Exploiting Switching of Transistors in Digital Electronics for RFID Tags

Prof. Alenka Zajic

Georgia Institute of Technology

April 2018

❖Outline

- What is a side-channel?
- Analog side-channels
- New side-channel: Impedance-based side channel
- Leveraging impedance-based side channels for RFID tags
- Programmable RFID tags
- What comes next?

❖Side Channels

- A side channel is a means of obtaining information about software execution outside of the program’s intended communication
  - Is X a side channel?
  - Depends on what we consider “intended”
- Boils down to “you were not supposed to consider X as a source of information” (YWNS)

❖Categories of Side Channels

- Timing
  - YWNS performance
- Cache, BPred, etc.
  - YWNS microarchitecture
- Power, EM, acoustics, etc.
  - YWNS physical (analog) aspects of the implementation
- Bus snooping, DRAM-freezing, etc.
  - YWNS open the computer!

❖TEMPEST: A Signal Problem

- Bell Labs discovered first wireless side-channel in 1943.

- Cryptography community is concerned about this problem because private-public key encryption can be broken via side-channels.

- Focus on simple hardware such as microcontrollers

❖EM Emanations From Computer Systems

- EM emanations from modern systems (laptops, desktops, cellphones, IoT) exist
  - Can they leak any "interesting" information? (yes)
  - From how far away can they be received? (several meters)

[1] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 4, pp. 885-893, August 2014.

[2] D. Genkin, I. Pipman, and E. Tromer, "Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs," in Proc. Crypto. HW and Emb. Sys. (CHES), 2014.

[3] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation," in Proc. Crypto. HW and Emb. Sys. (CHES), 2015.

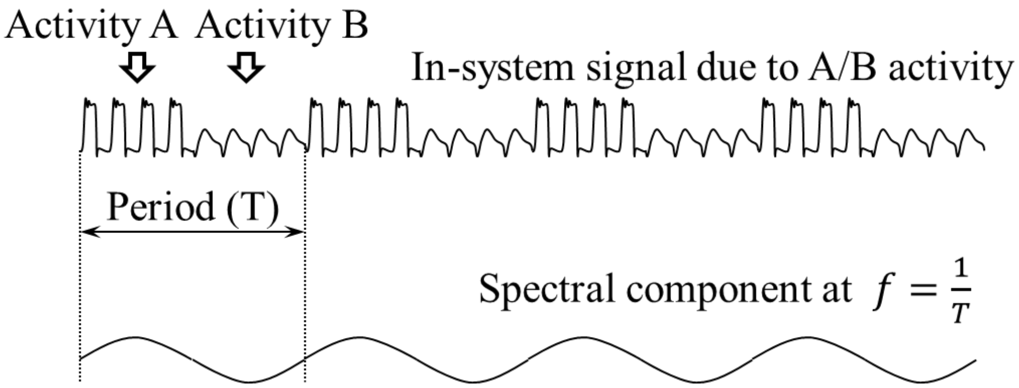
[4] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," Usenix Security Symposium 2015.

[6] R. Callan, A. Zajic, and M. Prvulovic, "FASE: Finding Amplitude-modulated side-channel emanations *Proceedings of the 42nd International Symposium on Computer Architecture (ISCA)*, pp. 592-603, June 2015.

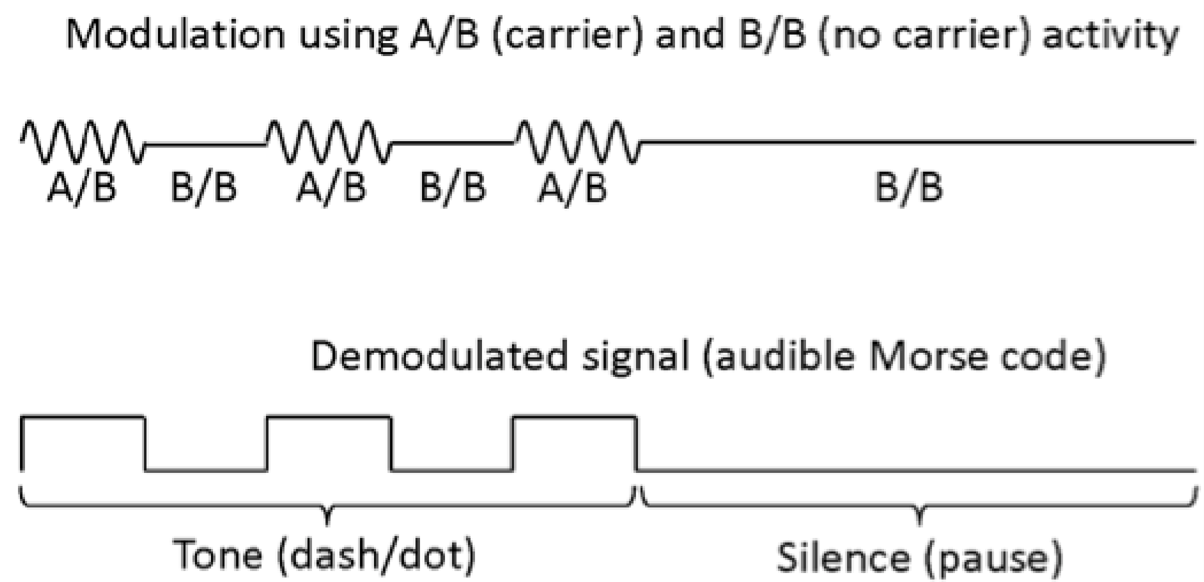
[7] R. Callan, A. Zajic, and M. Prvulovic, "A practical methodology for measuring the side-channel signal available to the attacker for instruction level events," *IEEE MICRO 14*, pp.1-12, Cambridge, UK, December 2014.

❖Creating the Alternating Signal

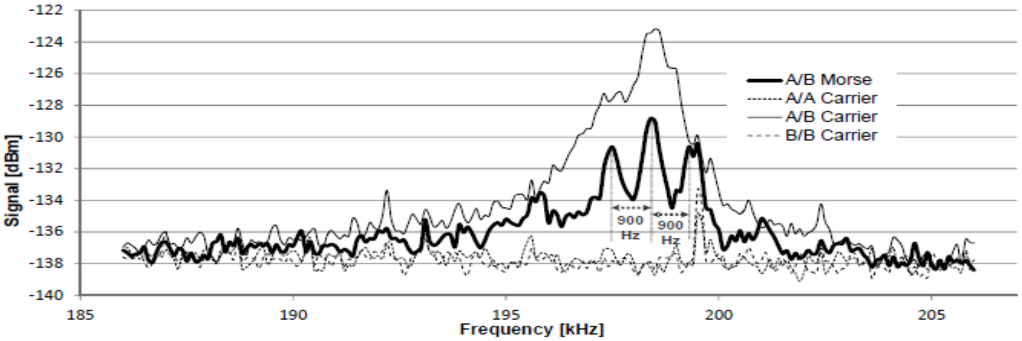
```
while(1){
  // Do some instances of the A instruction
  for(i=0;i<n_inst;i++){
    ptr1=(ptr1&~mask1)|((ptr1+offset)&mask1);
    // The A-instruction, e.g. a load
    value=*ptr1;
  }
  // Do some instances of the B instruction
  for(i=0;i<n_inst;i++){
    ptr2=(ptr2&~mask2)|((ptr2+offset)&mask2);
    // The B-instruction, e.g. a store
    *ptr2=value;
  }
}
```



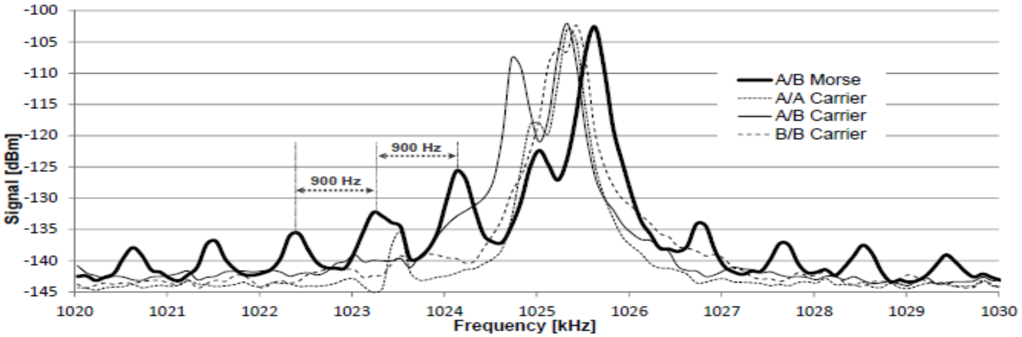
❖Transmitting Morse code



❖Modulation



(a) Spectrum at 200 kHz (Intended)



