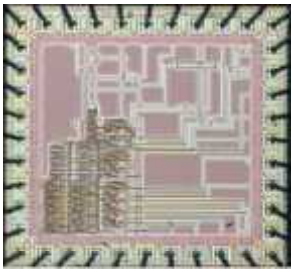


Reverse Engineering a passive UHF RFID Tag

Why not?

Brian Degnan, Ph.D.

Acknowledgements

white river technologies

- Dr. Ed Reiter
- Dr. Greg Schultz

Georgia Institute of Technology

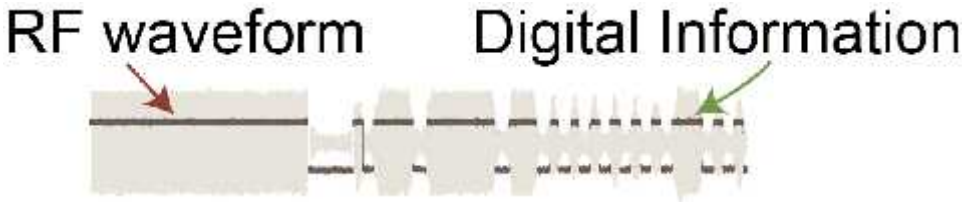
- Prof. Greg Durgin
- Prof. Jennifer Hasler

IC Postdoctoral Research Fellowship Program
Research Institutes · National Laboratories · Universities

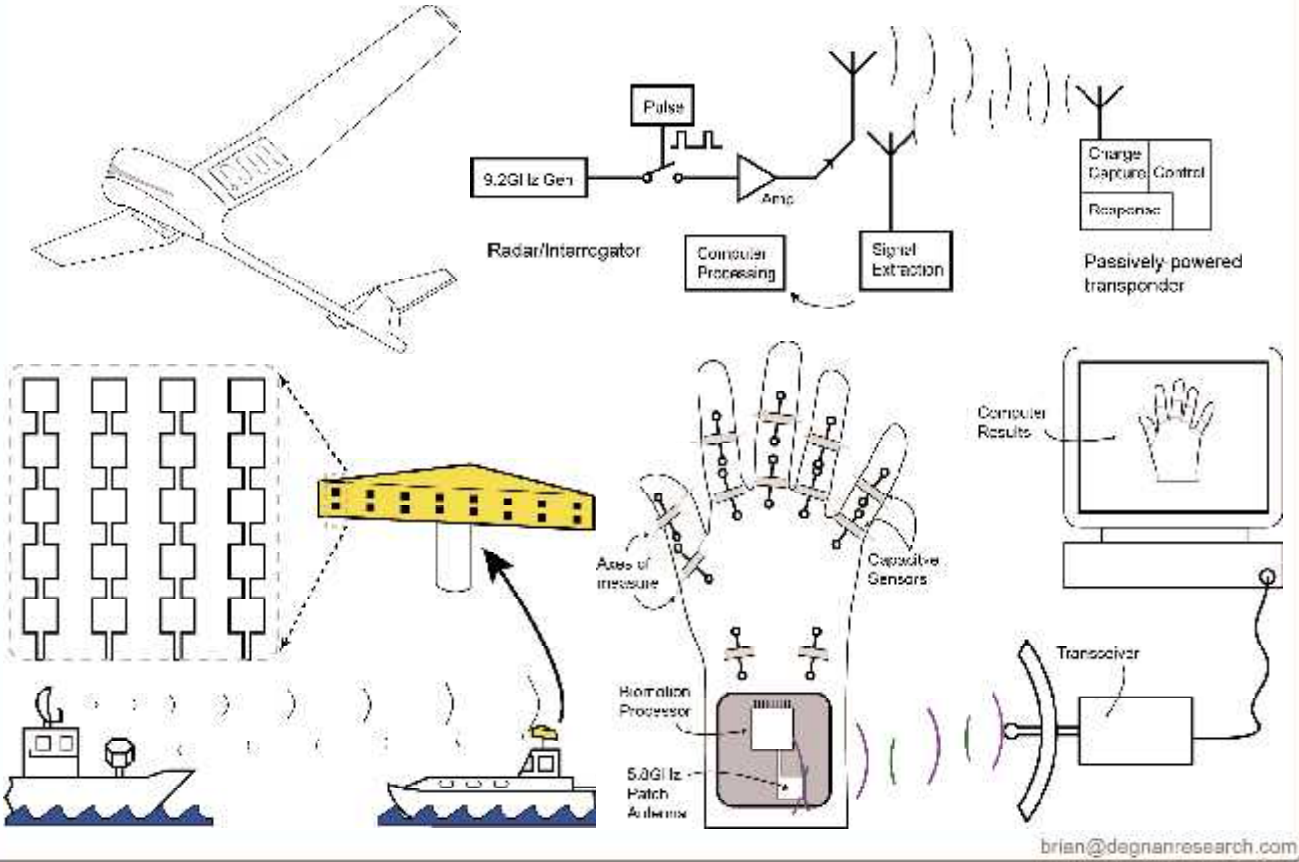
- The SIMON team
- Oakridge Nat. Lab

What's this about?

- Some circuits for Gen2v2 for UHF RFID
- Why the electronic side is relevant.
- Components (same but different)
- System components and bounding the problem
- System intuition

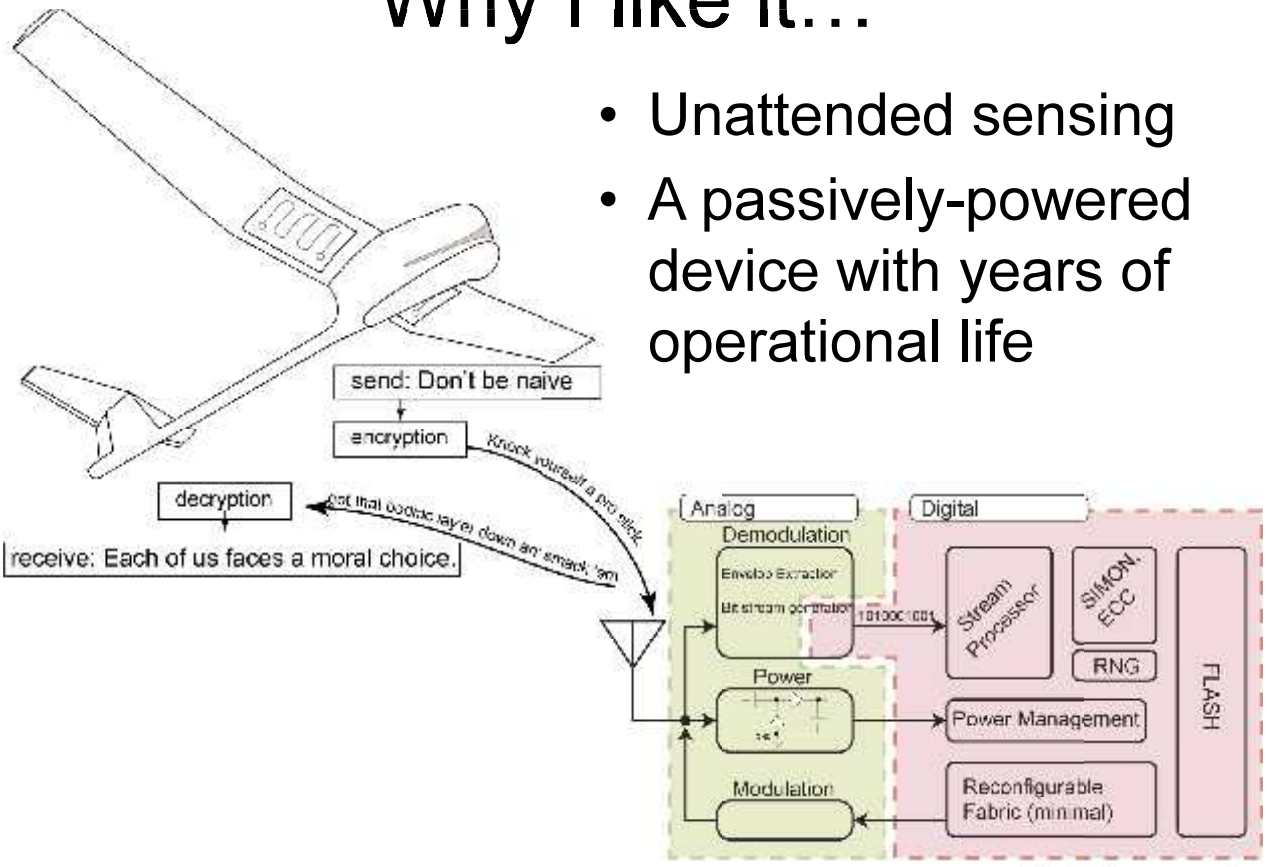


RFID Processor Applications

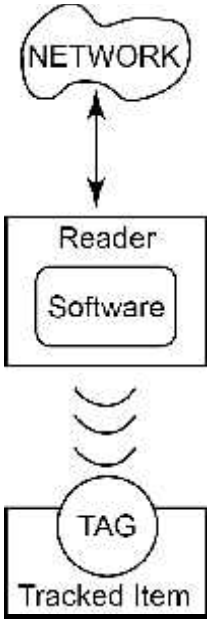


Why I like it…

- Unattended sensing
- A passively-powered device with years of operational life

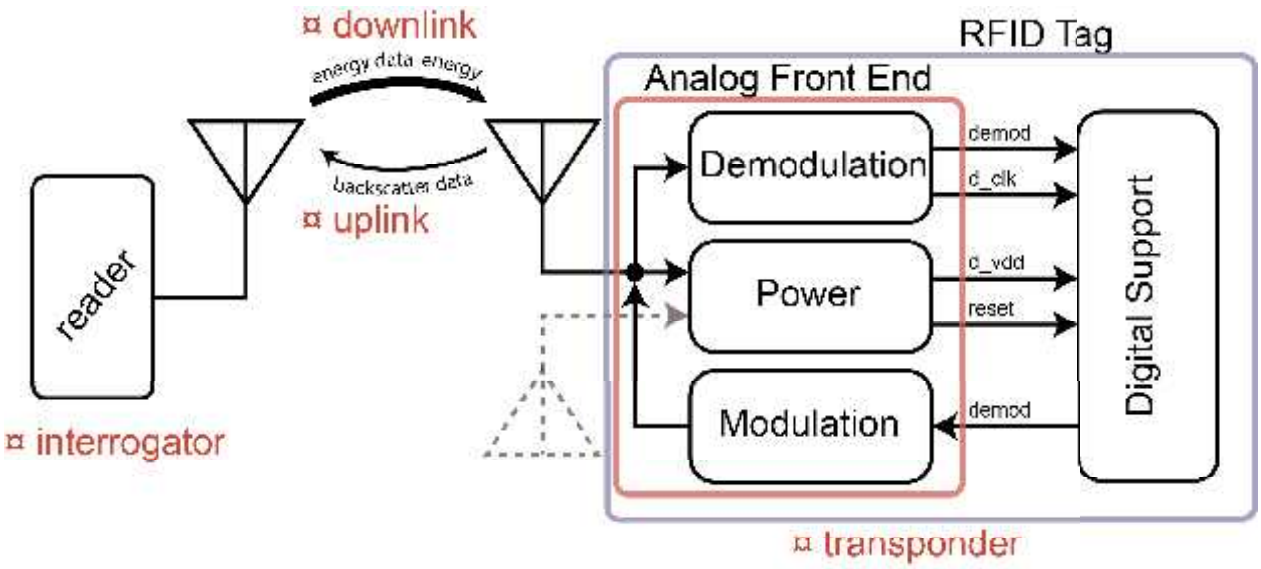


System Overview, in Context



- Tags communicate wirelessly
- Tag memory identifies individual items (TID, EPC, more)
- Small amount of memory
- Applications read/write small amounts of data

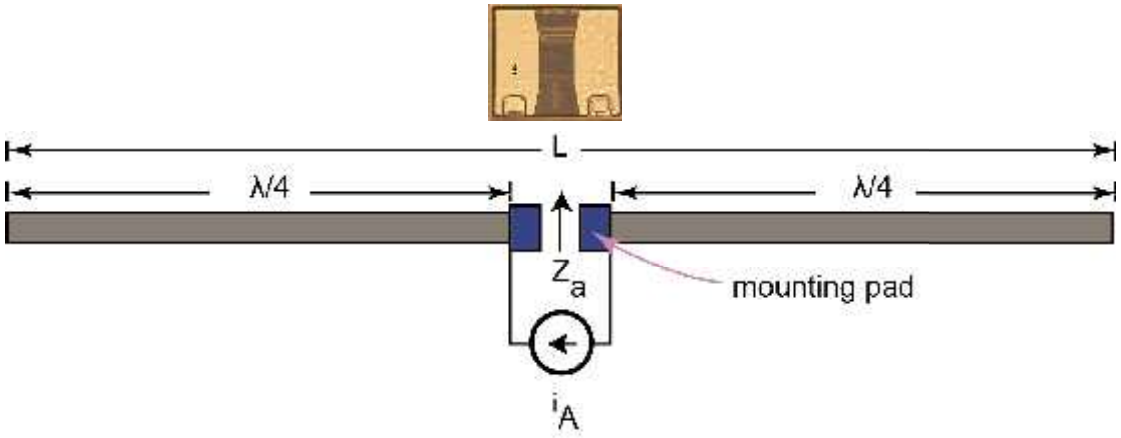
The RFID System



- Gen2: 860MHz-960MHz +- 40kHz-640kHz
- Passively Powered

brian@degnanresearch.com

"Antenna Powered"





brian@degnanresearch.com

Wireless, Tag System Datalink

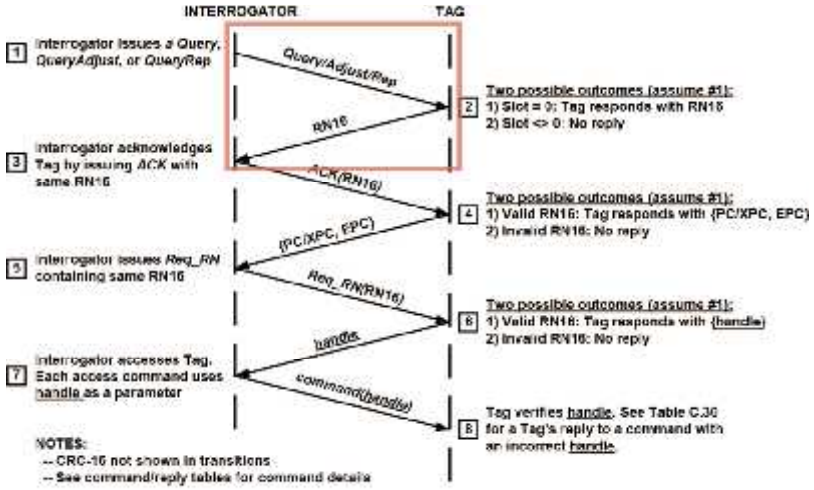
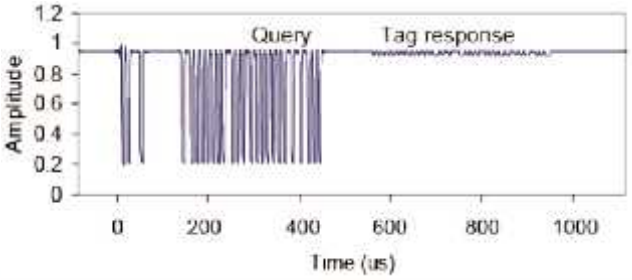
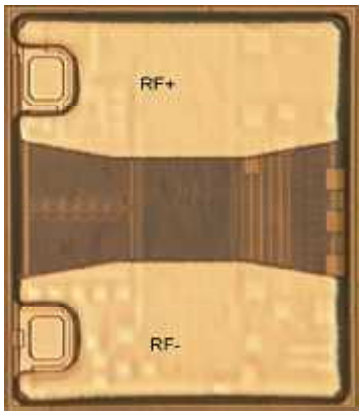
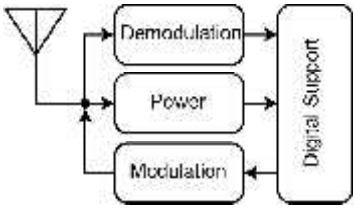


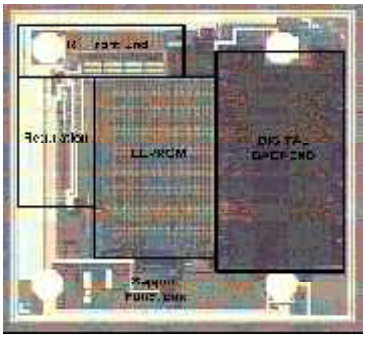
Figure E.1: Example of Tag inventory and access

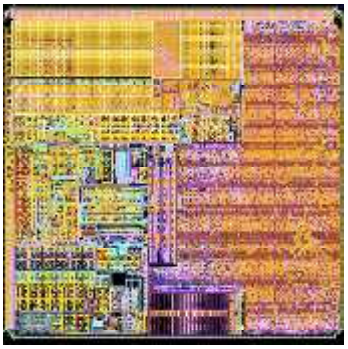






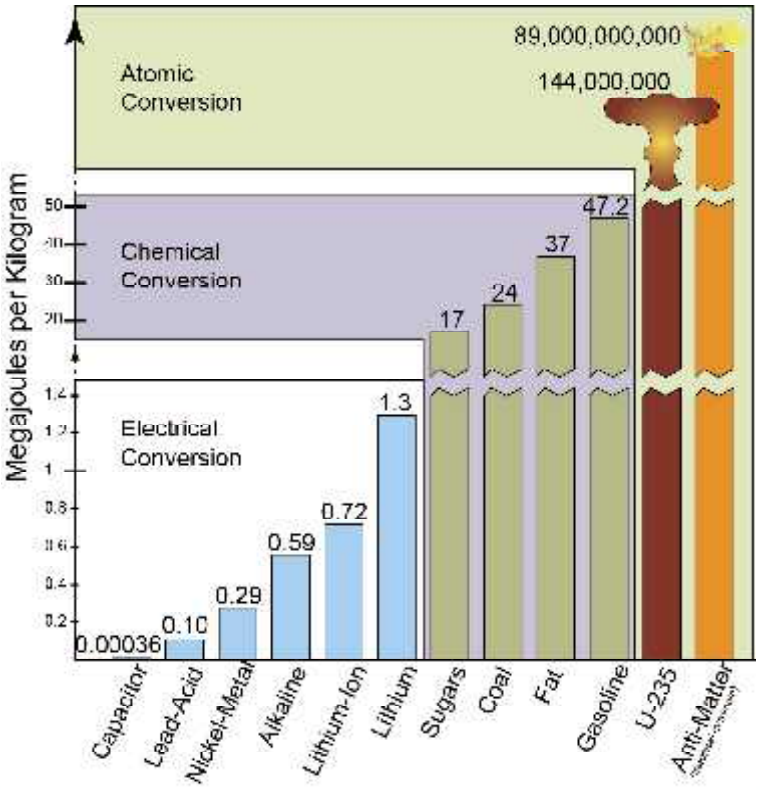
Economics of semiconductors



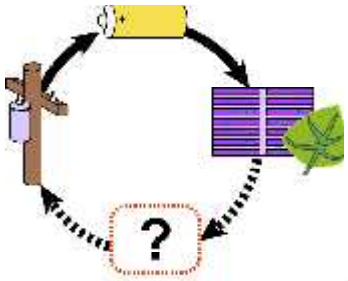


- About USD$ 0.05 per 1mm^2 (can be cheaper)
- Physically limited by the size of “sand”
- They must be attached to an antenna

Energy Storage



- 1000J ~ 1m^2 sunlight second second
- 100J released from a human per second
- USA uses 4W EIRP



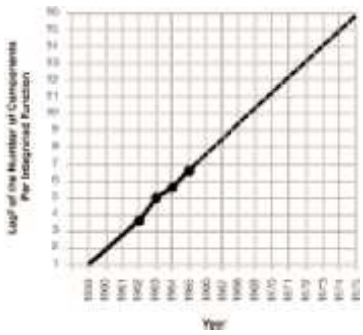
Brian Degnan, Ph.D. White River Technologies Inc.

