WMI-7

RF and DSP Techniques for Enabling Low-Cost Software-Defined RFID Readers

[1]Edward A. Keehr

[1]Superlative Semiconductor LLC, Carlsbad, CA 92009, USA

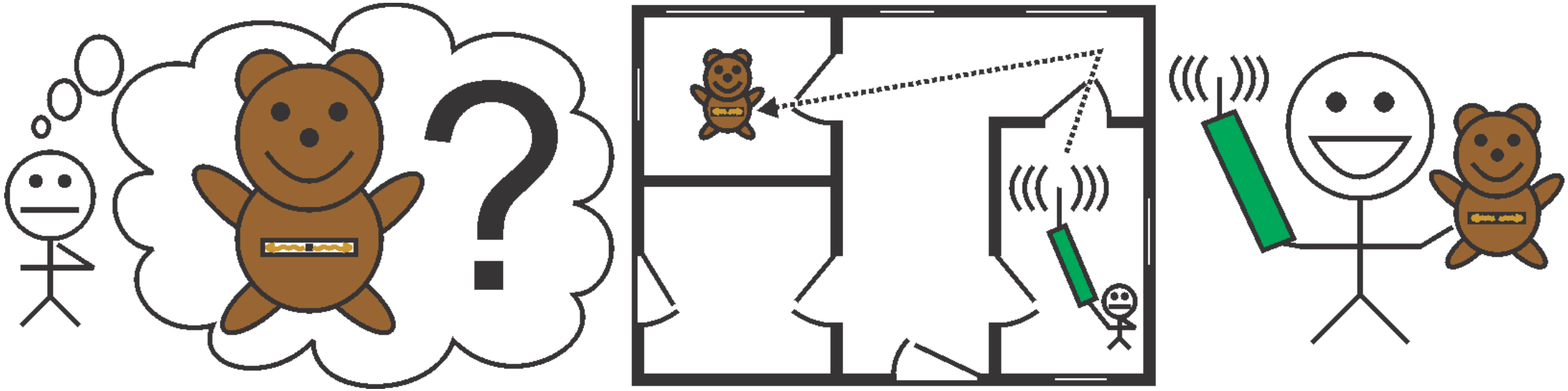
Outline

1. Global Context and Prior Art
2. Top Level Architecture
3. Transmit (TX) Leakage Cancellation
4. FPGA Circuit Design
5. Experimental Results
6. Conclusion
7. Backup

Outline

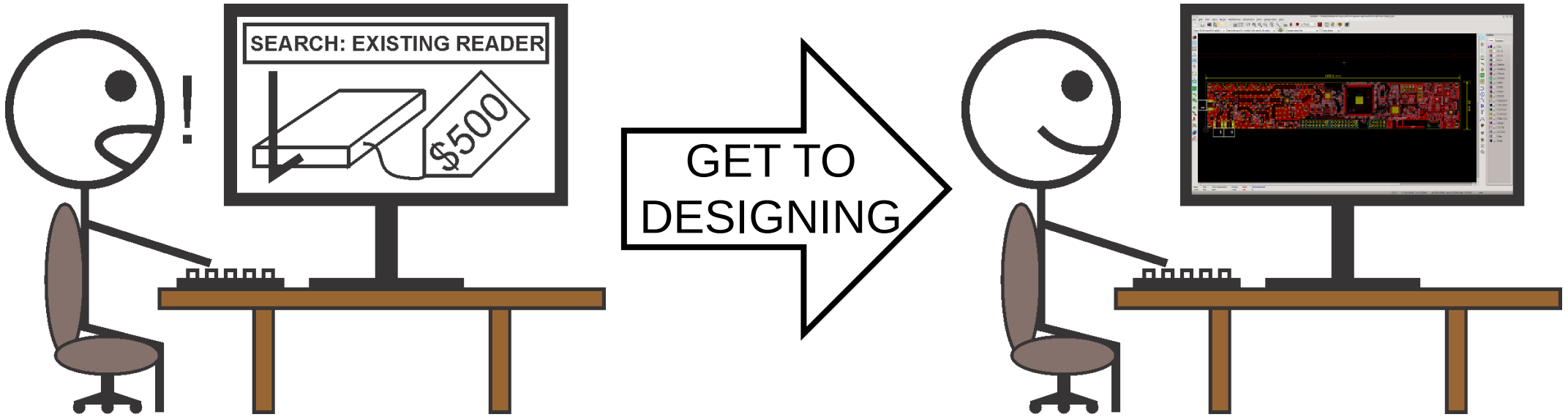
1. Global Context and Prior Art
2. Top Level Architecture
3. Transmit (TX) Leakage Cancellation
4. FPGA Circuit Design
5. Experimental Results
6. Conclusion
7. Backup

Global Context: Personal RFID for Home



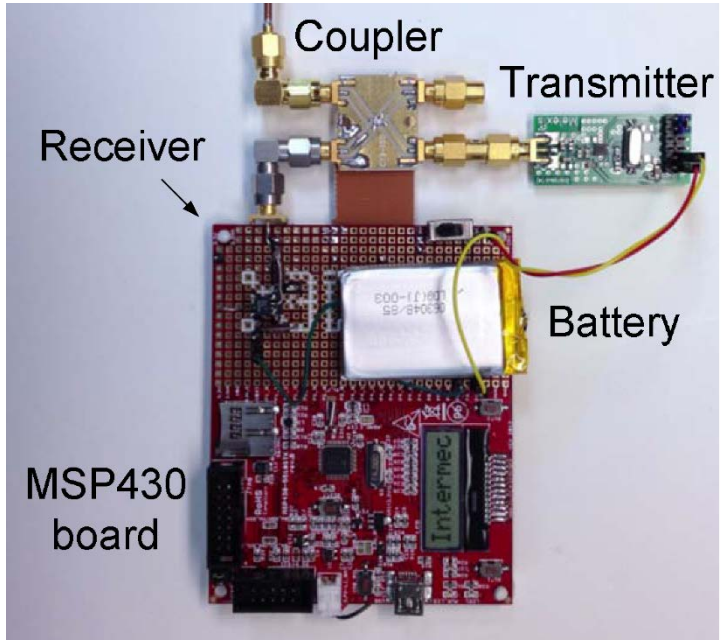
- Avg. American spends 2.5 days/year looking for lost items.
  - TV remote is most common item. [Pixie Lost & Found Survey]
- BTLE: $15/tracker, limited life, RSSI-only localization.
- **RFID: $0.05/tag, unlimited life, phase-based localization.**

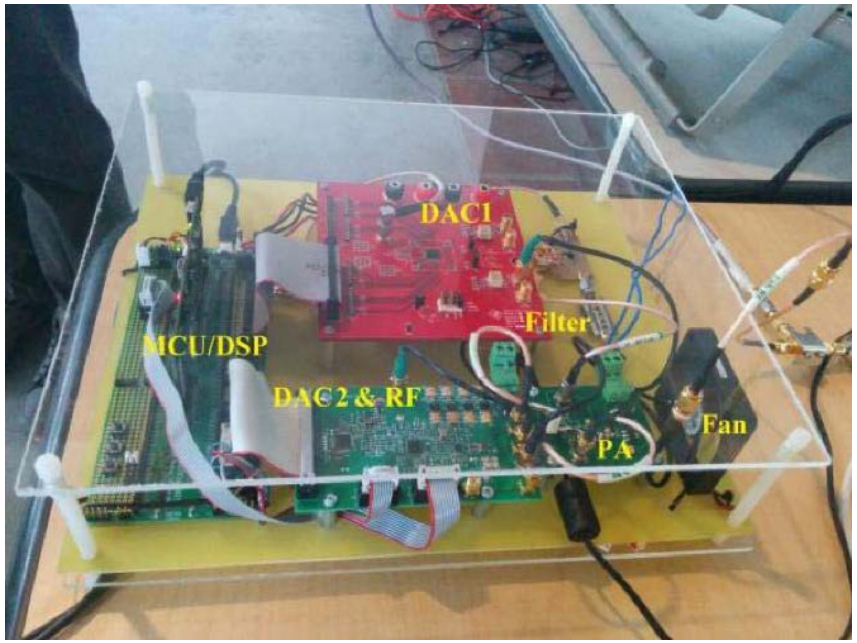
Global Context: Personal RFID for Home



- Problem: RFID Reader Module: $200-300 [RFID Journal].
  - Standalone reader: $500 [RFID Journal].
- One limiting factor: Reader ASIC > $24 in bulk.
- Solution: Leverage relatively new low-cost SDR components.

Prior Art – Low Cost SDR UHF RFID



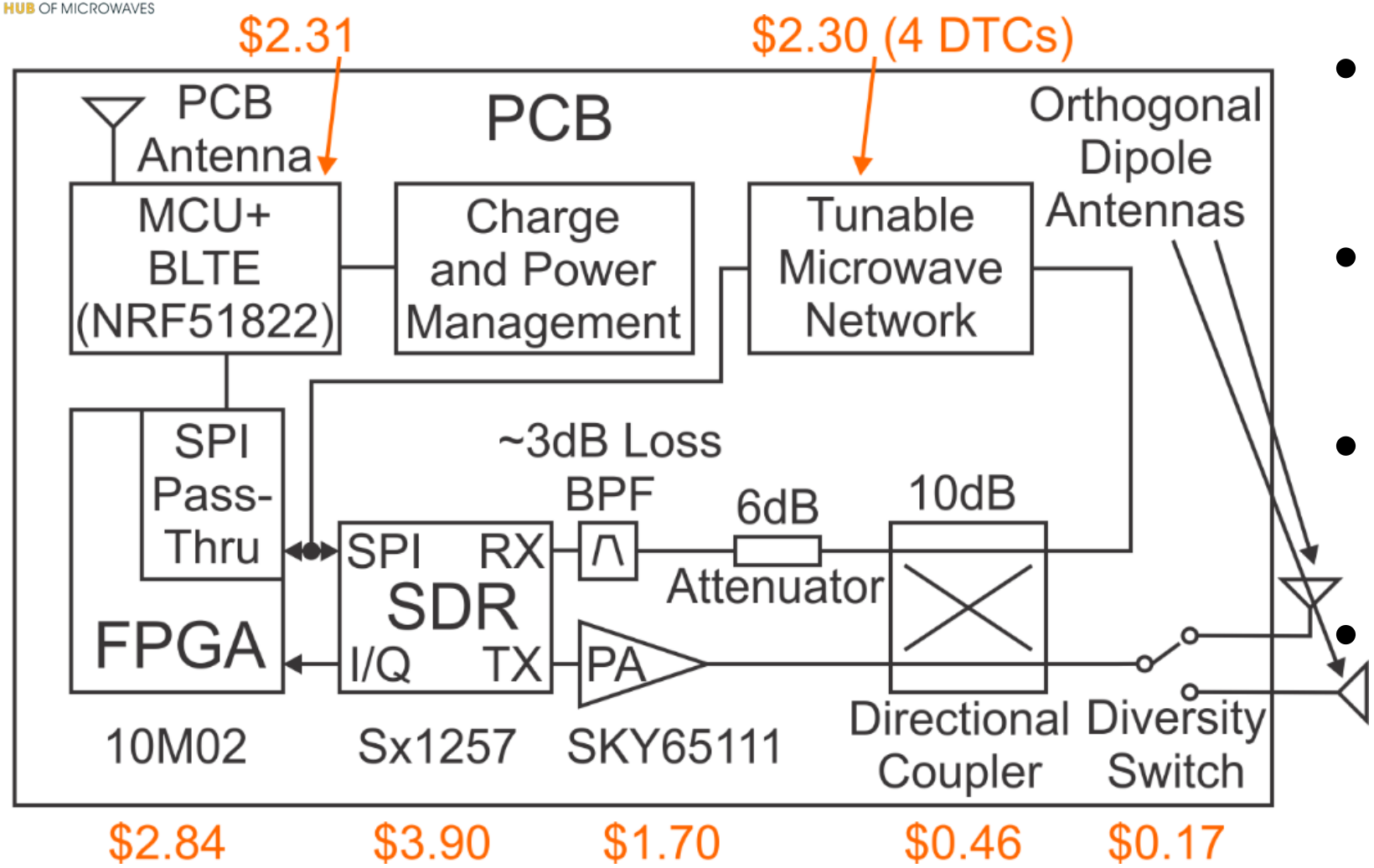


- [Nikitin, 2013]: $9 BOM (bulk) but 0.15m range.
- [Boaventura, 2017]: >$40 BOM (bulk) but only Query=0.
- Most academic designs use $$$ FPGA and full custom PCB radios.

Outline

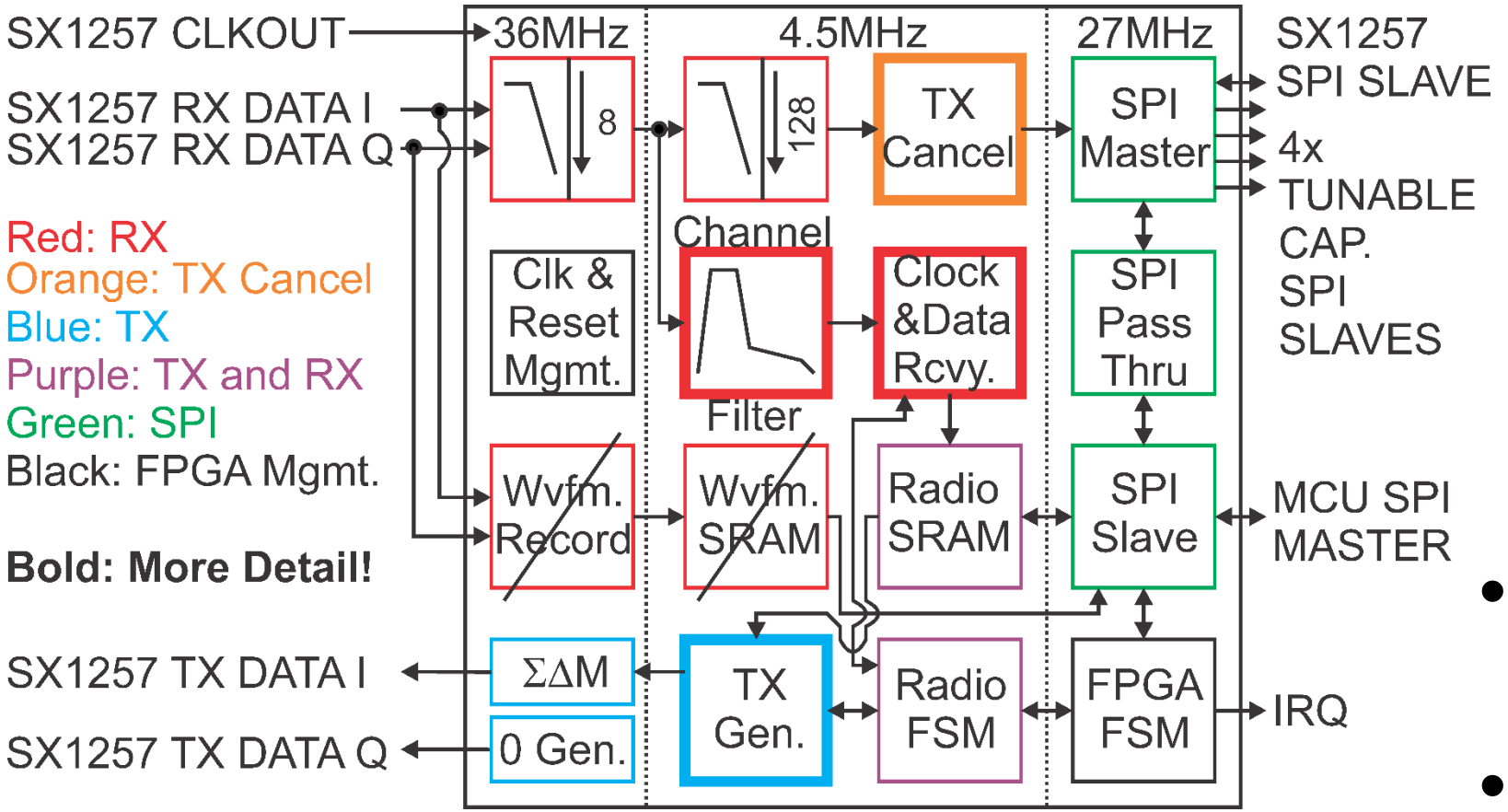
1. Global Context and Prior Art
2. **Top Level Architecture**
3. Transmit (TX) Leakage Cancellation
4. FPGA Circuit Design
5. Experimental Results
6. Conclusion
7. Backup

Proposed Reader Design – Top Level



- Prices listed are bulk on Digikey.
- Can replace Reader ASIC for $9.20.
- Adding BTLE MCU → $11.51.
- Offload display, high-level processing to smart device.

