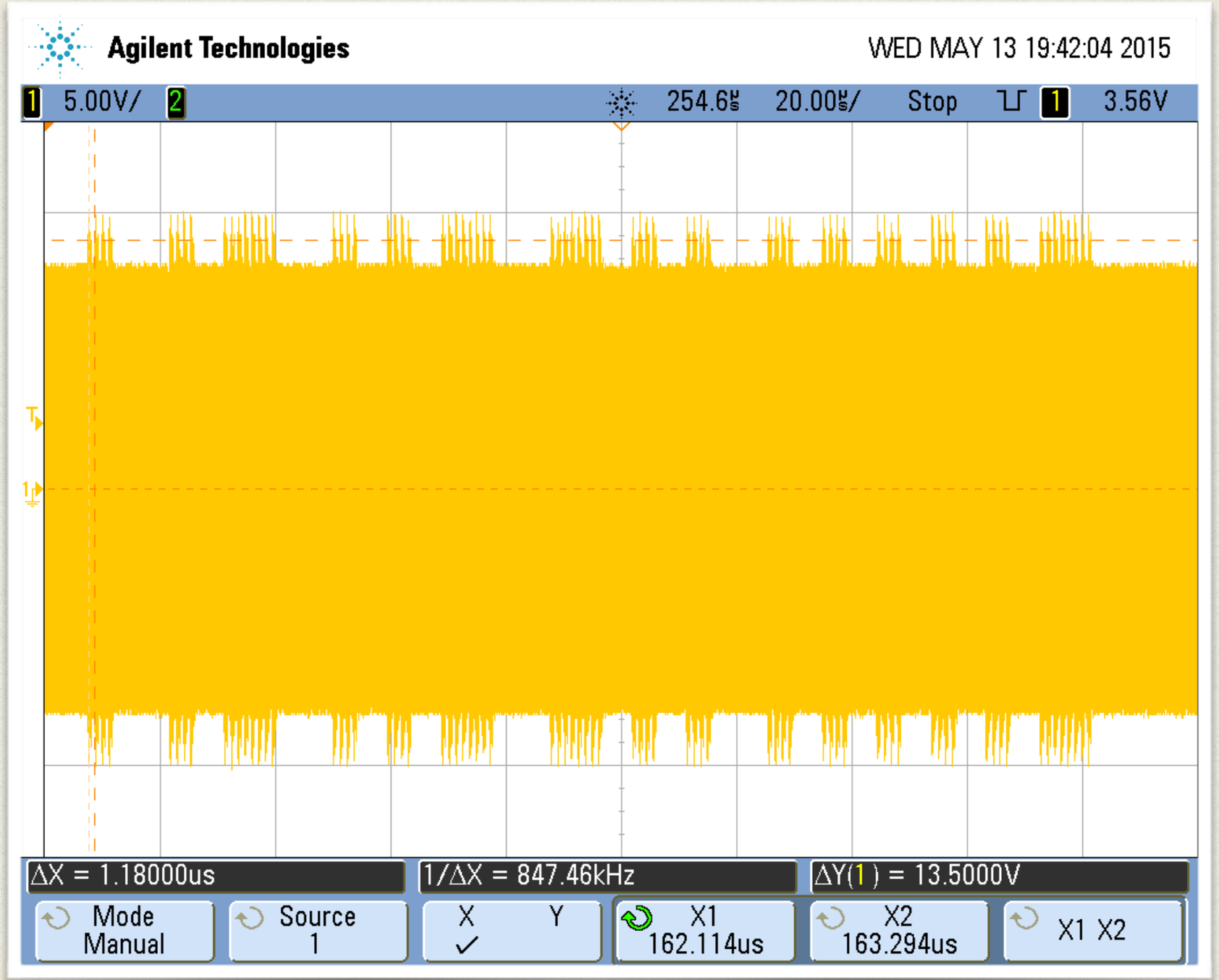
TARGET RESPONSE NFC-A



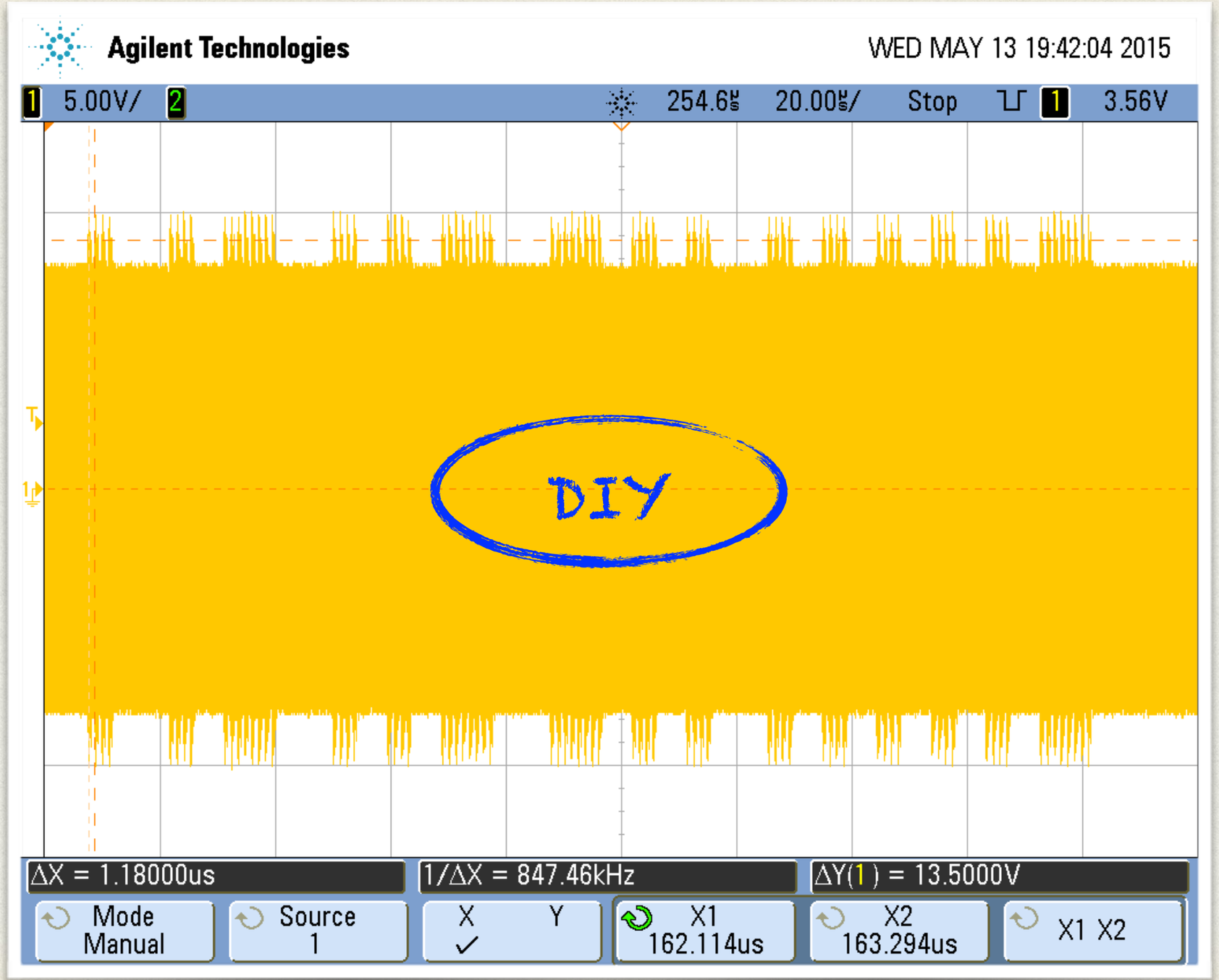
TARGET RESPONSE NFC-A



IF U LIKE IT HOT (THE WHOLE QUIZ)



IF U LIKE IT HOT (THE WHOLE QUIZ)



NFC OVERVIEW

<table>
<tr><th>Activity</th><th colspan="7">Technology / Device Platform</th></tr>
<tr><td>Listen, RF Collision Avoidance, Technology Detection, Collision Resolution</td><td colspan="4">NFC-A
Section 4</td><td>NFC-B
Section 5</td><td colspan="2">NFC-F
Section 6</td></tr>
<tr><td>Device Activation</td><td rowspan="3">NFC-DEP Protocol
Section 14</td><td>Type 1 Tag Platform
Section 8</td><td>Type 2 Tag Platform
Section 9</td><td>Type 4A Tag Platform
Section 11</td><td>Type 4B Tag Platform
Section 12</td><td>Type 3 Tag Platform
Section 10</td><td rowspan="3">NFC-DEP Protocol