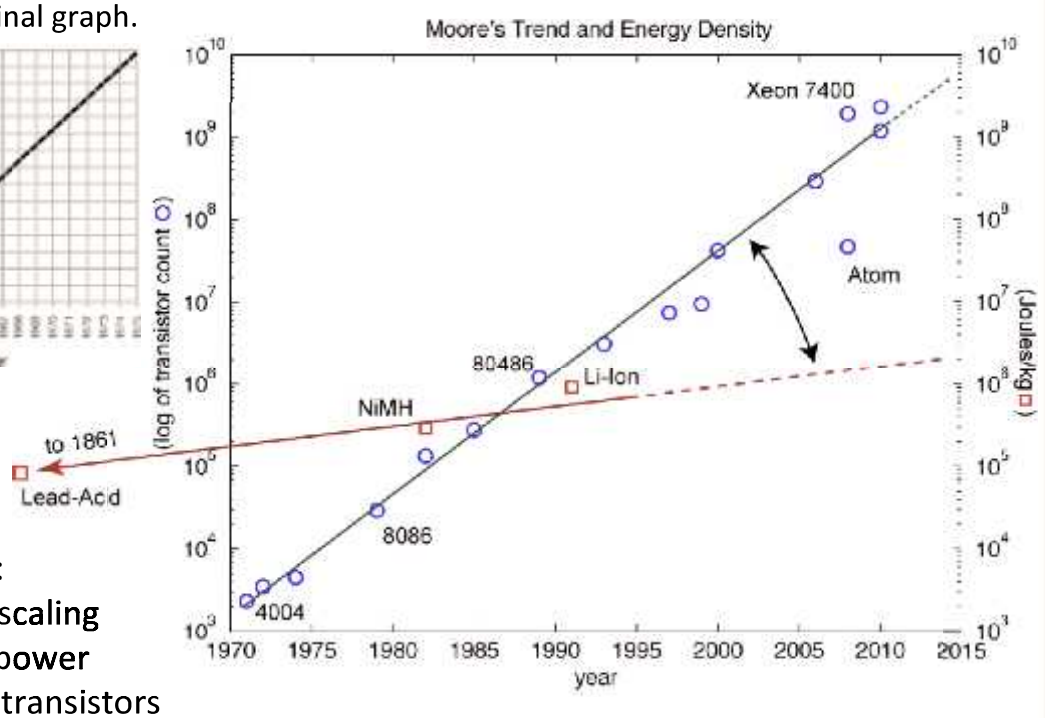
Components: Device Review

- MOSFET is one of many devices.
- Voltage controlled current source
- The input looks like a capacitor
- Multiple operating regimes
- Mathematics and physics are simple, but reality is terrible.

Moore More, Moore Less

Moore's original graph.

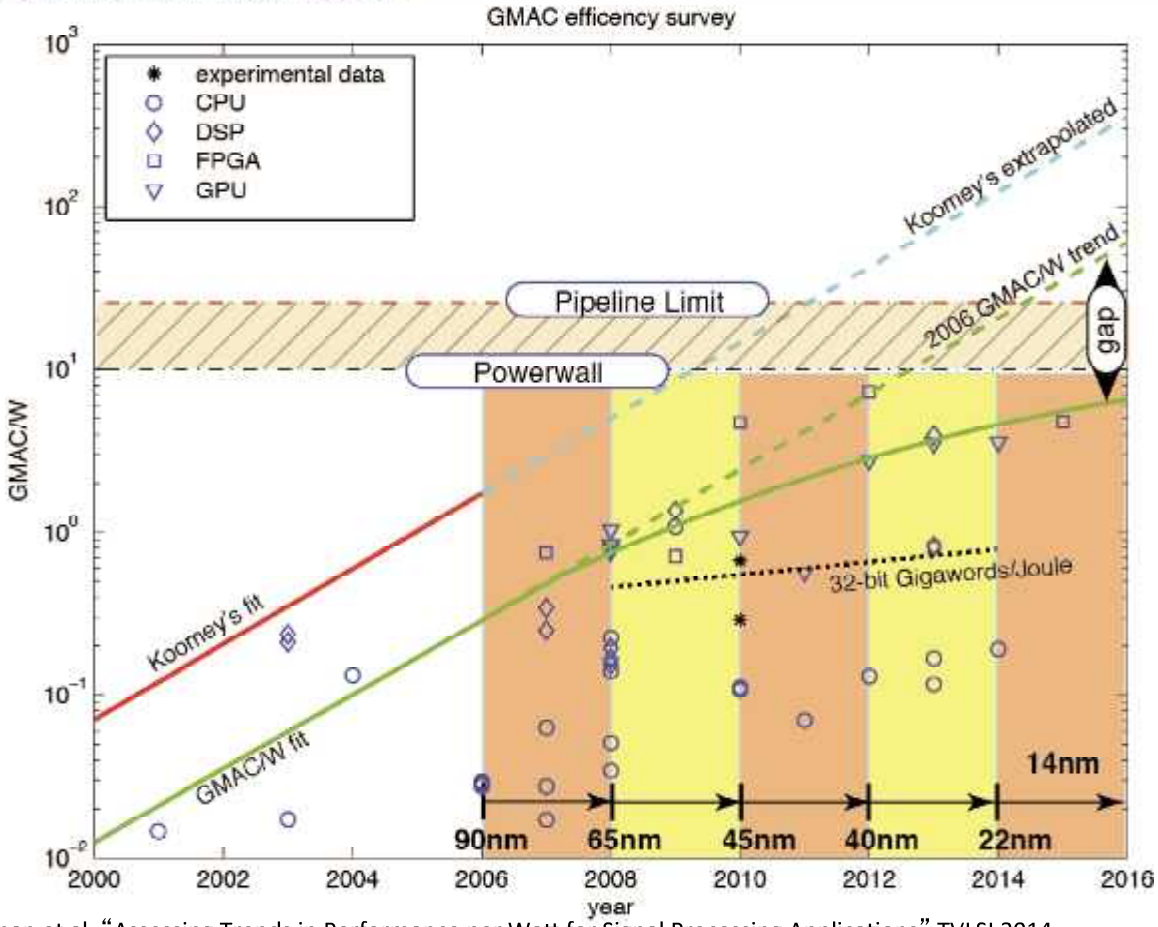




Assumptions:
--Transistors scaling
--Processing power correlates to transistors

brian@degnanresearch.com

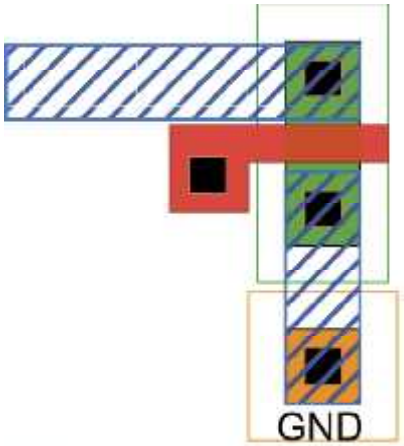
Brian Degnan, Ph.D. White River Technologies Inc.

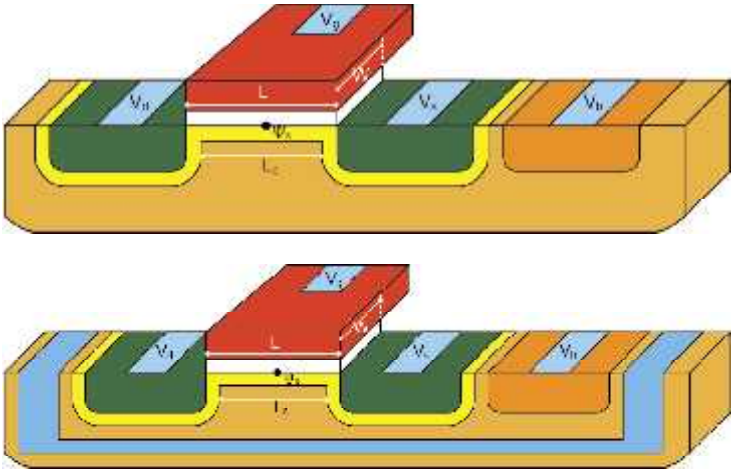


Degnan et al, "Assessing Trends in Performance per Watt for Signal Processing Applications" TVLSI 2014

brian@degnanresearch.com

Transistors: how things used to be.





contact

metal 1

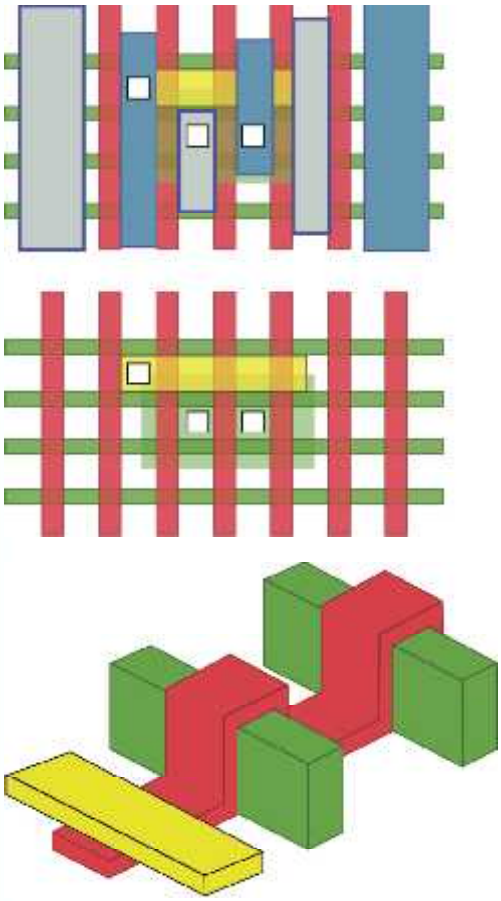
n-active

poly

p-active

brian@degnanresearch.com

Brian Degnan, Ph.D. White River Technologies Inc.



Metal 1C0

Metal 1C1

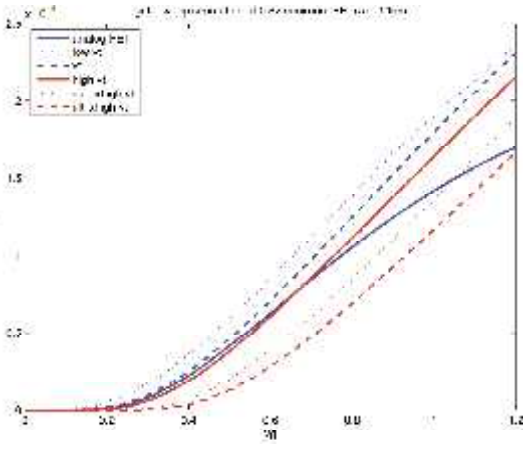
contact

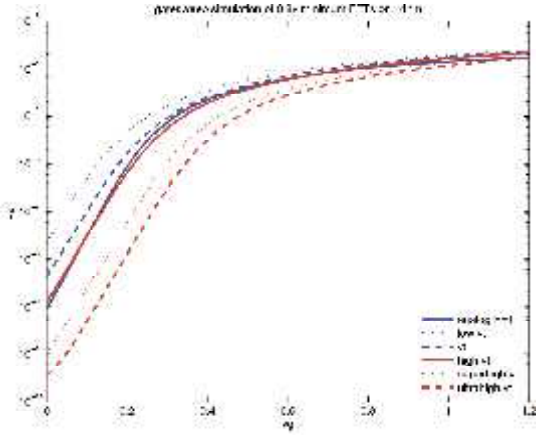
n implant

fin

polysilicon

contact poly





brian@degnanresearch.com

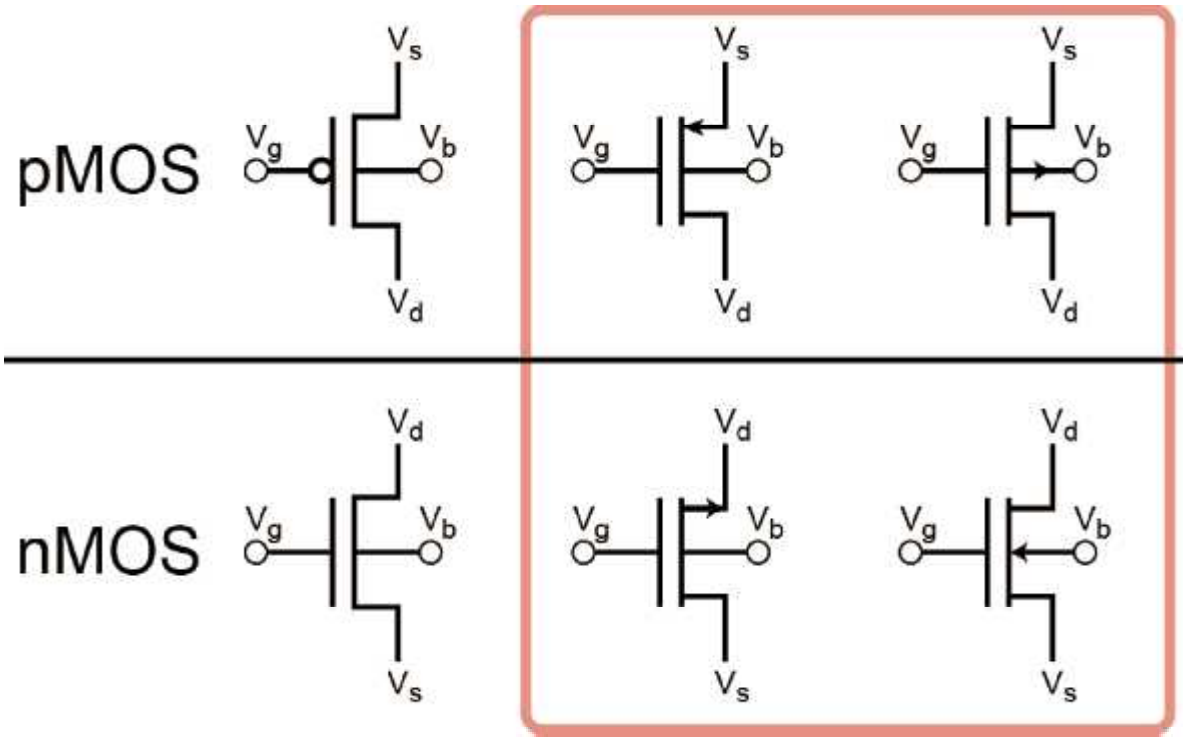
A 130nm Process, and Parts Review

	Transistors			
	thin oxide		thick oxide	
	nFET	pFET	nFET	pFET
V_{DD}	1.2V	1.2V	2.4V	2.4V
L_{min}	120nm	120nm	240nm	240nm
V_{th}	0.30V	-0.35V	0.4V	-0.45V
I_{off}	300pA/μm	200pA/μm	10pA/μm	10pA/μm
I_{Dsat}	530mA/μm	210mA/μm	660mA/μm	260mA/μm
t_{ox}	2.2nm	2.2nm	5.2nm	5.2nm
	Capacitors			
	thin oxide		thick oxide	
MIM	1.35fF/μm ^{2}			
MOS	11fF/ μm^2	9fF/μm^2	5.5fF/μm^2	4.5fF/μm^2

brian@degnanresearch.com

Brian Degnan, Ph.D. White River Technologies Inc.

Transistor Symbols



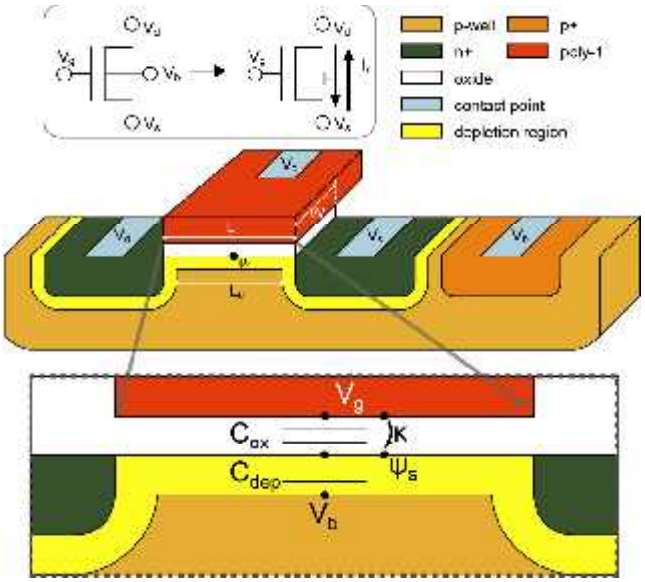
brian@degnanresearch.com

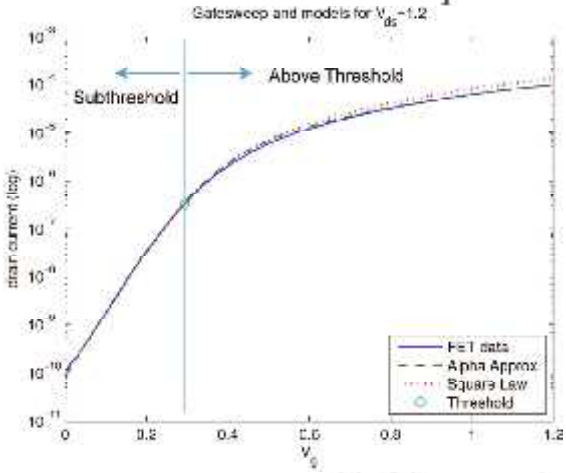
Compact EKV Model

$$I_{f,r} = \frac{W}{L} 2U_T^2 \frac{\mu C_{cox}}{2\kappa} \ln^2\left(1 + e^{\frac{\kappa(V_g - V_{T0}) + (1-\kappa)V_b - V_s + \sigma V_d}{2U_T}}\right)$$

$$I = I_f - I_r$$

$$\kappa = \frac{C_{ox}}{C_{ox} + C_{dep}}$$

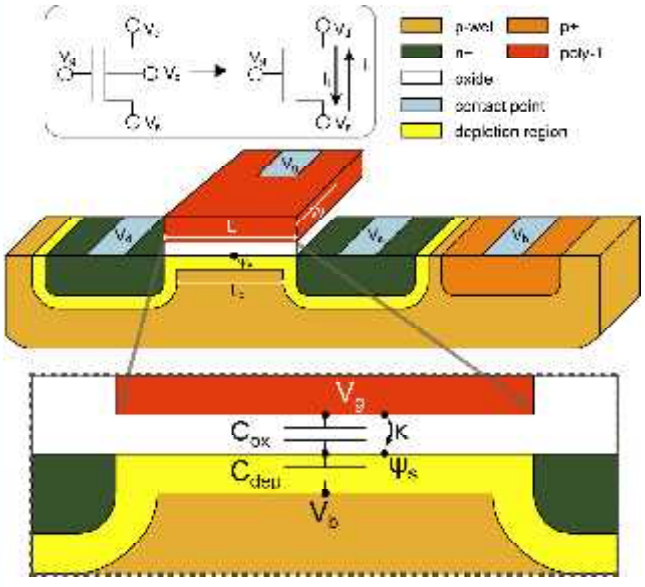


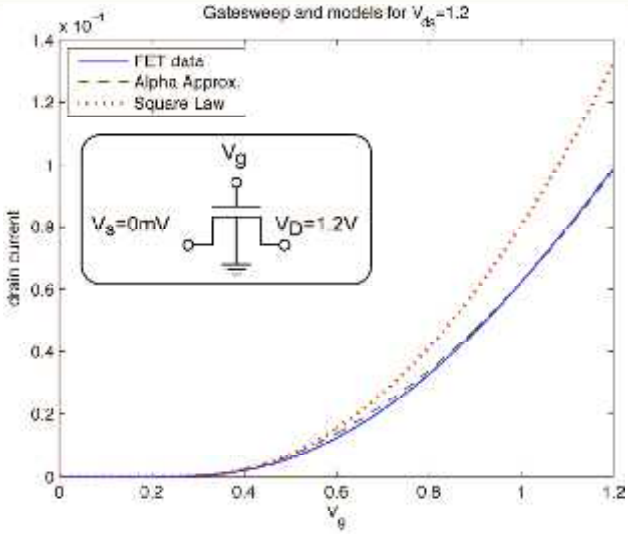


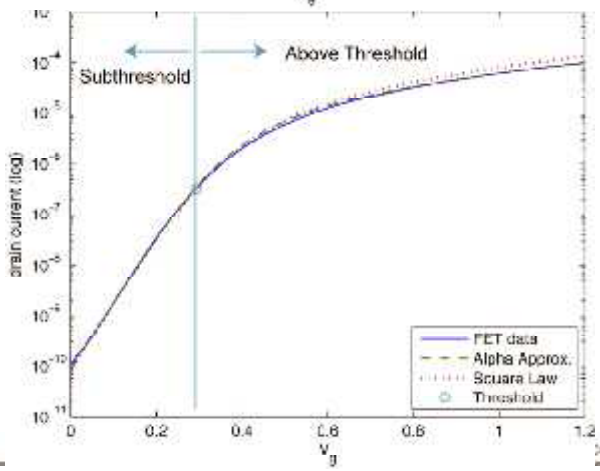
brian@degnanresearch.com

Brian Degnan, Ph.D. White River Technologies Inc.

