

Experimental Studies of Vulnerabilities in Devices and On-Chip Protection



Agis A. Iliadis

*Electrical and Computer Engineering Department
University of Maryland, College Park, MD 20742
Tel: 301-405-3651/agis@eng.umd.edu*

Research Students: Xingzhi Wen, Kye-chong Kim, Kai Zhang

Collaboration: J. Rodgers, Y. Carmel, T. Firestone

Interaction: Antonsen, Baker, Goldsman, Jacob, Melngailis, Ott, Ramahi

Acknowledgements: Support by the AFOSR-MURI Program is gratefully
acknowledged

6/8/02

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUL 2006		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Experimental Studies of Vulnerabilities in Devices and On-Chip Protection				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Electrical and Computer Engineering Department University of Maryland, College Park, MD 20742				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 26	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Introduction

- **Study effects on the fundamental units of IC circuits, ie individual devices (MOSFETs) and gates (CMOS Inverters).**
- **Identify most prominent vulnerabilities of the units to RF direct injection and irradiation, and examine how they critically affect circuit operation.**
- **Establish the failure mechanisms for each regime and develop hardened IC device/circuit designs.**
- **Evaluate response of device with RF pulse parameters and use MOSFET devices as on-chip sensing and protecting elements.**
- **Develop on-chip sensing, registration, and protection circuitry.**
- **Develop protective nano-composite polymer based “spin-on” coatings.**

Approach



- Assume RF signals couple to devices through I/O/antenna ports, and neglect bouncing signals within the packaged chip.
- Chips containing several individual enhancement mode N-channel MOSFETs of varying dimensions were fabricated and packaged in transistor headers for testing under RF.
- PC Boards were designed and fabricated and the packaged chips were placed on the boards with matching elements for RF injection.
- The RF vulnerabilities are examined both by simulation and experimental injection of RF at the MOSFET Gate, Drain, Source, and Body.
- The On-Chip “Sense-and-Protect” circuit is being developed. Several prototypes have been fabricated and tested.