Proposed Design – FPGA Top Level

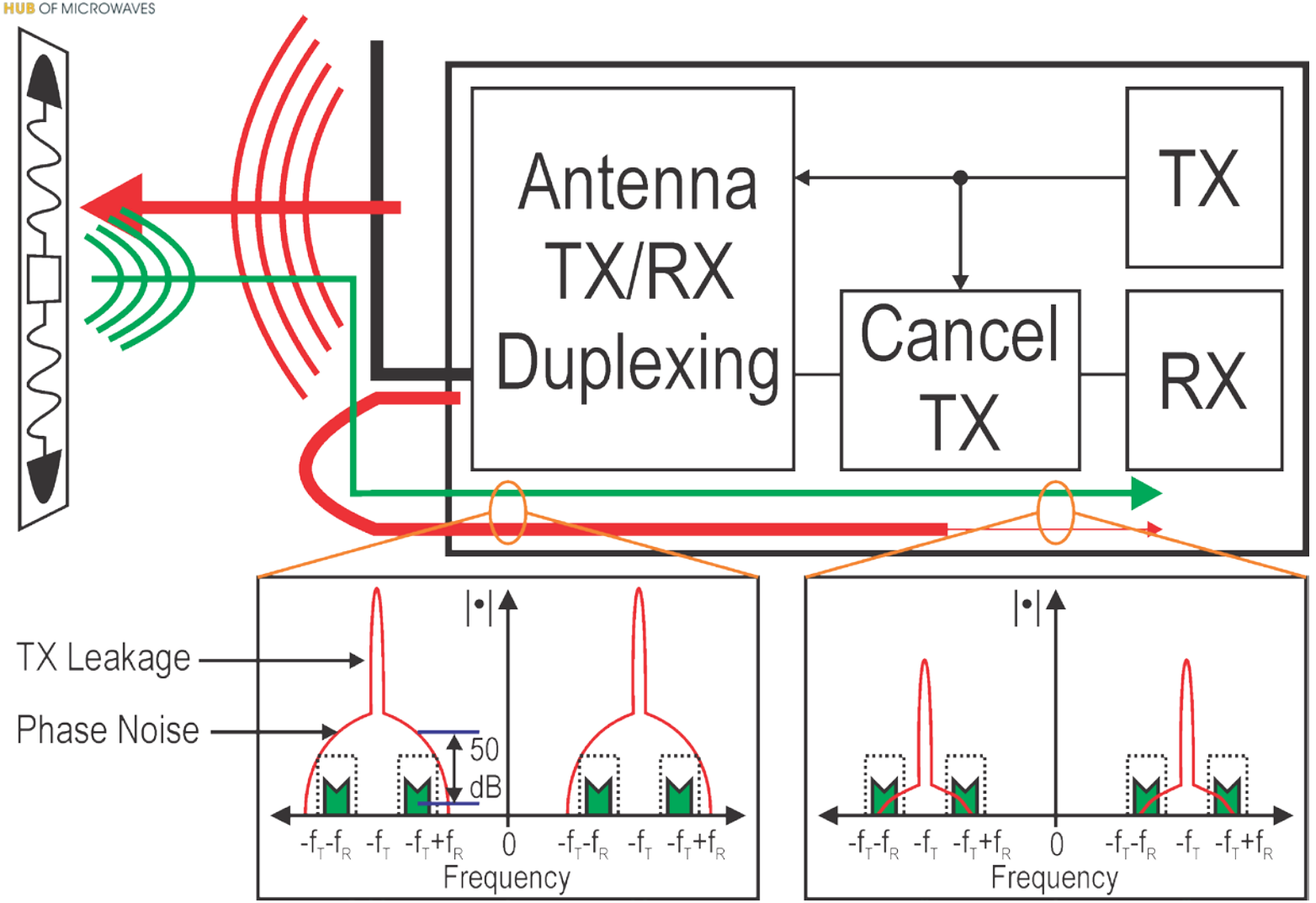


- Clock domain partitioning is key.
  - SX1257: 36MHz.
  - Bulk of design: 4.5MHz (easy timing closure).
  - Basic services: FPGA int'l oscillator (27MHz).
- TX Cancel Algorithm:
  - On same FPGA!
- 2,304 Logic Elements.
  - (LEs)

Outline

1. Global Context and Prior Art
2. Top Level Architecture
3. **Transmit (TX) Leakage Cancellation**
4. FPGA Circuit Design
5. Experimental Results
6. Conclusion
7. Backup

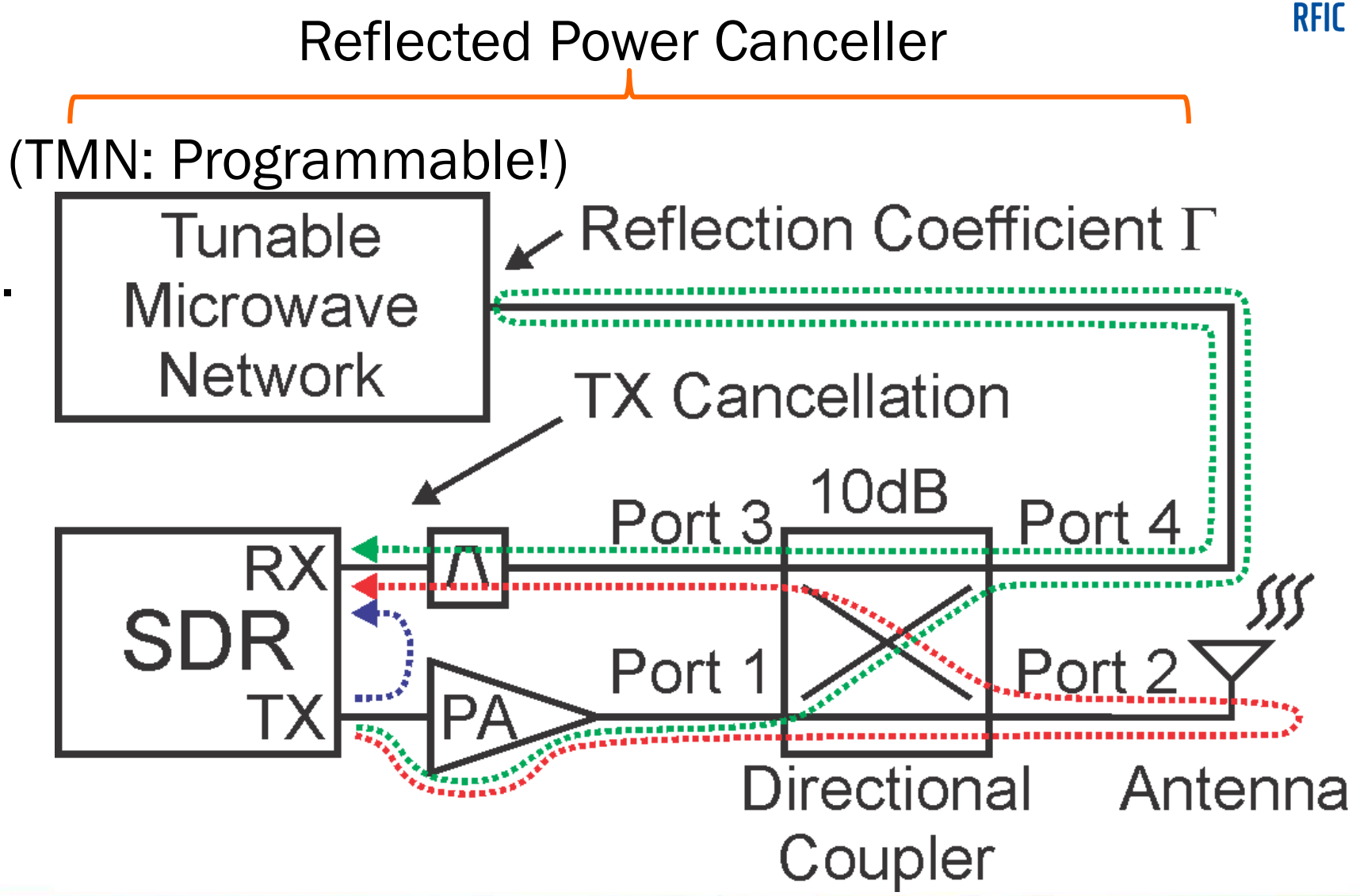
Full Duplex Problem in RFID



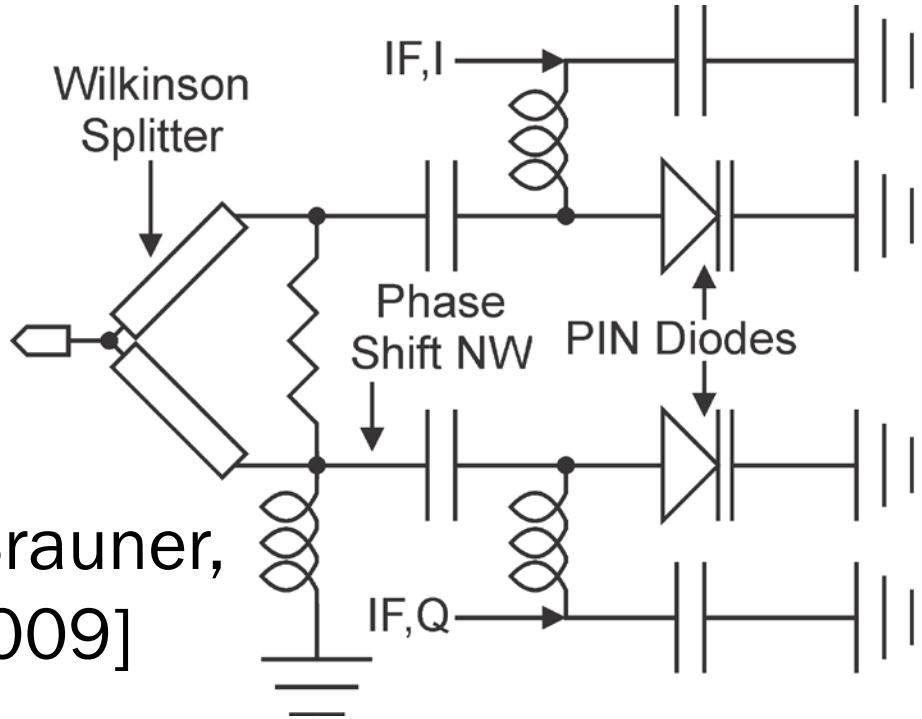
- Key challenge in designing this reader:
  - TX Leakage!
- SX1257 Phase Noise 50dB higher than allowed.
  - For $|\Gamma_{ANT}| < -10dB$.
  - Must cancel TX leakage by this amount (50dB).

TX Cancellation Architecture Options

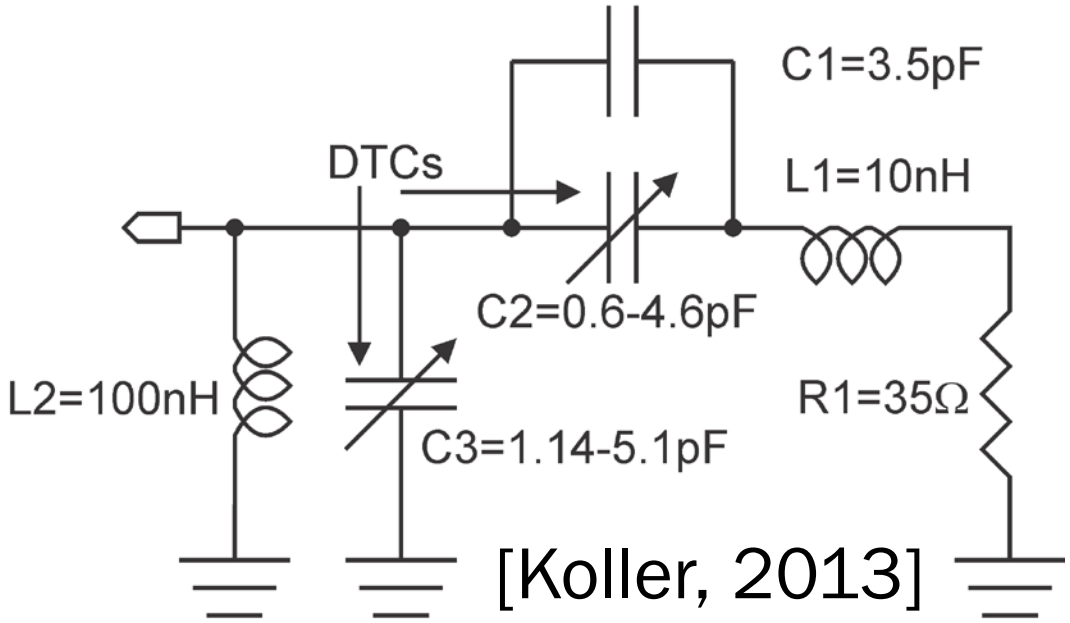
1. Vector Modulation:
   – High incremental cost and board area.
2. On-chip:
   – High fixed cost.
3. Reflected Power Canceller (Shown):
   – Low fixed and incremental cost.



Tunable Microwave Network – Prior Art



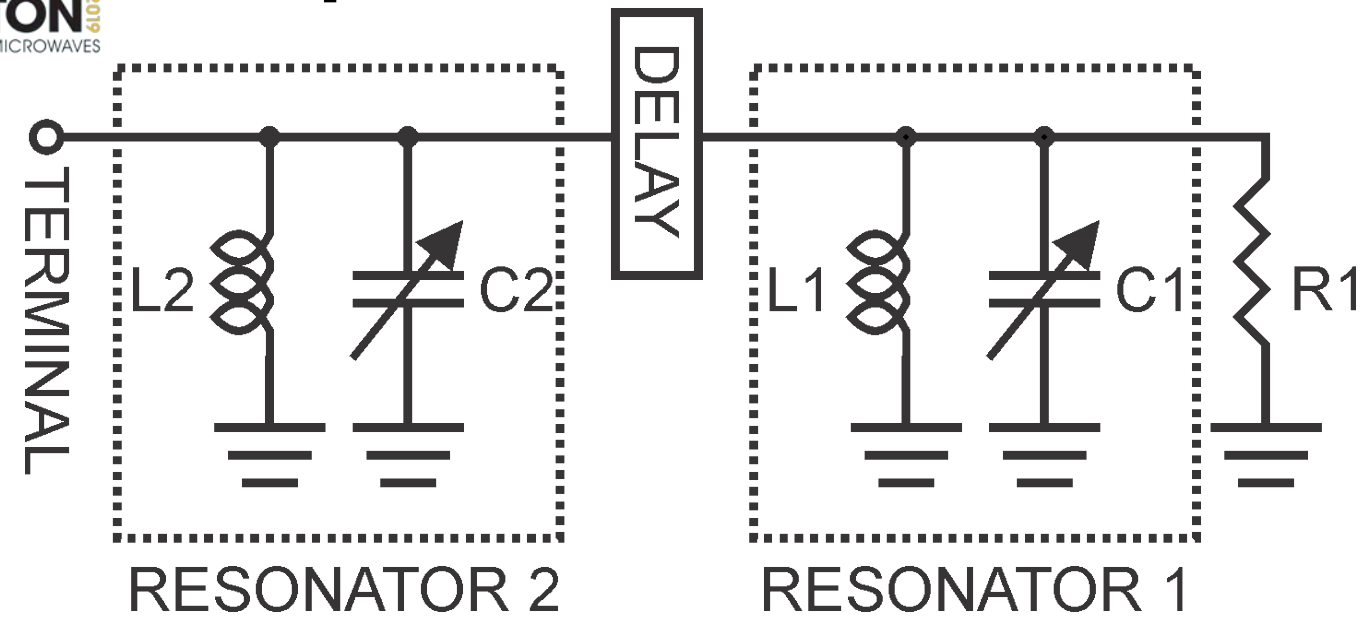
[Brauner, 2009]

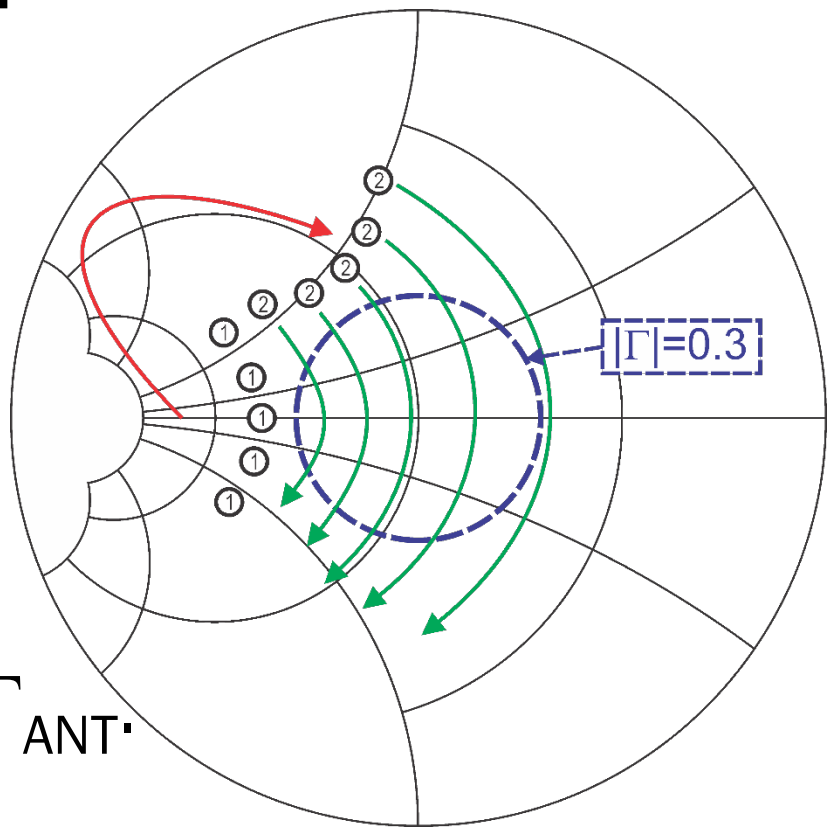


[Koller, 2013]

- PIN diodes controlled by programmable currents [Brauner, 2009].
  - Susceptible to noise current modulating PIN resistance.
- Digitally Tunable Capacitor – based network [Koller, 2013].
  - This DTC design has only 20dB of TX cancellation.