nFET@130nm





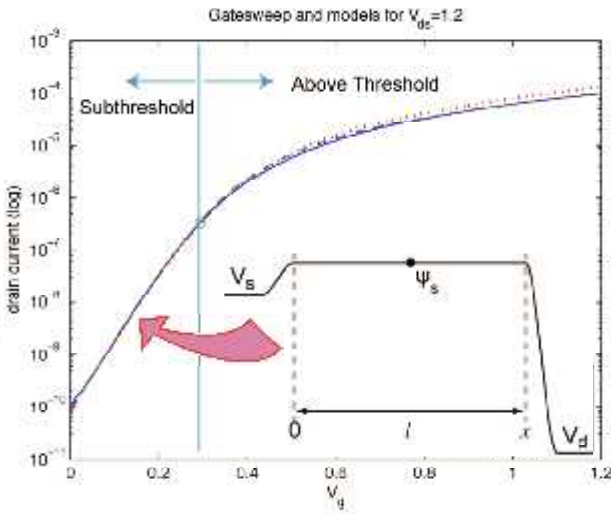


- Sub Vth

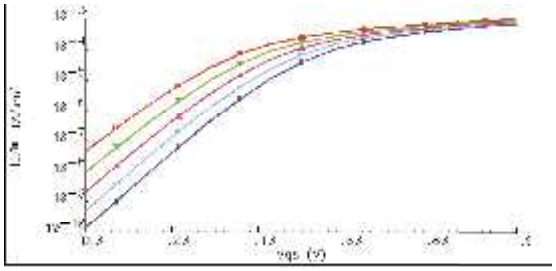
$$I = \frac{W}{L}\frac{2U_T^2\mu C_{ox}e^{\frac{-\kappa V_{T0}}{U_T}}}{2\kappa}\left(e^{\frac{\kappa V_g - V_s}{U_T}} - e^{\frac{\kappa V_g - \sigma V_d}{U_T}}\right)$$

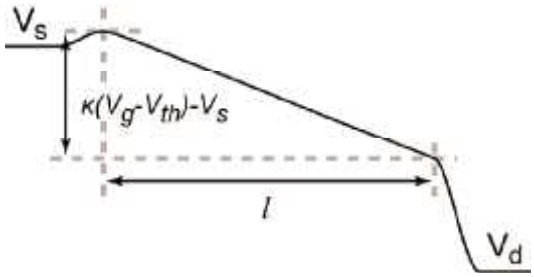
Node (nm)	Sub-Vt%
500	12.8
350	12.4
250	24.4
180	34.4
130	33.3
90	35.0
65	40.0

$V_{t0,n}$ nFET threshold voltage
Sub-Vt% = range of diffusion operation



- Above Vth





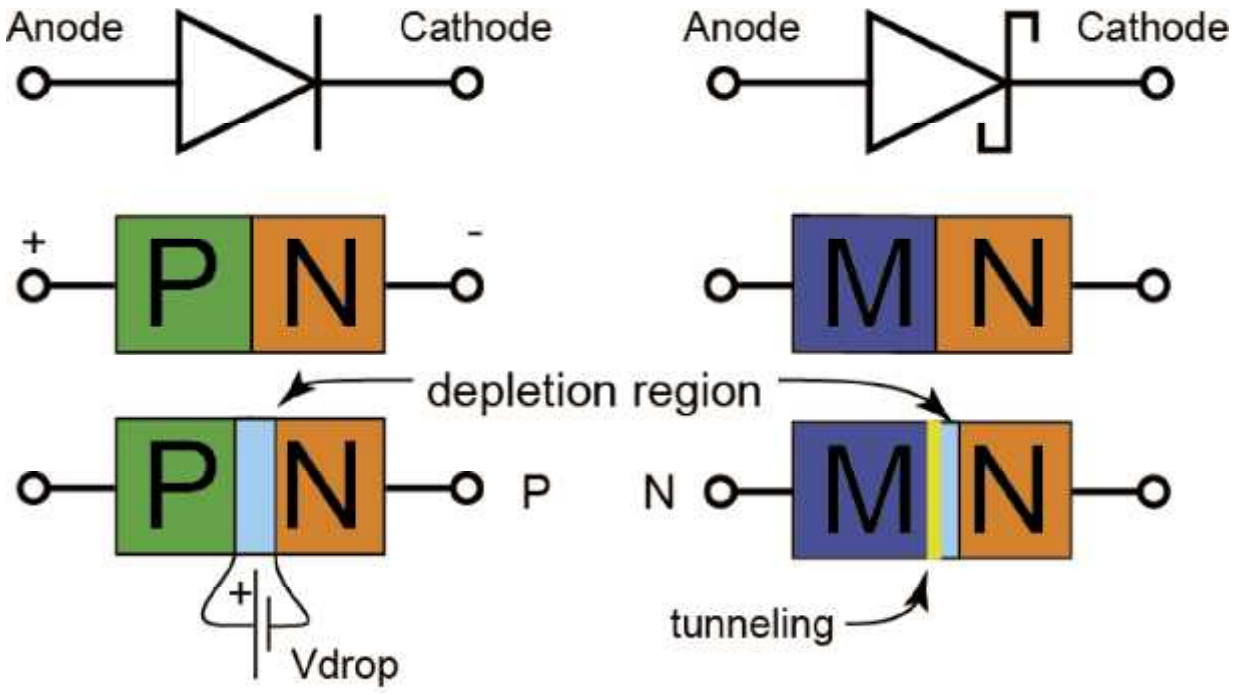
$$I = \frac{W}{L}U_T^2\frac{\mu C_{ox}}{2\kappa}\left[(\kappa(V_g - \kappa V_{T0}) - V_s)^2 - (\kappa(V_g - \kappa V_{T0}) - \sigma V_d)^2\right]$$

Graph: 65nm nFET gate sweep from IBM's 65nm advertisements.

brian@degnanresearch.com

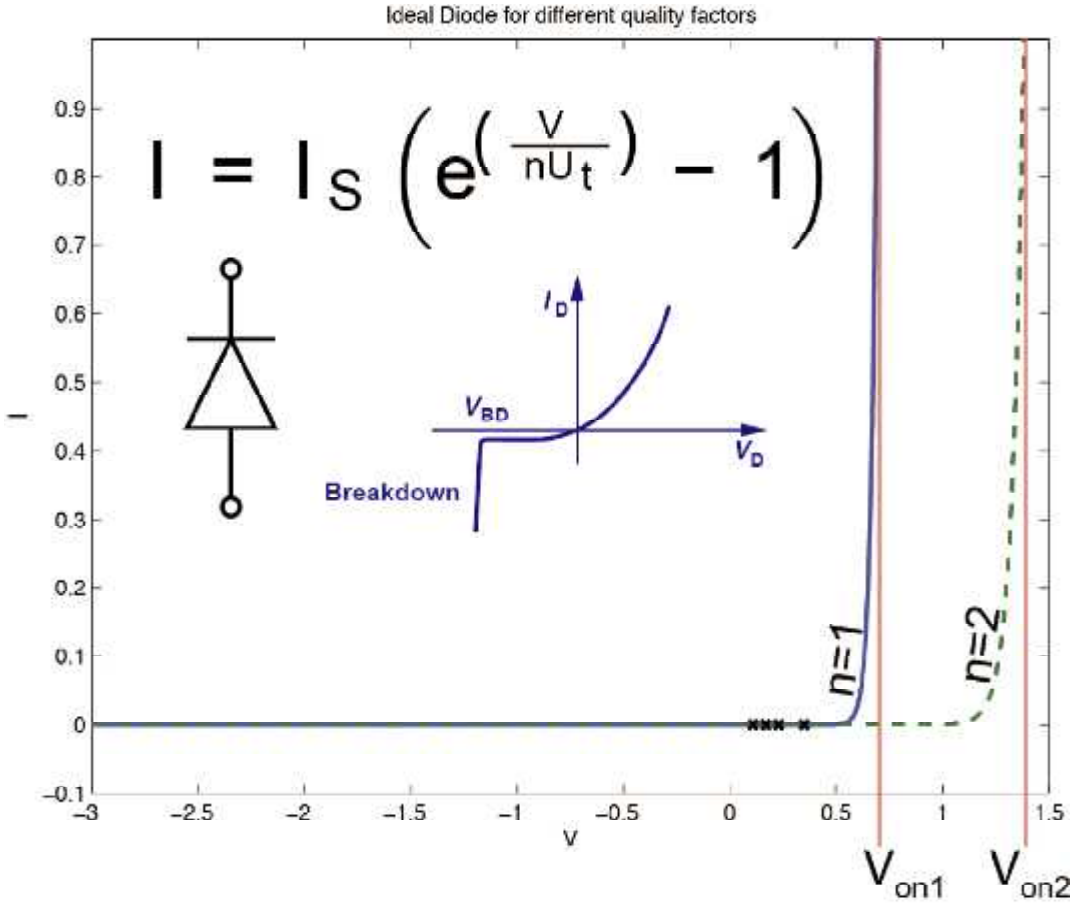
Brian Degnan, Ph.D. White River Technologies, Inc.

Diodes



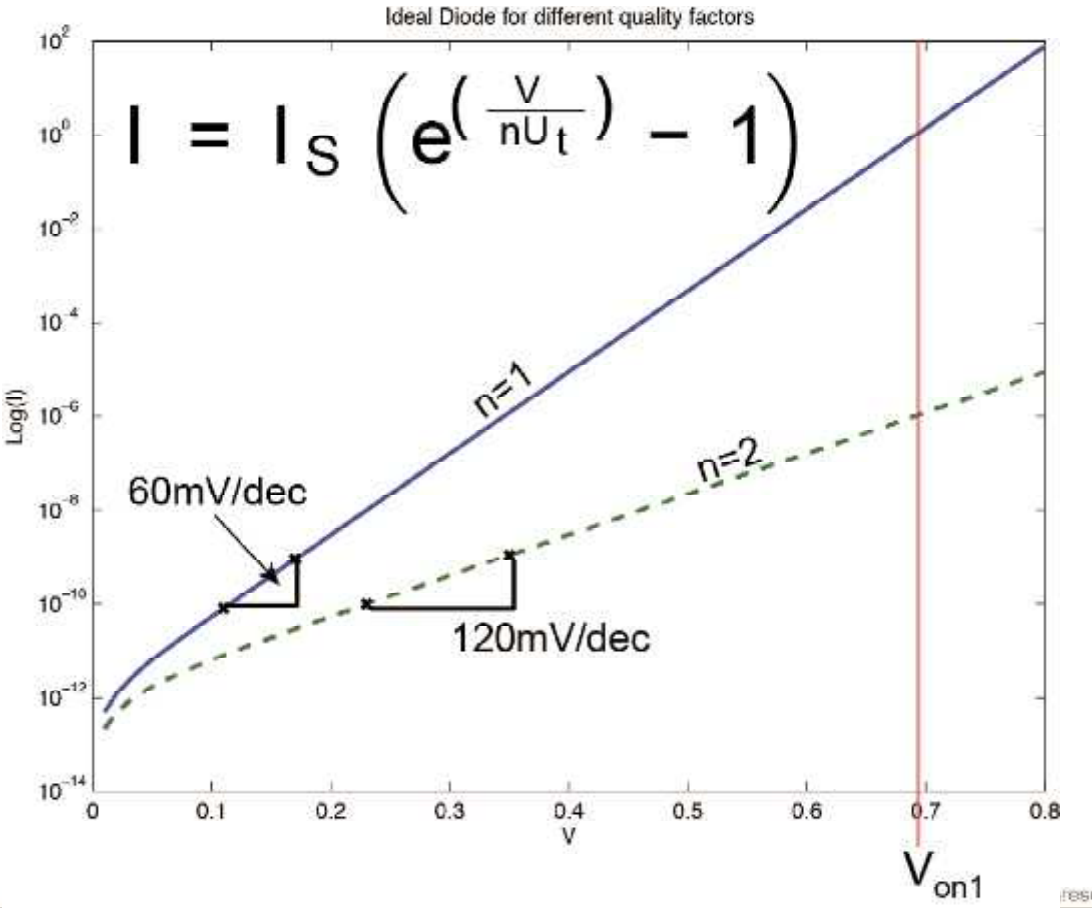
brian@degnanresearch.com

Brian Degnan, Ph.D. White River Technologies Inc.



brian@degnanresearch.com

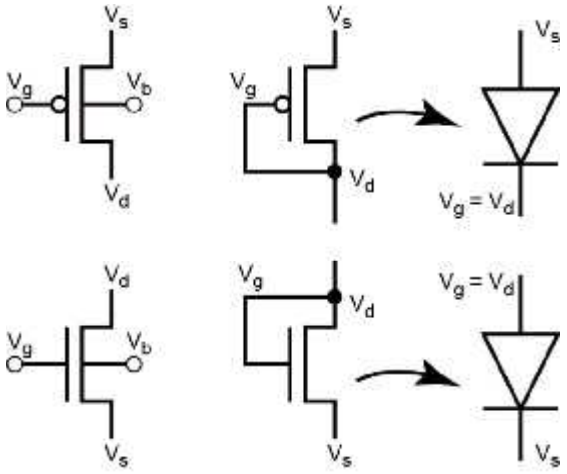
Brian Degnan, Ph.D. White River Technologies Inc.



research.com

Diode Connected MOSFET

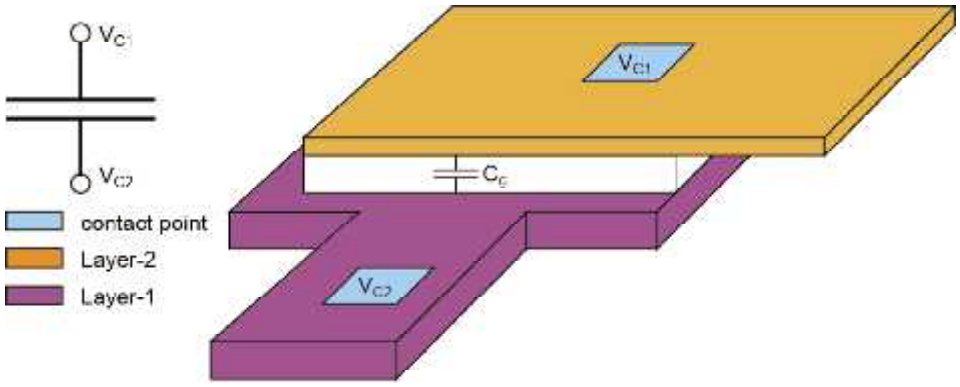
$$I_{f,r} = \frac{W}{L} 2U_T^2 \frac{\mu C_{ox}}{\kappa} \ln^2 \left[1 + e^{\frac{(\kappa(V_g - V_{T0}) + (1-\kappa)V_b - V_s + \sigma V_d)}{2U_T}} \right]$$



$$I_f = \frac{W}{L} 2U_T^2 \frac{\mu C_{ox}}{\kappa} \ln^2 \left[1 + e^{\frac{(\kappa(V_d - V_{T0}) + \sigma V_d)}{2U_T}} \right]$$

Brian Degnan, Ph.D. White River Technologies Inc.

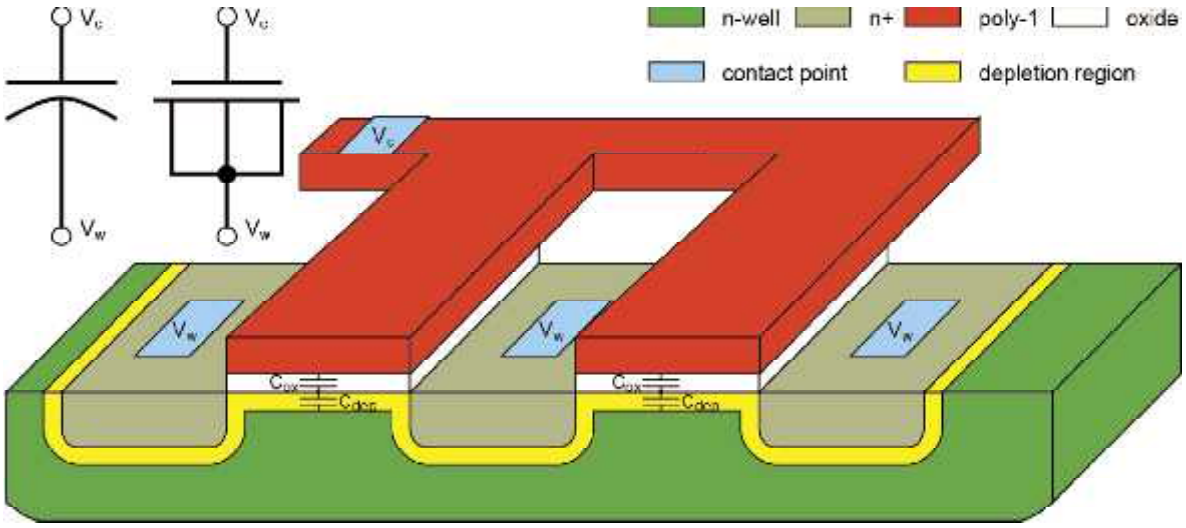
Linear Capacitor



- Linearity is excellent
- Frequency response is excellent
- Charge Density is Low

brian@degnanresearch.com

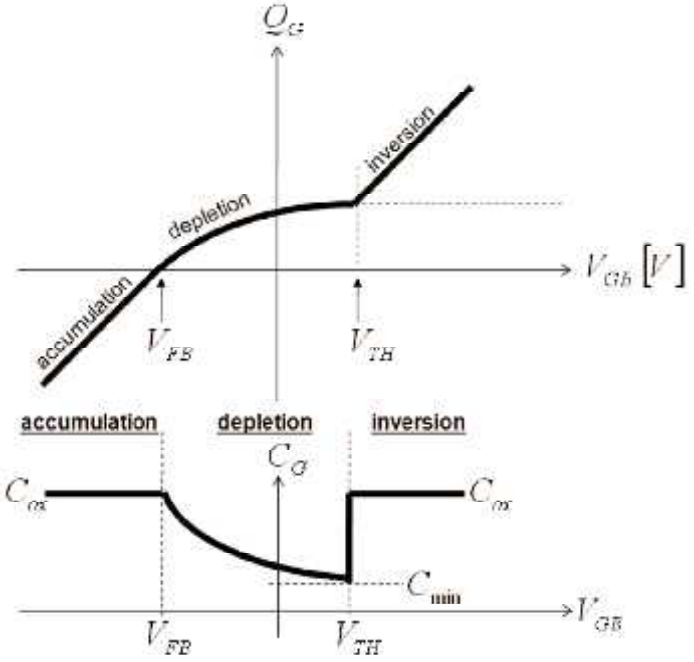
Depletion Capacitor



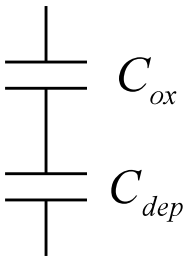
- Linearity is variable
- Frequency response is variable
- Charge Density is excellent

brian@degnanresearch.com

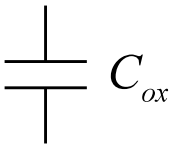
(n)MOS C-V curve



Depletion



Inversion



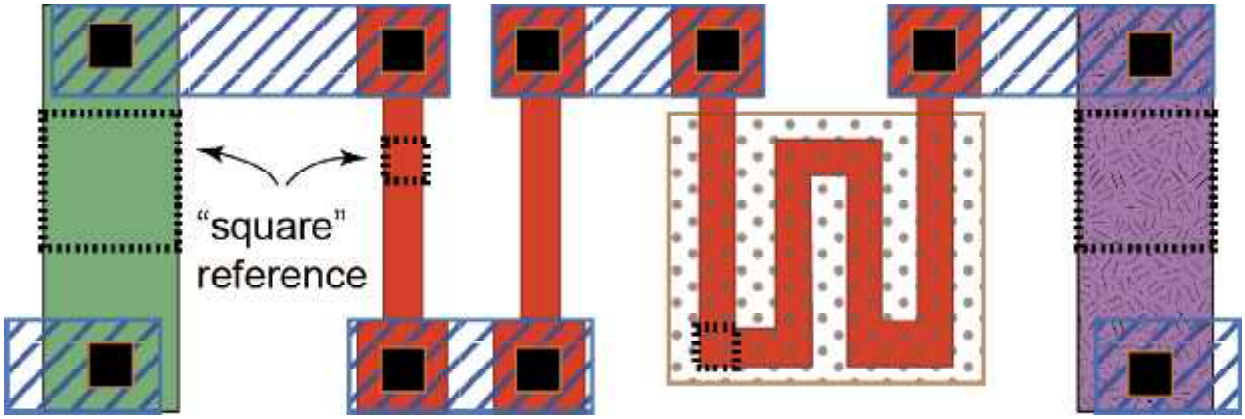
$$C_{\min} = \frac{C_{ox} C_{dep,\min}}{C_{ox} + C_{dep,\min}}$$

where $C_{dep,\min} \equiv \frac{\varepsilon_{Si}}{X_{d,\max}}$

$$C_{dep} \equiv \frac{\varepsilon_{Si}}{X_d} \qquad C_{ox} \equiv \frac{\varepsilon_{ox}}{t_{ox}}$$

brian@degnanresearch.com

Resistors			cost
n+ diffusion	75Ω/□	± 15%	included
p+ polysilicon	350Ω/□	± 20%	included
p- polysilicon	1500Ω/□	± 25%	extra
tantalum nitride	50Ω/□	± 5%	extra



Brian Degnan, Ph.D. White River Technologies Inc.