Outline

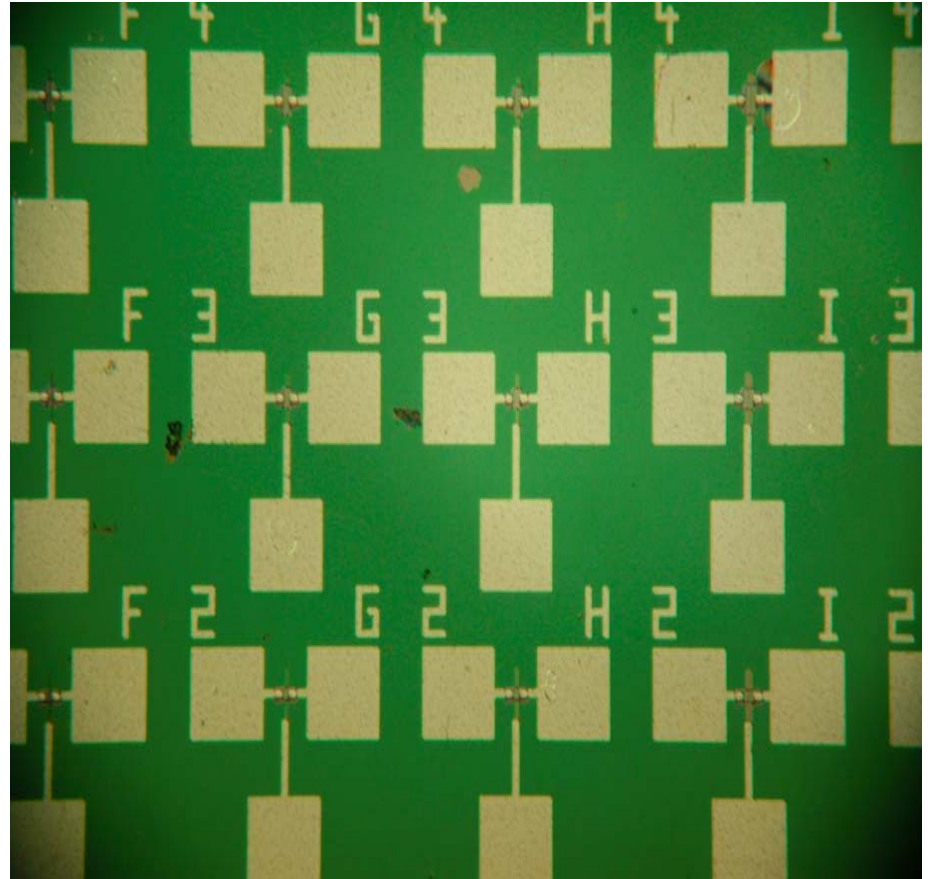


- MOSFET IC Chip and Packaging
- MOSFET simulation of RF injection using P-SPICE and MEDICI
- Two cases: **a.** dc operational point upset and **b.** upset with legitimate small ac signal at input
- Experimental RF injection in packaged devices
- On-chip "Sense-and-Protect" development and test
- Summary
- Continuing Work
- Future-Goals

IC Chip with Individual MOSFETs

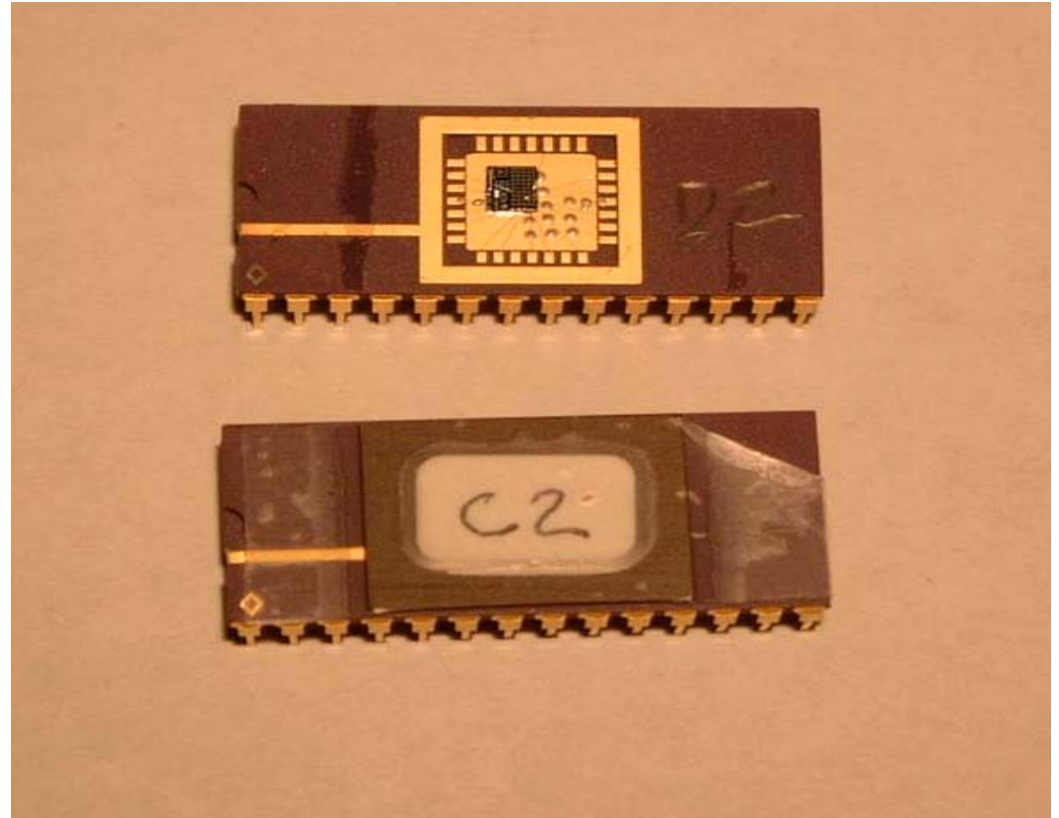


- IC Chip with Enhancement-Mode n-channel MOSFETs
- Gate Length varies between $2\mu\text{m}$ - $20\mu\text{m}$.
- Parameters affected:
- Electronic: I-V, Q point, g_m , gain, delay times, f_t , f_m , s, impedances
- Physical: Gate oxide, junction boundaries, metallizations.