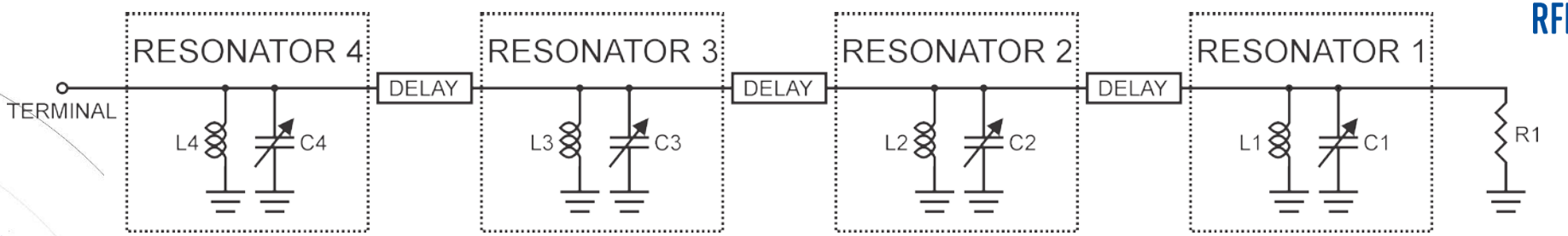
Proposed Baseline – Coupled Res. NW





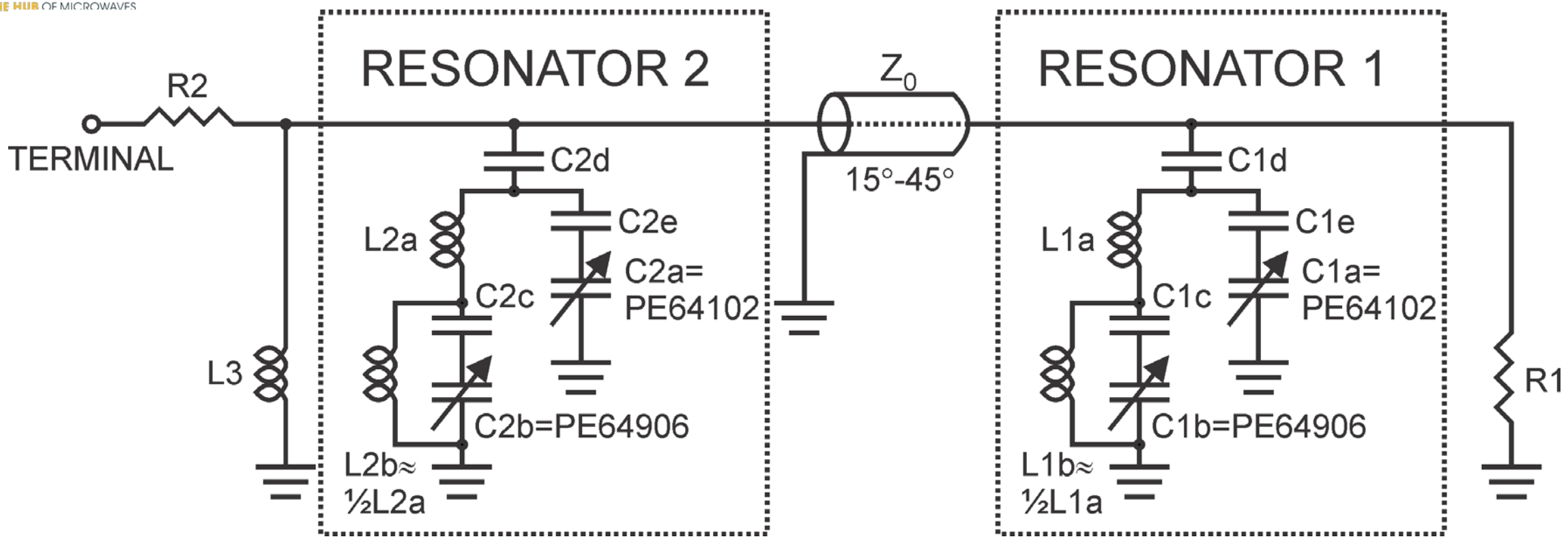
- Goal is to program $\Gamma_{TMN} = -\Gamma_{ANT}$ for any Γ_{ANT}.
- For Γ_{ANT} spec'd as |S11| < -10dB:
  - Γ_{TMN} must cover disk with radius=0.3 in the complex plane.
- Starting point: coupled resonator NWs (CRNs) [Whatley, 2011].
- Add suitable R to one port of CRN to get above characteristic.

Improving Resolution – More Resonators



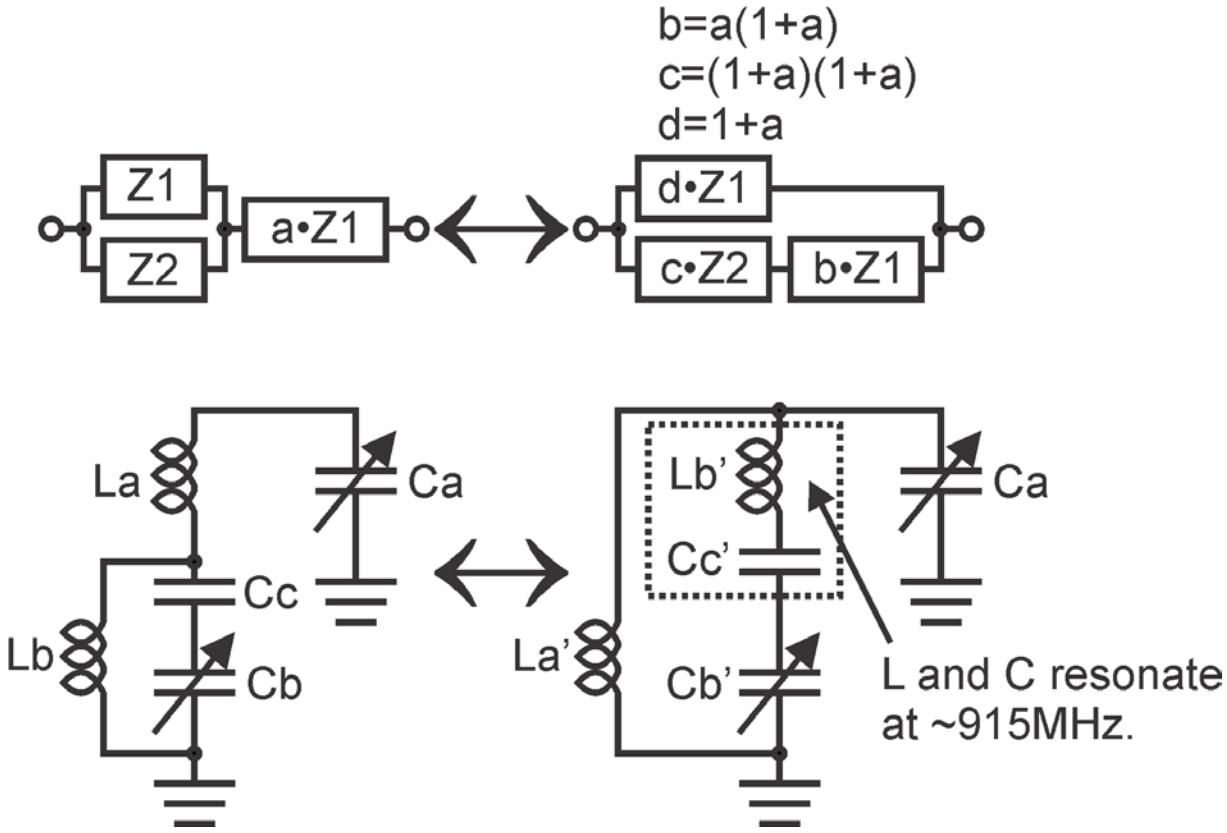
- Goal: 50dB cancellation ratio ⟶ 1Mpoints.
- For 5-bit DTCs ⟶ 4 capacitors for $(2^5)^4$=1048576 states.
- 4 resonators: Uneven coverage, confusing for tuning algorithm.

Improving Resolution – Subranging (1)



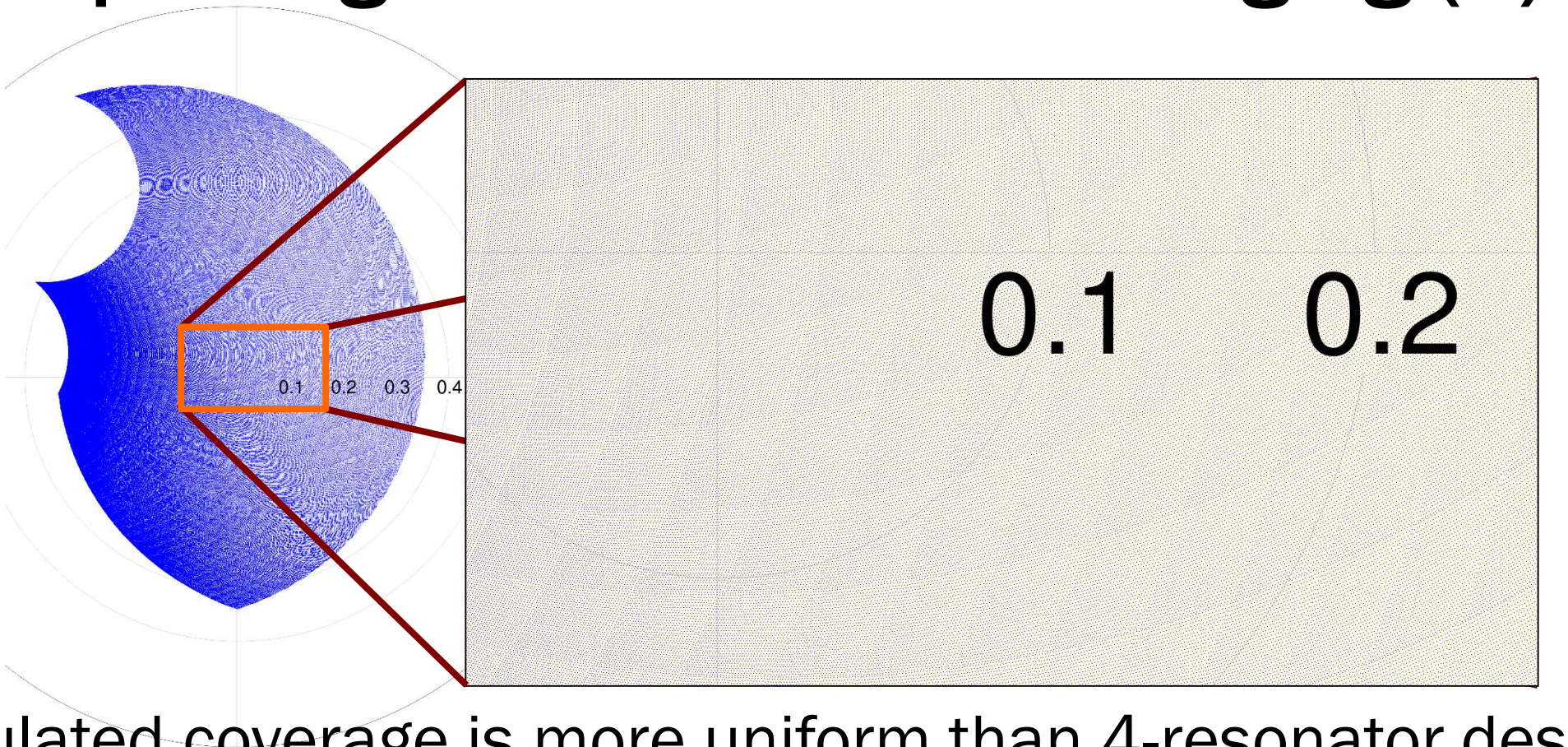
- Key novelty of this work – incorporating subranging into DTC TMN.
- Inductive divider of LXa/LXb scales CXb so it subranges CXa.
- Fixed capacitors fine-tune coverage characteristics.

Improving Resolution – Subranging (2)



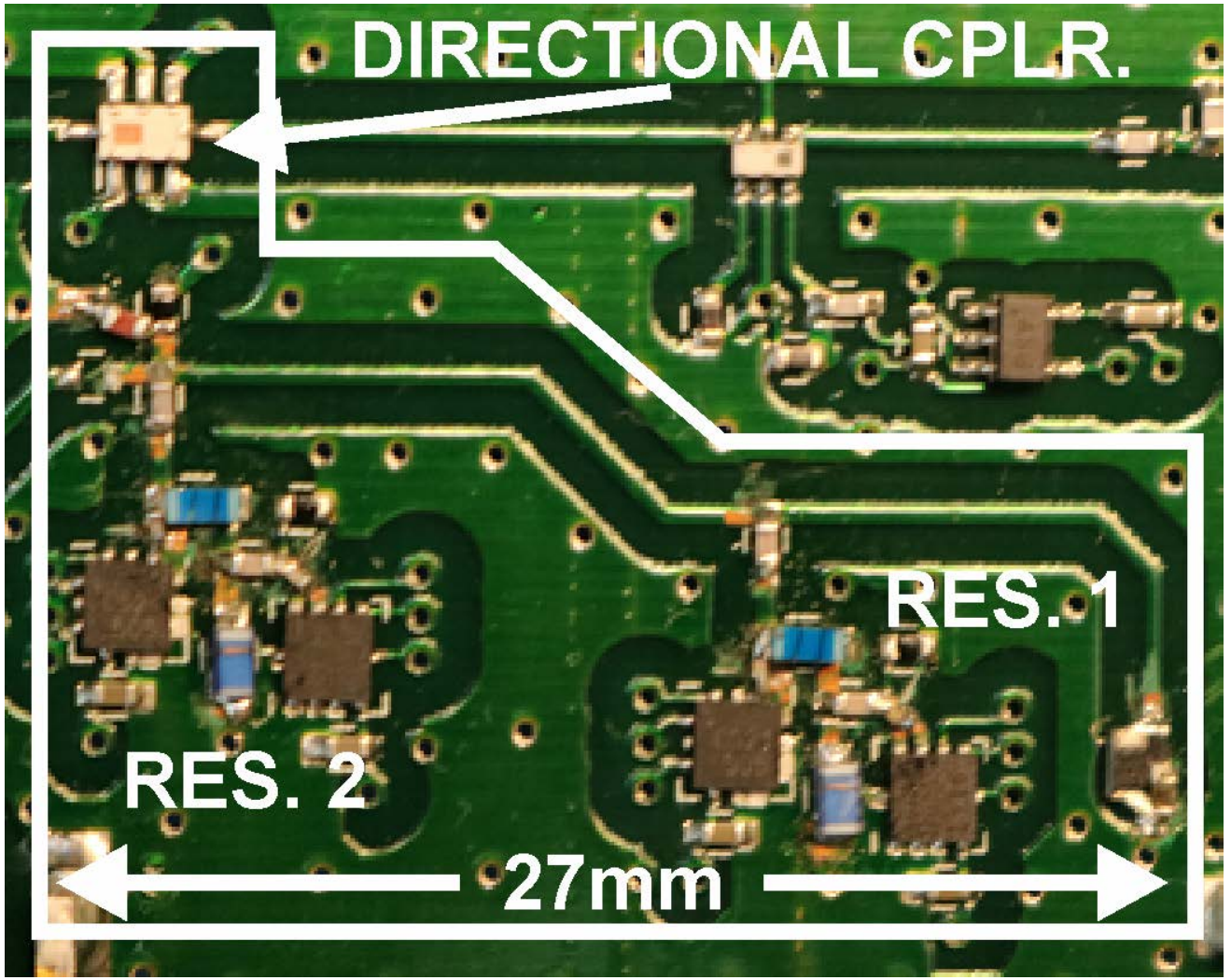
- Transforms from Zobel (1923) show subranging explicitly.
- A parasitic series Lb' ends up in series with Cb'.
- This is the reason for Cc – to resonate out Lb' after transformation.

Improving Resolution – Subranging (3)



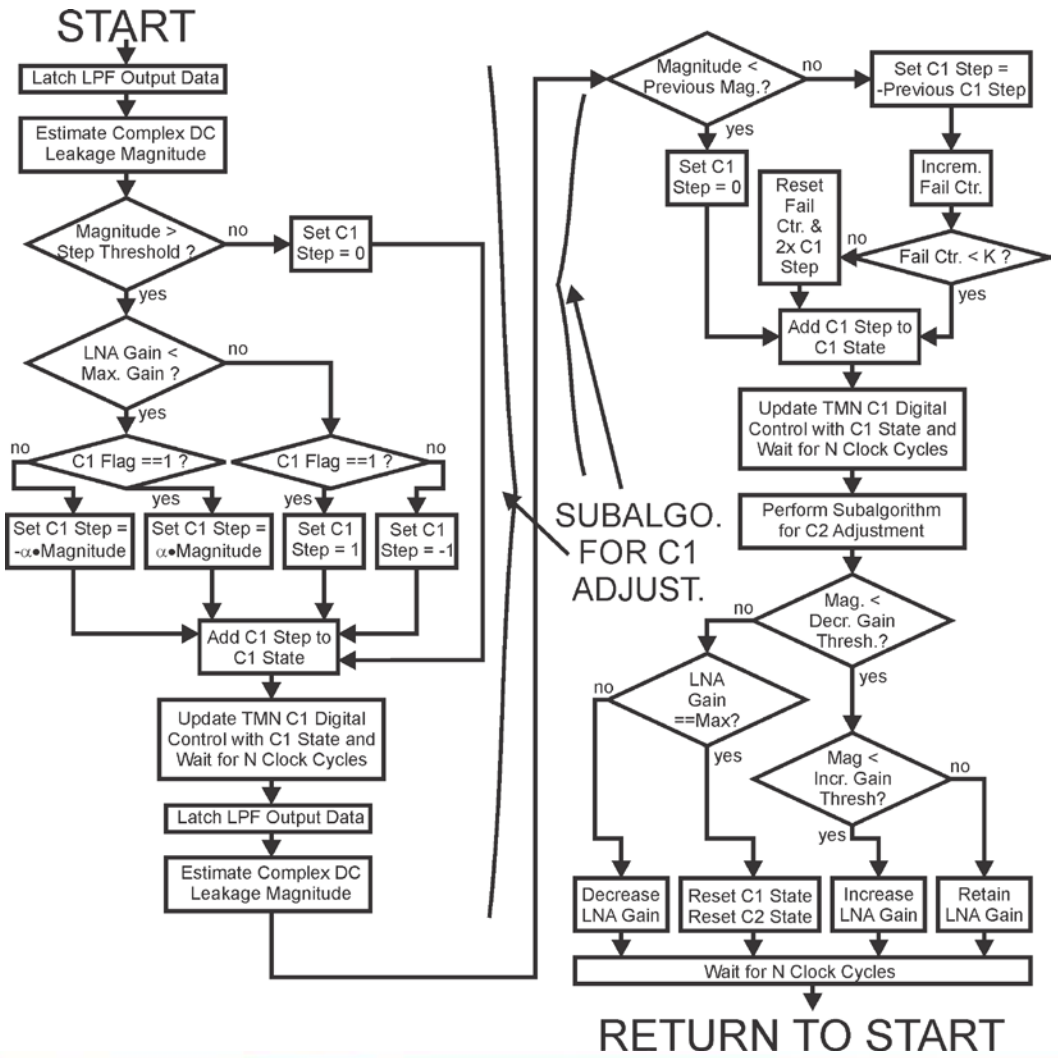
- Simulated coverage is more uniform than 4-resonator design.
- Simulated worst-case cancellation for |S11| < -10dB is 50dB.
- Having only 2 resonators (state variables) simplifies tuning.