System Punch List

- Harvest Energy (carrier wave supplied)
- Create a stable power supply (use the energy)
- Reset the System (ready the system)
- Decode the incoming data stream (extract)
- Respond to the decoded data (return)

brian@degnanresearch.com

Gen2 Protocol

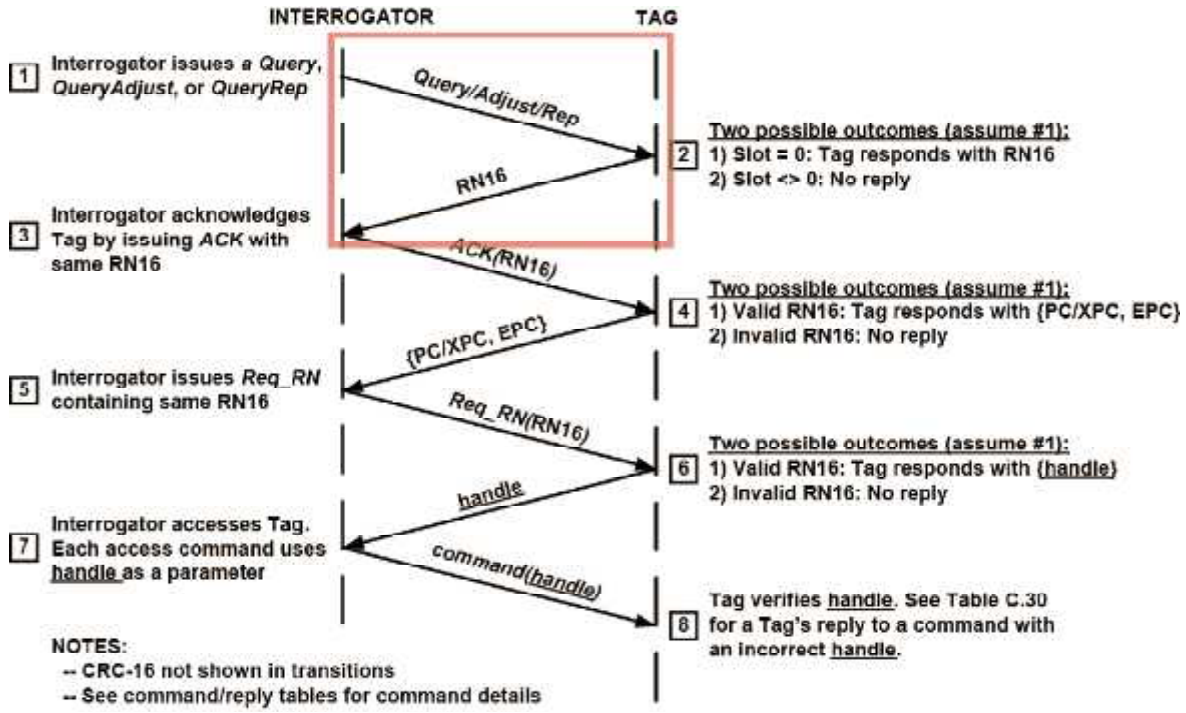
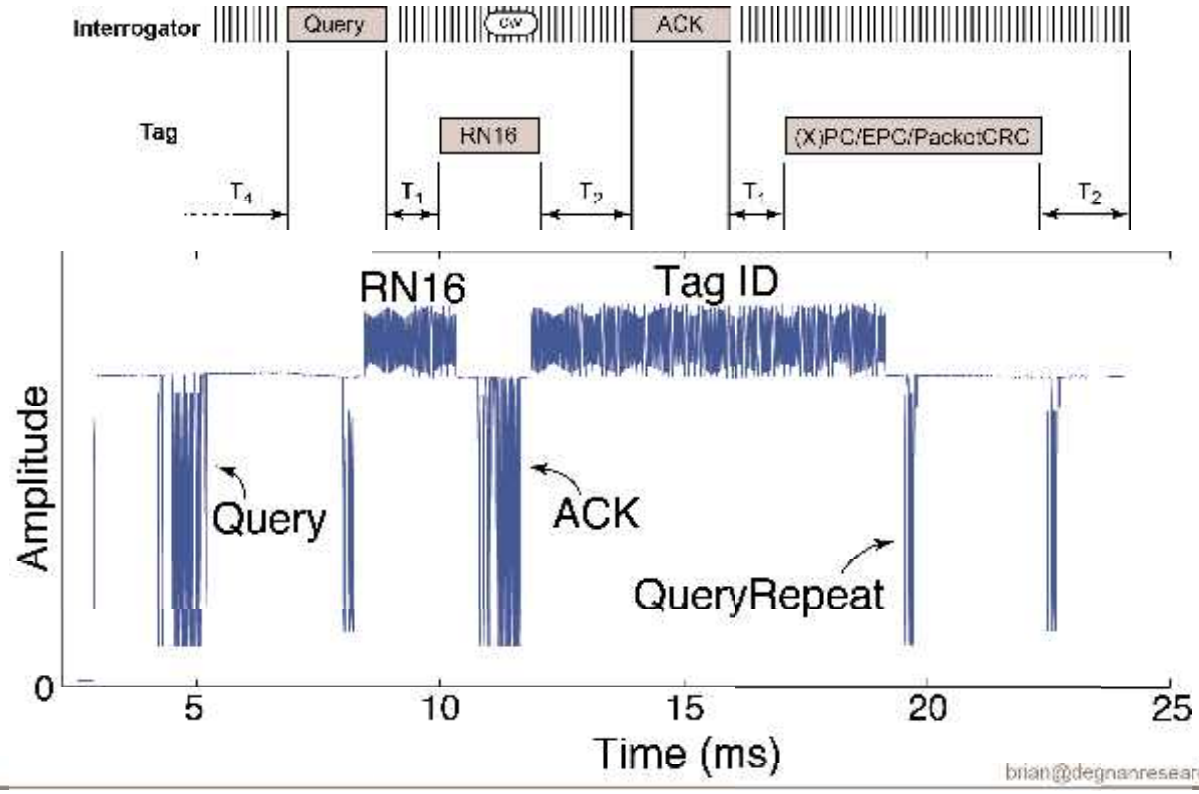


Figure E.1: Example of Tag inventory and access

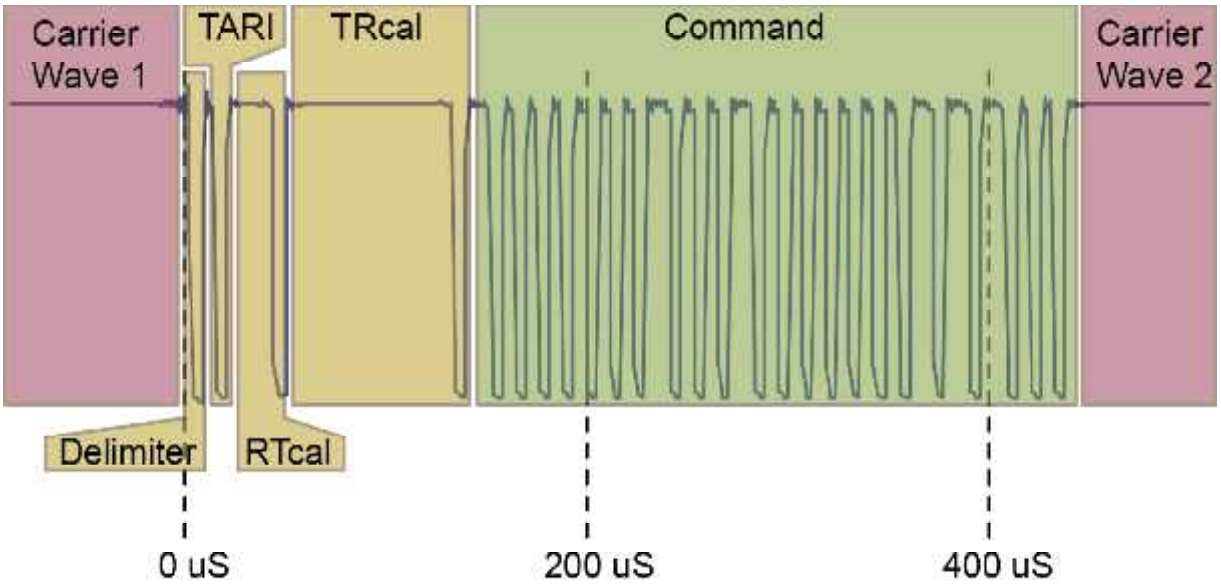
Brian Degnan, Ph.D. White River Technologies Inc.

Commands in Context

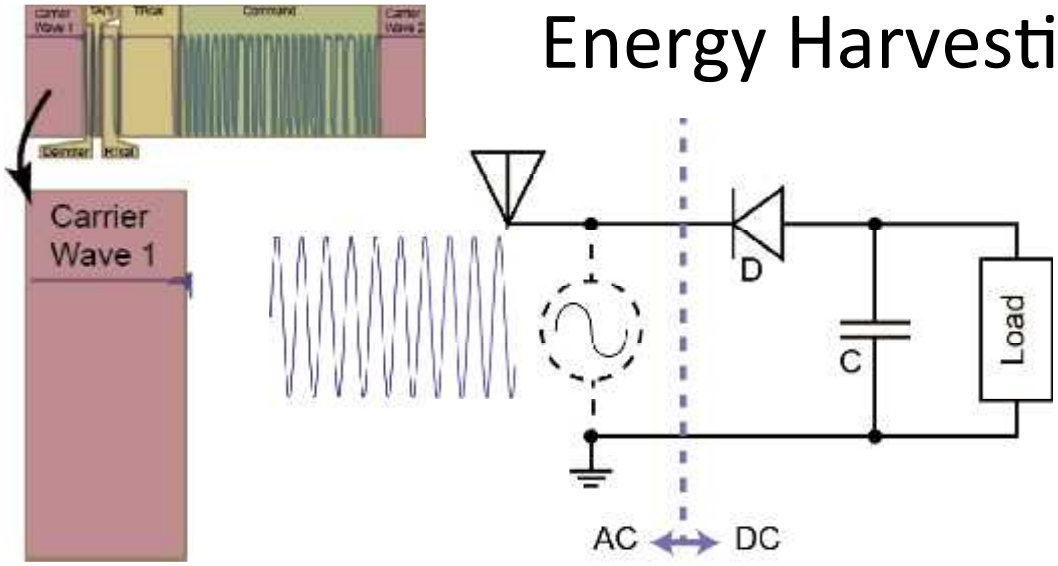


brian@degnanresearch.com

Gen2 Waveform and Vocabulary

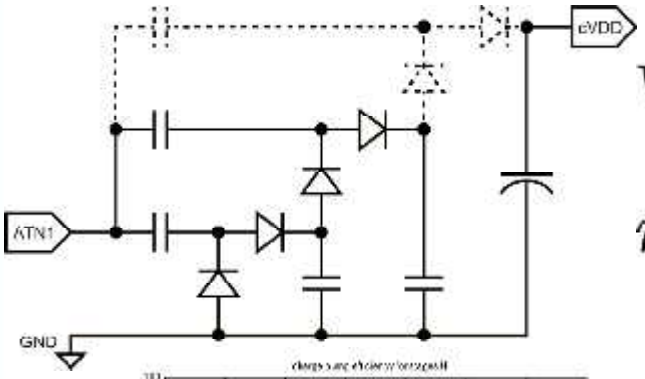


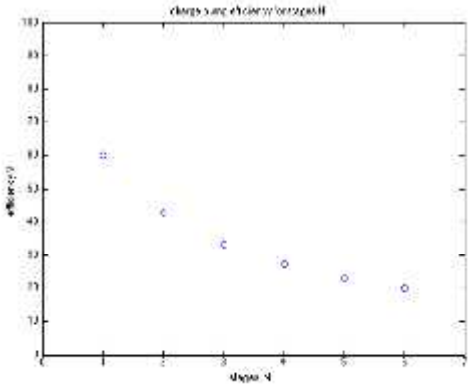
Energy Harvesting



Node (nm)	V_{DD}	I_{sat} (μA)	V_{thn}	Sub-Vt%	I_{DS0} (pA)	ITRS target $I_{DS0}(pA)$
130	1.2	55.5	0.4	33.3	167.1	130
90	1.0	44.4	0.38	38.0	960.3	900
65	1.0	48.5	0.4	40.0	8138.7	6500

Energy Harvesting



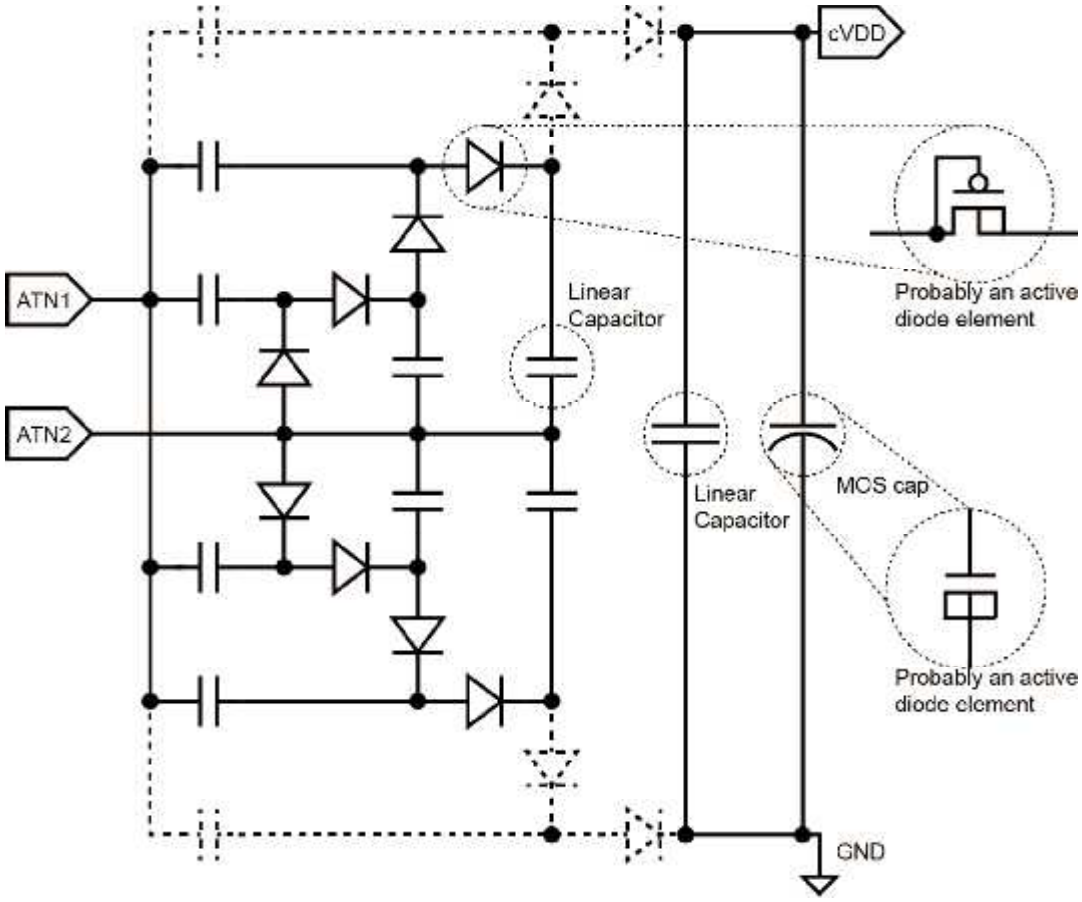


$$V_{DD_{id}} = 2N\left(V_p - V_{on}\right)$$

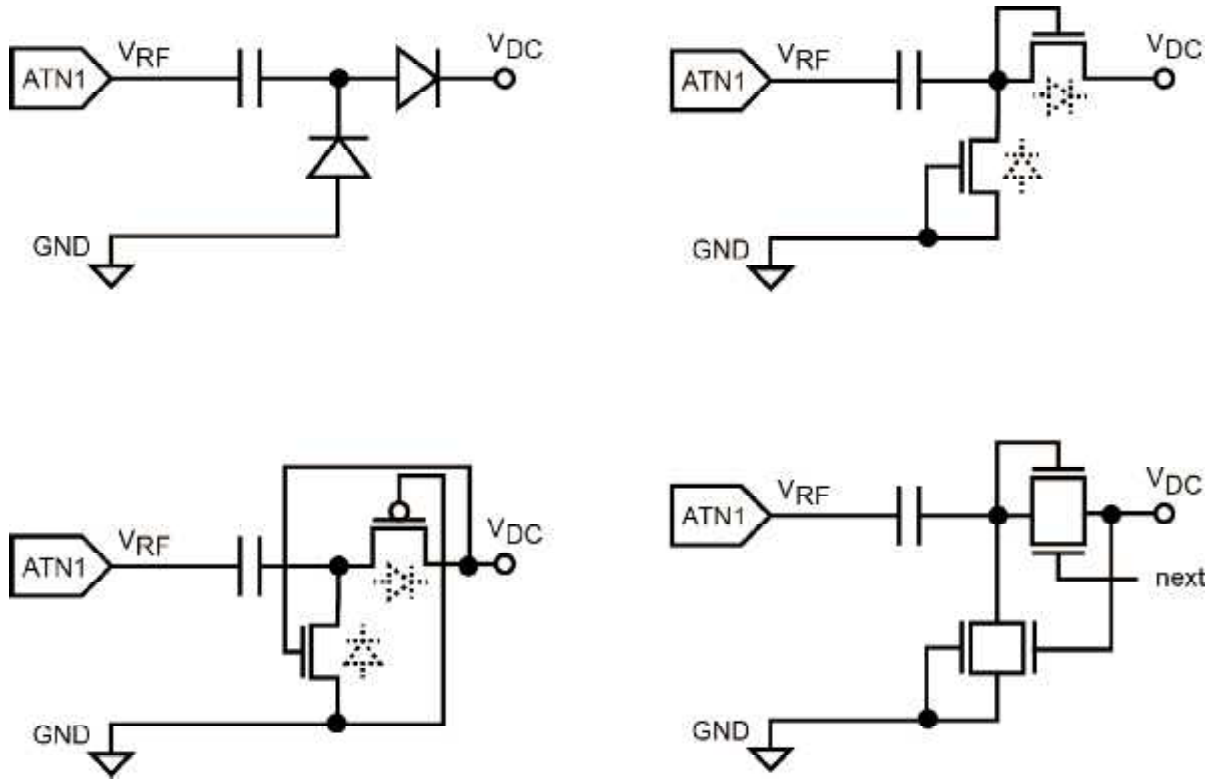
$$\eta_{cp} = \frac{V_{DD}}{V_{DD} + 2NV_{on}}$$

- Number of stages
- Received Energy
- Current Load
- Et Cetera

Brian Degnan, Ph.D. White River Technologies Inc.