Packaged Chip for RF Test

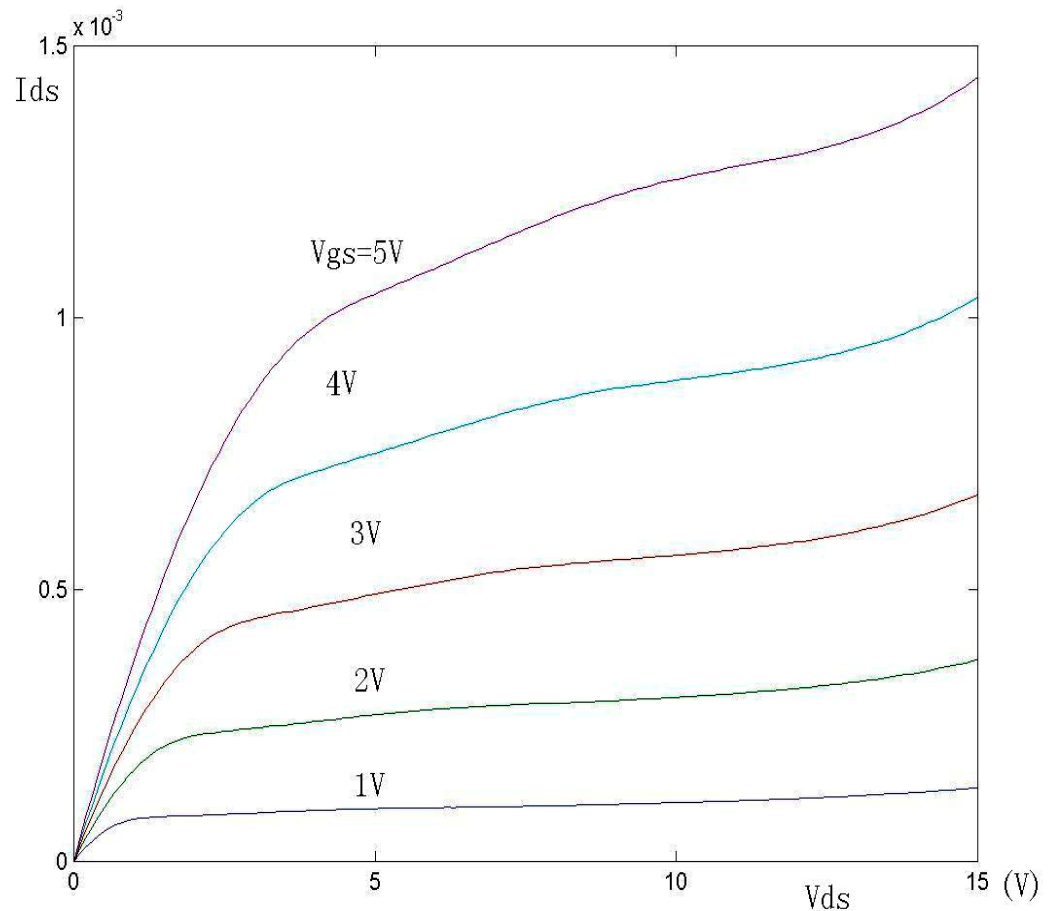
- Bonded and packaged IC Chip
- Several devices are wire-bonded for RF testing
- Operating conditions: $V_{DD}=5\text{ V}$
- Packaged chip is placed on PC board for RF test