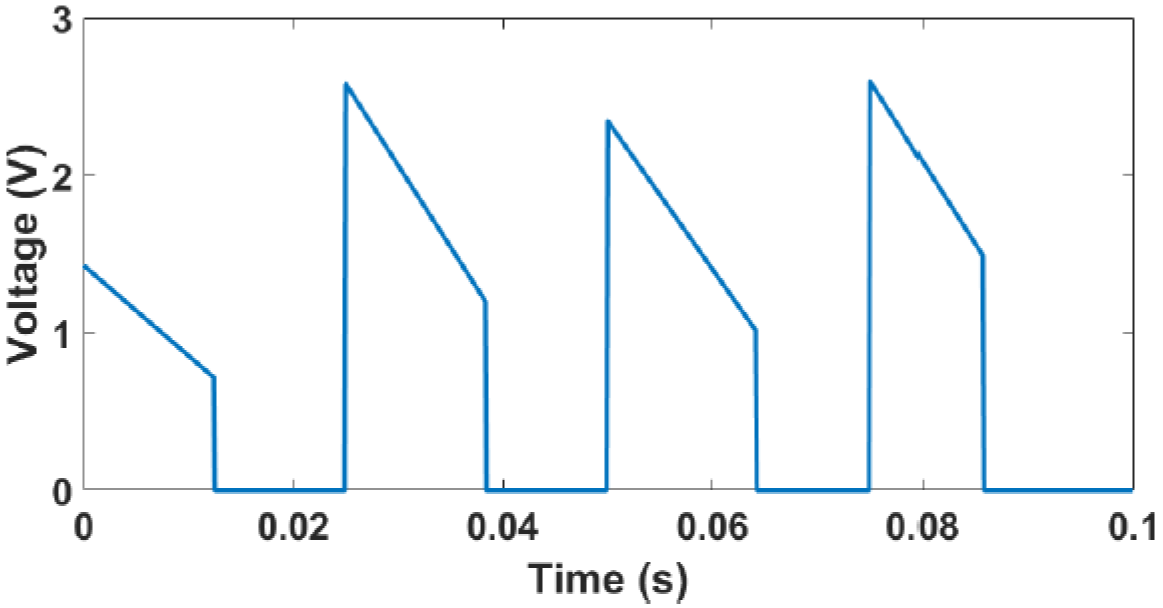
(b) Spectrum at 1025 kHz (Unintended)

Play video

Received spectra for the i7-based laptop when the program is creating emanations at 200 kHz

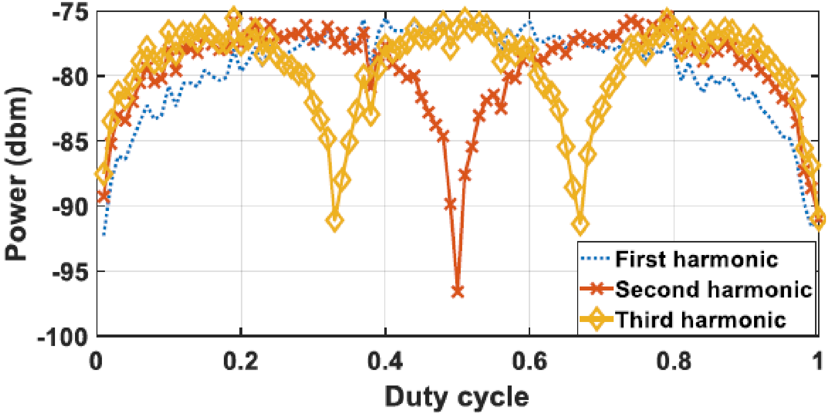
❖How Signal Gets Modulated?

Current-based side-channels (power, EM, acoustic measurements)

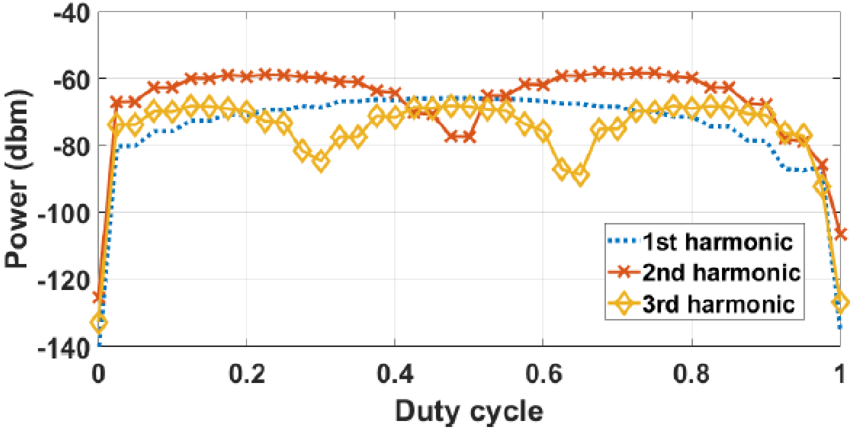


❖How Signal Gets Modulated?