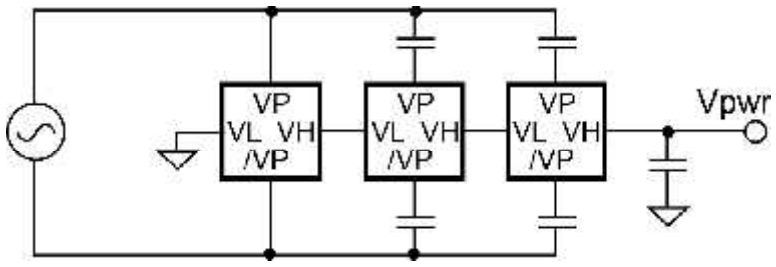


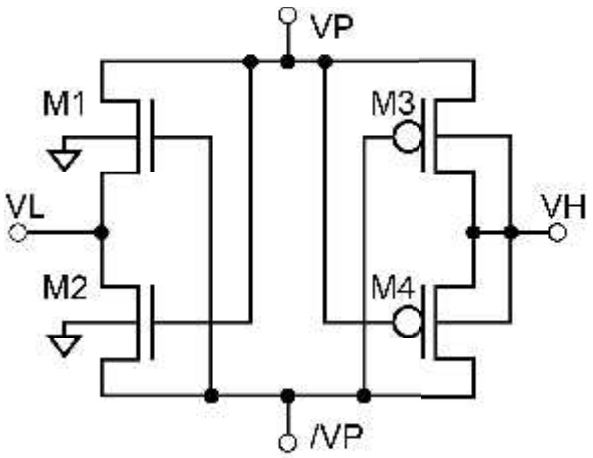
brian@degnanresearch.com



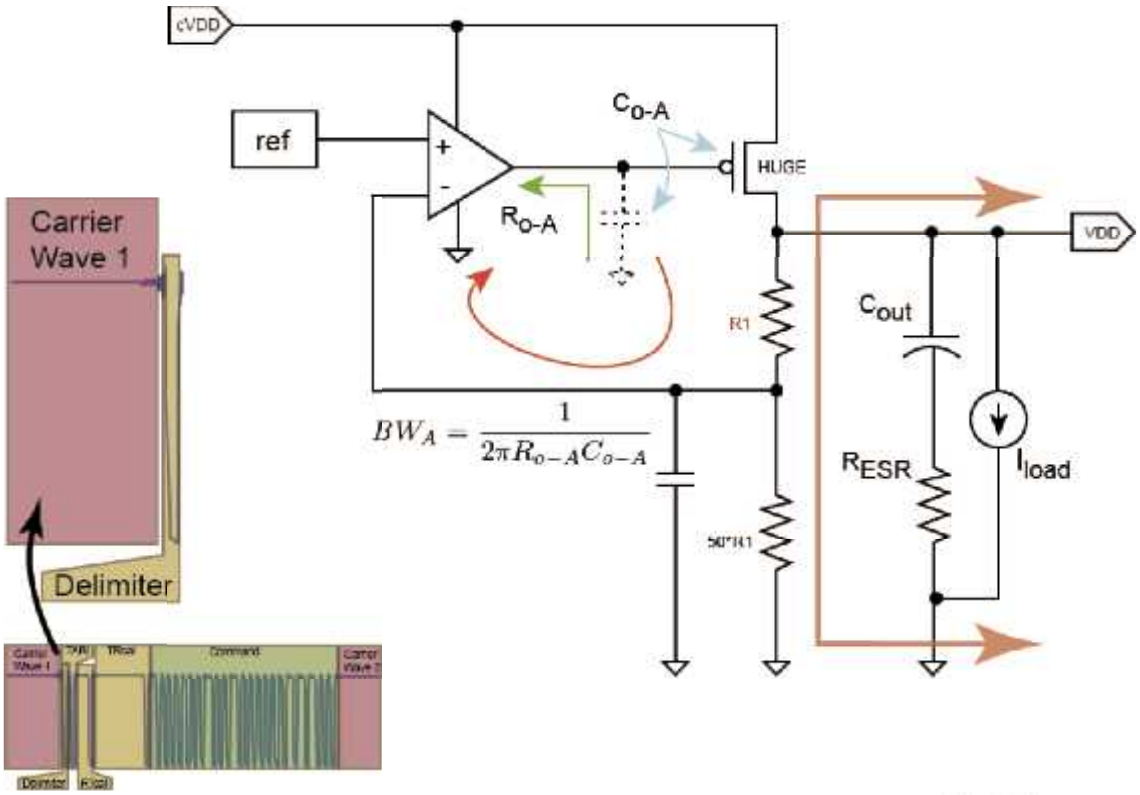
Wu et al, "MOS Charge Pumps for Low-Voltage Operation" JSSCC 1998

CMOS H-Bridge Charge Pump

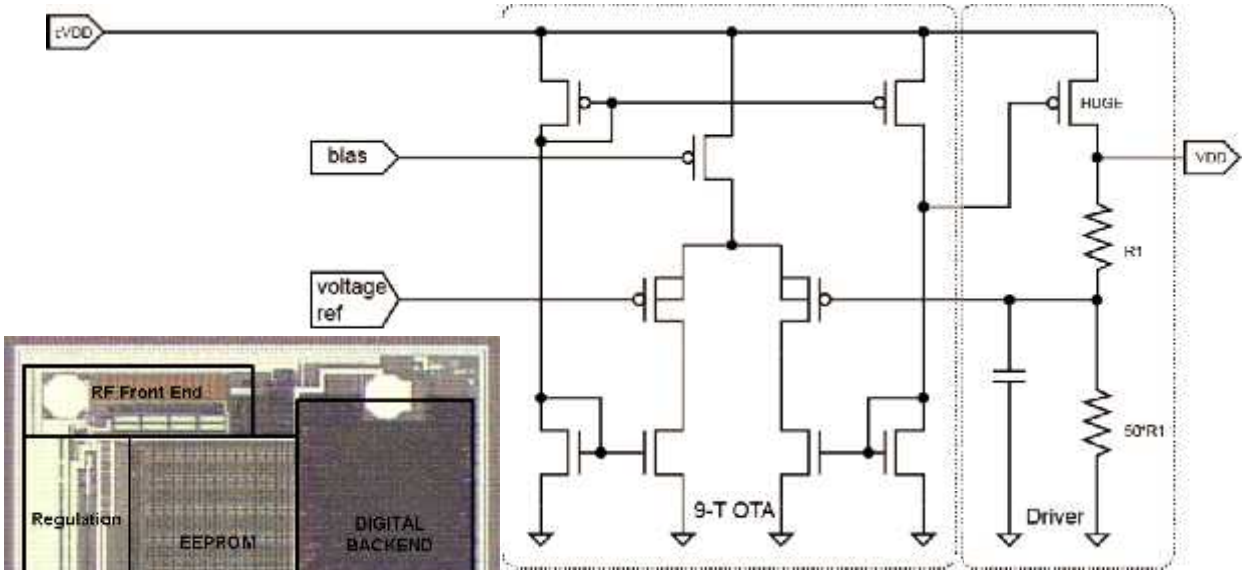




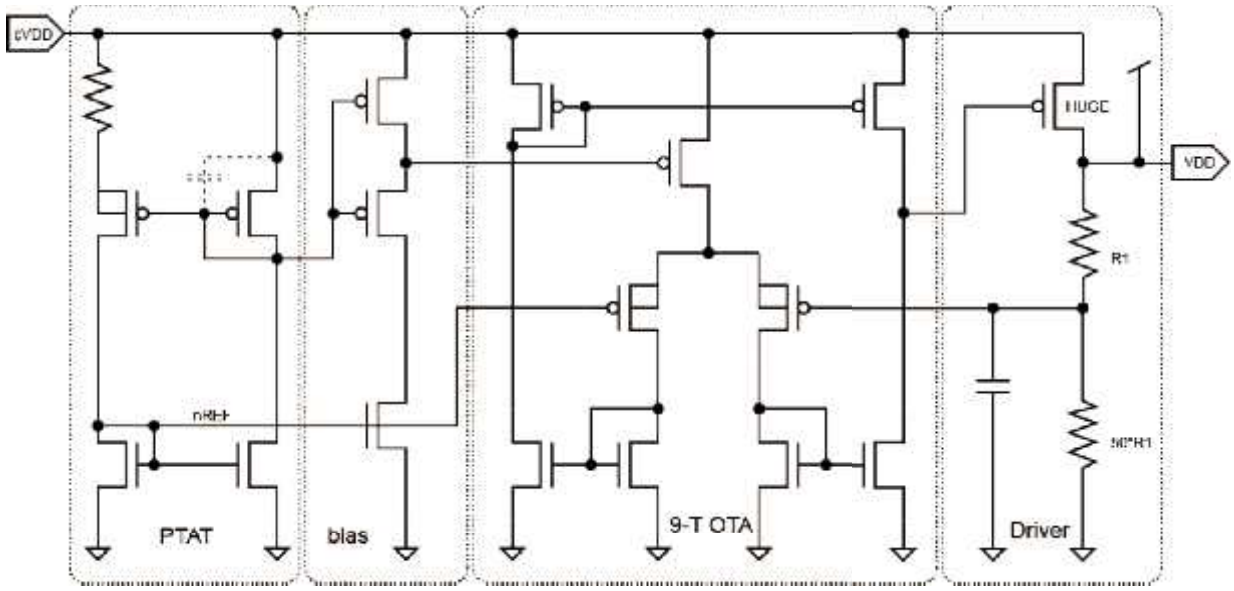
Power Regulator



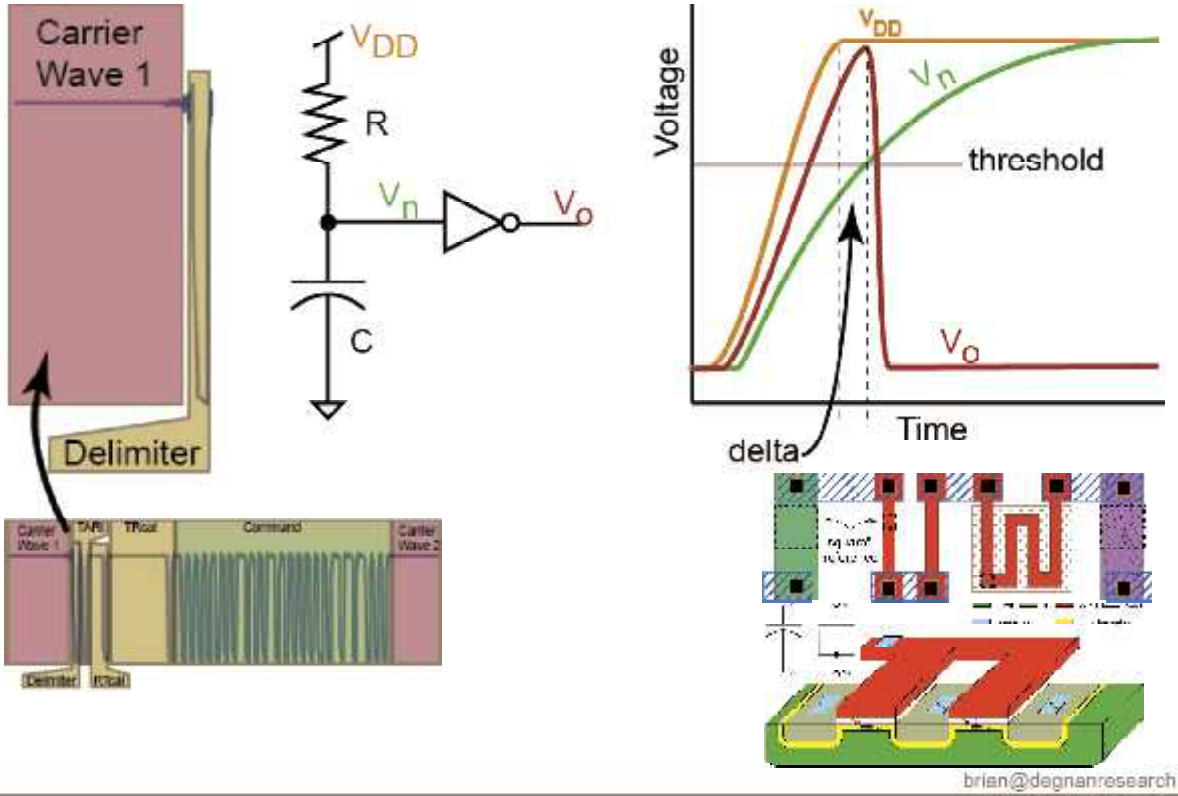
Amplifier and "load"