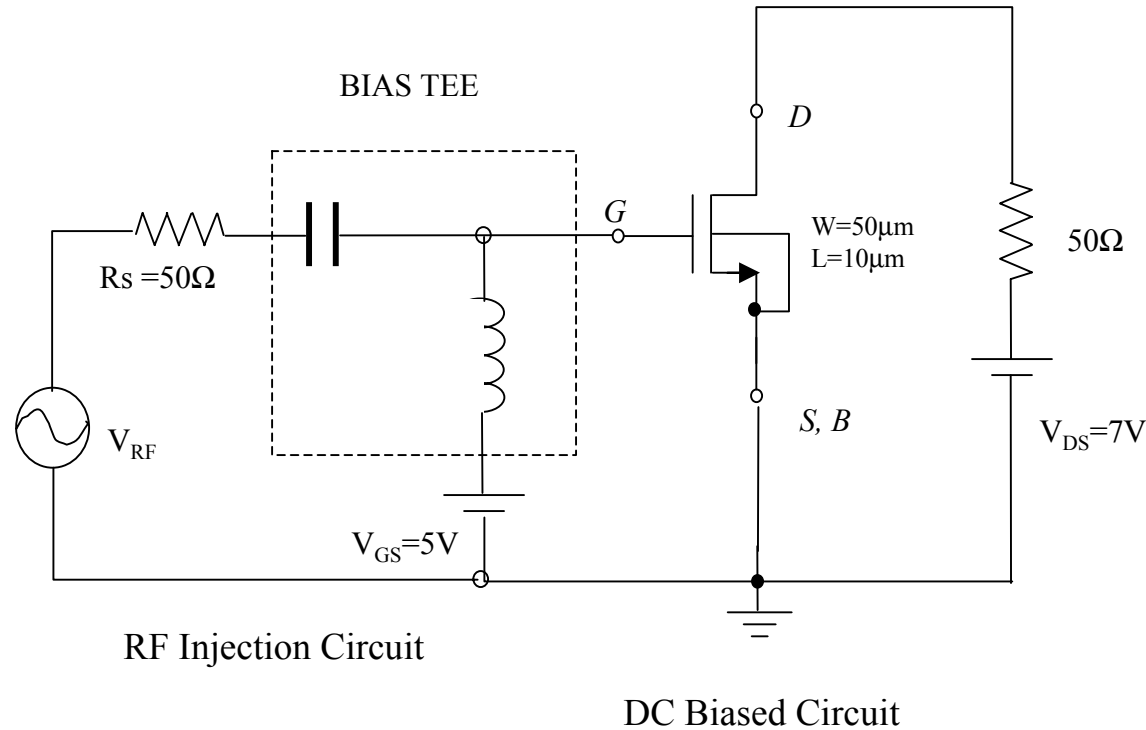
Family of I-V Output Characteristics



- Typical dc I-V characteristic of a MOSFET
- Operating point at $V_{ds}=7V$ and $V_{gs}=2.5V$



Simulation using P-SPICE



**Circuit for P-SPICE simulation using a T junction for RF injection.
RF amplitude: 1 and 4 V.**

RF frequencies : 20MHz, 100MHz, 500MHz, 2GHz, & 20GHz.