Measured first three harmonics of power and EM signal

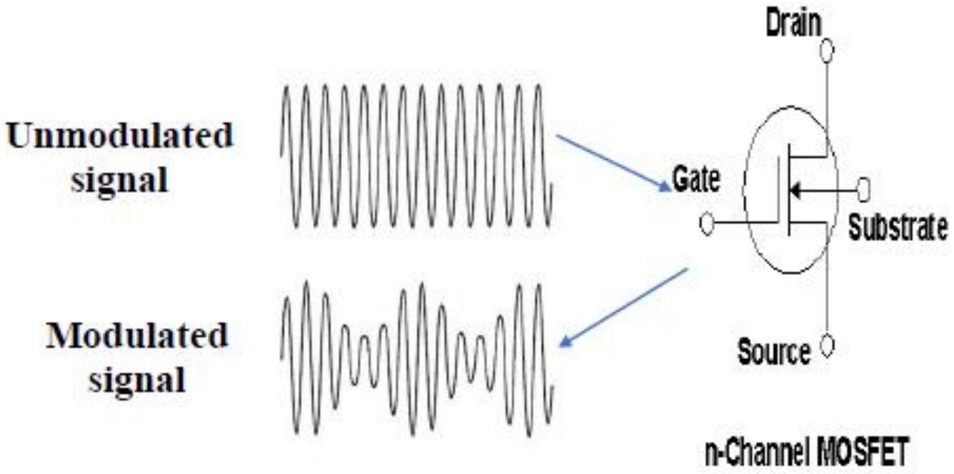


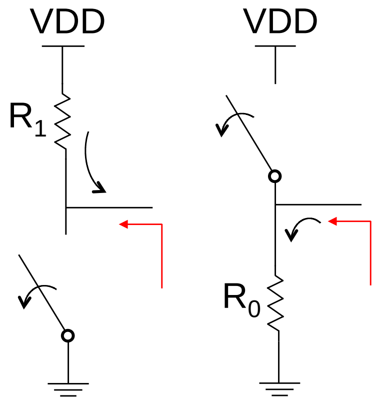
Power Measurements



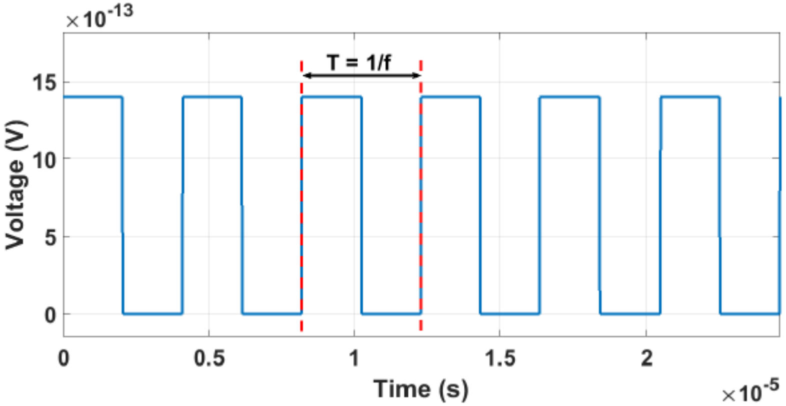
EM Measurements

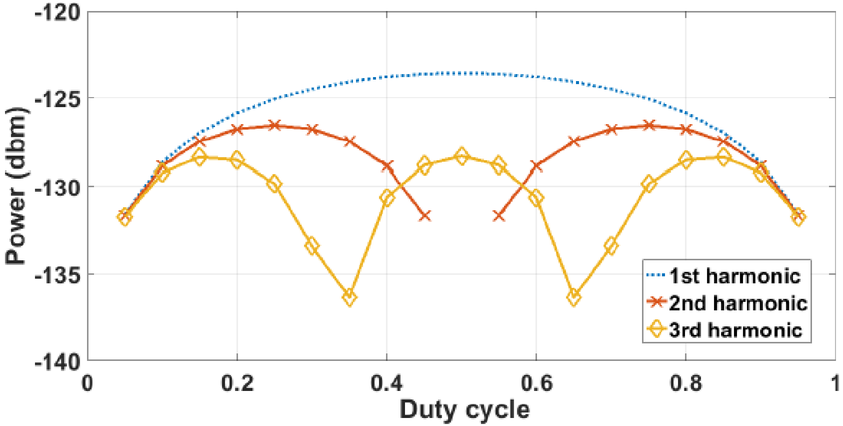
❖Impedance Based Side-Channel?



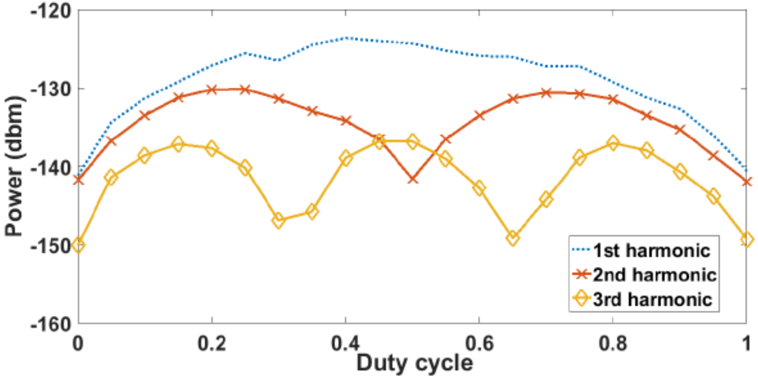


❖Impedance-based Side-Channel



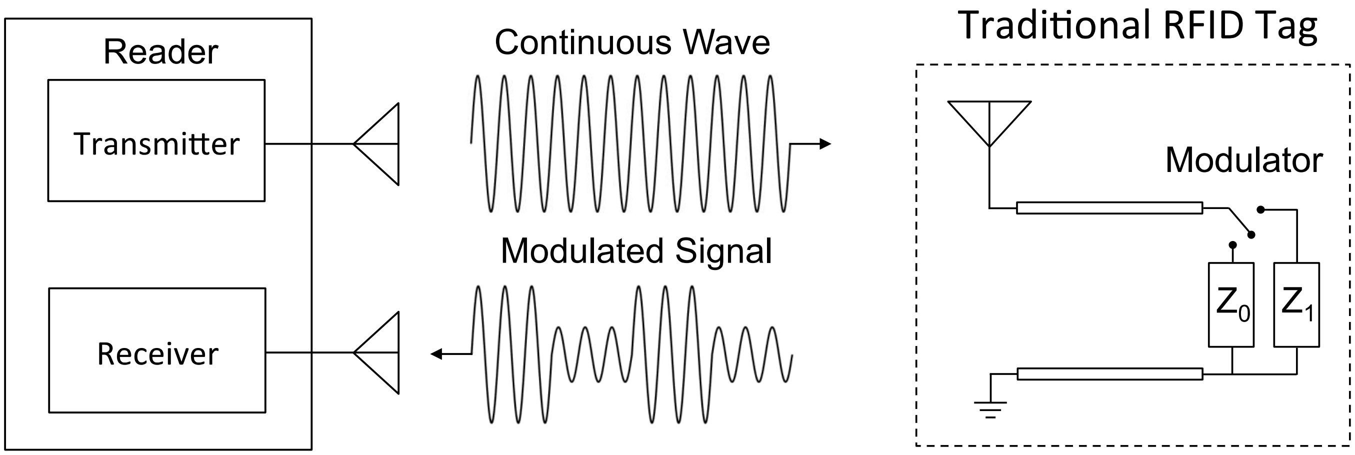


Ideal square-wave signal – time and frequency domain

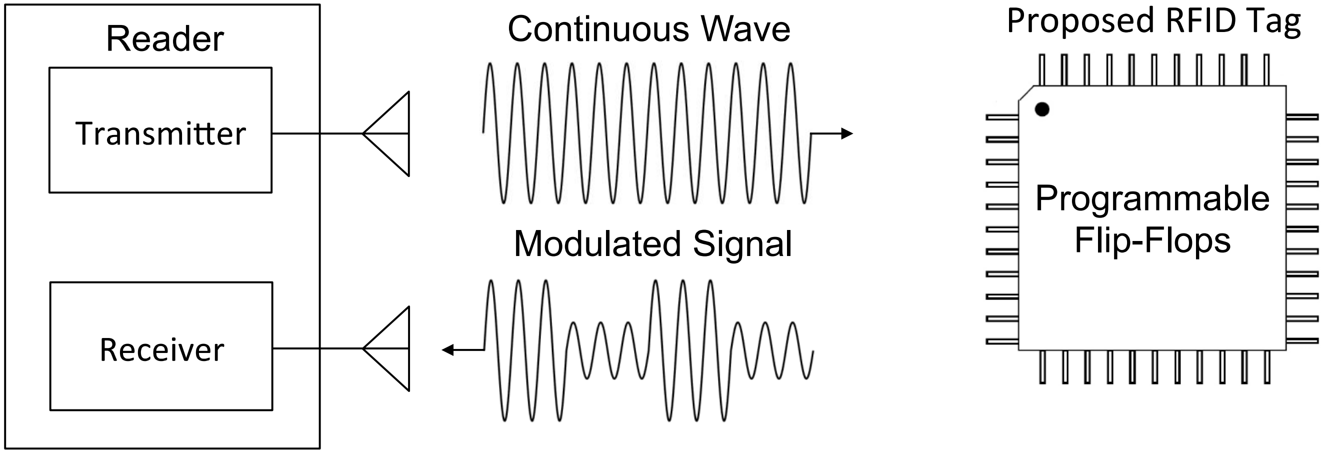


Measured backscattering side-channel

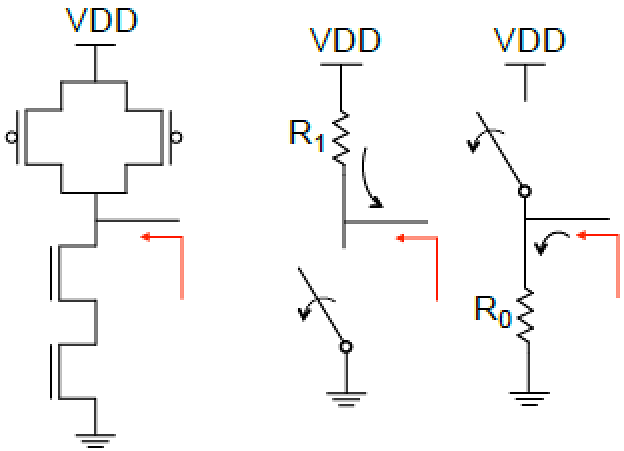
❖Traditional RFID Tag



❖New RFID Tag


Reader
Transmitter
Receiver
Continuous Wave
Modulated Signal
Proposed RFID Tag
Programmable
Flip-Flops