Physical Implementation and Cost of TMN



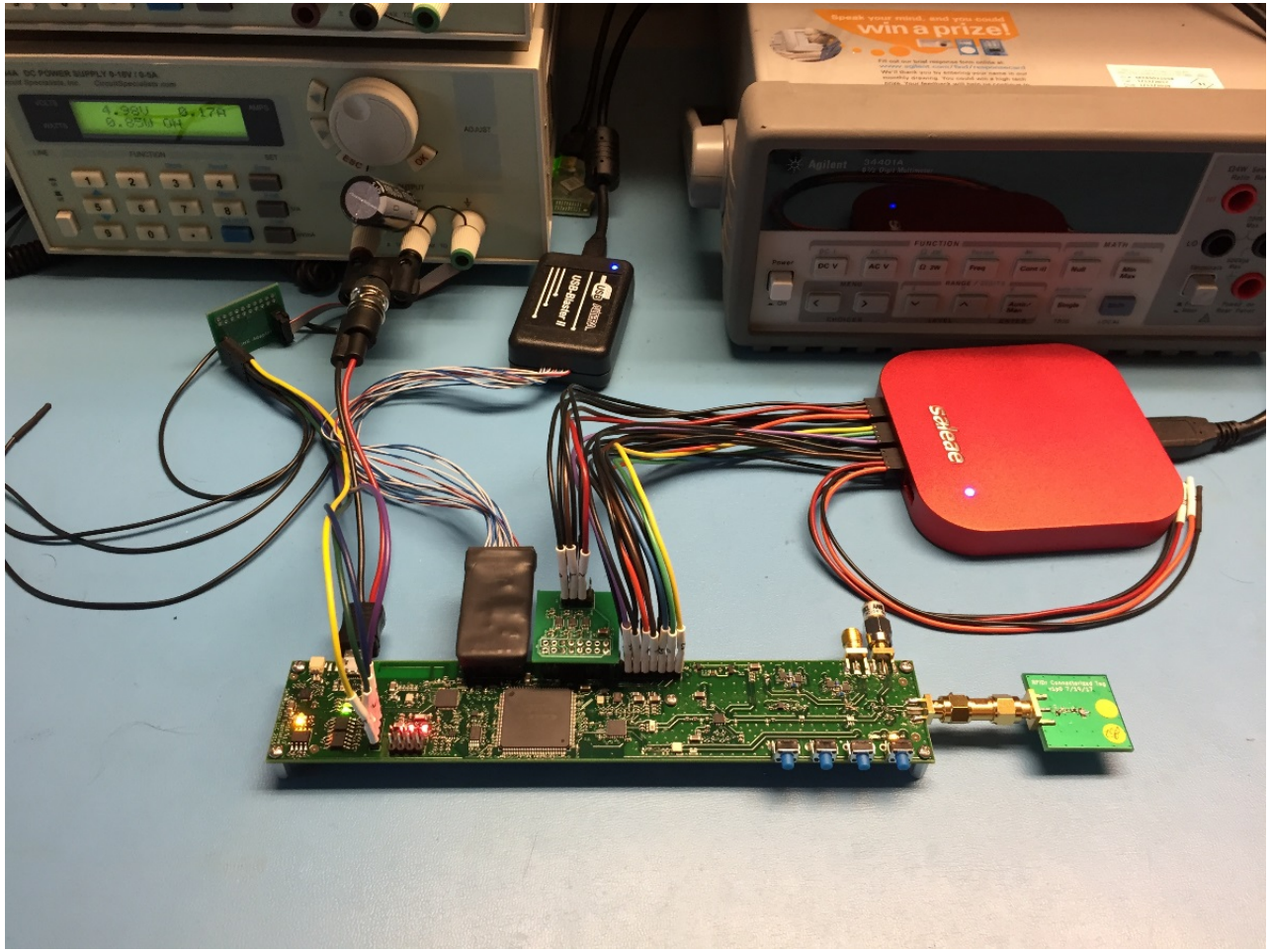
- Cost of 4 DTCs in QTY of 15,000: $2.30.
- Dir. Cplr: $0.46
  - Needed anyway.
- RF Inductors: $0.67
  - 4 Blue components.
  - Can use cheaper.
- T-lines used as delay elements.

Blind Tuning Algorithm



- Tune based on estimate of TX leakage magnitude.
- Scale Dig. BB Mag. by SDR gain.
- Use trial {C1, C2} steps to compute local gradient of magnitude.
- Adjust SDR ASIC LNA gain.
- If SDR gain is not at maximum:
  - Steps proportional to TX leakage.
  - Otherwise, only +/- 1LSB steps.

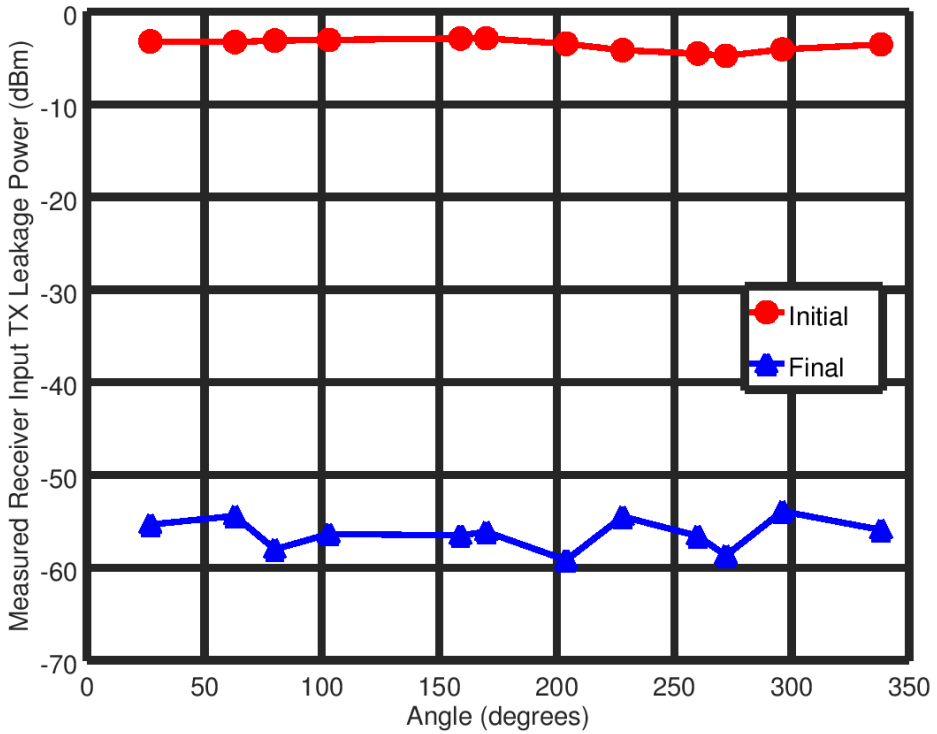
Test Setup - Convergence



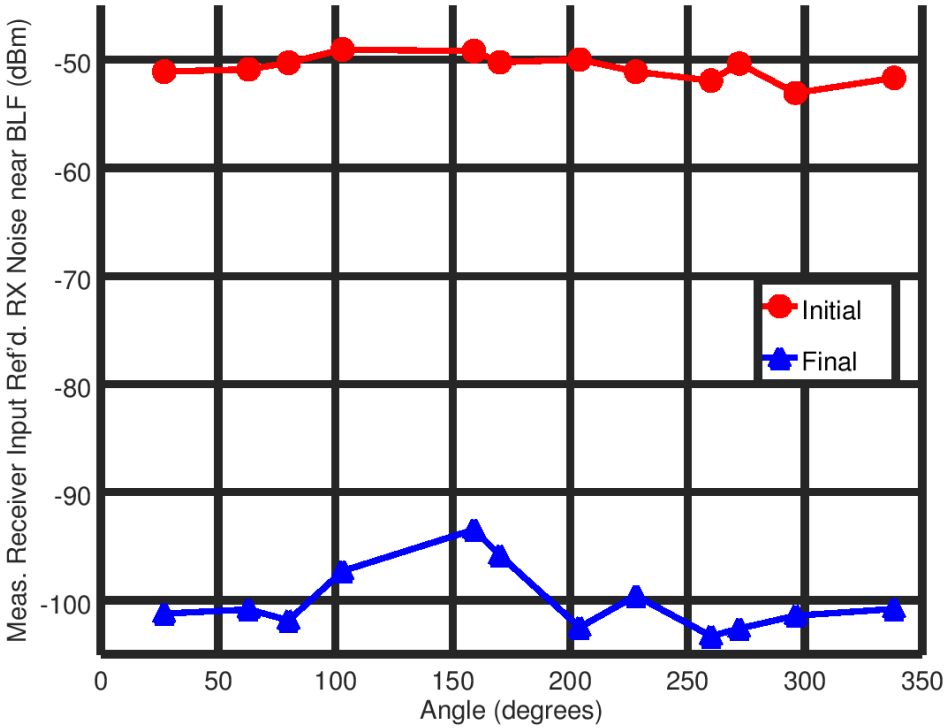
- Reader antenna port connected to dummy tags with |S11|≈-11dB.
- FPGA image modified to send out +26dBm CW for 40ms.
- SDR digital I/Q data captured using buffer board & logic analyzer.
- I/Q data postprocessed using model of FPGA digital filters.

Test Results – TX Leakage Cancellation

Initial/Final Leakage

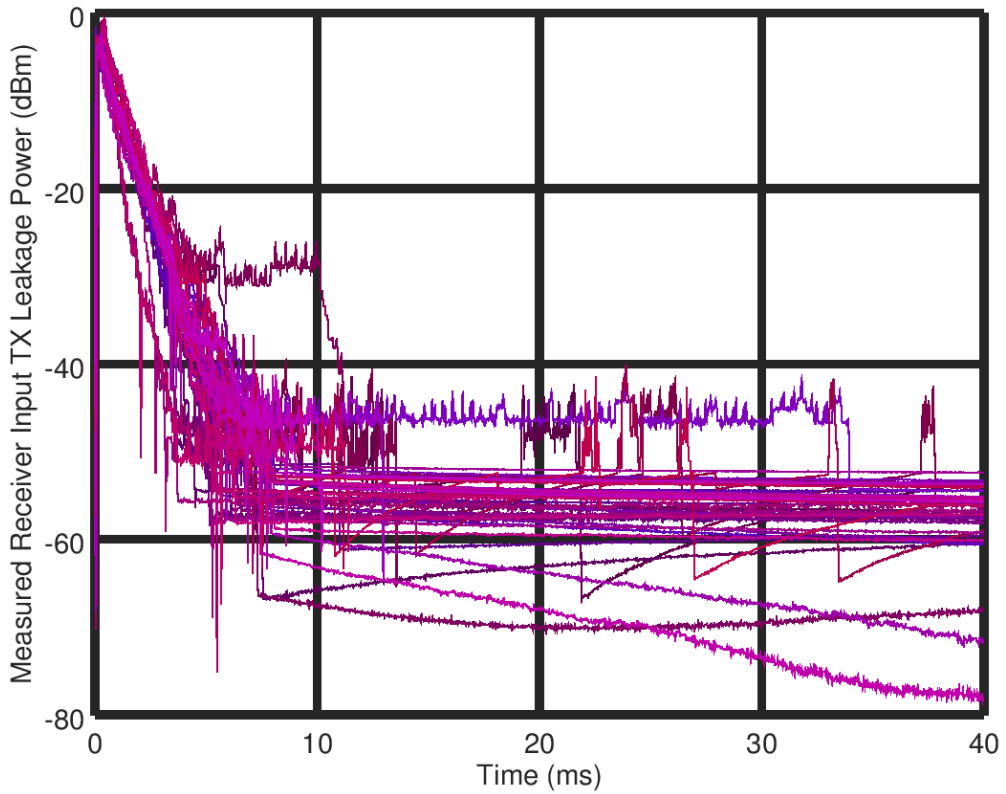


Initial/Final RX Noise



- Left: Suppression at SDR ASIC RX Input is > **49dB.**
- Right: Suppression similarly reduces RX phase noise.
- Noise is typically improved by over **48dB**, for 2 points by > **44dB.**

Test Results – TX Leakage Convergence



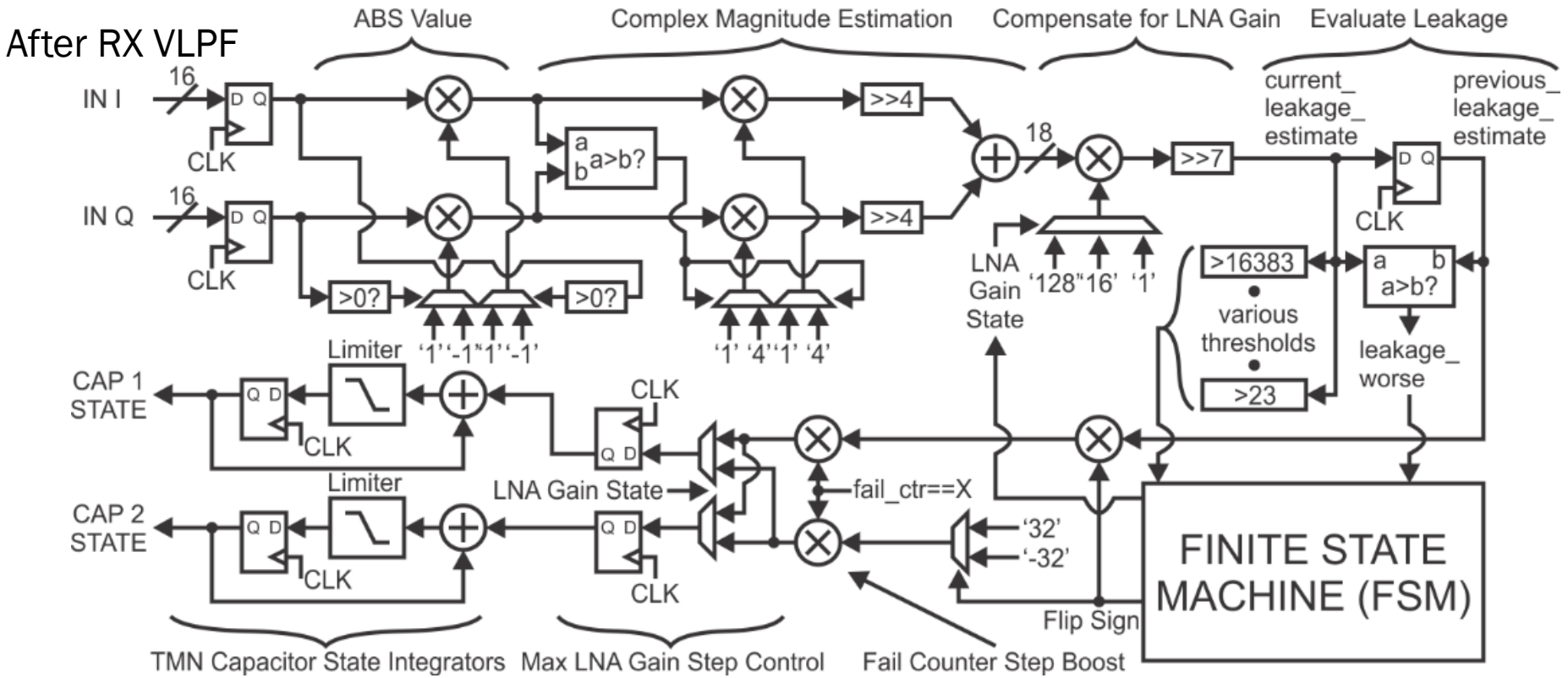
- Median time to achieve -50dBm IR'ed error: **7.3ms**.
- Max time: **34ms**.
- These results on par with recent published prior art at IEEE RFID.
  - For similar TX leakage cancellation
    - (50dB)
  - But for < $4 vs. > $70.

- Plot shows 4 runs each for 12 $\Gamma_{DUMMYTAG}$ (48 runs total).
- 'Blips' due to use of low-wattage tag resistors.
  - If really needed, could turn off convergence during RX to prevent this.