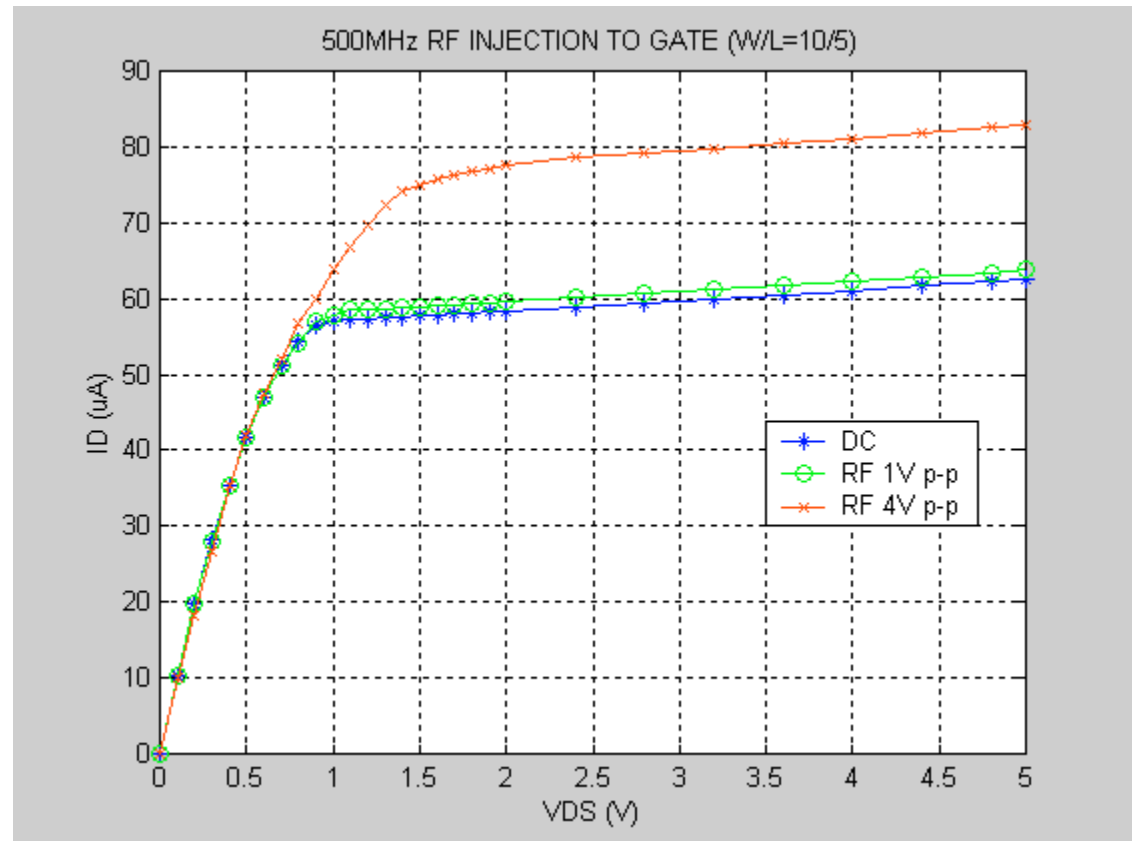
500MHz RF Injection to Gate

$$I_{\text{DRF}} = I_{\text{D}} + \Delta I_{\text{DRF}}$$

Where :