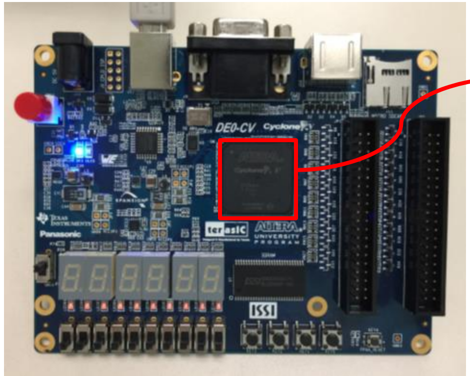
❖Backscattering from CMOS-NAND Latches

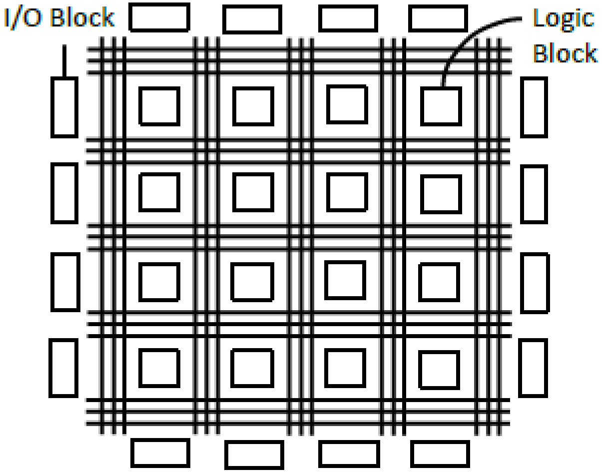


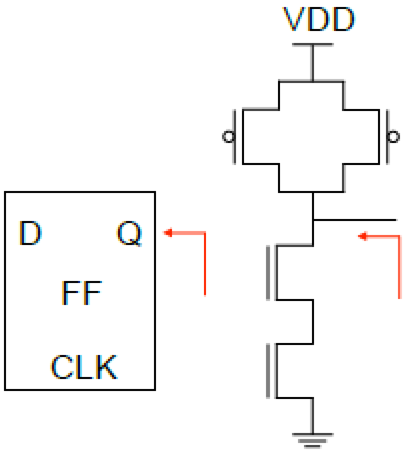
Output circuit of a CMOS-NAND latches

New RFID Tag

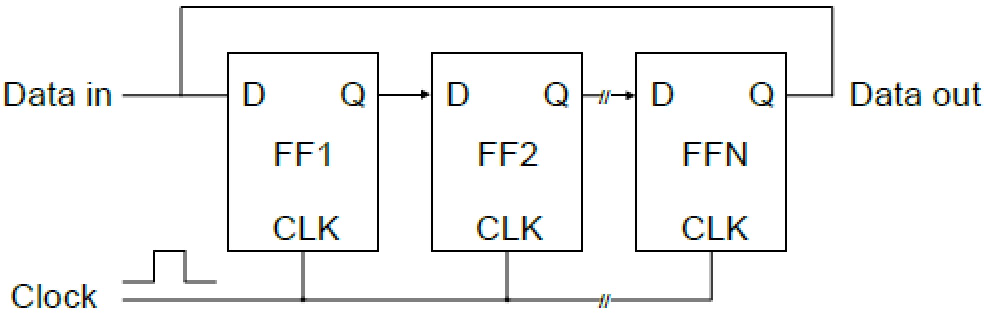
Altera Cyclone V FPGA







❖New RFID Tag

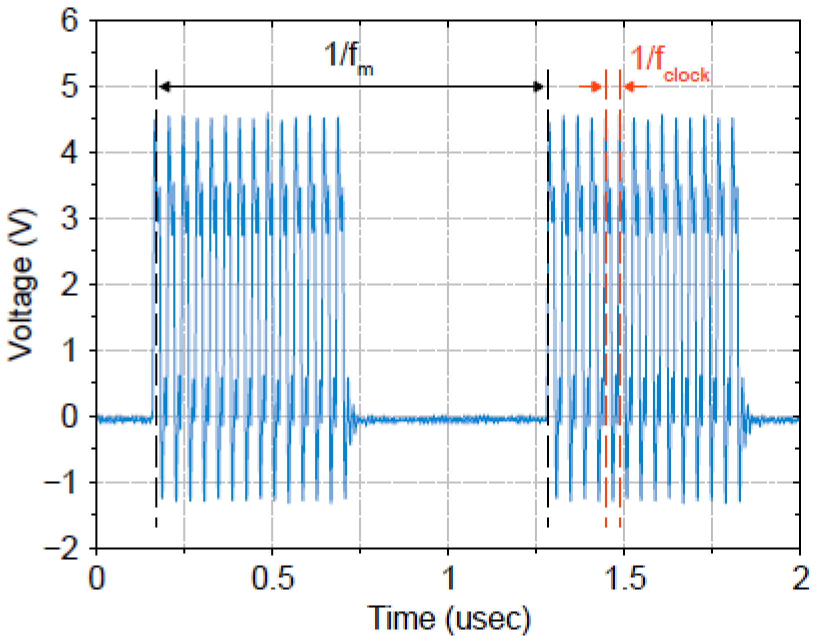


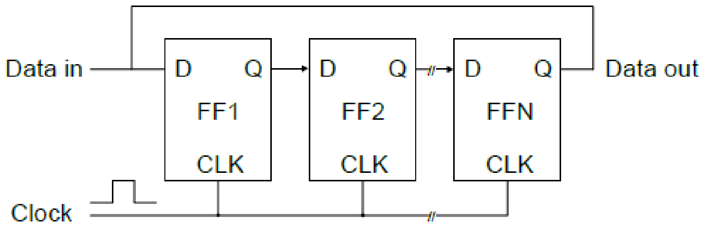
Toggling circuit that generates hardware switching activity.

- Output impedance is a parallel combination of output impedances of individual flip-flops.

- Total input impedance of the proposed RFID tag is inversely related to the logic utilization.

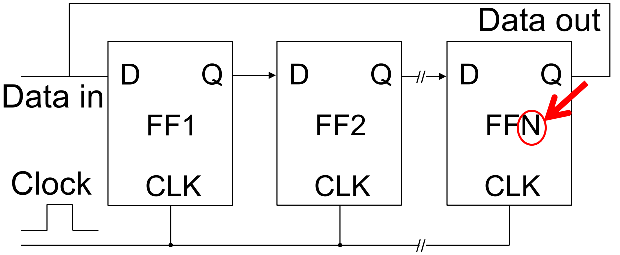
❖Modulated Signal of Proposed RFID Tag



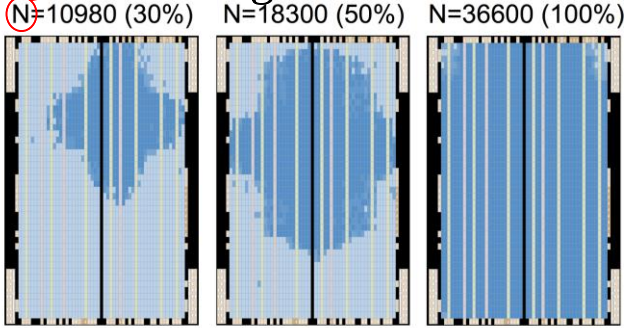


Flip-flops switching signal pattern at f_m=900 kHz.