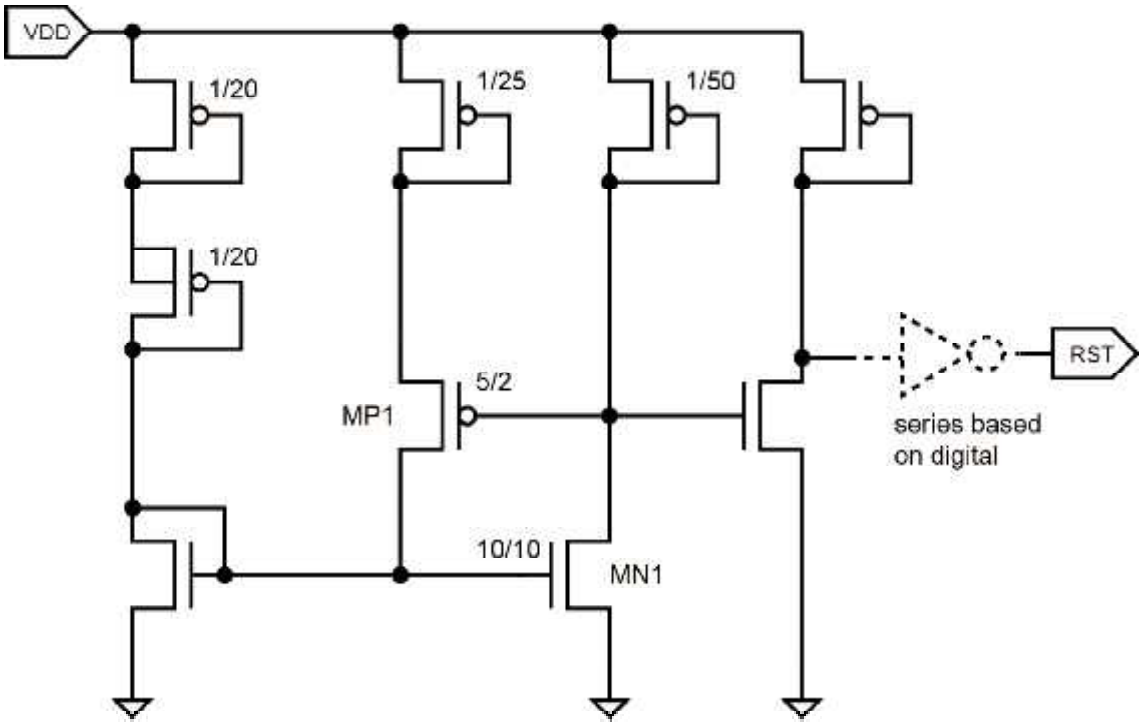
Power Regulator Complete



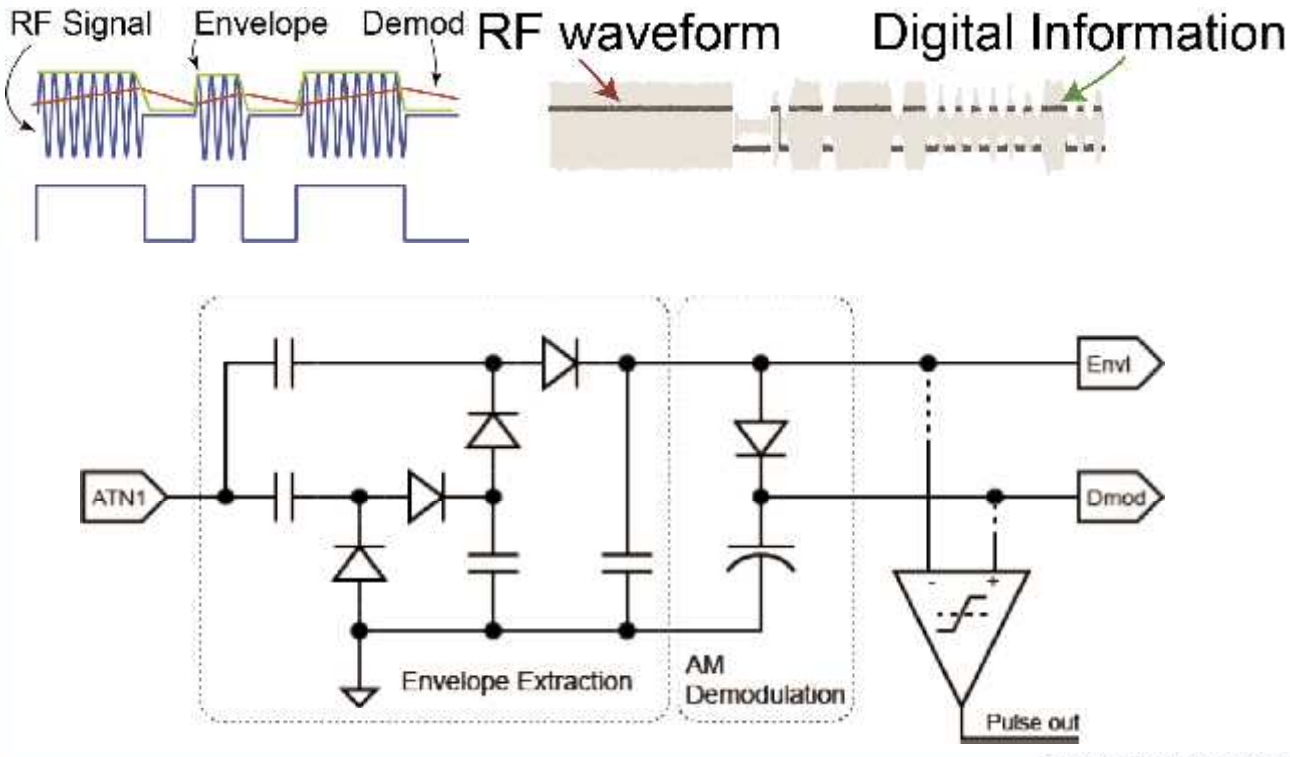
Digital POR



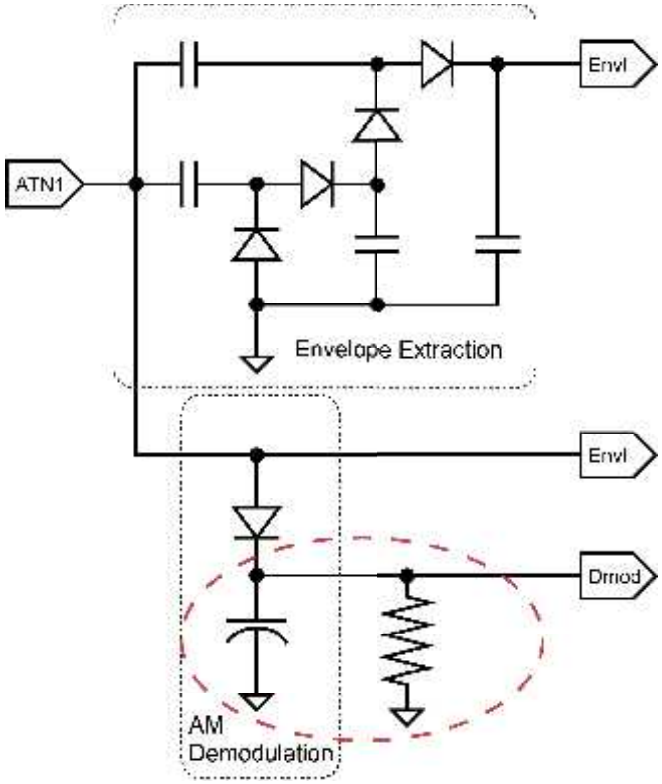
Power-On-Reset

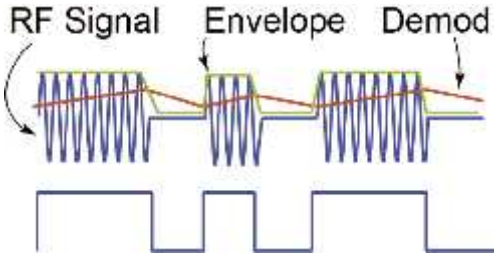


Demodulation

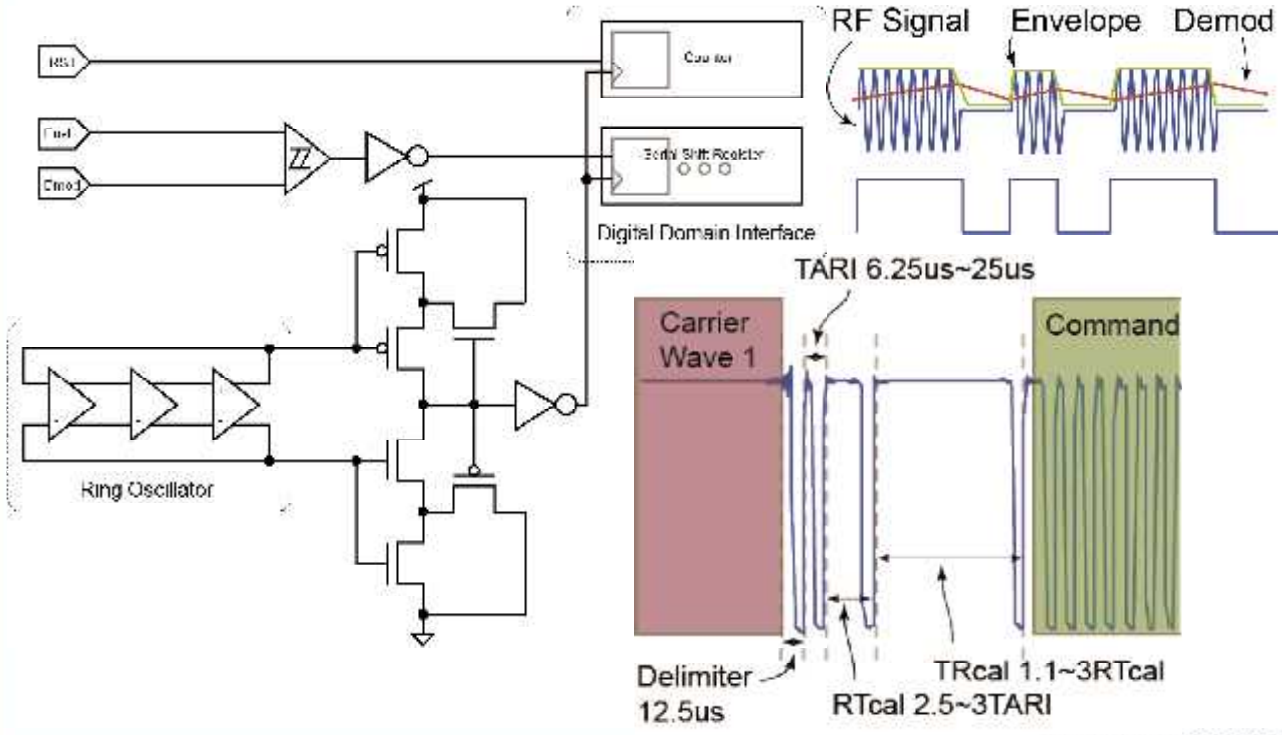


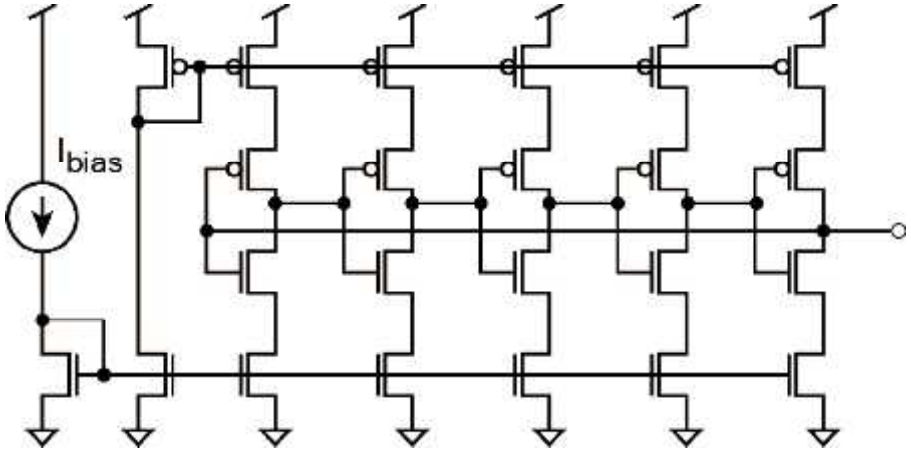
Demodulation pitfalls

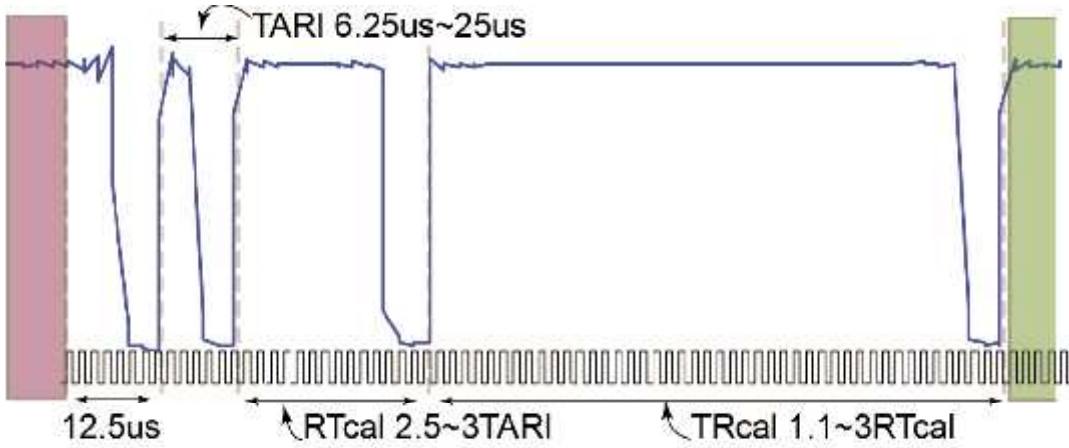




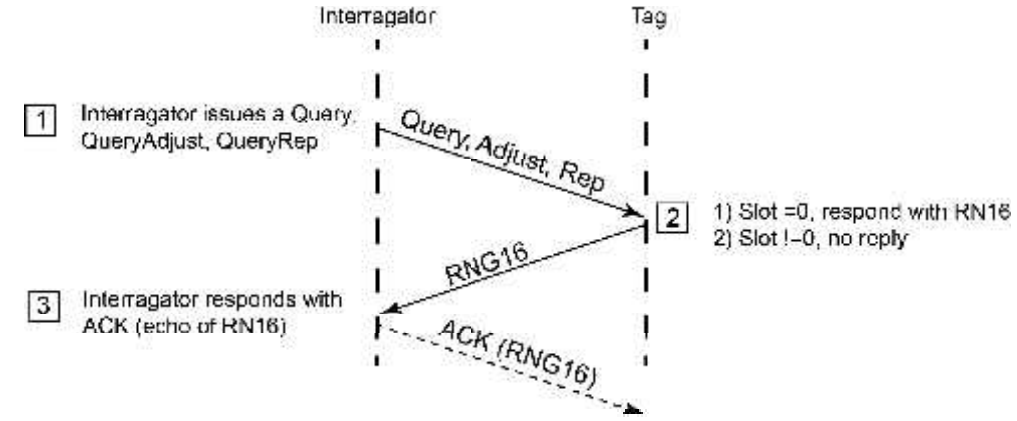
Data Extraction

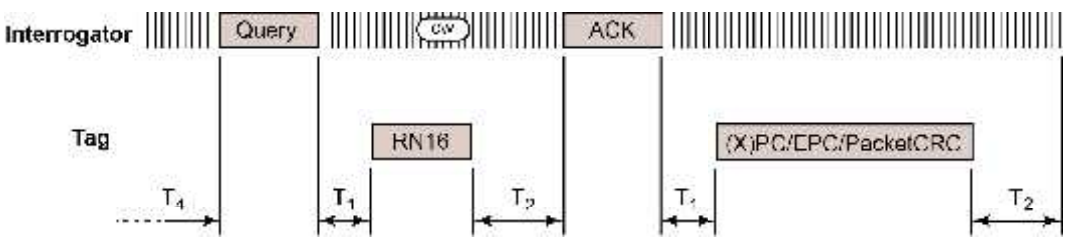


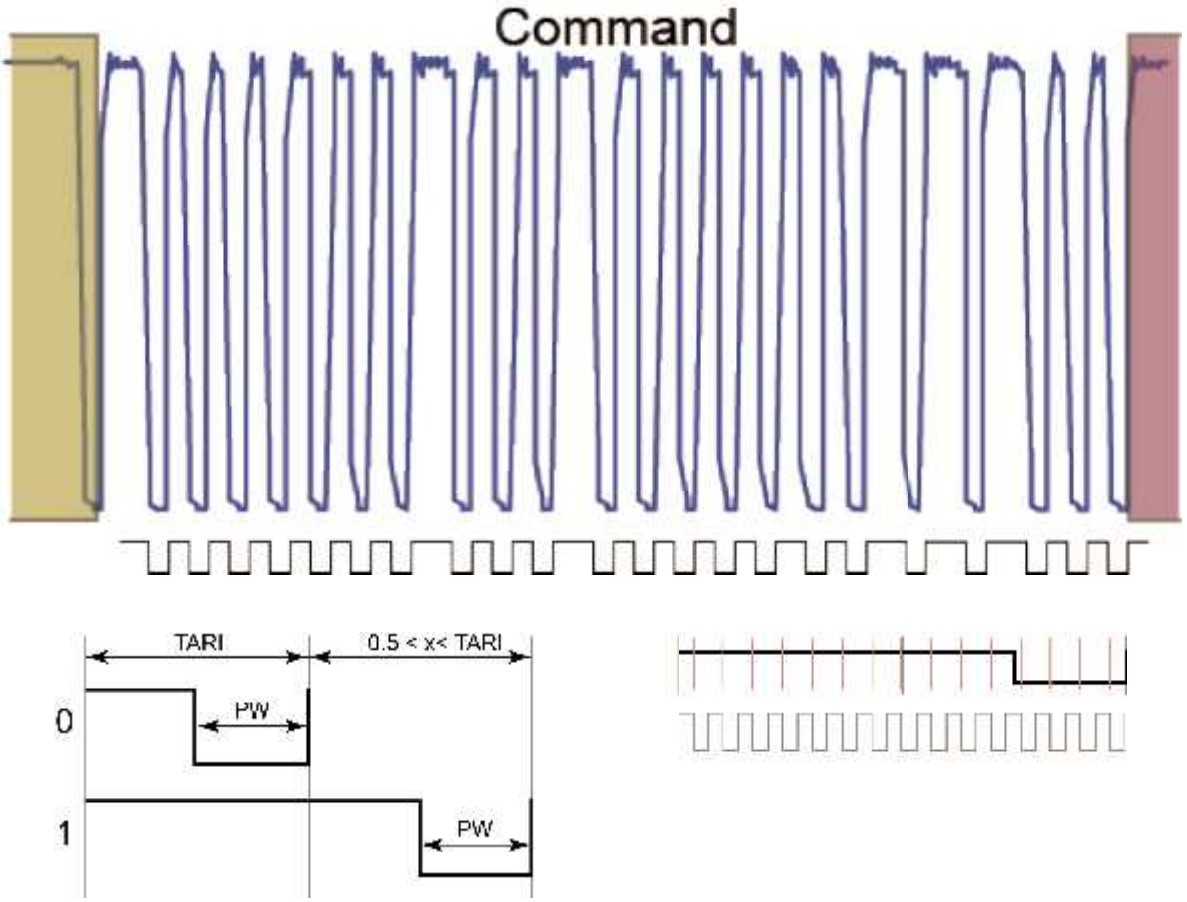




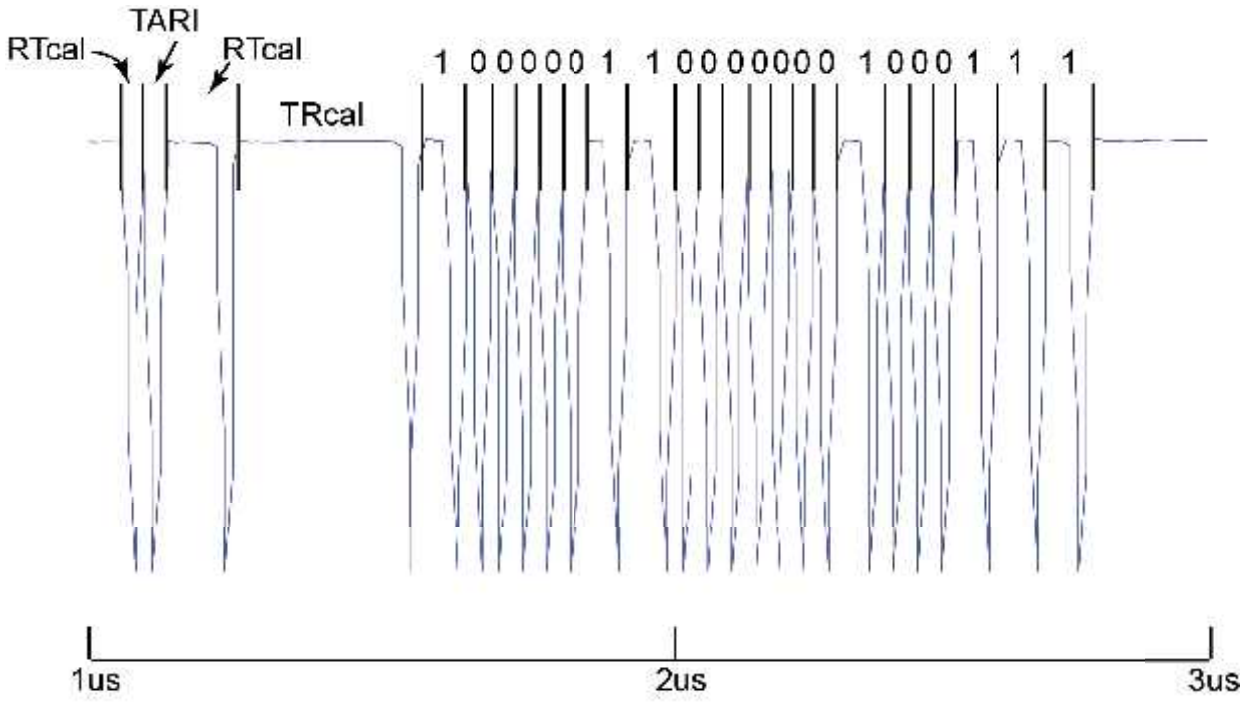
Gen2
State Machine



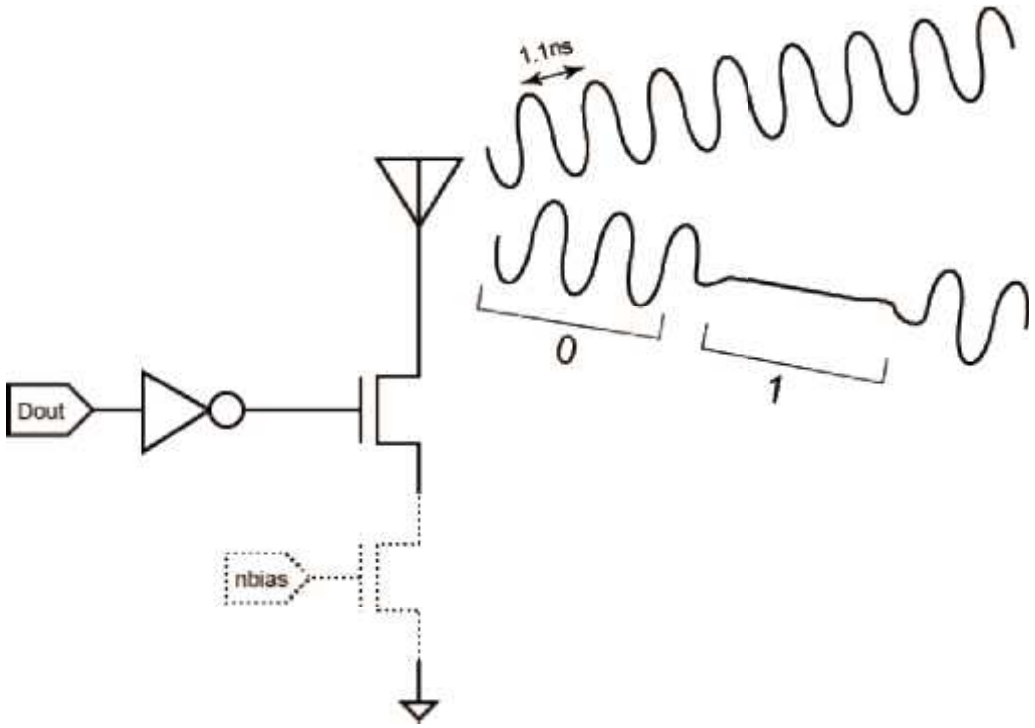




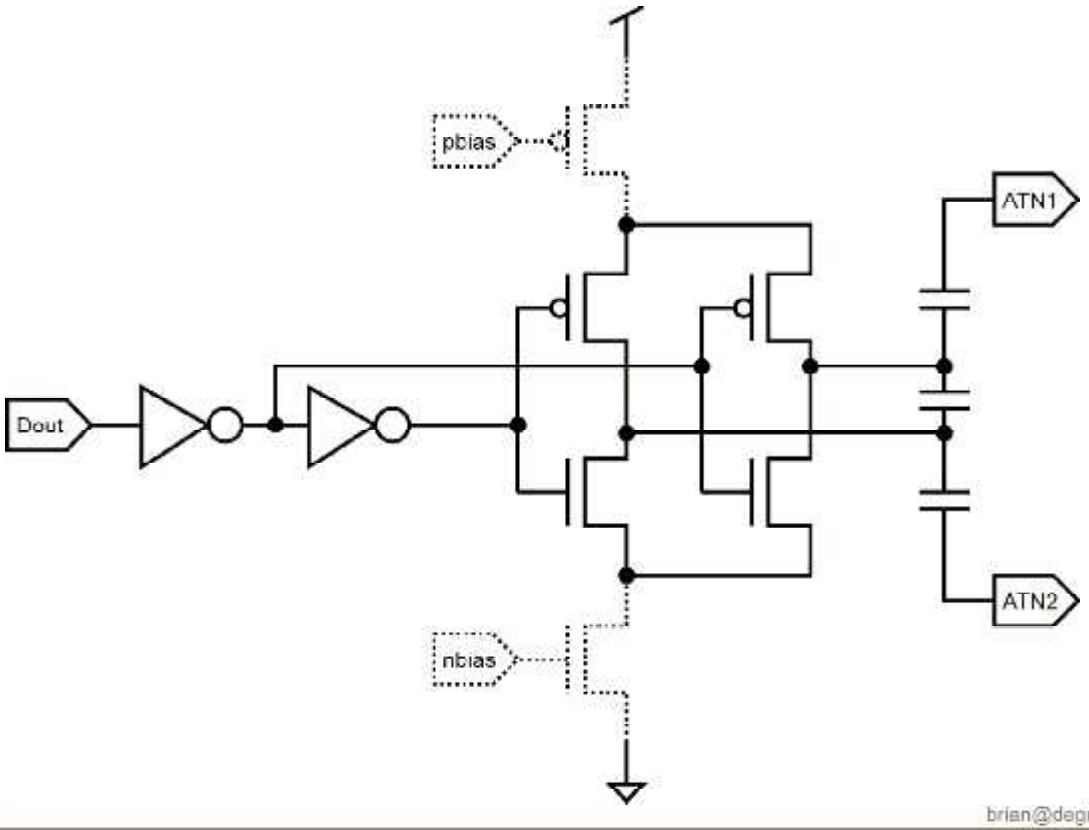
QUERY command



Conceptual Modulated Response



Modulated Response Circuit



Gen2 Protocol, again

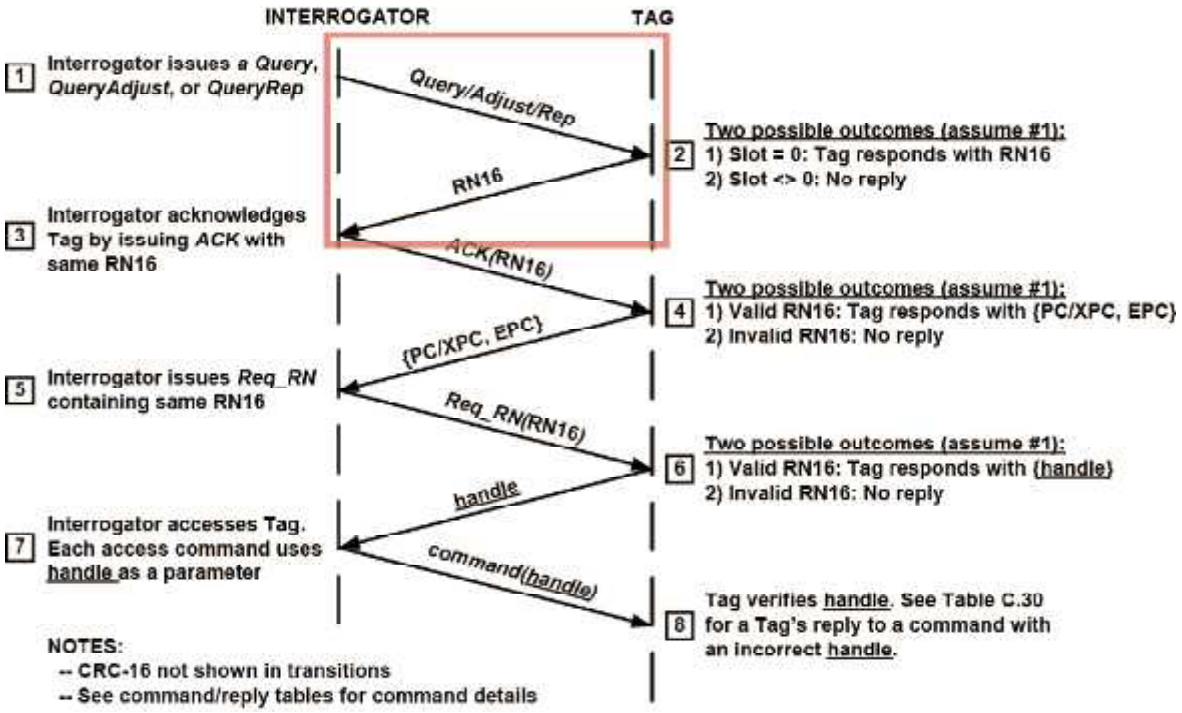
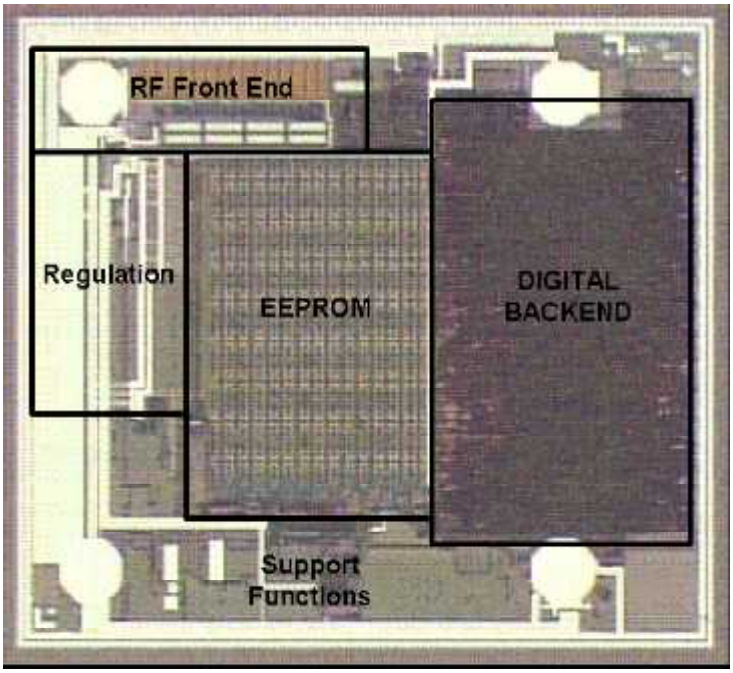


Figure E.1: Example of Tag inventory and access

Brian Degnan, Ph.D. White River Technologies, Inc.

Example Tag



0.5mm^2 Tag:

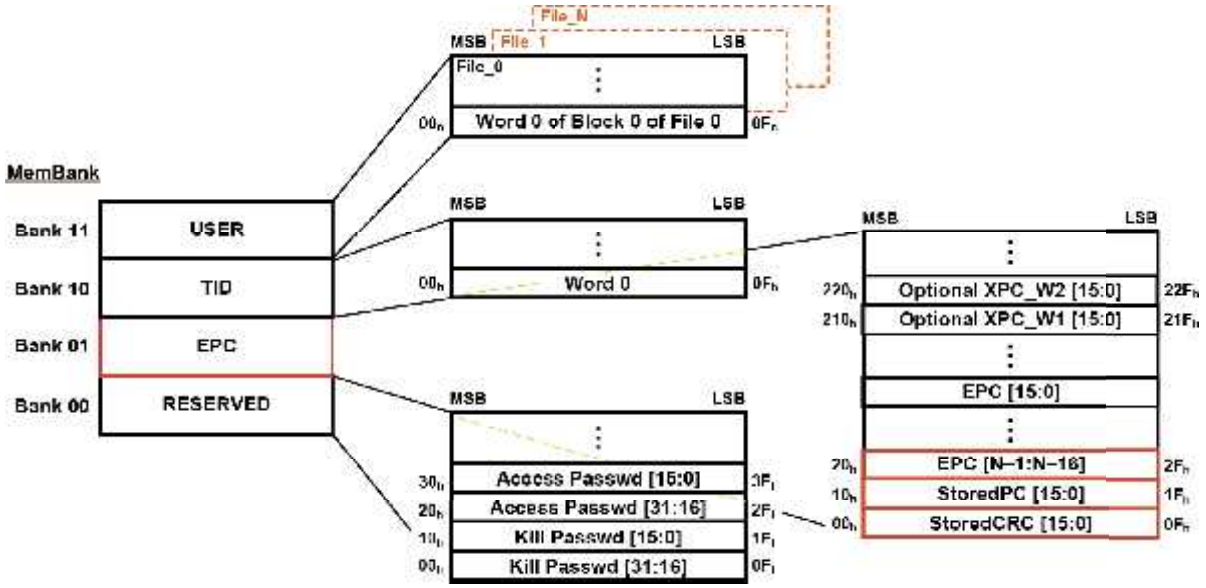
Digital ~ 30%
EEPROM ~ 20%

RF + DC reg ~ 20%

Others (RNG, Charge Pump, support functions): 30%

Barnet et al, "A Passive UHF RFID transponder for EPC Gen2 in 0.13um CMOS" (TI's gen2 tag) ISSCC 2007

Tag Memory: What is stored?



EPC Memory

EPC Word Address	EPC word Contents	EPC Word Values			
0x00	StoredCRC	0xE2F0	0xCCAE	0x968F	0x78F6
0x10	StoredPC	0x0x0000	0x0800	0x1000	0x1800
0x20	EPC word 1	N/A	0x01111	0x1111	0x1111
0x30	EPC word 2	N/A	N/A	0x2222	0x2222
0x40	EPC word 3	N/A	N/A	N/A	0x3333

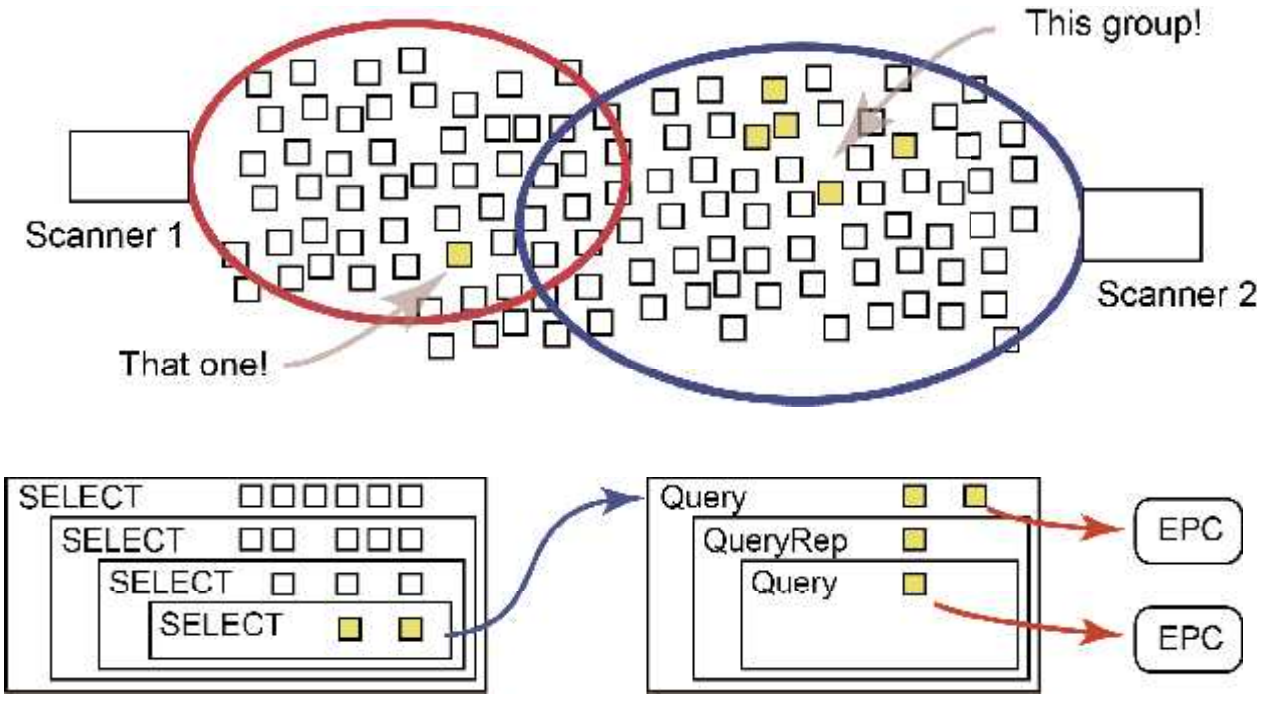
dec	bin	polynomial
0	000	0
1	001	1
2	010	x
3	011	$x+1$
4	100	x^2