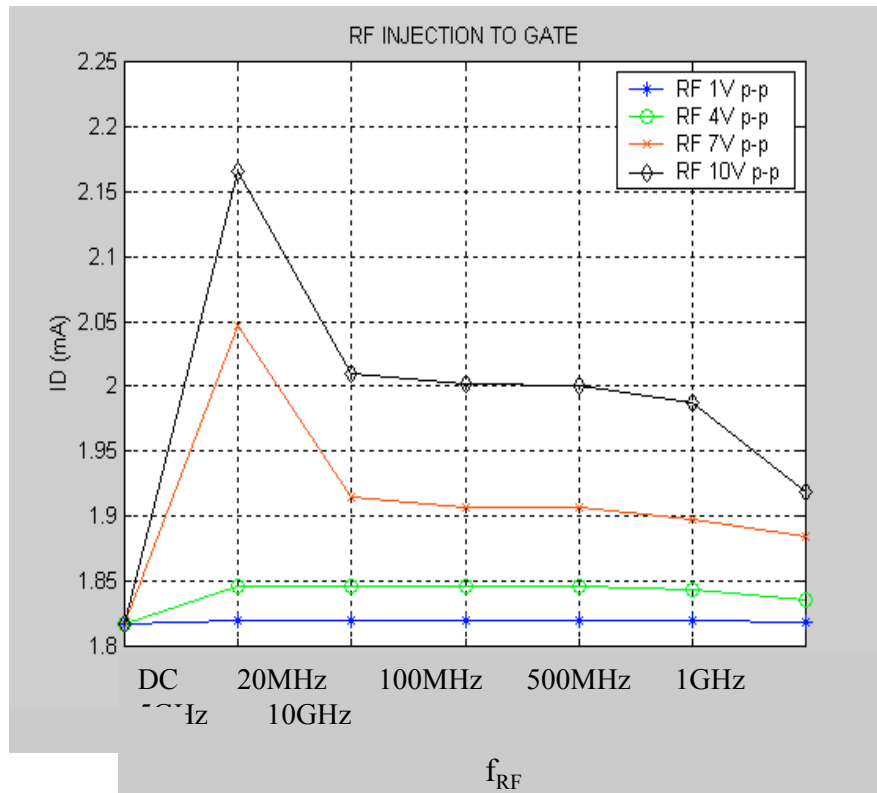
I_{D} : DC bias
current

ΔI_{DRF} : increase of
drain current due
to RF injection

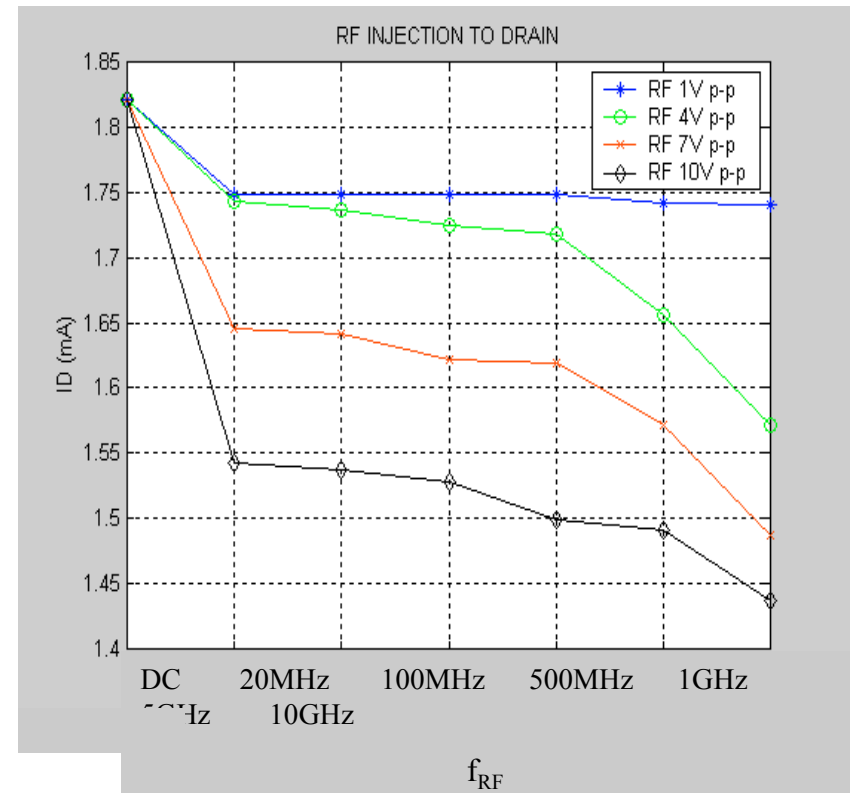


Family of I-V characteristics at DC and 500 MHz for sinusoid RF. The DC gate bias per characteristic is at $V_{\text{GS}}=2$ V and $W/L=10/5$

RF Injection to Gate, Drain



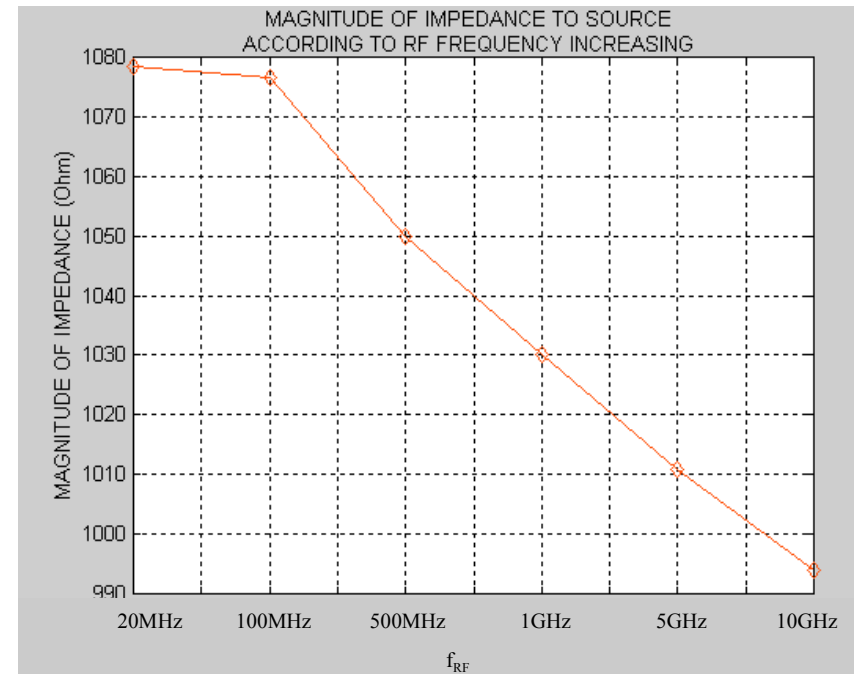
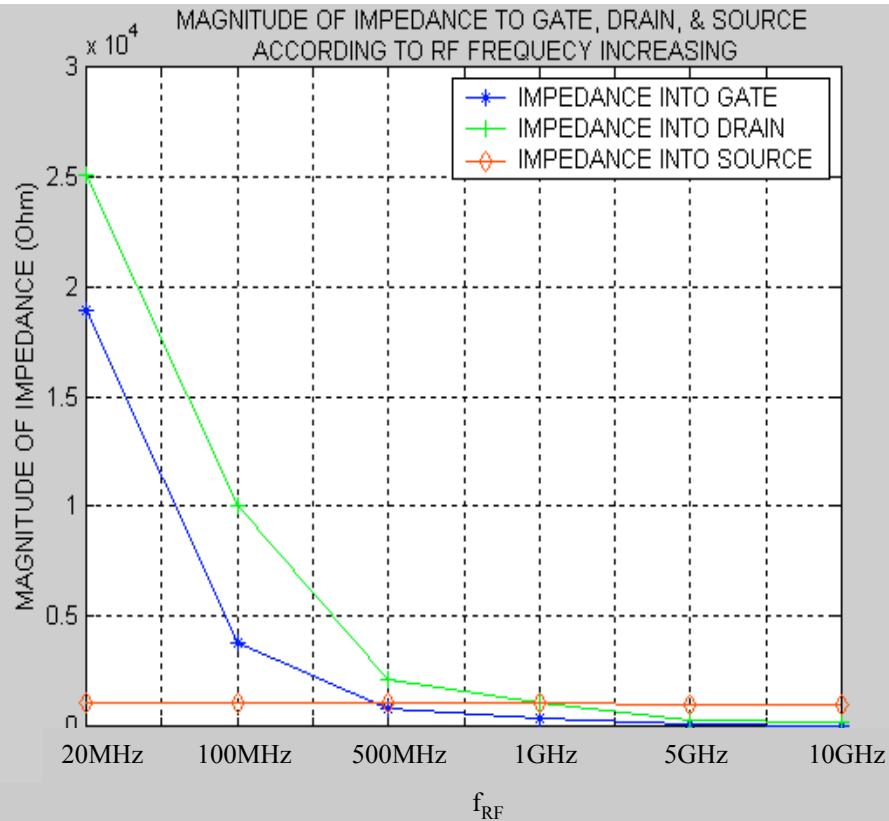
Gate