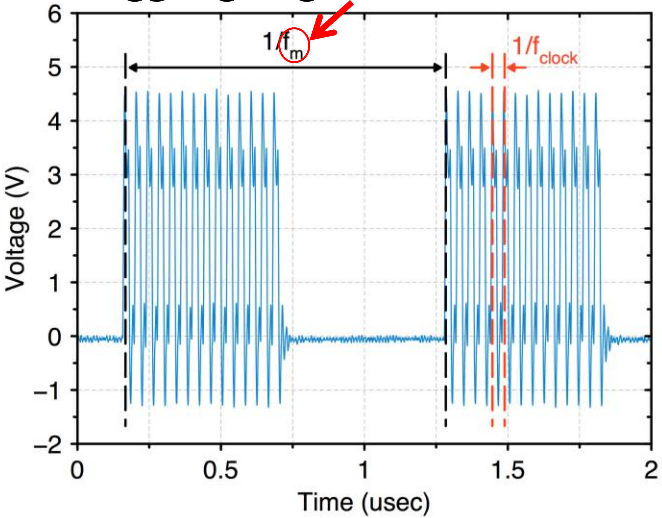
❖ Single-Bit RFID Design



Logic Utilization



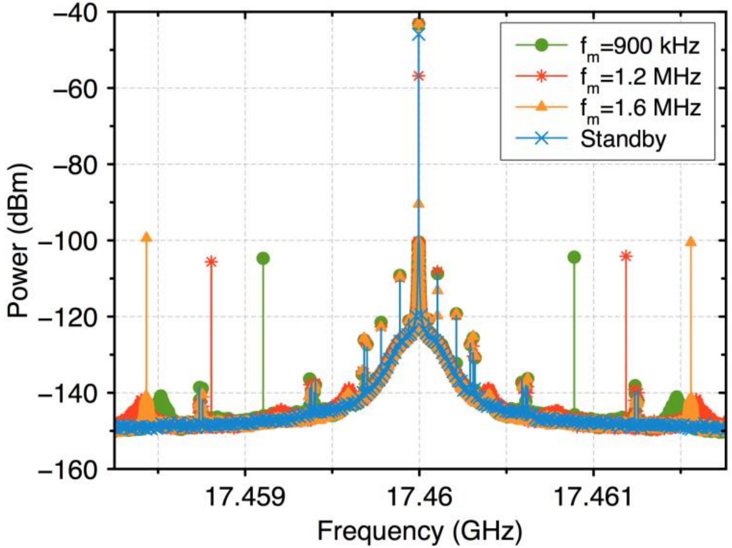
Toggling Signal Pattern



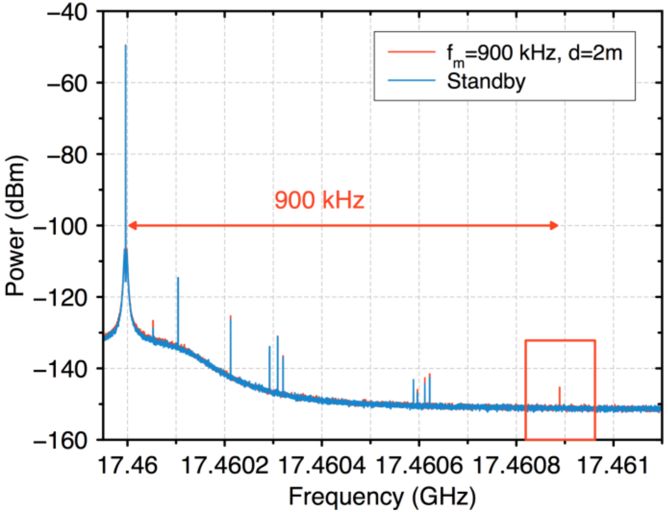
Parameter	Description	Controls
f_m	Modulating frequency	Location of modulated sideband
N	Number of configured flip-flops	SNR

❖Single-Bit RFID Design

Logic Utilization=100 %
f_m=900 kHz, 1.2 MHz, 1.6 MHz



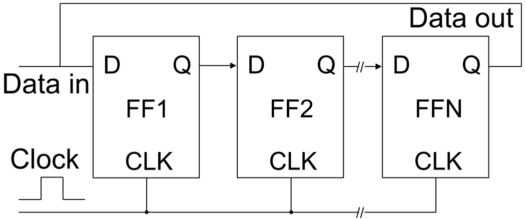
Max. Distance Measurement
Logic Utilization=100 % f_m=900 kHz



- Maximum SNR ~ 40 dB
- Maximum distance < 2 m
- Carrier frequency range: 1-20 GHz; lowest SNR~6 dB;
- Highest SNR~40 dB between 17 GHz and 18 GHz