Section 14</td></tr>
<tr><td>Data Exchange</td><td colspan="2" rowspan="2">Type 1, 2, and 3 Tag Half-duplex Protocol
Section 7</td><td colspan="2" rowspan="2">ISO-DEP Protocol
Section 13</td><td rowspan="2">Type 1, 2, and 3 Tag Half-duplex Protocols
Section 7</td></tr>
<tr><td>Device Deactivation</td></tr>
</table>

[NFCForum-TS-DigitalProtocol-1.0, 2010]

NFC RADIO ATTACKS

(With the focus on the passive NFC mode.)

INITIATOR RANGE EXTENSION

- Allows RF skimming or wormhole (relay) attacks.
- Due to very low e_r and very high power consumption, it is practically limited to the reactive near field region (XNF).
- Antenna diversity separating downlink and uplink channels may help significantly.
- Distance: Decimetres (confirmed), reliably working at around 20 cm. Principal upper limit ≈ $\lambda/2\pi$, i.e. circa 3.5 m, is infeasible to achieve practically. So, we are limited to a kind of *bumping attack*.

TARGET RANGE EXTENSION

- Allows covert communication with NFC terminal.
- Combines the techniques for a long range sniffing with the reciprocal problem of an extended-range signal injection into the RF front-end of the terminal.
- Based on direct DSB (Double Side Band) or even SSB (Single Side Band) injection, basing on the particular terminal signal processing.
- Principally possible even from the Fraunhofer region.
- The terminal antenna gain together with its input sensitivity limits the distance.
- Distance: Metres (confirmed). Working from the Fraunhofer region is practically very hard.

SNIFFING

- Sensitive data capture, identity theft.
- Works over all zones, from XNF to Fraunhofer region.
- **Often, this scenario induces the most serious risks.**
- For regions outside XNF, the important idea is to look for higher harmonics of the 13.56 MHz carrier.
- Furthermore, antenna design and orientation varies through the regions.
- Distance: Metres to dekametres. Confirmed for both downlink and uplink channels.

ALL YOU NEED IS *LOOP*

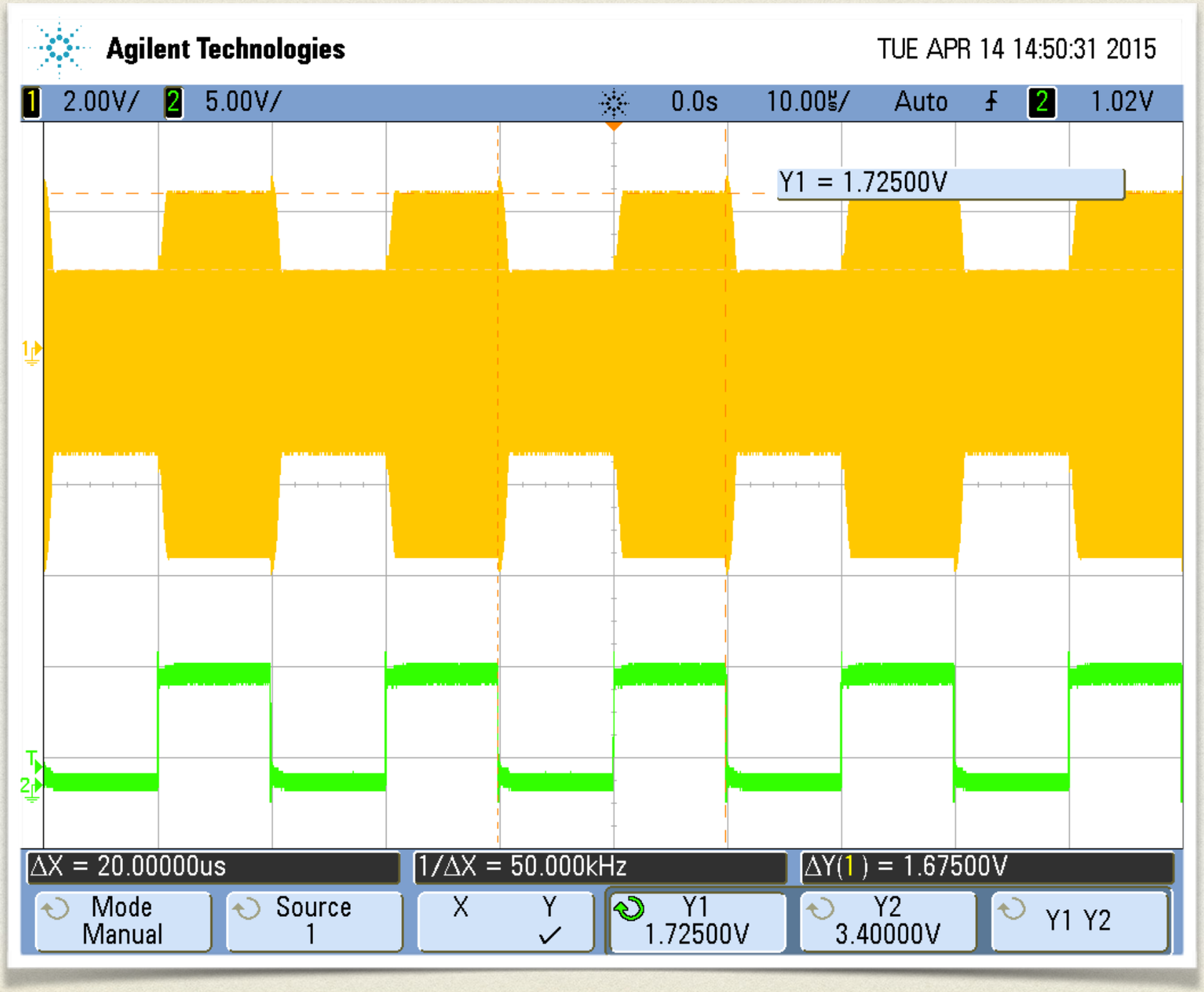
SPYING IN THE LANE (STILL IN XNF)