Drain

$\Delta I_{D,RF}$ vs RF Frequency and amplitude. RF amplitude from 1V to 10V and frequency from DC to 10GHz. $V_{GS} = 5V$, $V_{DS} = 7V$.

Magnitude of effective impedance with injected RF frequency

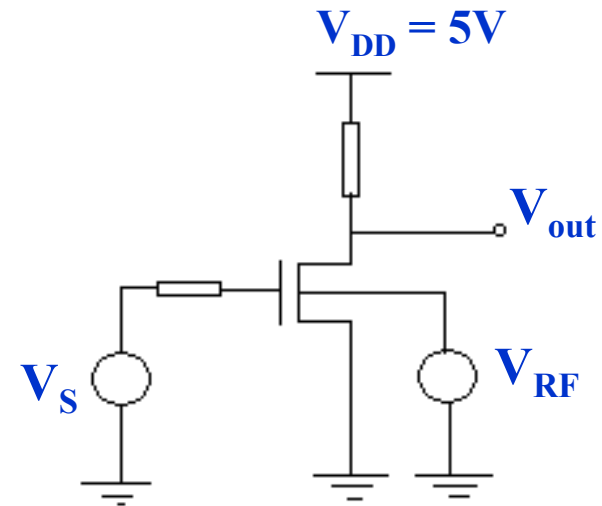
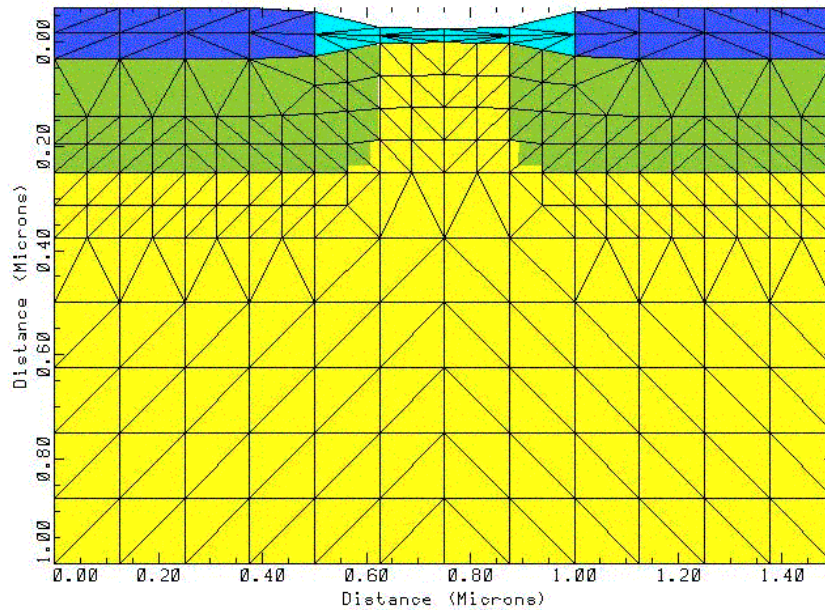


The magnitude of impedance looking into Gate, Drain, and Source is decreasing with RF frequency.