❖Multi-Bit RFID Design

Single-Bit Design

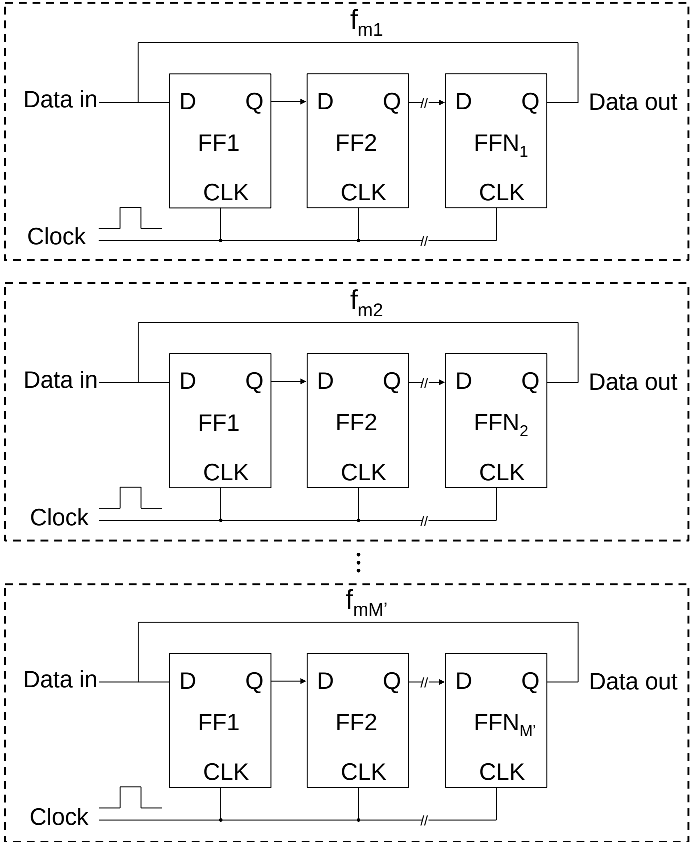


Multi-Bit Design

1st Bit

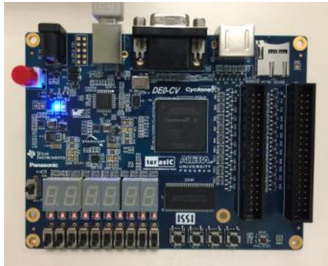
2nd Bit

M'th Bit

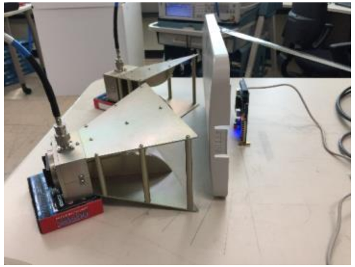


❖Measurement Setup

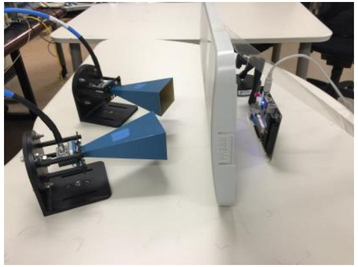
Altera Cyclone V FPGA



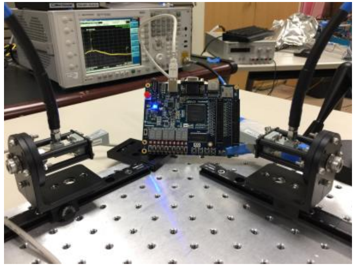
5.8 GHz



17.46 GHz



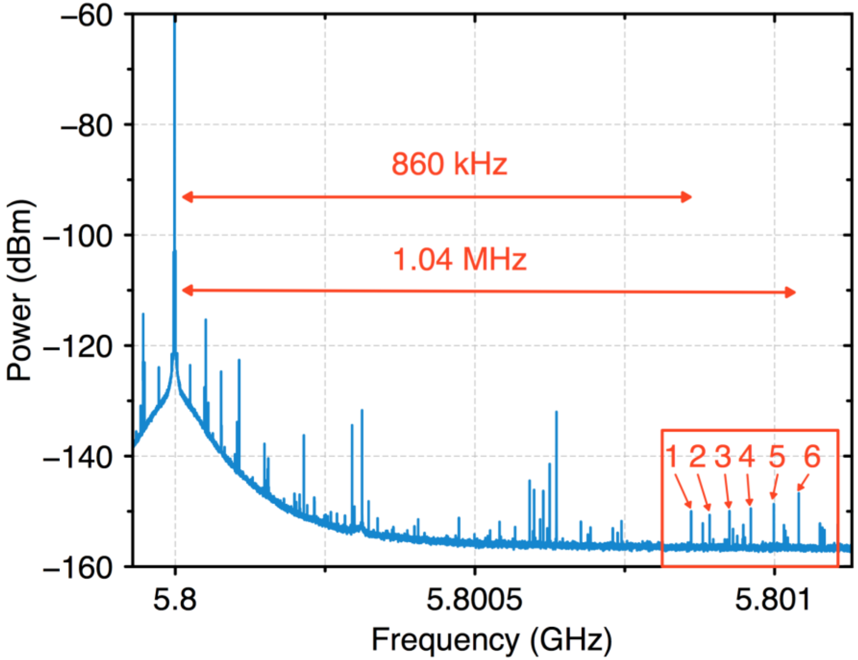
26.5 GHz



Antenna Parameters

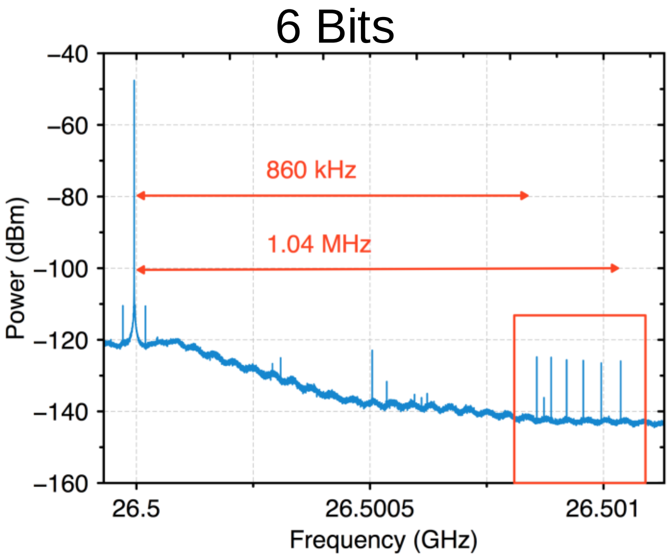
Antenna Model	Frequency	Gain	Half-Power Beamwidth
Com-Power AH-118	5.8 GHz (1-18 GHz)	10 dBi	50°
WR-62 PE9854/SF-20	17.46 GHz (12.4-18 GHz)	20 dBi	24°
A-INFO LB-28-10	26.5 GHz (26.5-40 GHz)	10 dBi	55°

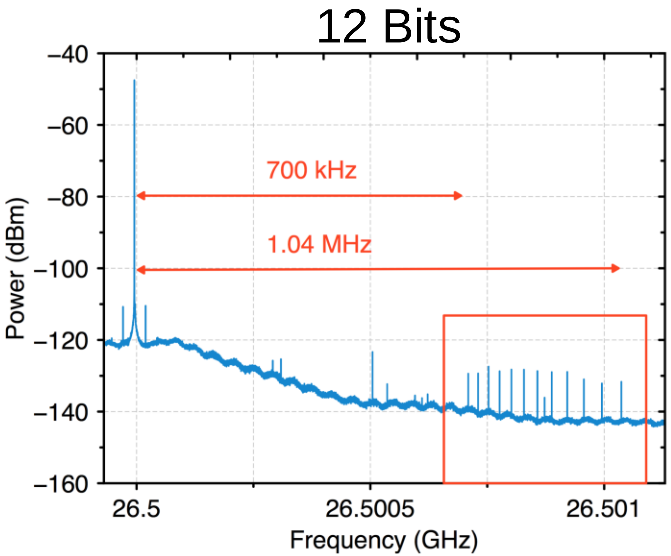
❖5.8 GHz 6 Bits Static ID



- P_t=15 dBm, d=20 cm
- SNR > 6 dB

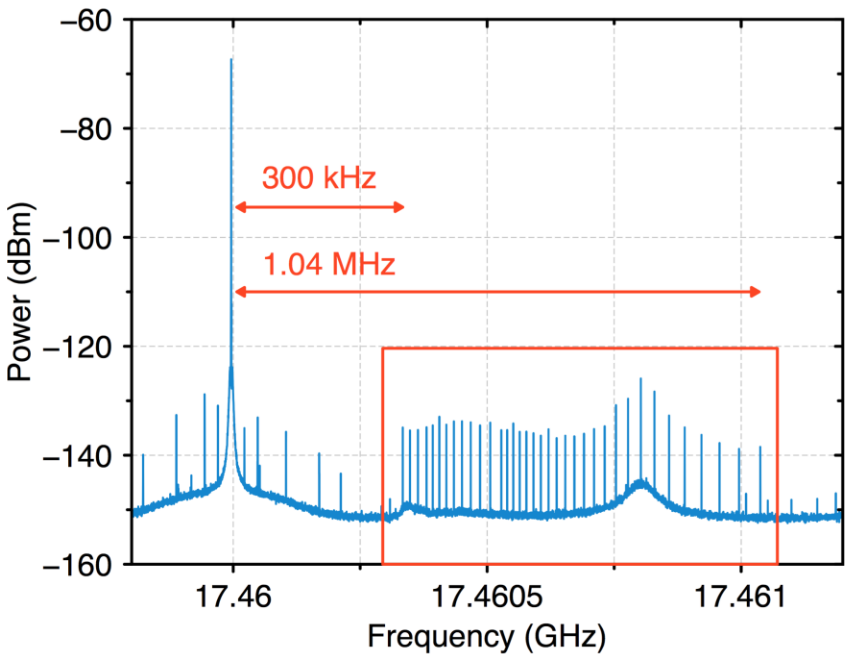
❖26.5 GHz 6 and 12 Bits Static IDs





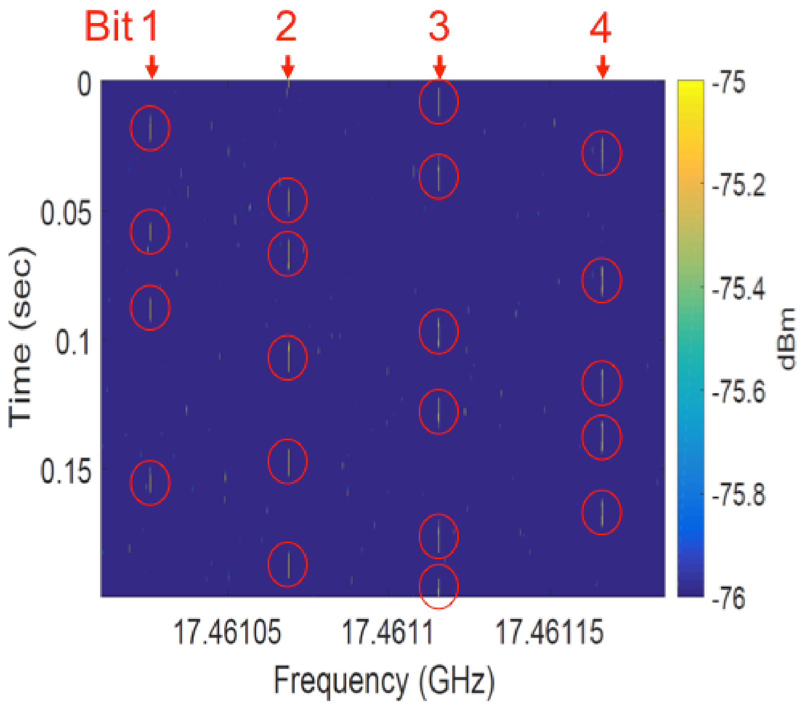
- Flexible bit design and carrier frequency selection
- SNR > 10 dB
- Each bit can be turned on and off individually to generate binary signals 1s and 0s with up to 4096 (2^12) combinations of unique ID