Outline

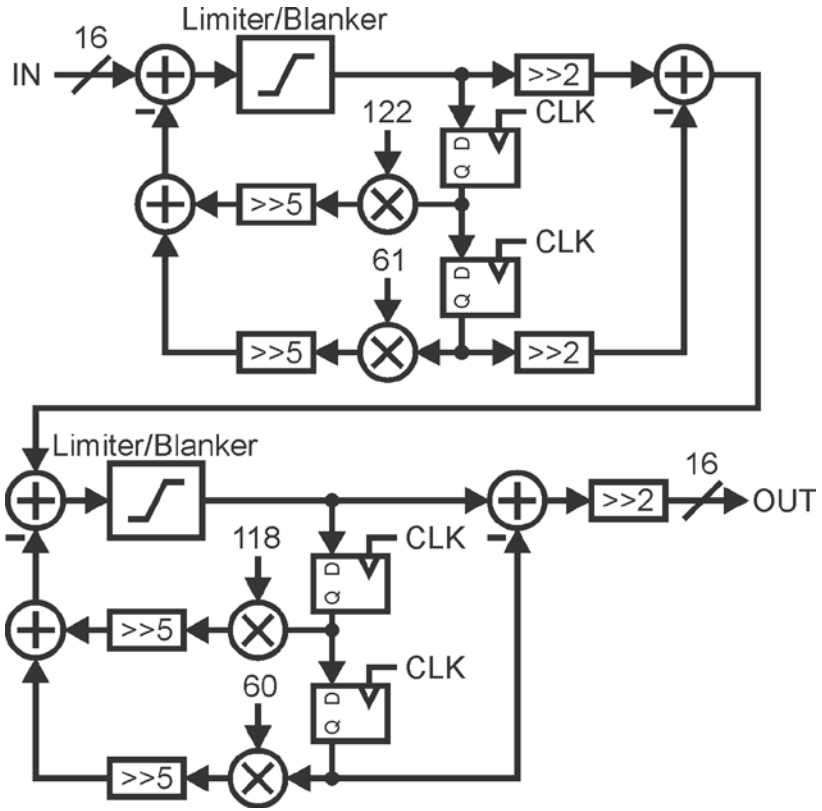
1. Global Context and Prior Art
2. Top Level Architecture
3. Transmit (TX) Leakage Cancellation
4. **FPGA Circuit Design**
5. Experimental Results
6. Conclusion
7. Backup

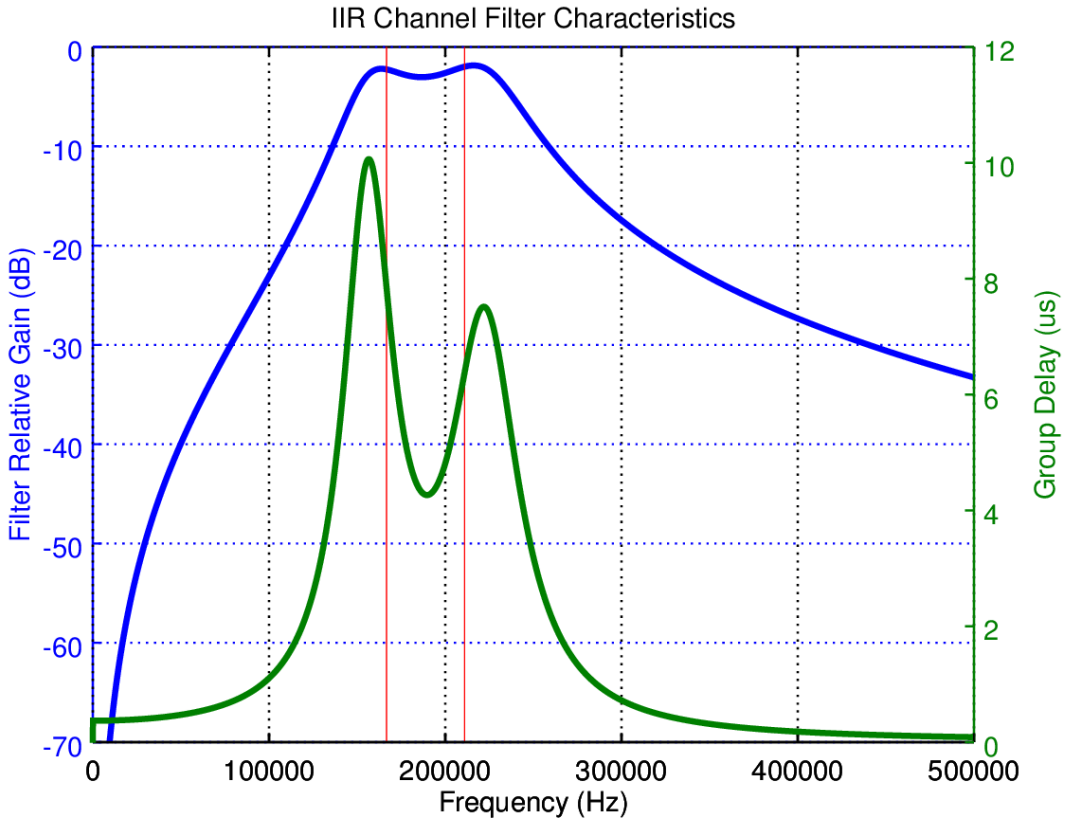
Tuning Algorithm FPGA Implementation



- Resource Count: 222 4-LUT, 118 FF, 222 LE (~10% of total).
- Also: 16 9x9 Multipliers implemented as 8 18x18 Multipliers.
- Above depiction accounts for ~90% of LE (rest is in FSM detail).

Major HW Consumer – Channel Filters

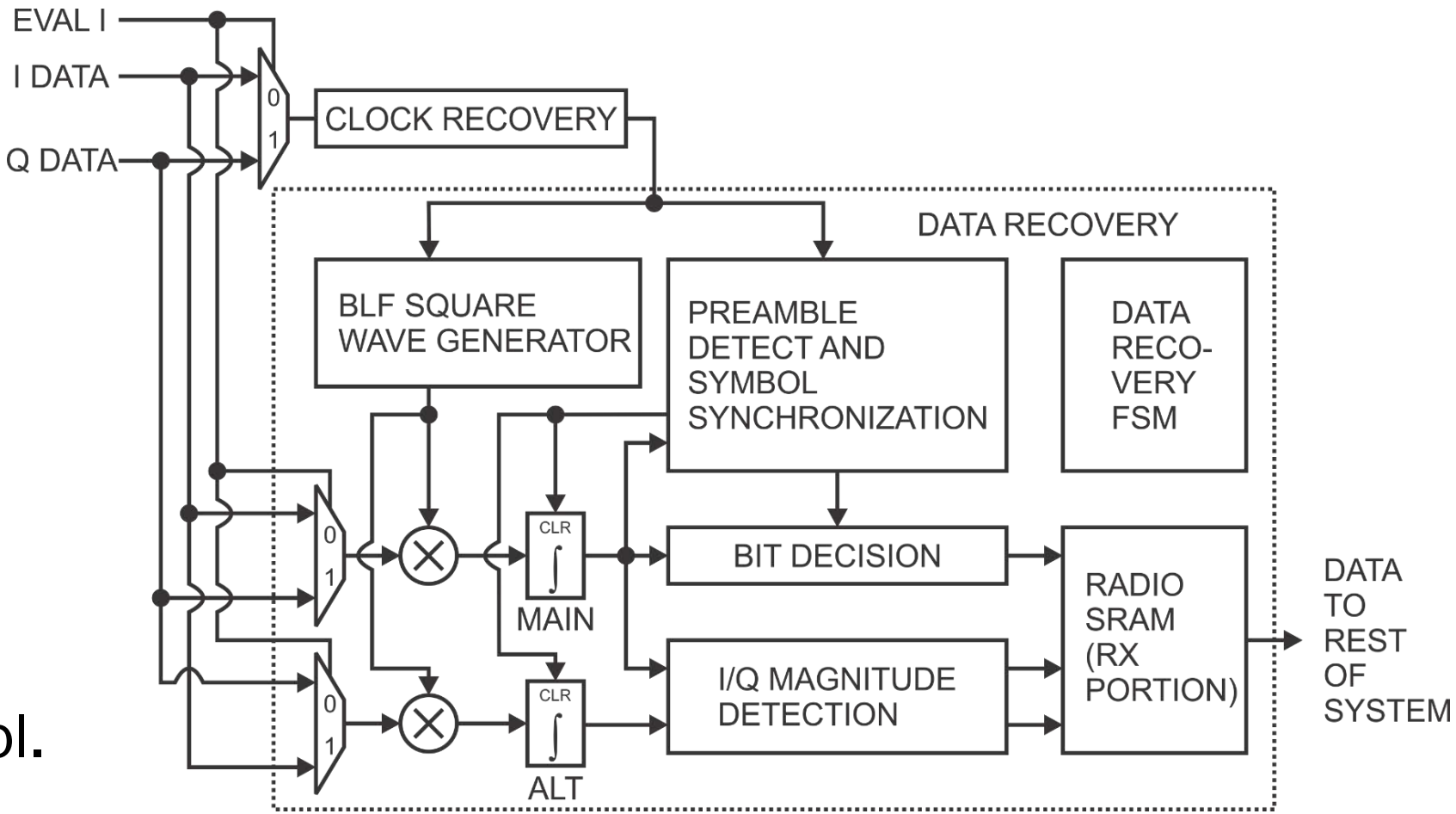




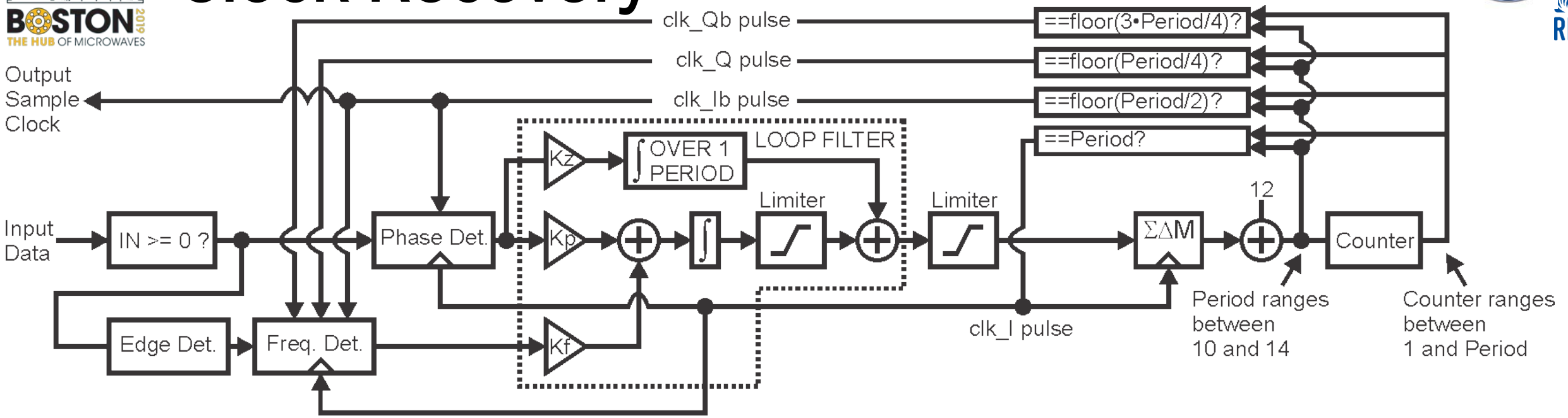
- Removes DC TX leakage and low-freq. phase noise.
- Dual-digital-resonator IIR design is more HW efficient than FIR.
- Uses ~27% of all FPGA LEs, 50% of all FPGA multipliers.

Major HW Consumer – Clock/Data Rcvy.

- Consumes
  - 27% of all FPGA LEs
  - 0% of multipliers.
- CDR performed on only I or Q at a time.
- Data Recovery:
  - Multiply by Clock
  - Then Integrate-and-Dump over ½ symbol.

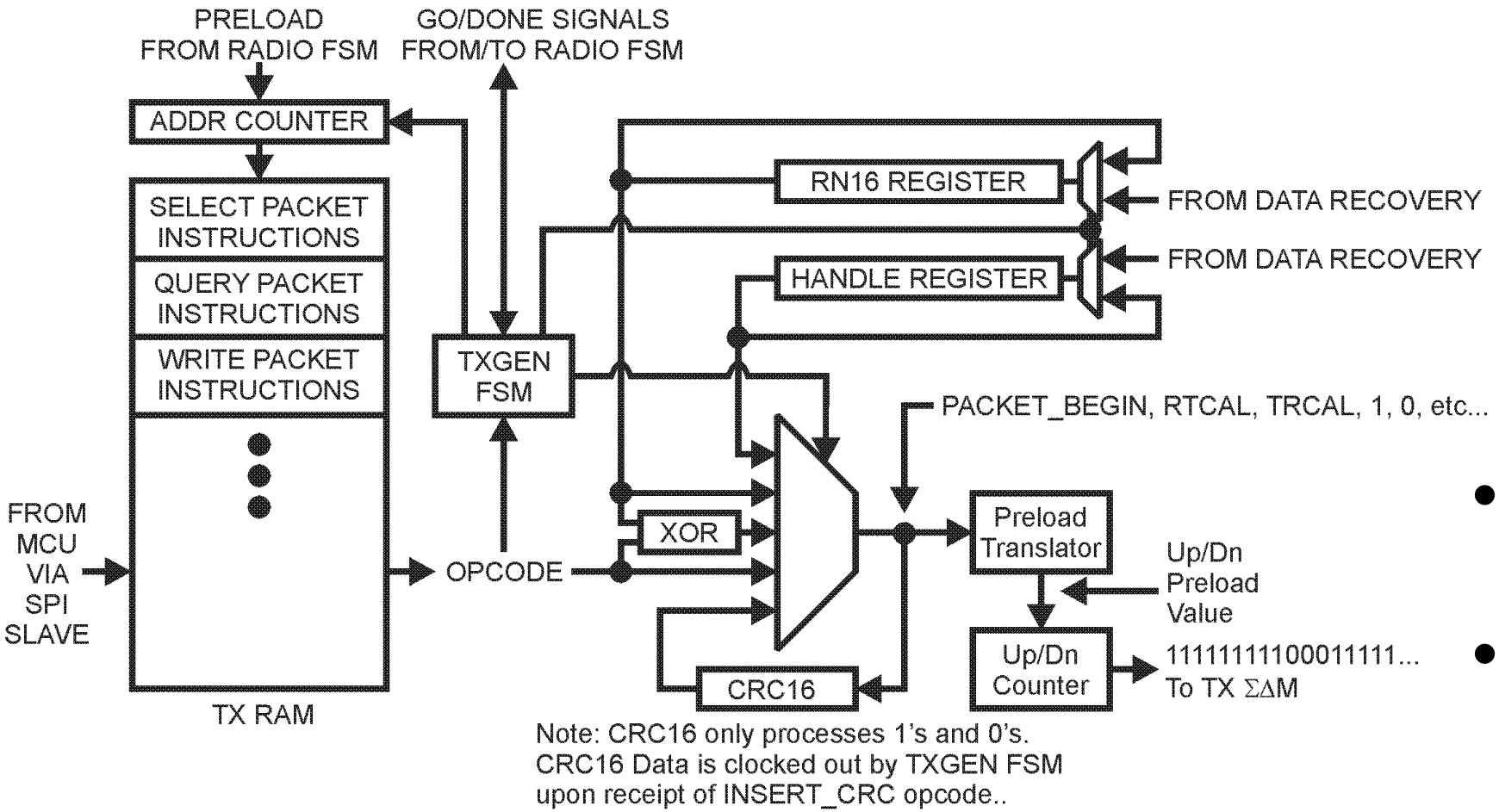


Clock Recovery



- Consumes 126 4-LUT, 49 FF, 129 LE (~5.6% of total).
- Most prior art uses HW intensive correlator-based methods.
- First reported UHF RFID CR to best of our knowledge with:
  - Hogge-type phase detector / Rotational frequency detector.
  - Sigma-delta modulator to dither counter (Numerically Controlled Osc.)

TX Waveform Generation (1)



- An opcode-driven FSM.
  - Loaded prior to fast RFID operations.
  - Controls ↑↓ counter.
  - Counter generates DSB-ASK at BB.
- Permits use of slow, cheap MCU.
- To best of our knowledge, novel in context of UHF RFID.

TX Waveform Generation (2)

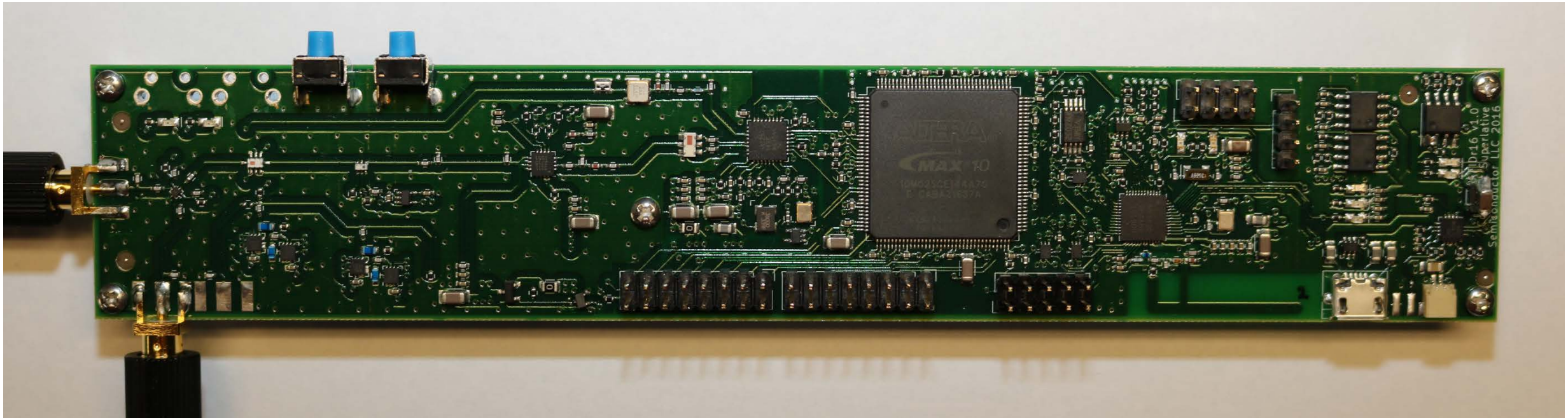
Opcode	Value	Explanation
TXCW	0000	TX CW Tone for 1.8ms.
BEGIN SELECT	0001	Begin a select packet.
BEGIN REGULAR	0010	Begin a regular packet.
DUMMY ZERO	0011	Insert a zero, don't count it in CRC.
SINGLE ZERO	0100	Insert a zero, count towards CRC.
SINGLE ONE	0101	Insert a one, count towards CRC.
RTCAL	0110	Insert RTCAL.
TRCAL	0111	Insert TRCAL.
NAK END	1000	Provides short TX CW time after NAK.
XOR NEXT 16b	1001	XOR next 16b with RN16.
INSERT CRC	1010	Insert CRC.
INSERT RN16	1011	Insert RN16.
INSERT HANDLE	1100	Insert Handle.
LAST WRITE	1101	Break write loop in Radio FSM.
END PACKET	1110	Return control to Radio FSM.
BEGIN IMMED	1111	Begin an immediate response packet.