5	101	x^2+1
6	110	x^2+x
7	111	x^2+x+1

$$x^{16} + x^{12} + x^5 + 1$$

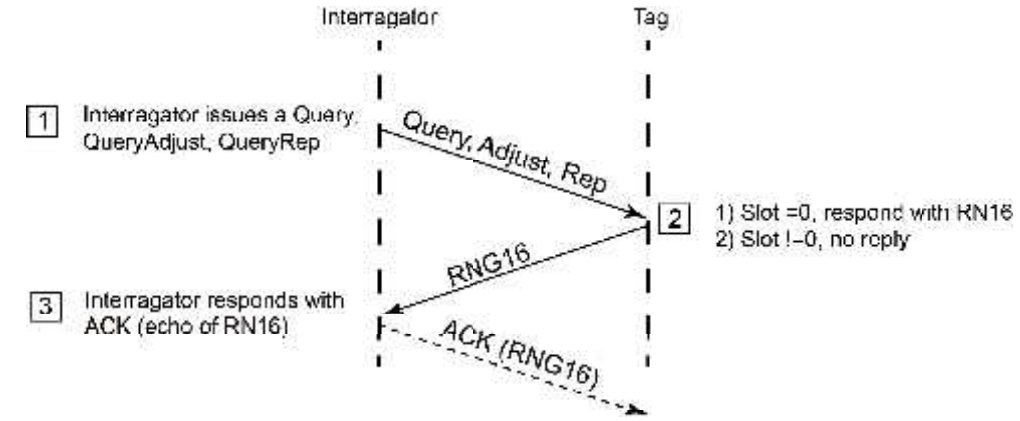
Mandatory Commands

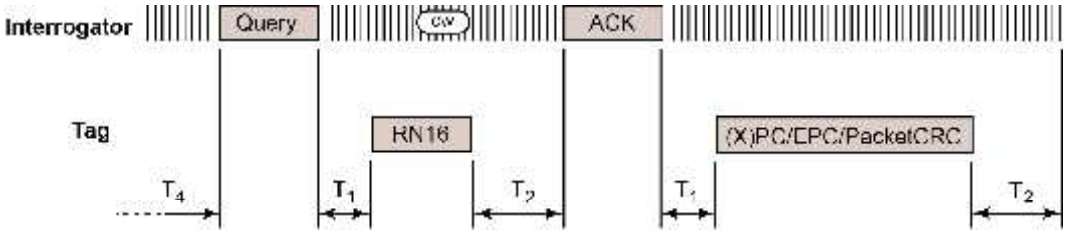
Command	Code	Bits	Description
ACK	01	18	Tag sends RN16 or Handle
Kill	11000100	59	Permanently disable tag
Lock	11000101	60	Prevents memory overwrites
NAK	11000000	8	Keep state bits
Query	1000	22	Send back information
QueryAdjust	1001	9	Changes Slot total
QueryRep	00	4	Decrement Slot Counter
Read	11000010	>57	Read word from memory
Req RN	11000001	40	Tag sends new RN16
Select	1010	>44	Select groups of tags
Write	11000011	>58	Write word to memory

Tags! Management of chaos



Gen2 State machine, getting the EPC.



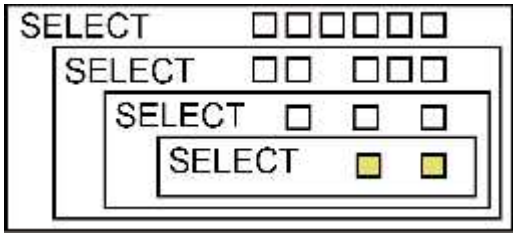


Select

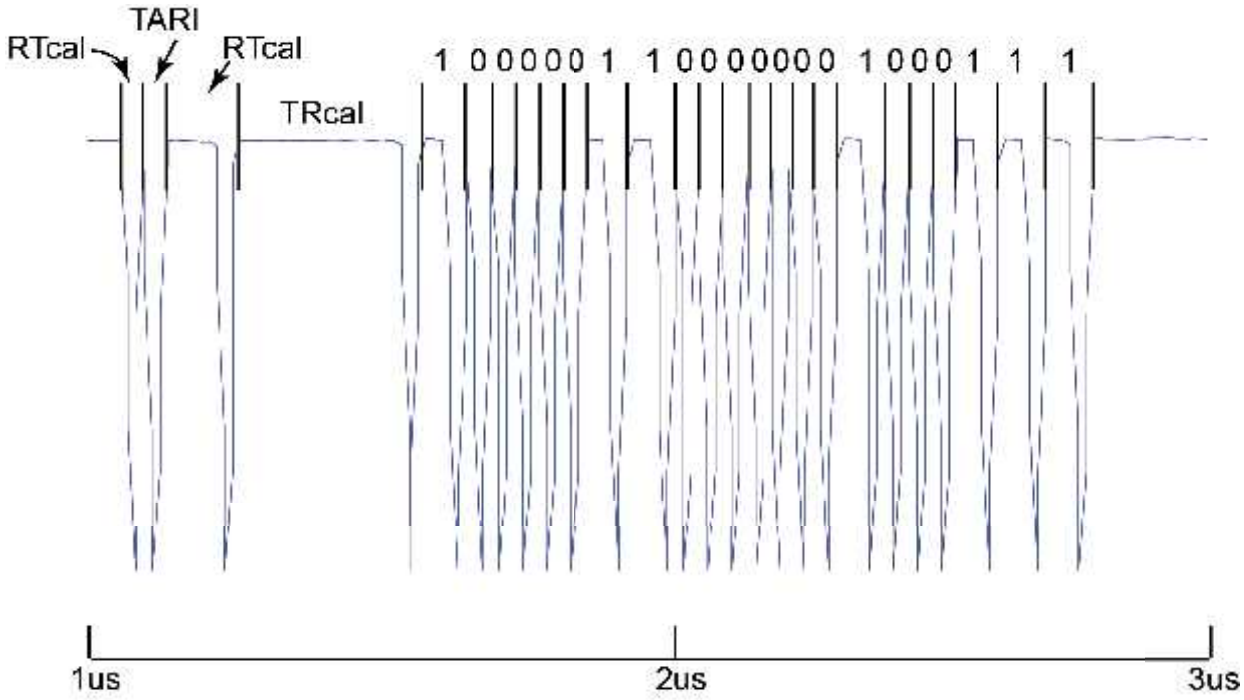
	Command	Target	Action	MemBank	Pointer	Length	Mask	Truncate	CRC
# of bits	4	3	3	2	EBV	8	Variable	1	16
description	1010	000: **Inventoried** (S0) 001: **Inventoried** (S1) 010: **Inventoried** (S2) 011: **Inventoried** (S3) 100: **SL** 101: RFU 110: RFU 111: RFU		00: FileType 01: EPC 10: TID 11: File_0	Starting Mask address	Mask length (bits)	Mask value	0: Disable truncation 1: Enable truncation	CRC 16

Matching | Non-Matching

Change SL or Inventoried

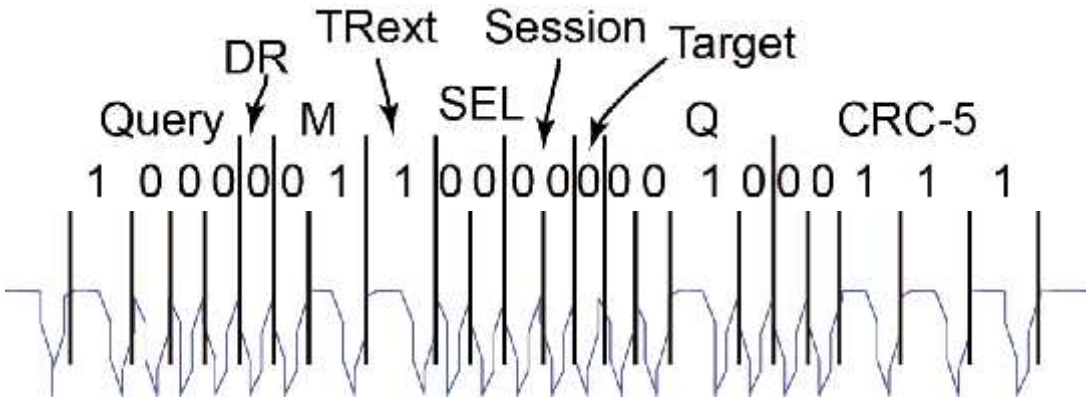


QUERY command

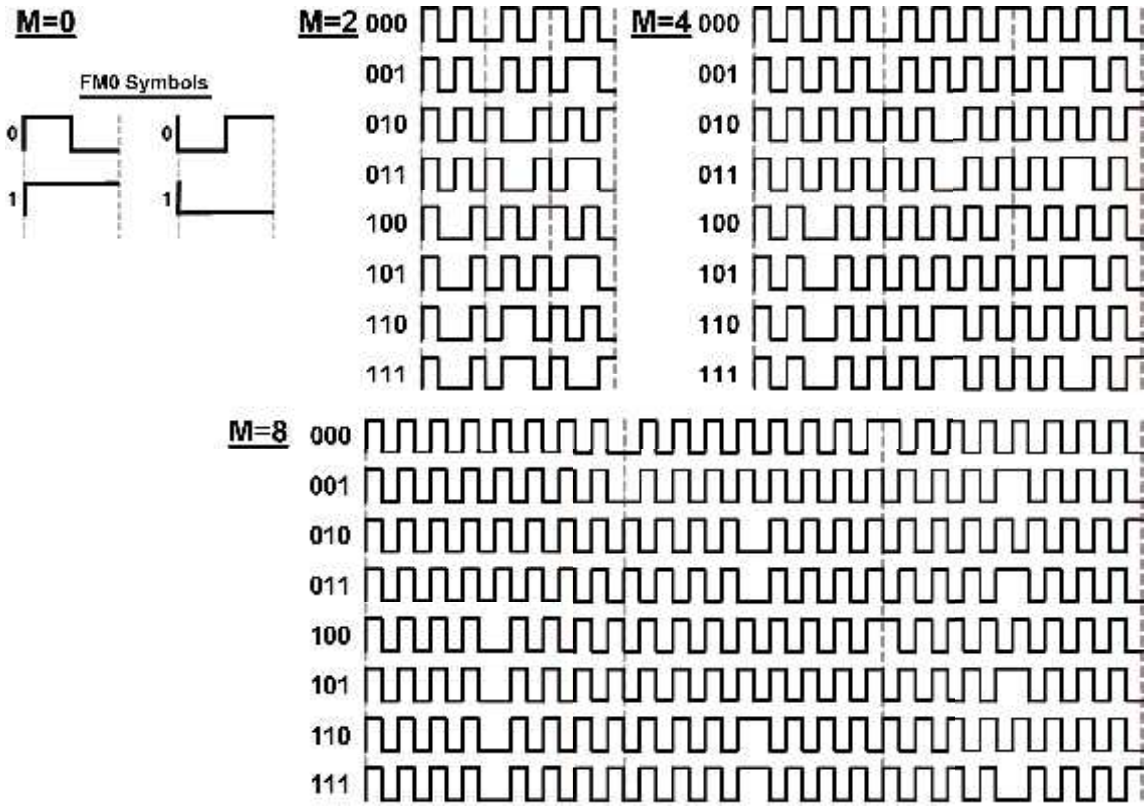


Query Bits

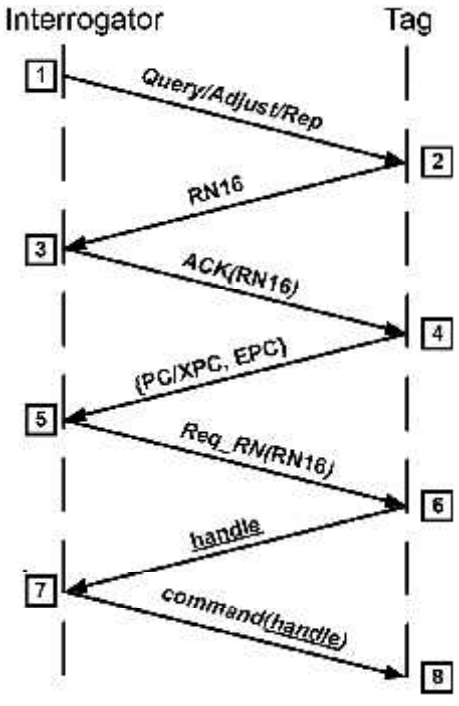
	Command	DR	M	TRext	Sel	Session	Target	Q	CRC
# of bits	4	1	2	1	2	2	1	4	5
description	1000	0: DR=8 1: DR=64/3	00: M=1 01: M=2 10: M=4 11: M=8	0: No pilot tone 1: Use pilot tone	00: All 01: All 10: ~SL 11: SL	00: S0 01: S1 10: S2 11: S3	0: A 1: B	0–15	CRC-5