❖17.46 GHz 36 Bits Static ID



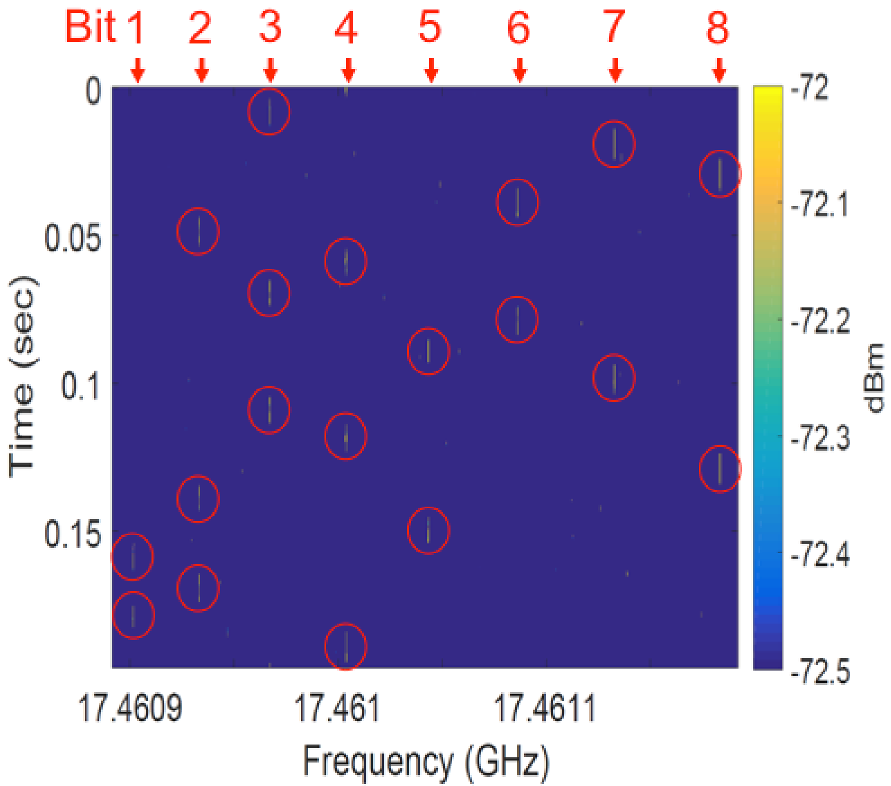
- Flexible bit design and carrier frequency selection
- SNR > 12 dB
- Each bit can be turned on and off individually to generate binary signals 1s and 0s with up to 68.7 billion (2^36) combinations of unique ID

❖4 Bits Dynamic ID



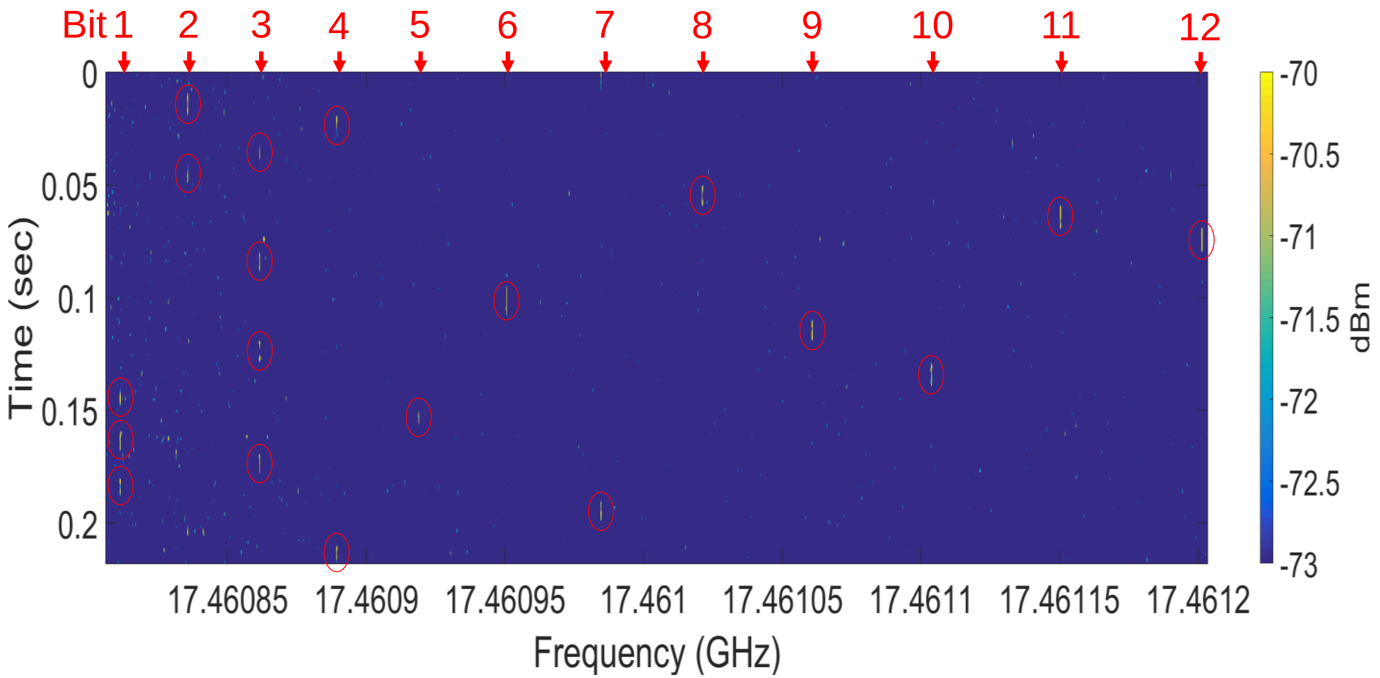
- f_s=100 Hz, providing a data rate of 400 bits/sec.
- All designed symbols are successfully detected.

❖8 Bits Dynamic ID



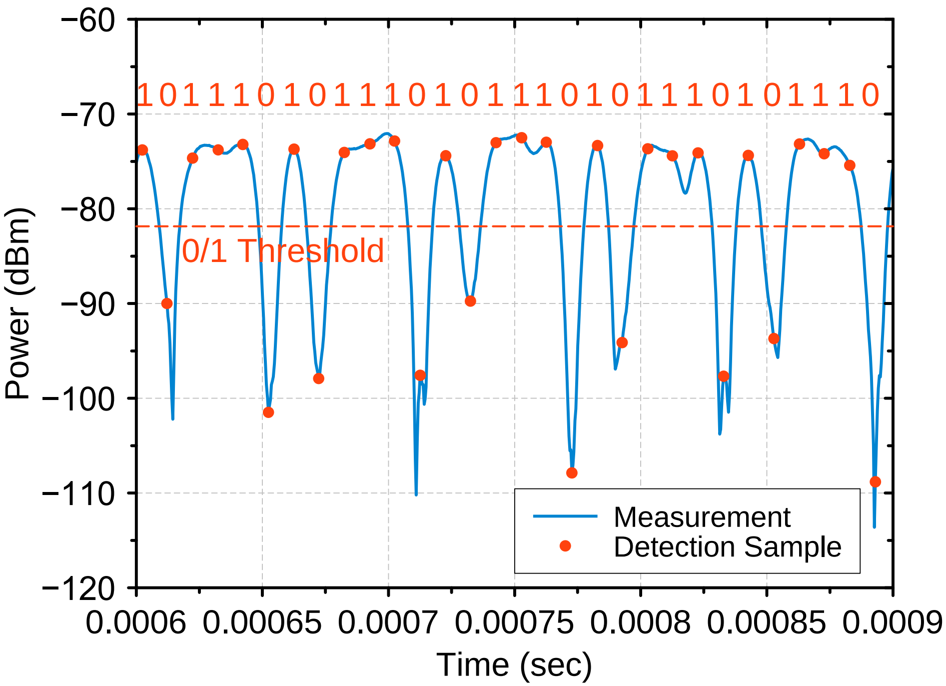
- f_s=100 Hz, providing a data rate of 800 bits/sec.
- All designed symbols are successfully detected.