- Two opcodes fit in 1 byte of SRAM.
- Can build all mandatory EPC GEN 2 waveforms with this set.
- Entire TX GEN block consumes 211 LE (9% of FPGA).

Outline

1. Global Context and Prior Art
2. Top Level Architecture
3. Transmit (TX) Leakage Cancellation
4. FPGA Circuit Design
5. **Experimental Results**
6. Conclusion
7. Backup

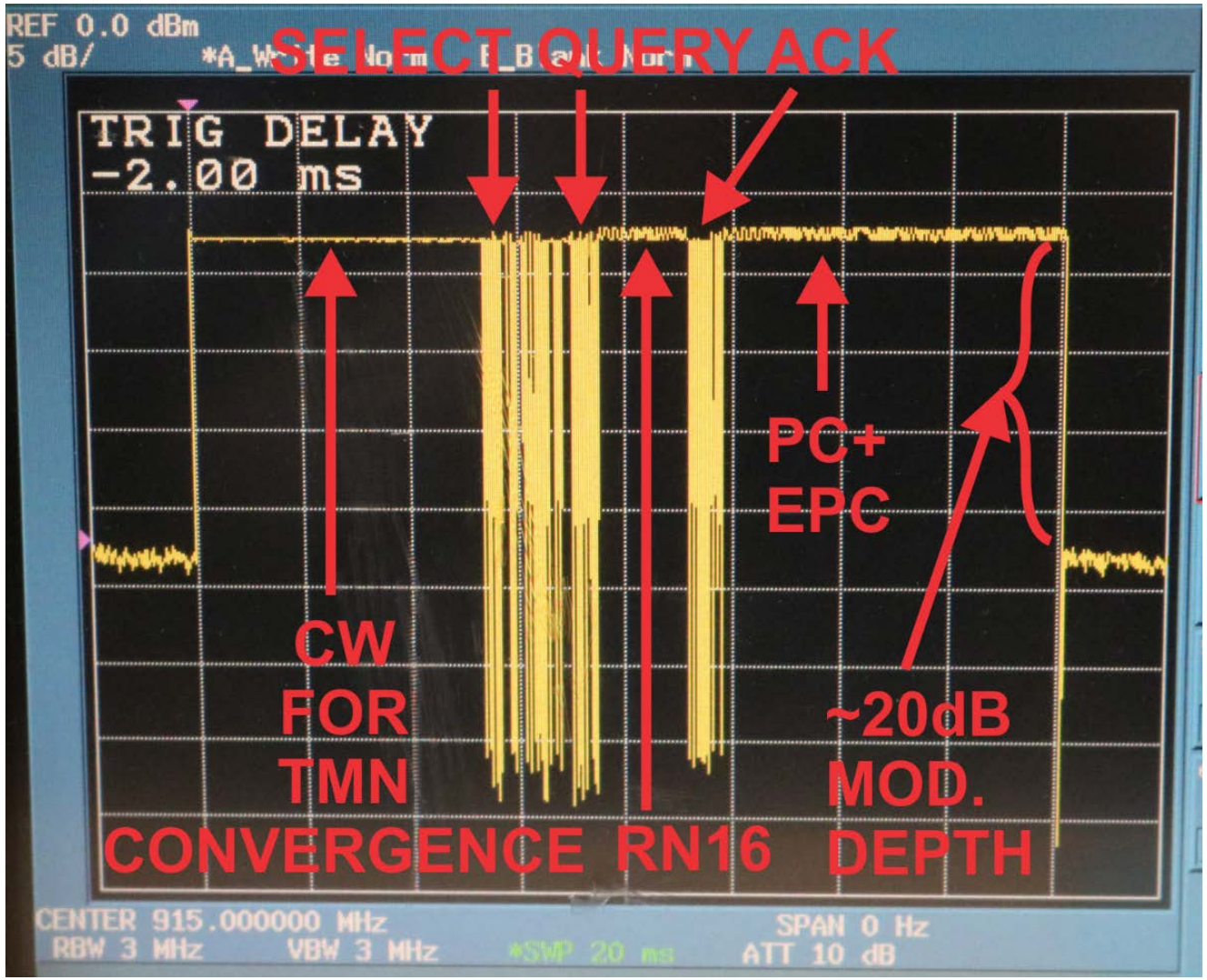
The Reader



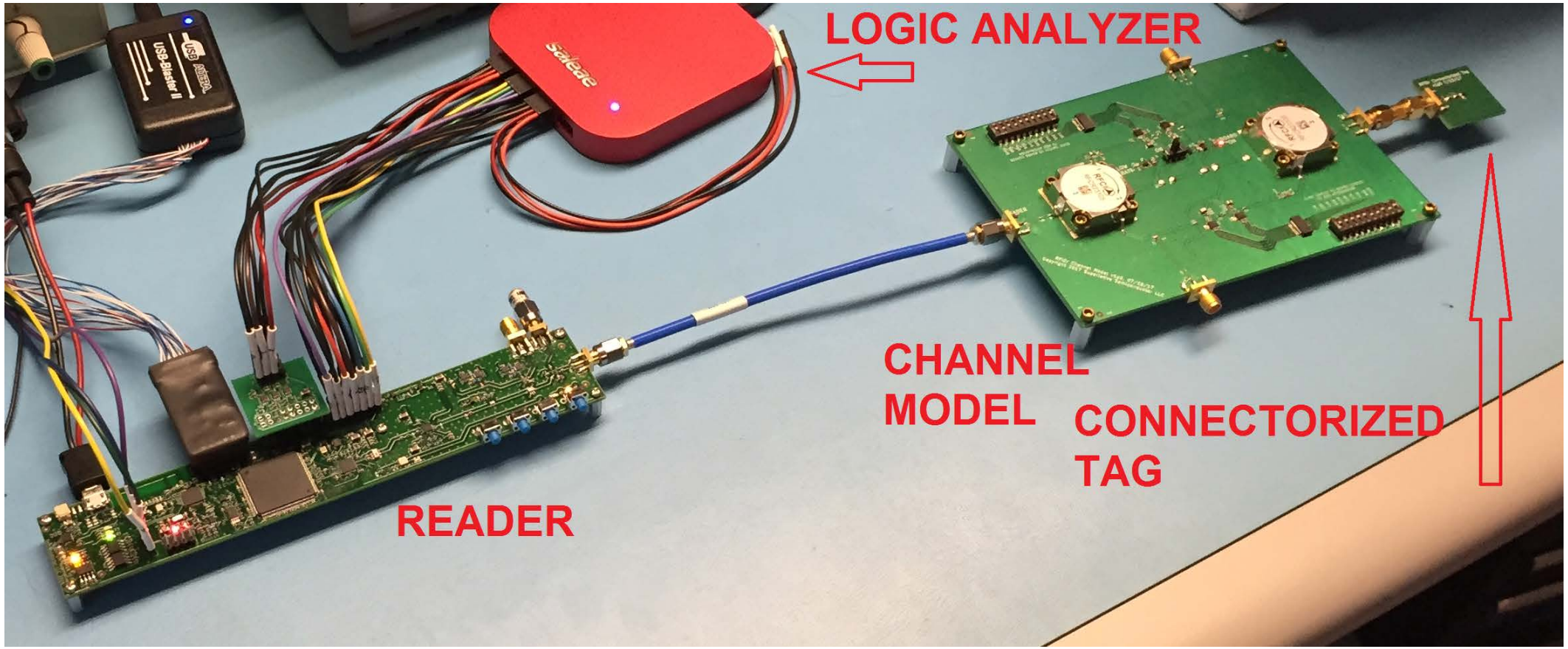
- 188.5mm x 34mm (7.42” x 1.34”) 4-layer PCB.
- Components only on top side.
- Board is powered by 5V Micro USB receptacle.

Output Characteristics

- Output Power: +26dBm
- Modulation depth > 18dB from build to build.
- TMN state retained from packet to packet.
  - Usually permitting 5.4ms reconvergence time.



Sensitivity Test



- Sensitivity measured at **-73dBm** (at least 50% valid I or Q reads).

Range Test

- With 1.2dBi dipole: > 50% correct I or Q reads @ **2.6m**
- With 12.5dBi patch: > 50% correct I or Q reads @ **15.2m**

Caveats

- Fixed Tari/BLF/Miller M=8.
- Reads only I or Q data at any given time (slows read rate x2).
  - Similar compromises made in comparable $24 reader ASIC, however.
- Large FPGA package used for cheap prototyping.
  - Design does fit in cheapest 10M02 part including # of pins.
- All mandatory EPC 2 Gen commands except “Kill”.
  - Goal was to make it hard to kill tags in personal/home usage.
  - Also didn’t want to kill limited # of tags during debugging.
- Only single reader mode (i.e. not multi- or dense-) supported.
- Requests long pilot from tag to ensure CR convergence.
- Not tested with frequency hopping yet.

Outline

1. Global Context and Prior Art
2. Top Level Architecture
3. Transmit (TX) Leakage Cancellation
4. FPGA Circuit Design
5. Experimental Results
6. **Conclusion**
7. Backup

Conclusion

- First reported fully-functional SDR UHF RFID reader with:
  - Reader ASIC replacement cost less than comparable ASIC.
  - Subranging digitally tunable capacitor-based TX cancellation.
  - Several techniques to reduce FPGA resource and MCU needs.

- Hope of this research is to spur the use of UHF RFID in the home and personal markets.

- Complete FPGA resources have been enumerated to provide a benchmark for future work.

Outline

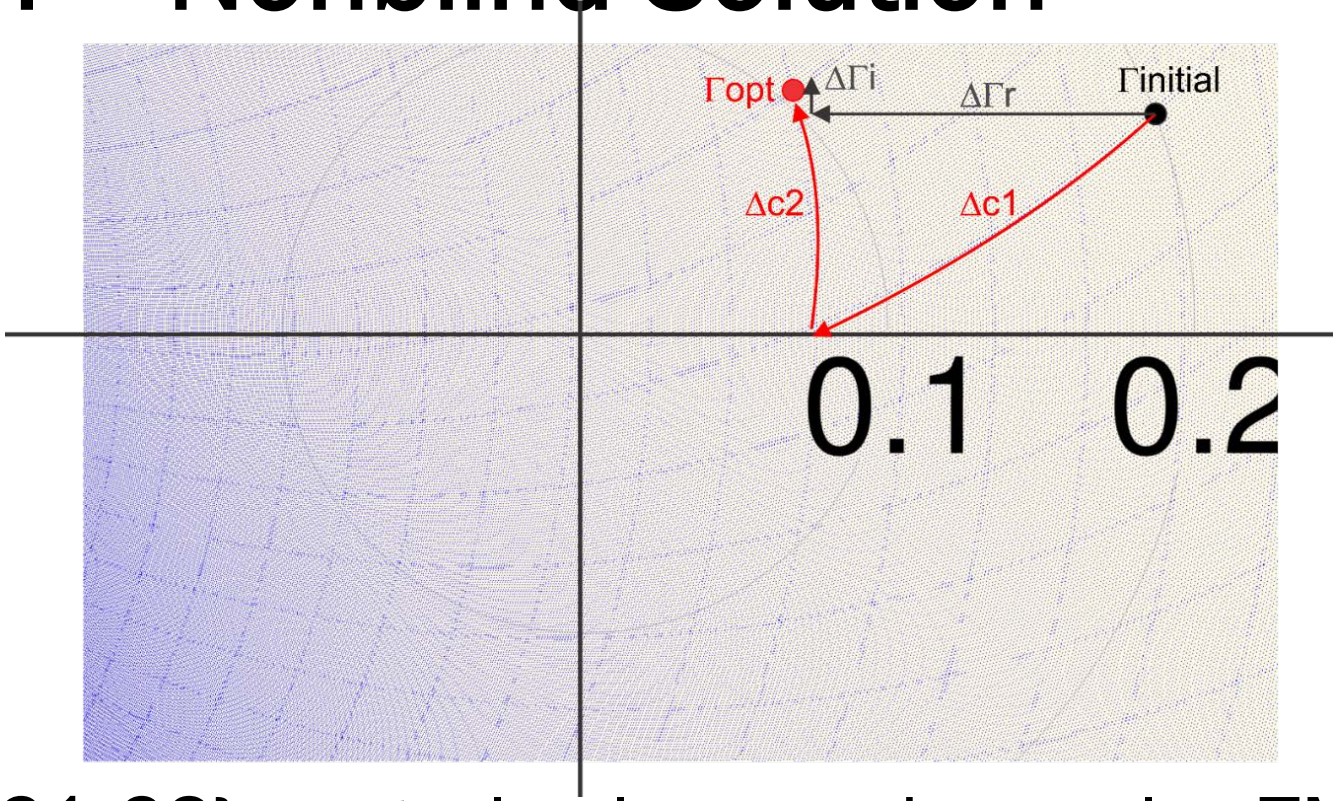
1. Global Context and Prior Art
2. Top Level Architecture
3. Transmit (TX) Leakage Cancellation
4. FPGA Circuit Design
5. Experimental Results
6. Conclusion
7. **Backup**

TMN Algorithm – Nonblind Solution

$$\begin{bmatrix}\Delta\Gamma_r \\ \Delta\Gamma_i\end{bmatrix} = J\begin{bmatrix}\Delta C_1 \\ \Delta C_2\end{bmatrix}$$

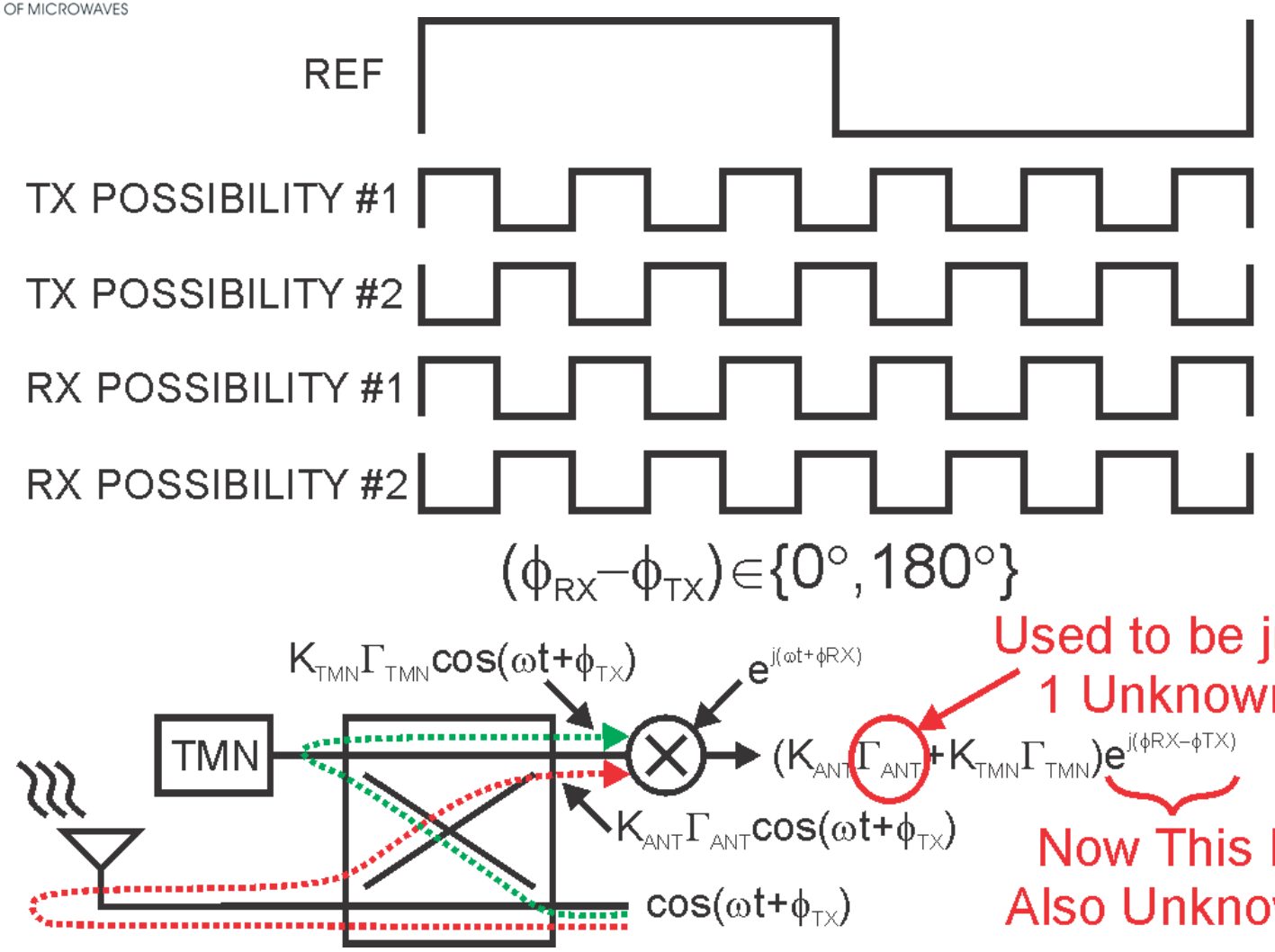
$$= \begin{bmatrix}\frac{\partial\Gamma_r}{\partial C_1}(C_1,C_2) & \frac{\partial\Gamma_r}{\partial C_2}(C_1,C_2) \\ \frac{\partial\Gamma_i}{\partial C_1}(C_1,C_2) & \frac{\partial\Gamma_i}{\partial C_2}(C_1,C_2)\end{bmatrix}\begin{bmatrix}\Delta C_1 \\ \Delta C_2\end{bmatrix}$$

$$\begin{bmatrix}\Delta C_1 \\ \Delta C_2\end{bmatrix} = J^{-1}\begin{bmatrix}\Delta\Gamma_r \\ \Delta\Gamma_i\end{bmatrix}$$



- ∃ a mapping between {C1,C2} control values and complex TMN Γ.
- Can use inverse Jacobian to implement gradient descent.
- 2-bit quantization of J^{-1} actually worked, allowing fit in 8KB SRAM.
- Can use baseband TX leakage as proxy for Γ_{TMN} - Γ_{OPT}.