[https://www.youtube.com/watch?v=9QjxwejBPHs]

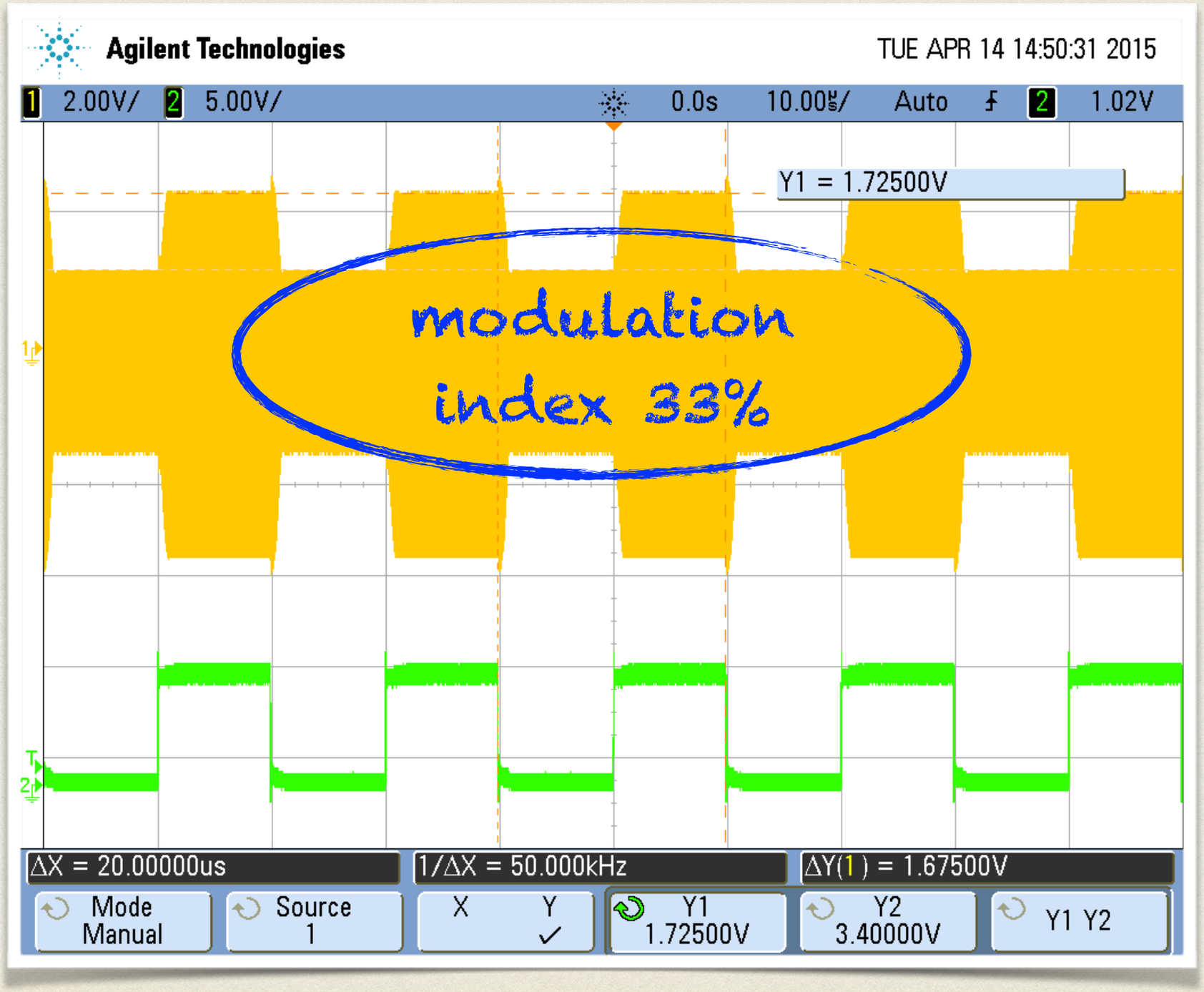
TRAFFIC INJECTION

- Allows Man-In-The-Middle scenarios.
- Due to the linear superposition in the EM field, the attacker does not have to be geometrically right in the middle, neither to break the original channel spatially.
- Again, a few turns of a wire around the original reader can be enough.
- Note we can also spoof the Initiator packets, besides the Target responses.
- Covering the path to the Target (downlink) requires XNF. One sided injection can work from the Fresnel or Fraunhofer regions as well.
- Distance: Decimetres (downlink TX covered) up to metres (TX for uplink only). Confirmed indirectly by other experiments together with own observations (cf. below).