❖12 Bits Dynamic ID



- f_s=100 Hz, providing a data rate of 1.2 kbits/sec.
- All designed symbols are successfully detected.

❖Single-Bit Dynamic ID with Max. Data Rate



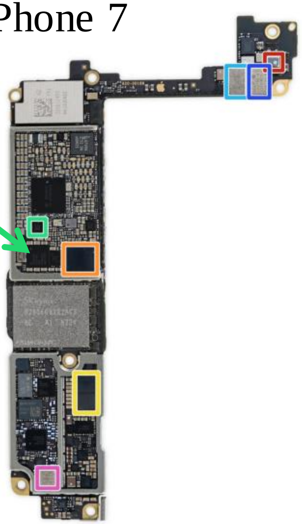
- f_s is set at 100 kHz, providing a data rate of 100 kbits/sec.
- More than 1 million transmitting bits (1091227 bits) are recorded over around 11 seconds. The proposed RFID tag modulates the carrier signals with a testing symbol pattern of (111010).
- Only 2 errors are detected among all 1091227 transmitted bits, providing a BER of 0.00000183 (10^-6) at a data rate of 100 kbits/sec.

❖Advantages

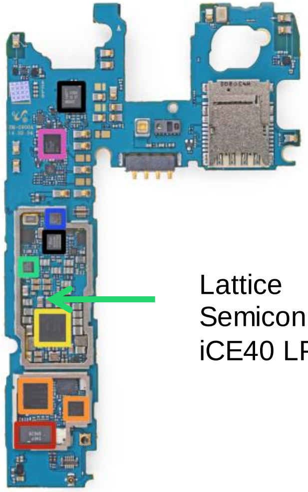
- Advantages of the proposed RFID tag:
  1. Zero cost, e.g., enabled by existing digital circuits (e.g., FPGAs) in commercial electronics
  2. Zero form factor, e.g., no antenna/RF front-end circuit
  3. High robustness
  4. Design flexibility

Apple iPhone 7

Lattice Semiconductor ICE5LP4K FPGA



Samsung Galaxy S5

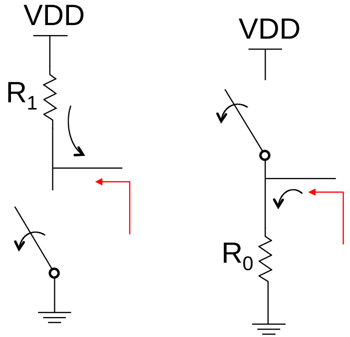


Lattice Semiconductor iCE40 LP1K FPGA

❖What Comes Next?

- This design is just a proof of concept
- It does not have to be implemented in FPGA.
- Optimization of impedances is needed
- Models to predict this behavior are needed

❖Impedance Model



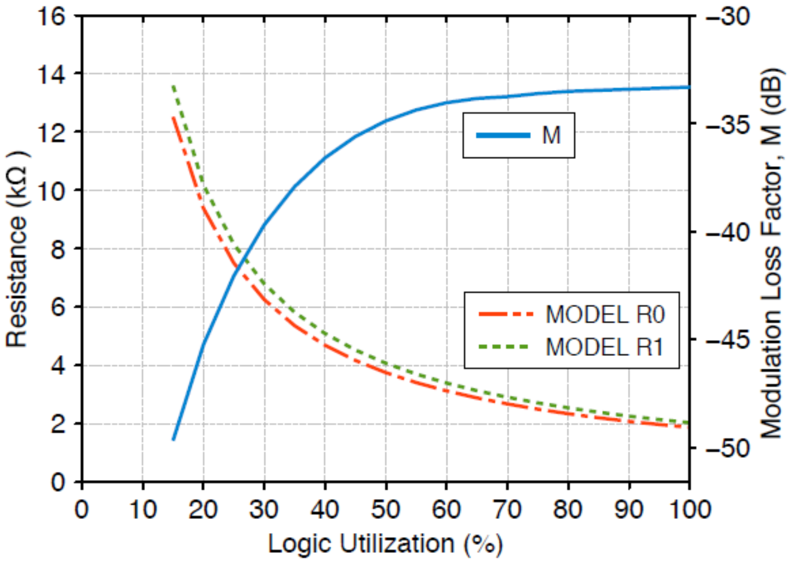
"x" relates to logic utilization

$$M(x\%) = \frac{1}{4}\left|\frac{R_1(x\%) - 377^*}{R_1(x\%) + 377} - \frac{R_0(x\%) - 377^*}{R_0(x\%) + 377}\right|^2$$

$$R_0(x\%) = \frac{R_0(10\%)}{\frac{x\%}{10\%}} \qquad R_1(x\%) = \frac{R_1(10\%)}{\frac{x\%}{10\%}}$$

- A modified modulation loss factor, M, which relates total backscattering modulation loss to FPGA's logic utilization.

❖Modulation Loss Factor, M



Logic Utilization (%)	(R0, R1) (kΩ)	(Γ0, Γ1)	M (dB)
20	(9.4, 10.2)	(0.85, 0.86)	-45.2
40	(4.7, 5.1)	(0.51, 0.54)	-36.6
60	(3.1, 3.4)	(0.16, 0.20)	-34.0
80	(2.3, 2.5)	(-0.12, -0.08)	-33.8
100	(1.9, 2.0)	(-0.34, -0.3)	-33.3

❖Summary

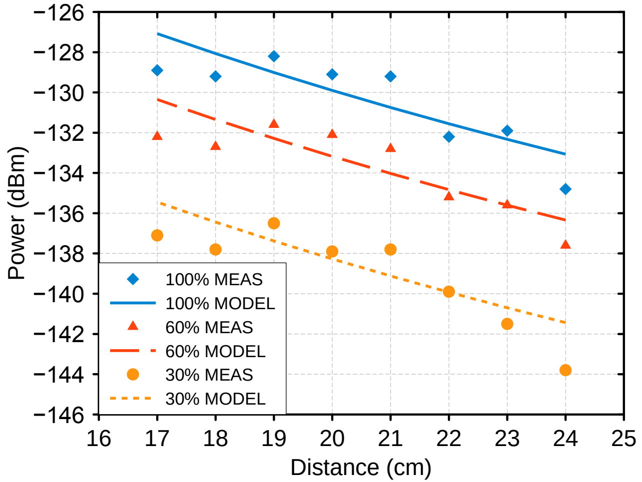
- New side-channel: Impedance-based side channel
- Leveraging impedance-based side channels for RFID tags
- Programmable RFID tags- static and dynamic

THANK YOU

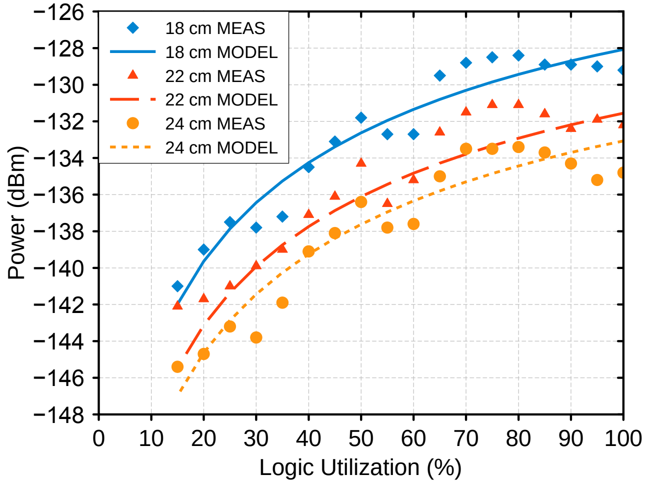
Questions?

❖Backscattered Power Model and Measurements

Backscattered Power V.S. Distance



Backscattered Power V.S. Logic Utilization



$$P_{rx\_backscattered} = \frac{P_{tx} G_{tx} G_{rx} L_{refl}^2 M \lambda^4}{(4\pi d)^4}$$

- ➢Results show good agreements between the measured and modeled backscattered power.
- ➢Compared to carrier power, backscattered power is less susceptible to the constructive and destructive interference that results from multipath than the carrier power.