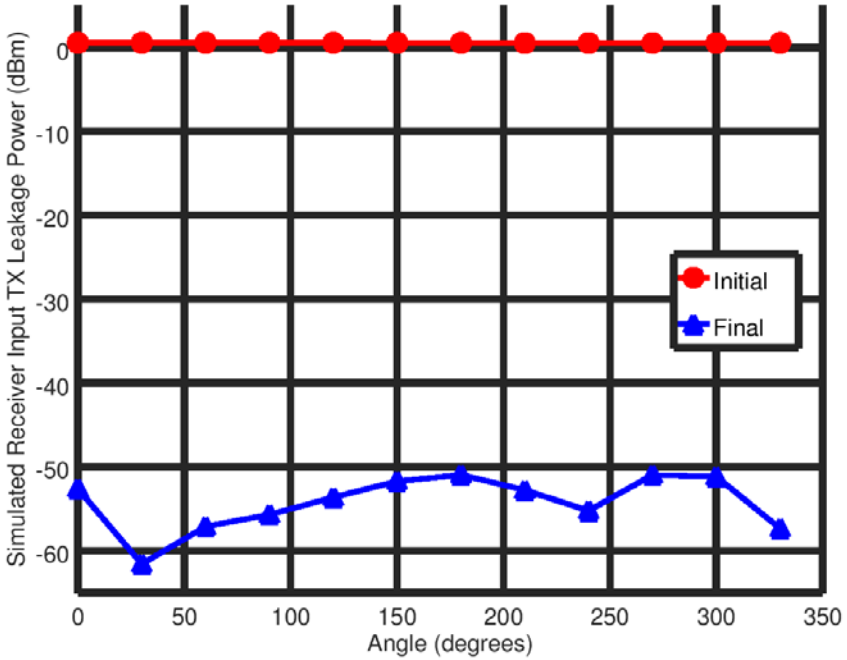
TMN Algorithm – Nonblind Problem



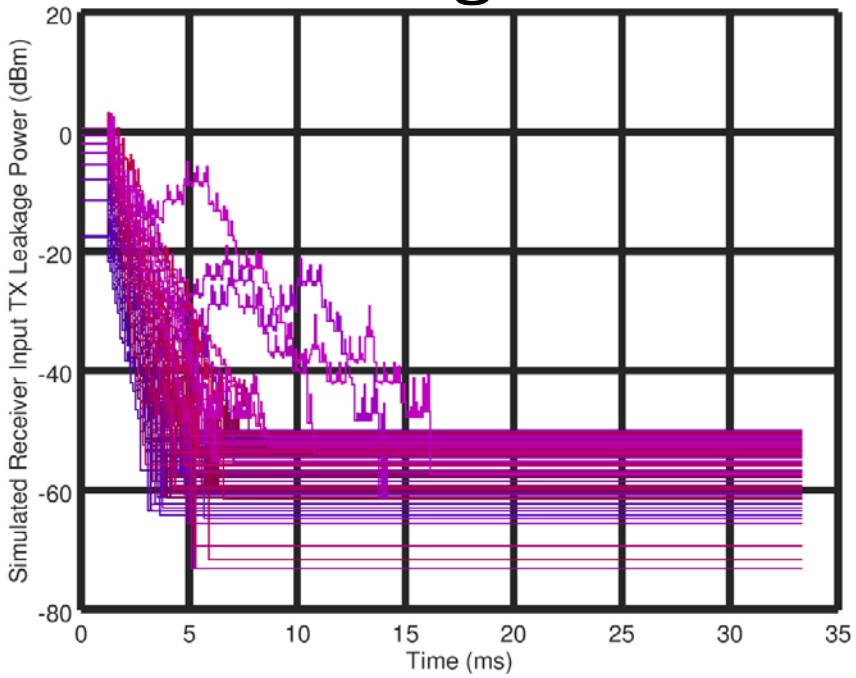
- Problem: phase relationship between TX and RX is unknown.
- This is due to independent Frac-N PLLs in TX and RX.
- Therefore, tuning algorithm must be at least partially blind.
- May work for some SDR ASIC though!

TMN Tuning Simulation Results

Initial/Final Leakage

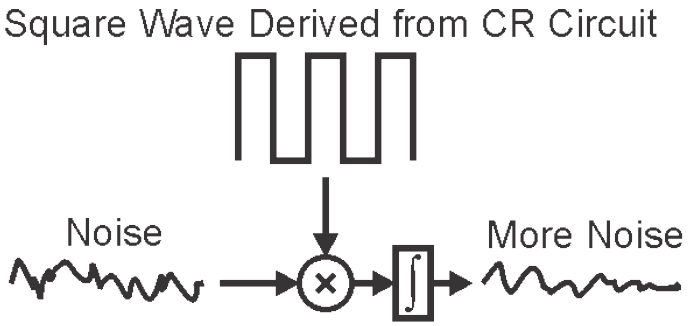


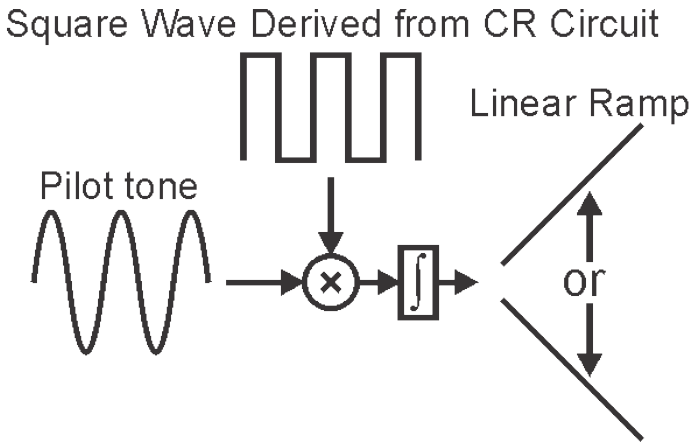
Convergence

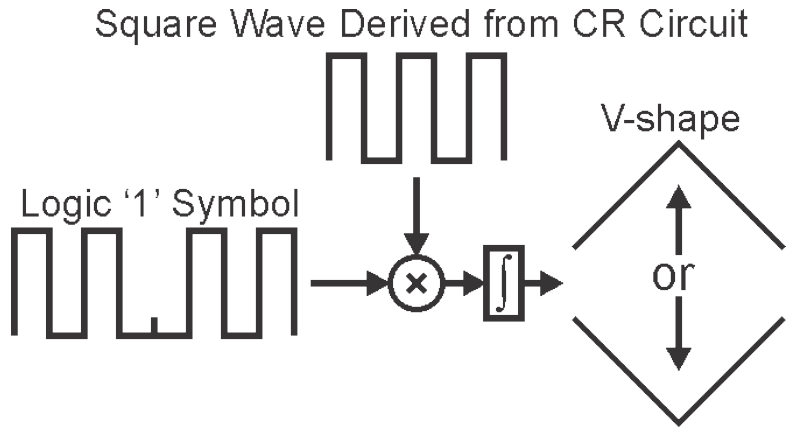


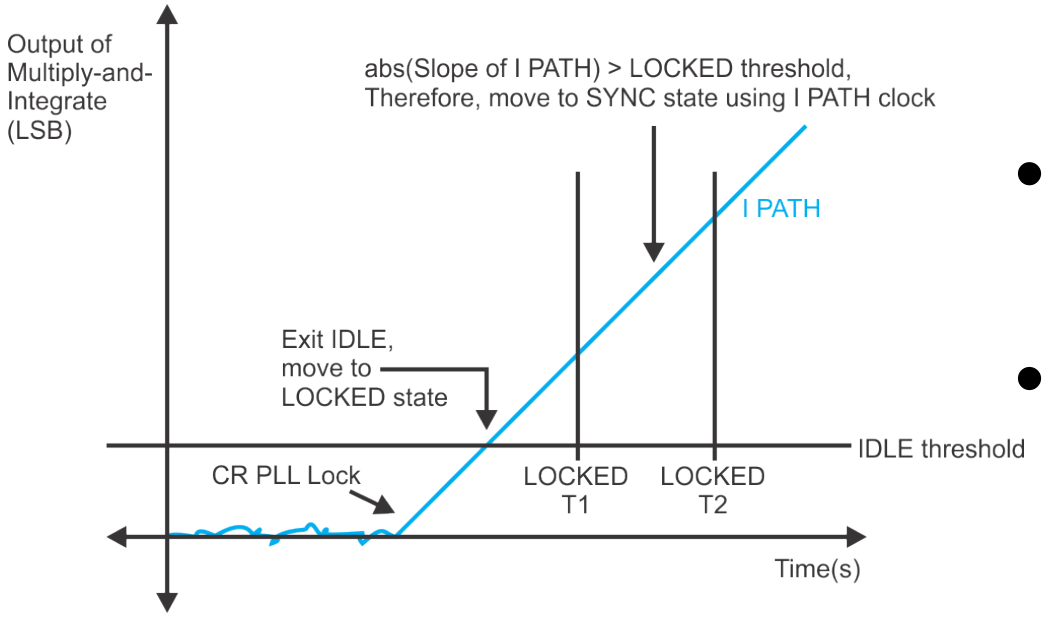
- Test algorithm with 96 Γ_{ANT} with $|\Gamma_{ANT}| < 0.3$ for 29dBm out.
- Left Plot: Initial/Final (0/30ms) TX Leakage at SDR RX Input.
  - For $|\Gamma_{ANT}| == 0.3$ at 12 different $\angle$.
- Right Plot: TX Leakage at SDR RX Input for all 96 Γ_{ANT}.

Reader Data Recovery – Correlation with Clock



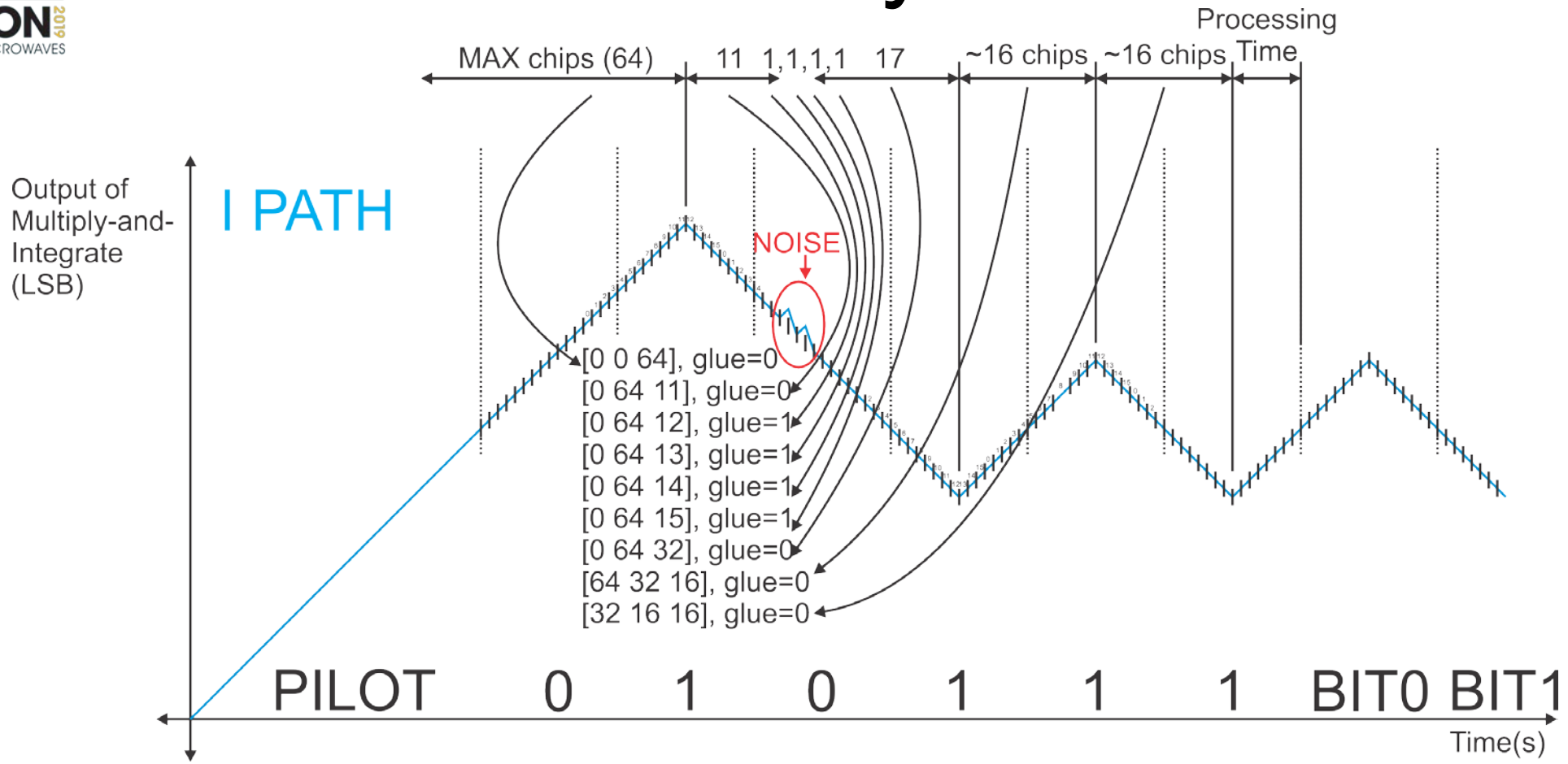






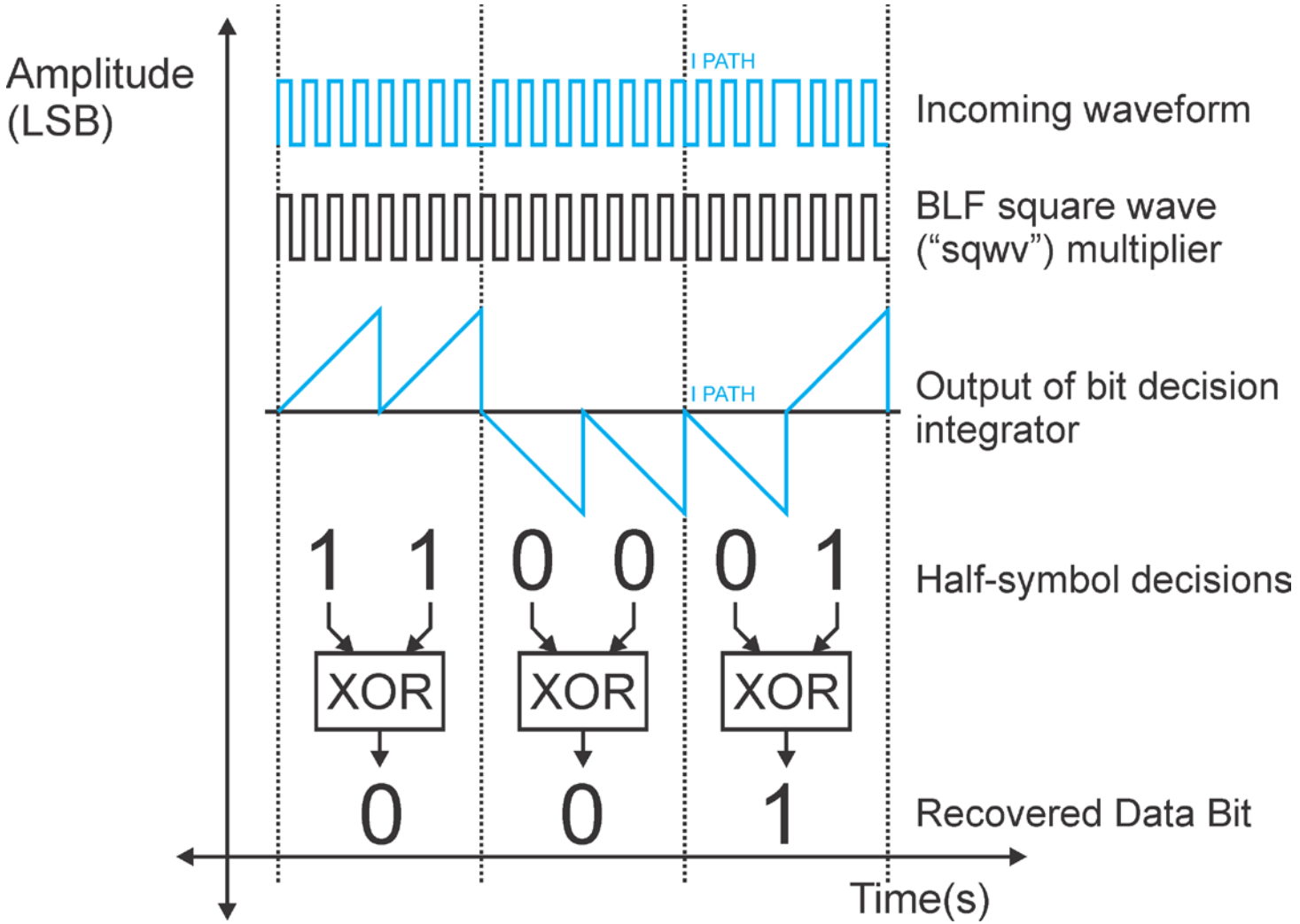
- Recovered clock multiplies incoming signal.
- Result is then integrated to determine if pilot or preamble is present.