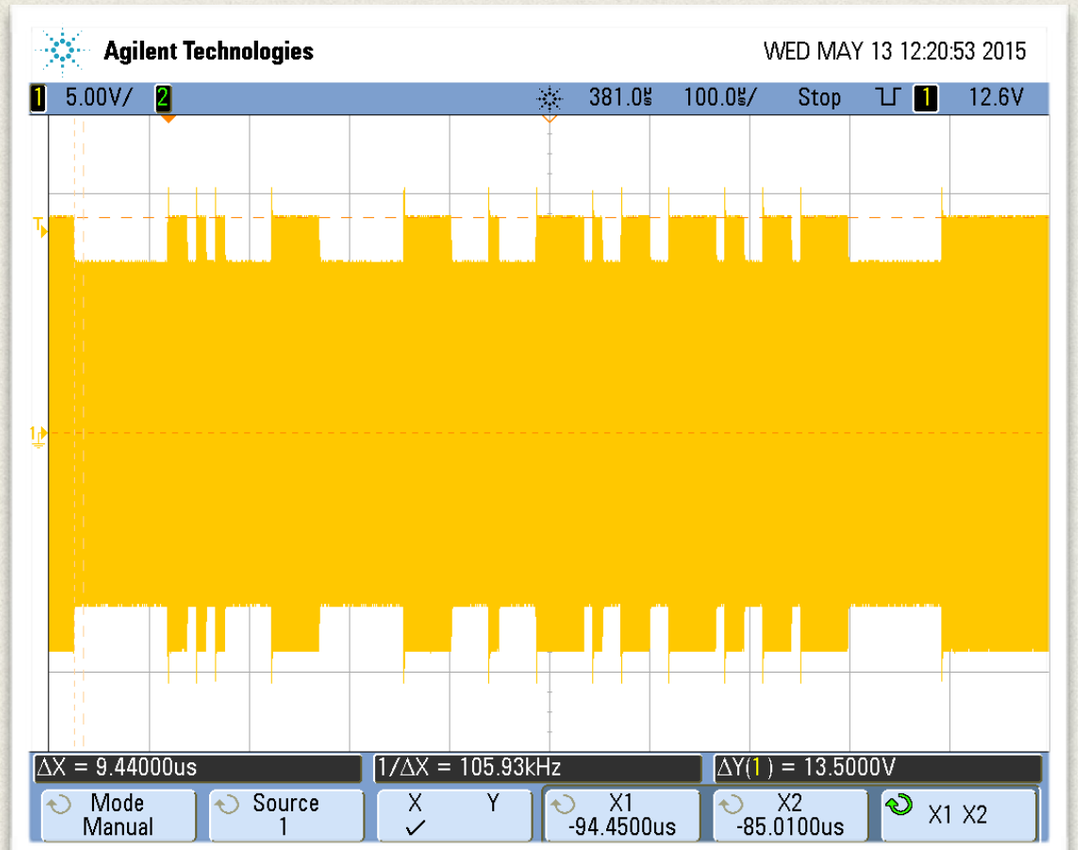
LENZ'S LAW BASED
"PASSIVE" DOWNLINK TX FOR NFC-B



LENZ'S LAW BASED
"PASSIVE" DOWNLINK TX FOR NFC-B

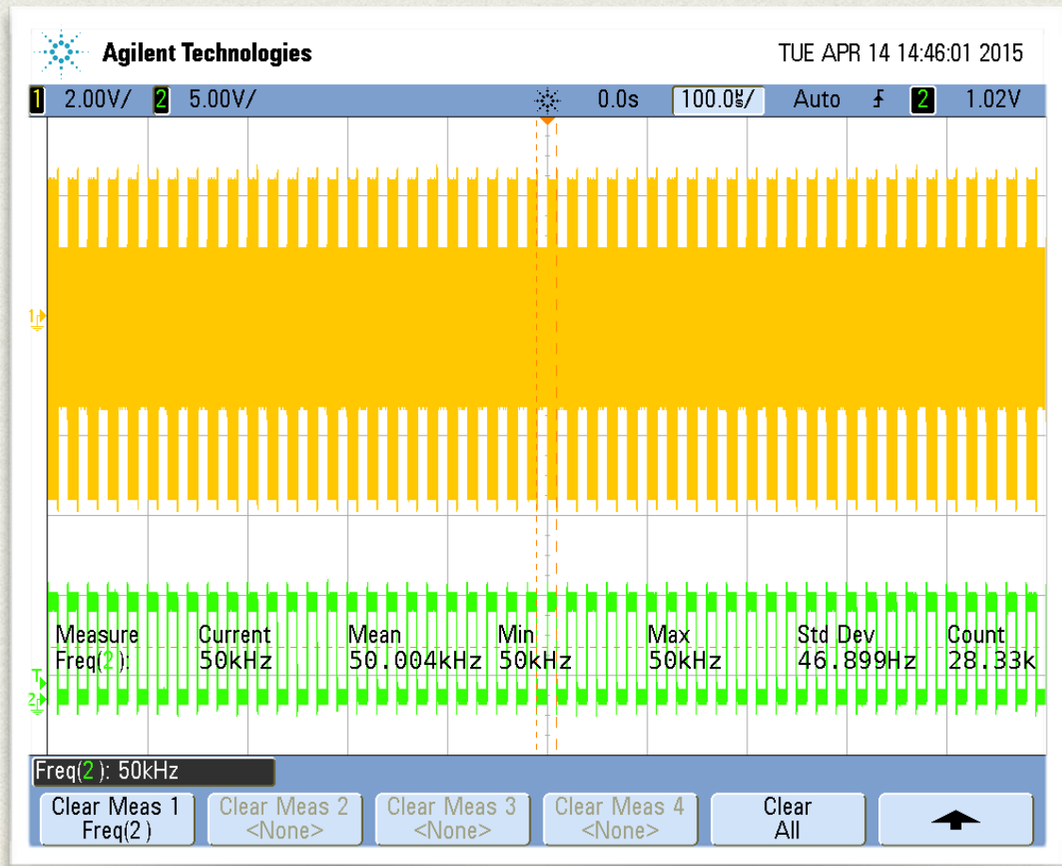


LET'S FACE IT



Original NFC-B Initiator

Lenz-style Fake TX



INITIATOR LOCATION

- Allows searching for active terminals - for instance, exposing passengers inspection, etc.