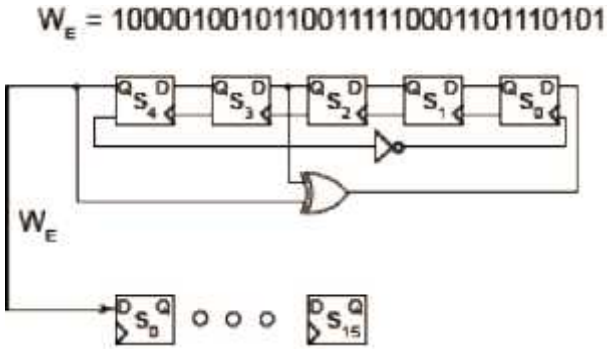


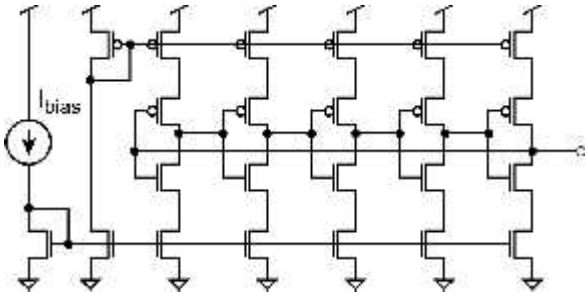
Talking Back, the "M" bit



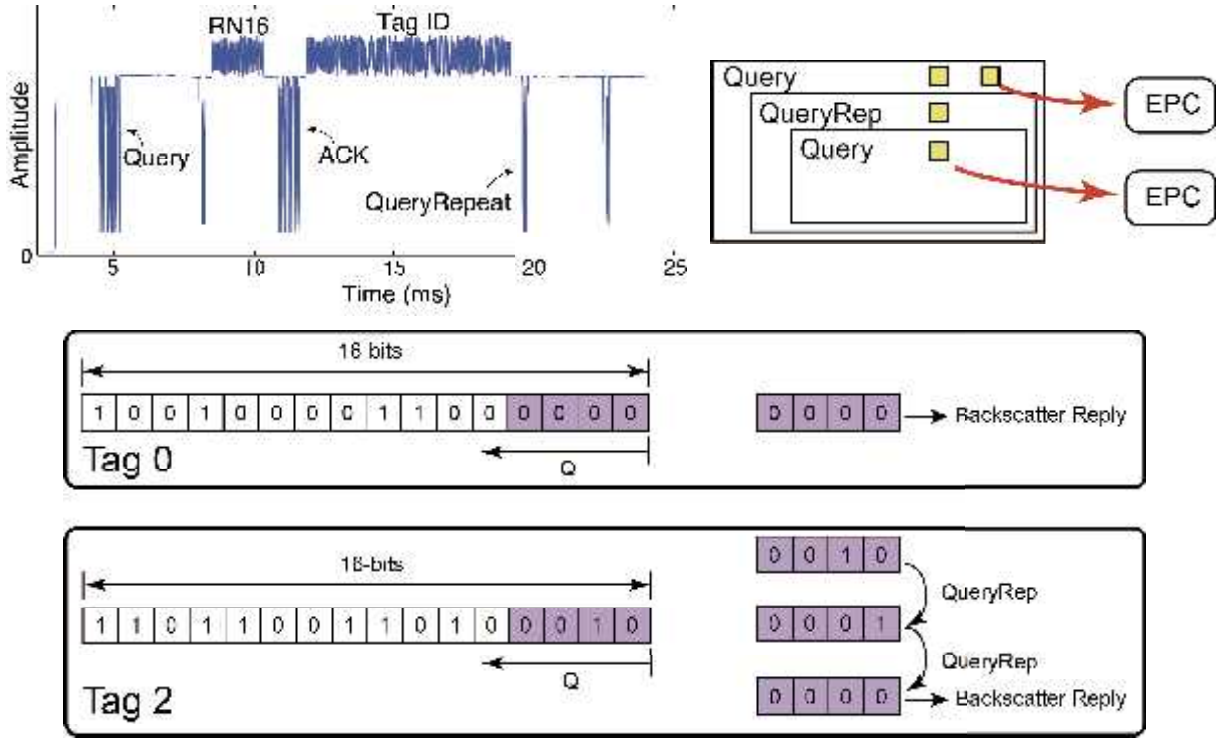
RN16 for response and slot counter



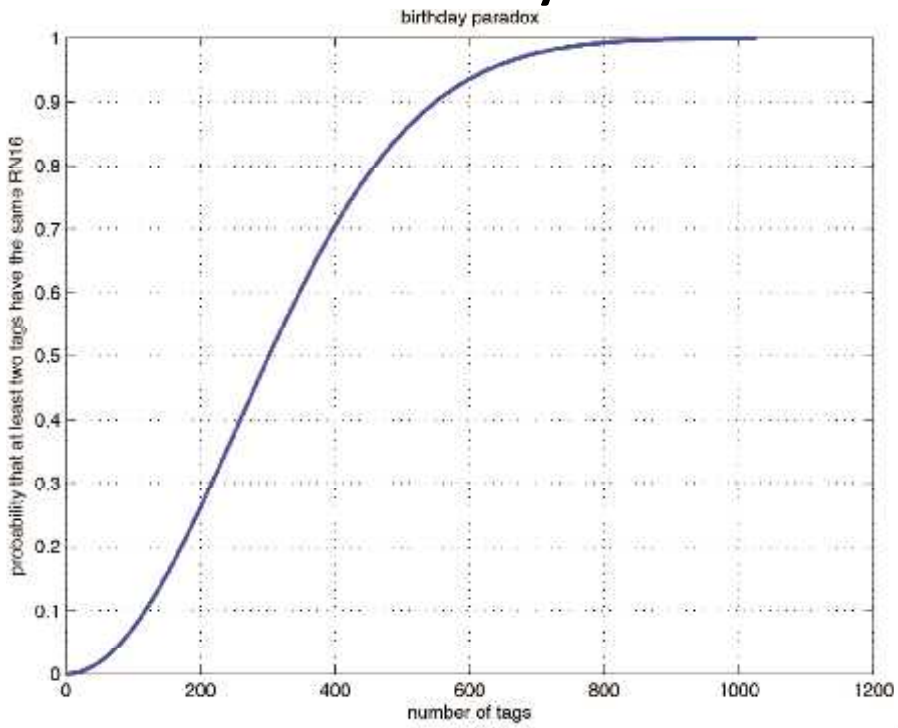




Slot Counter, QueryRep



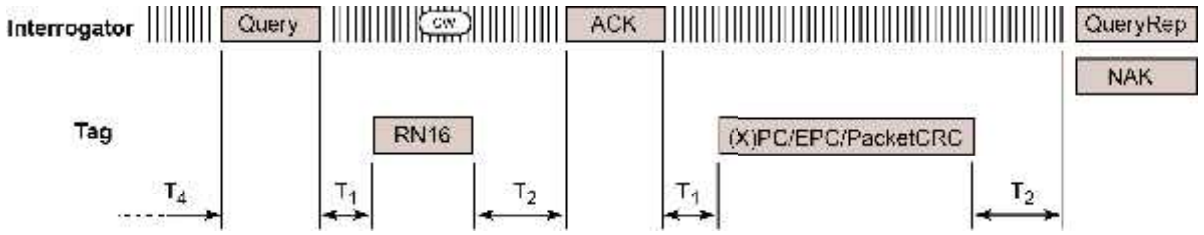
RN16: Birthday Paradox

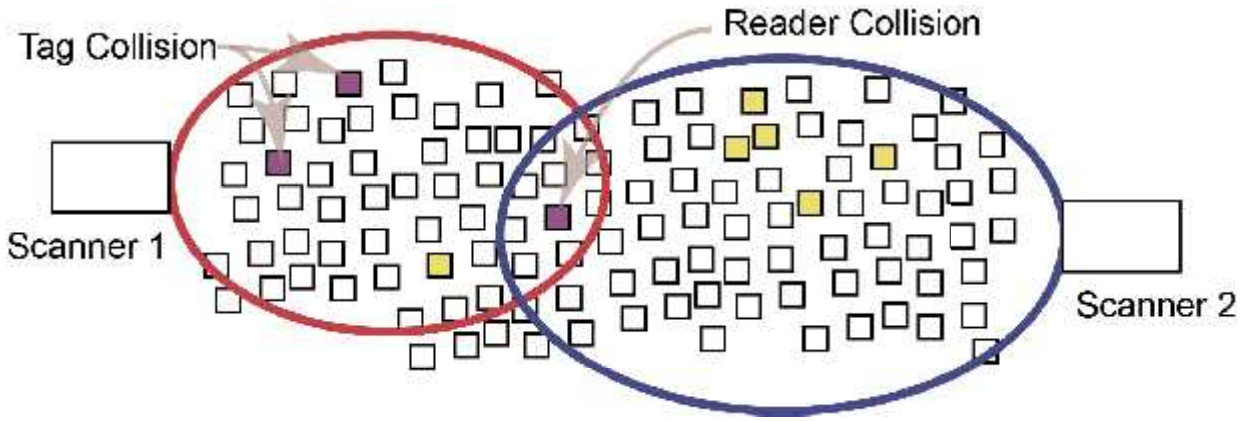


$$p = 1 - e^{\frac{-k^2}{2N}}$$

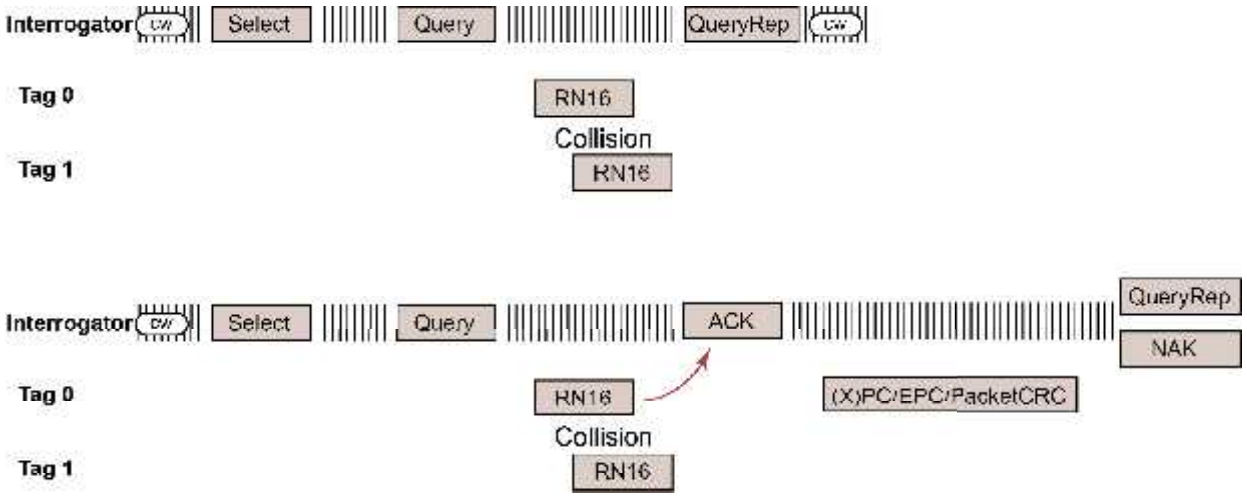
$$p = 1 - e^{\frac{-k^2}{2(2^{16})}}$$

Collisions, but first: a good packet





Packet Collision and Recovery



Introduction to Cryptography

- Asymmetric
- Public/private key
- Send over insecure channel
- Bit widths ~1000s
- Relatively Slow

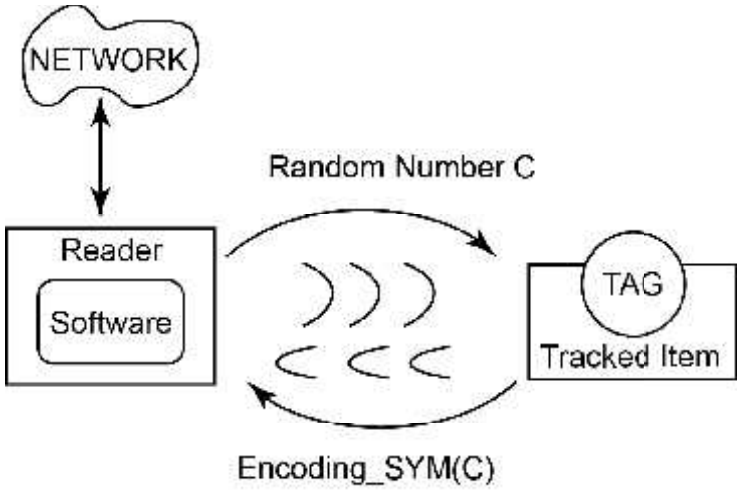
- Symmetric
- Private Key
- Uses Asymmetric crypto to send key
- Bit widths 64~256
- Quite Fast

Cryptography in Gen2V2

- Gen2v2 has NONE (by design)
- User's choice of underlying cryptography
- Defines the commands and responses

Command	Code	Description
Authenticate	11010101	Authenticate against Challenge
AuthComm	11010111	Encapsulate command securely
Challenge	11010100	Crypto "Select" command
KeyUpdate	11000101	Update an encryption key
SecureComm	11010110	Encapsulate command securely
TagPrivilege	1110001000000011	Set tag access
Untraceable	1110001000000000	Hide from other interrogators

How it works in theory




```
  C=00000000000000000000000000000000
Key=00000000000000000000000000000000
Enc=66e94bd4ef8a2c3b884cfa59ca342b2e
```


Lots of Standards

The missing link is provided by work in ISO/IEC SC31/WG4

- Automatic Identification and Data Capture Techniques, Radio Communications
- In particular the multi-part standard ISO/IEC 29167

Each part of ISO/IEC 29167 is dedicated to a cryptographic technology

- A cryptographic suite
- Each suite has a CSI number
- Each suite describes how it should be used with air-interface commands

ISO/IEC 29167 can be extended with new algorithms

ISO/IEC 29167

29167-10	AES-128	Published (revision in progress)
29167-11	PRESENT-80	Published
29167-12	ECDH	Published
29167-13	Grain-128a	Published
29167-14	AES-128	Published
29167-15	XOR	Halted
29167-16	ECDSA	Published
29167-17	CryptoGPS	Published
29167-18	Hummingbird v2	Withdrawn
29167-19	RAMON	Published
29167-20	Algebraic Eraser	Working draft
29167-21	Simon	Working draft
29167-22	Speck	Working draft

Brian Degnan, Ph.D. White River Technologies Inc.

The crypto problem?

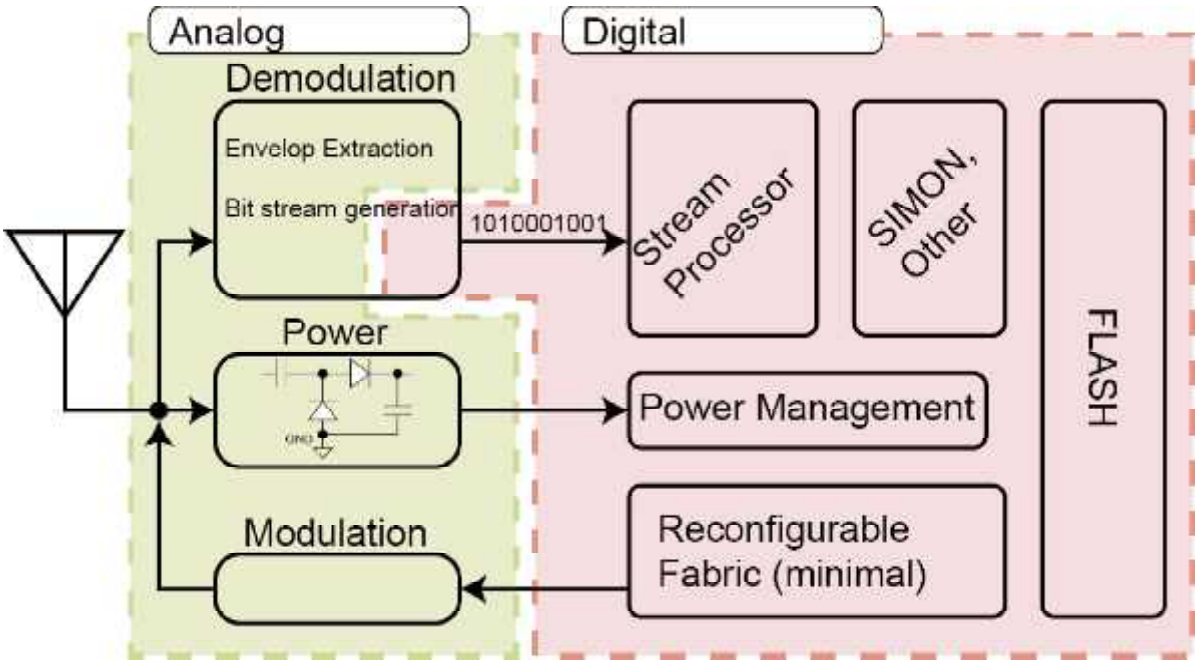
- Passive RFID is a long read range, but is very power constrained
- Different use-cases prioritize different performance attributes
- Different use-cases have different security/ threat models
- Deployment is complex
- Symmetric ciphers: lowest complexity

brian@degnanresearch.com

Cryptography on RFID

- No device authentication
- 128-bit keys with poor side-channel profiles vs 80-bit keys with good side−channel profiles vs "it's a $10 t-shirt"
- Tags often only used a few times
- Cryptography is used to authenticate the tag, not protect the data.

RFID tag of the future



Example of Key Exchange

Me	You
$Prime, P = 29, \alpha = 2$	
$secret_{me} = 5$	$secret_{you} = 12$
$\alpha^{secret_{me}} = 2^5 = 32$	$\alpha^{secret_{you}} = 2^{12} = 4096$
$= x \pmod P$	$= y \pmod P$
$= 3 \pmod{29}$	$= 7 \pmod{29}$
$y^{secret_{me}} = Z \pmod P$	$x^{secret_{you}} = Z \pmod P$
$7^5 = Z \pmod{29}$	$3^{12} = Z \pmod{29}$
$Z = 16$	

brian@degnanresearch.com

Brian Degnan, Ph.D. White River Technologies Inc.

Questions?

brian@degnanresearch.com

Brian Degnan, Ph.D. White River Technologies, Inc.

brian@degnanresearch.com