Reader Data Recovery – Preamble Detect



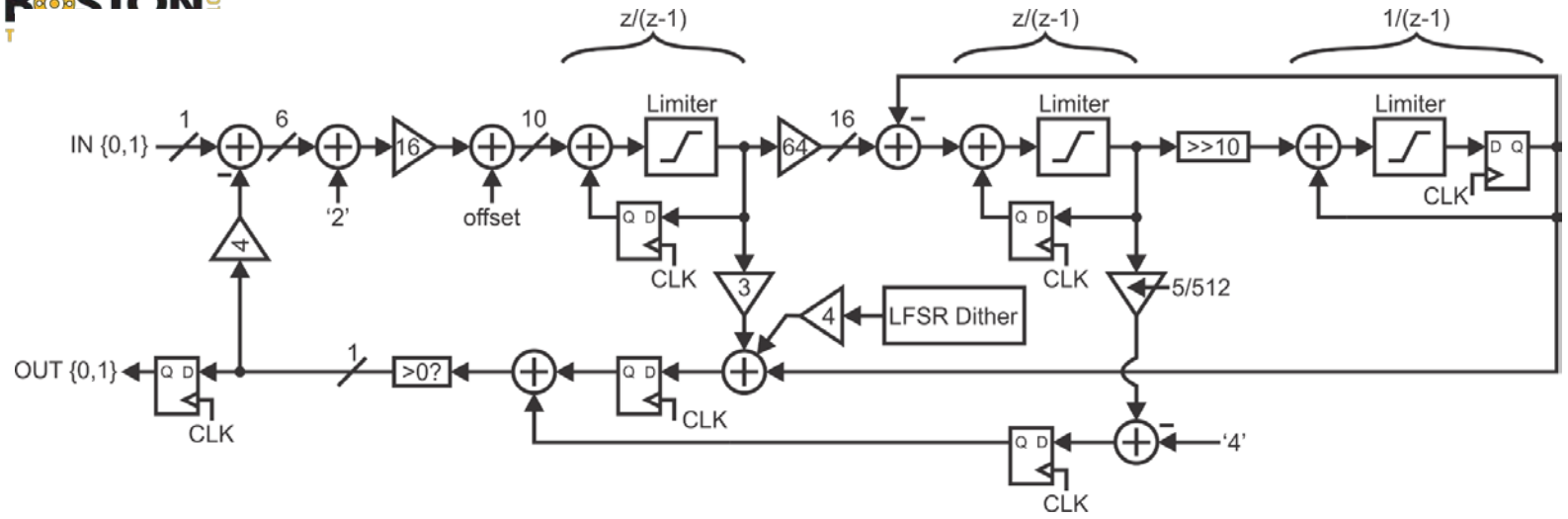
- Count Miller BLF half-periods between peaks to find preamble.
- Filter out noisy short peaks by gluing short peak intervals.

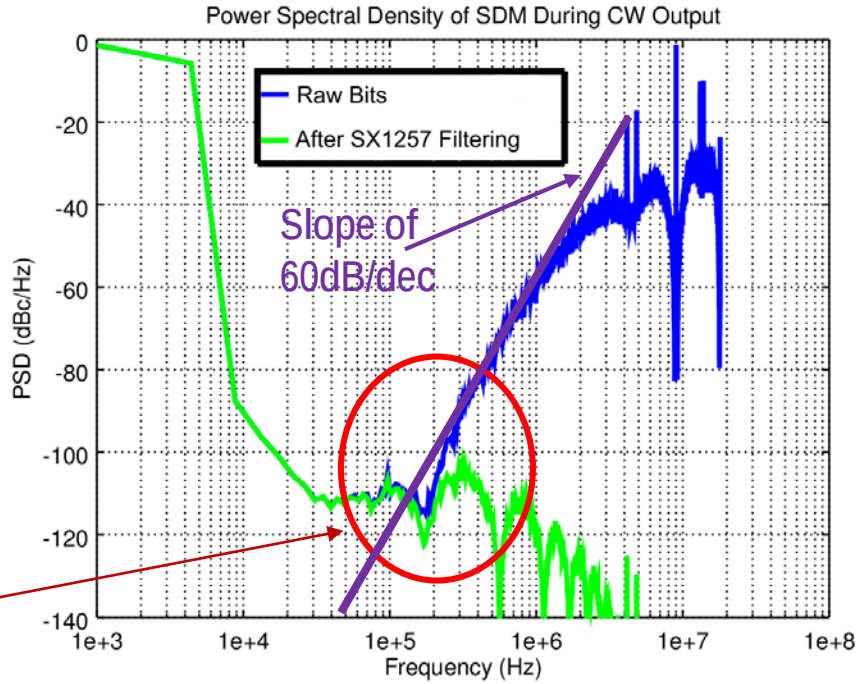
Reader Data Recovery – Bit Decisions



- Perform bit decisions on half-periods.
- XOR results to recover the data bit.
- Lose 3dB sensitivity
  - Clock recovery dictates sensitivity anyway.
- Additional error correction is possible in future.

Reader: Sigma-Delta Modulator



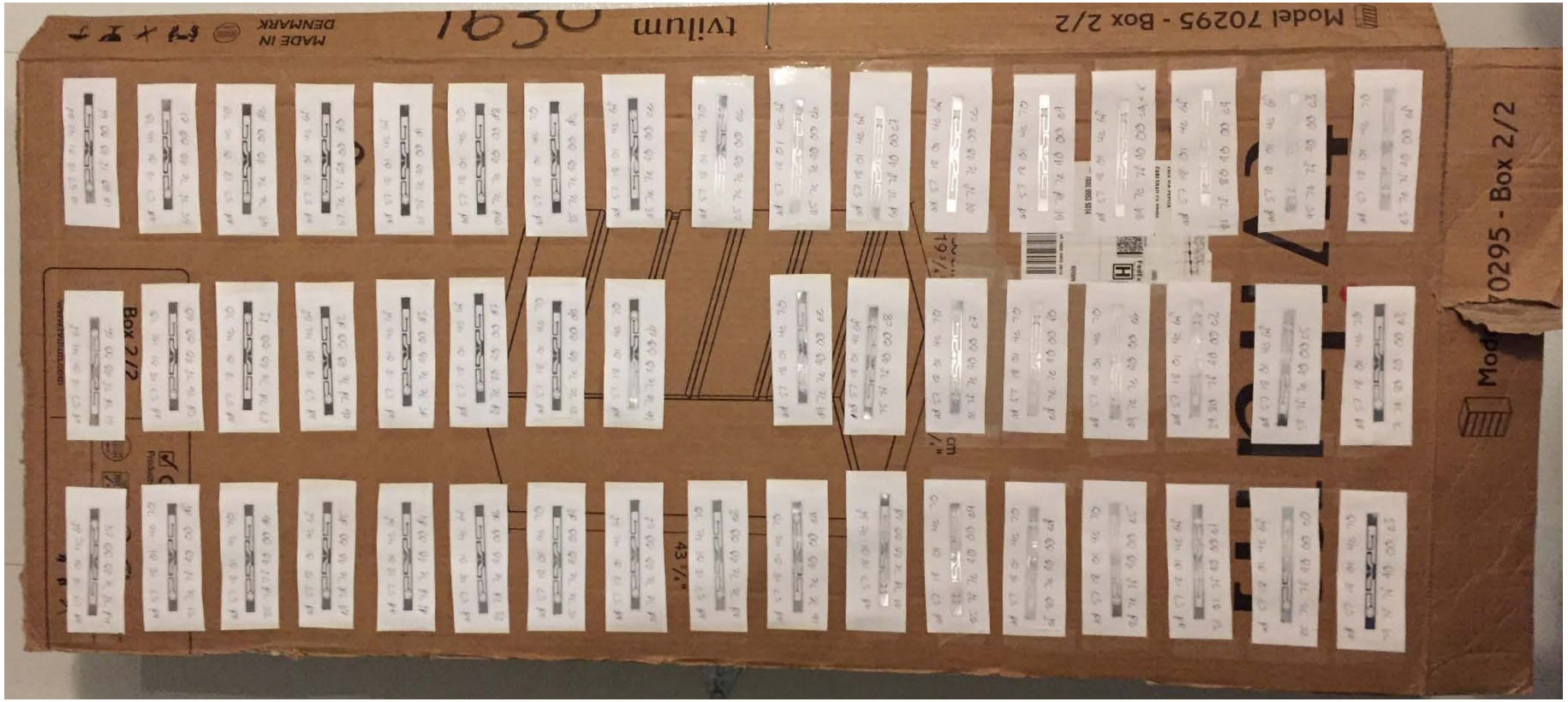


- As specified by SX1257 Data Sheet
  - But with a zero notch at the BLF.
- Zero notch is critical!
- -110dBc noise at BLF is less than SX1257 phase noise.
- Consumes 160 logic elements (LEs) (7% of total).

Reader: FPGA Resource Allotment

Block	4-LUT	FF	LE	9x9 Mult.	RAM Bits
RX Filters	569	437	631	16	0
Clock Recovery	126	49	129	0	0
DR-PMF & Bit Decis.	50	33	50	0	0
DR-Symbol Sync.	117	61	117	0	0
DR-I/Q Magnitudes	160	88	160	0	0
DR-SRAM Muxing	68	8	68	0	128
DR-Local Protocol	86	81	86	0	0
DR-Total	499	286	499	0	128
Radio FSM	137	17	142	0	0
SPI	199	146	218	0	0
TX Cancel	222	118	222	16	8192
TX Gen	210	71	211	0	0
TX $\Sigma\Delta$M	159	82	160	0	0
Others	35	37	69	0	8320
Total	2156	1320	2281	32	16,512
Limit	2304	2304	2304	32	110,592

Reader - Inventory Test

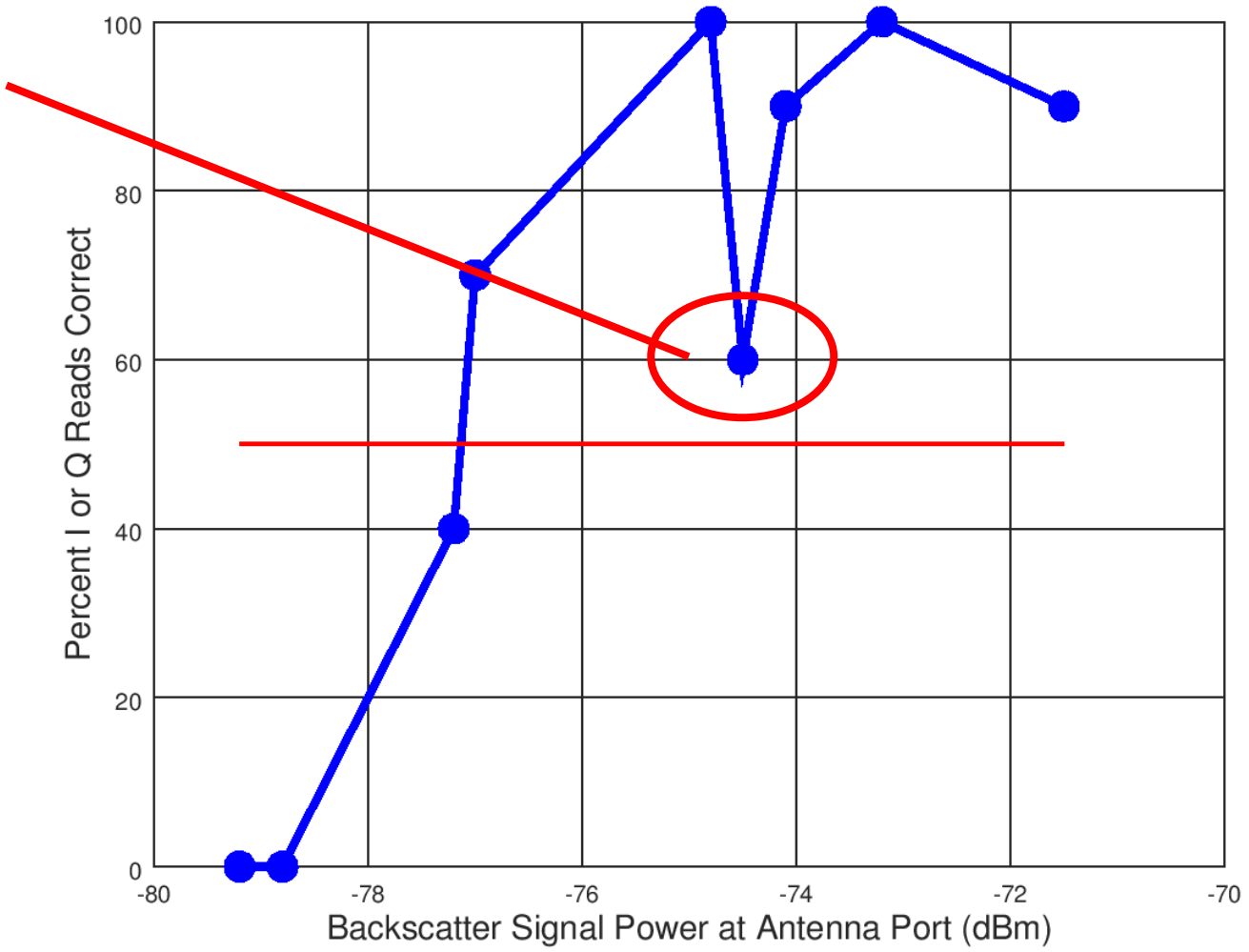


- 50 tags could be read in 20 seconds.
- Read speed is limited by slow Apple BTLE comms. to phone.

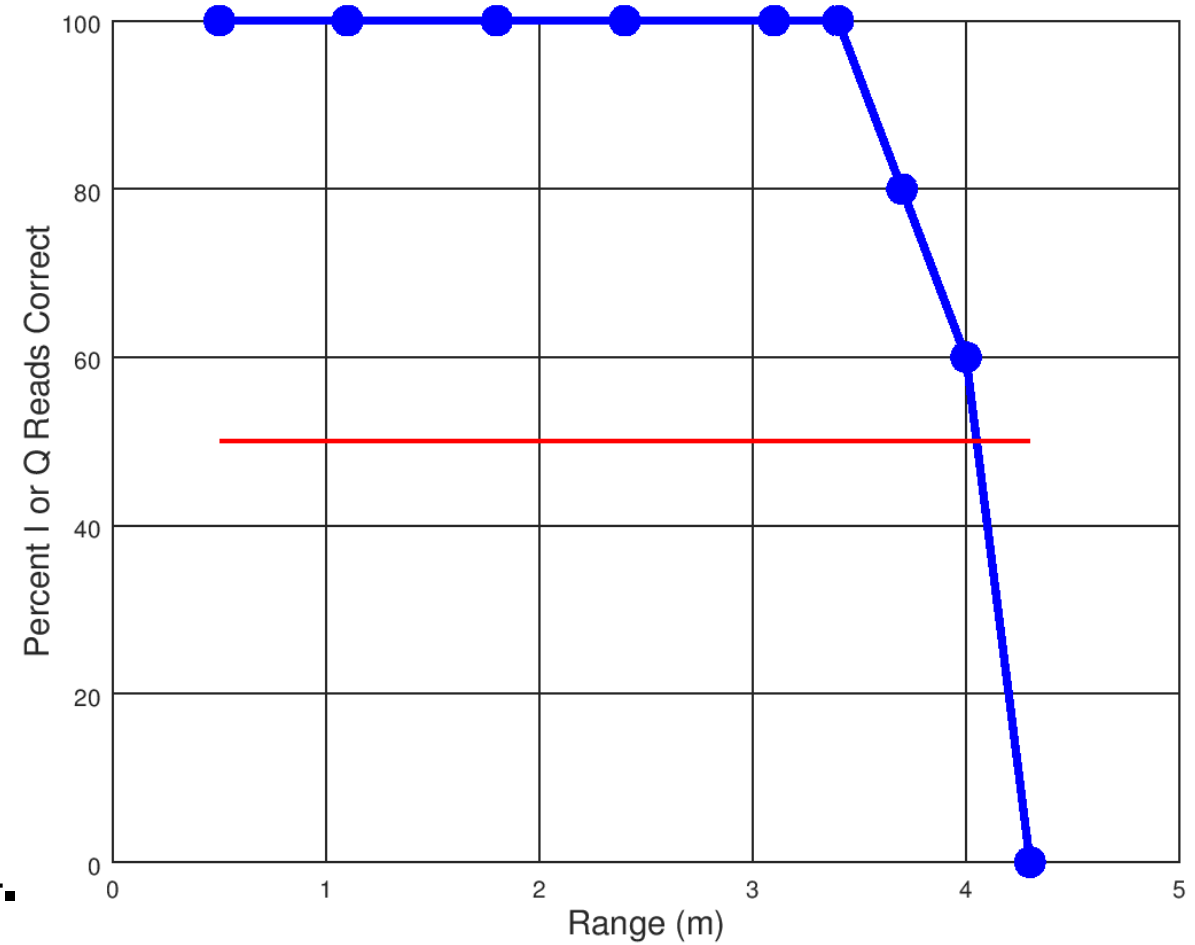
Reader – Sensitivity Curve

- Original publication board recently remeasured.
- Sensitivity measures better than before.
- Read success rate falls off very rapidly.

- This point remeasured twice at 80% after this data was taken.



New Hardware Range



- New hardware at +30dBm P_{OUT}.
- 5V on antenna diversity SPDT control solves distortion issue.
- Range with 1.2 dBi dipole antenna is 4m in open area.