- Carrier detection at 13.56 MHz or higher harmonics, possibly also with the communication footprint.

- Distance: Dekametres. Indirectly confirmed by the eavesdropping experiments that can serve as a lower bound.

TARGET LOCATION

- Allows searching for potentially valuable assets.

- Searching based on radio characteristics without querying the higher protocol layers.

- Electronic Article Surveillance (EAS) style to search for the particular resonant circuits.

- Distance: Decimetres (confirmed by the range extension experiments) to metres (estimated).

JAMMING

- Allows DoS attacks at airport, office entry, market centre etc.

- We can use reciprocity theorems to estimate the effect an attacker's (measurement) antenna would have on the terminal input.

- Distance: Metres (confirmed by the range extension experiments) to dekametres (estimated).

DEVICE DESTRUCTION

- Allows selective DoS on the terminal or transponder.

- In principle, it requires a strong power pulse, so a near field approach is assumed.

- Distance: Decimetres.

CONCLUSIONS

- After all, **there is only one electromagnetic field out there**. NFC devices do not live in a separate universe. It is just a *different approach to the same theory*.
- Besides the wanted near field effects, there is always a plenty of other, possibly unwanted characteristics that can be exploited.
- We shall analyse the whole picture when designing NFC components to eliminate those undesired RF effects as much as possible.
    - Communication protocol engineers shall be fully aware of the residual threats then.
- We shall look for the remaining EM footprint carefully during security analysis and-or penetration tests.

POST SCRIPTUM

REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)

1. Brown, T.-C.-W. and Diakos, T.: *On the Design of NFC Antennas for Contactless Payment Applications*, 2011
2. Brown, T.-C.-W., Diakos, T., and Briffa, J.-A.: *Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards*, 2013
3. Diakos, T.-P., Briffa, J.-A., Brown, T.-W.-C., and Wesemeyer, S.: *Eavesdropping near-field contactless payments: a quantitative analysis*, 2013
4. Engelhardt, M., Pfeiffer, F., Finkenzeller, K., and Biebl, E.: *Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics*, 2013
5. Finkenzeller, K.: *Research Homepage*, http://rfid-handbook.de
6. Finkenzeller, K.: *Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities*, 2009
7. Finkenzeller, K.: *Battery powered tags for ISO/IEC 14443, actively emulating load modulation*, 2011
8. Finkenzeller, K., Pfeiffer, F., and Biebl, E.: *Range Extension of an ISO/IEC 14443 type A RFID System with Actively Emulating Load Modulation*, 2011
9. Francis, L., Hancke, G.-P., Mayes, K., and Markantonakis, K.: *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, 2011
10. Hancke, G.-P.: *Research Homepage*, http://www.rfidblog.org.uk/research.html
11. Hancke, G.-P.: *Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens*, 2011

REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)

12. Kfir, Z. and Wool, A.: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, 2005
13. Kirschenbaum, I. and Wool, A.: *How to Build a Low-Cost, Extended-Range RFID Skimmer*, 2006
14. Lee, Y.: *Antenna Circuit Design for RFID Applications*, Application Note 710, Microchip Tech. Inc., 2003
15. NXP: *AN1445 - Antenna design guide for MFRC52x, PN51x, and PN3x*, 2010
16. Oren, Y., Schirman, D., and Wool, A.: *Range Extension Attacks on Contactless Smart Cards*, 2013
17. Pfeiffer, F., Finkenzeller, K., and Biebl, E.: *Theoretical Limits of ISO/IEC 14443 type A Eavesdropping Attacks*, 2012
18. Rosa, T.: *RFID Wormholes – the Case of Contactless Smart Cards*, 2011
19. Thevenon, P.-H., Savry, O., Tedjini, S., and Malherbi-Martins, R.: *Attacks on the HF Physical Layer of Contactless and RFID Systems*, 2011
20. ISO/IEC 14443-1: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics*, 2000
21. ISO/IEC 14443-2: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface*, 2001
22. ISO/IEC 14443-3: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision*, 2001
23. ISO/IEC 14443-4: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol*, 2001
24. ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1), 2004

REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)

25. NFC Forum: *NFC Digital Protocol, Technical Specification*, 2010
26. EMV Contactless Specifications for Payment Systems: *Book D - EMV Contactless Communication Protocol Specification*, 2015