Simulation with both input signal and RF injection using MEDICI-Avanti

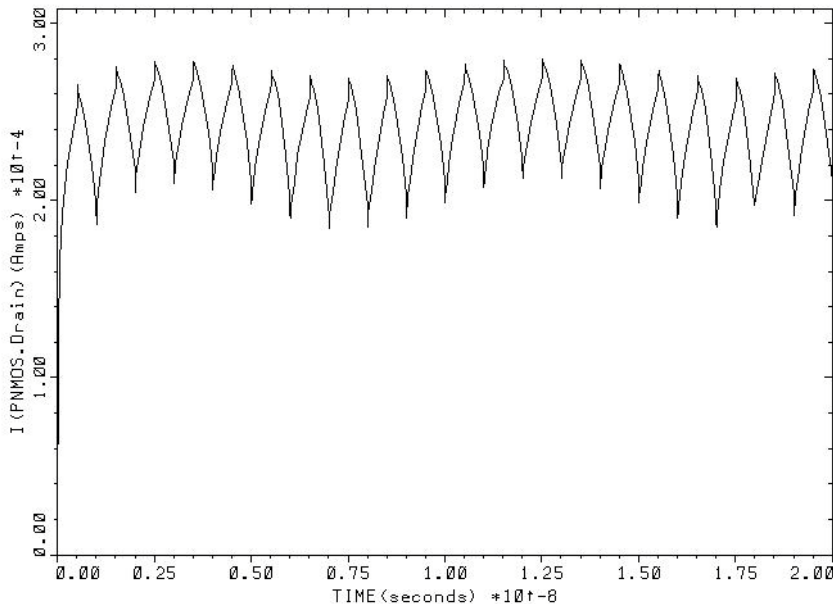


0.5 Micron N-MOSFET

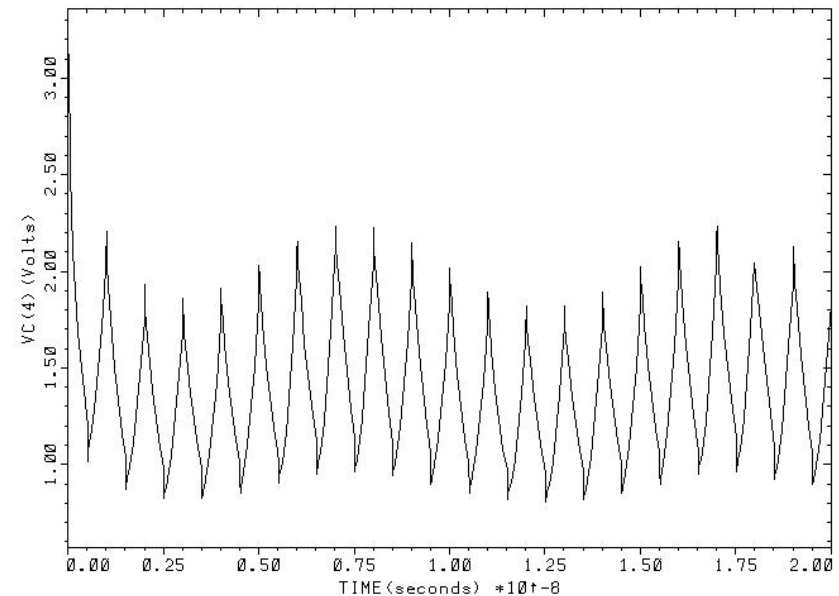


- $V_{AC} = 0.2\sin(10^8 2\pi t)$, f : 100MHz
- $V_{gs} = 2.5 V$
- $V_{RF} = 1V, 3V, 5V$.
RF pulses: 500MHz, 1GHz

Small signal at gate and RF Injected at Body (Substrate)



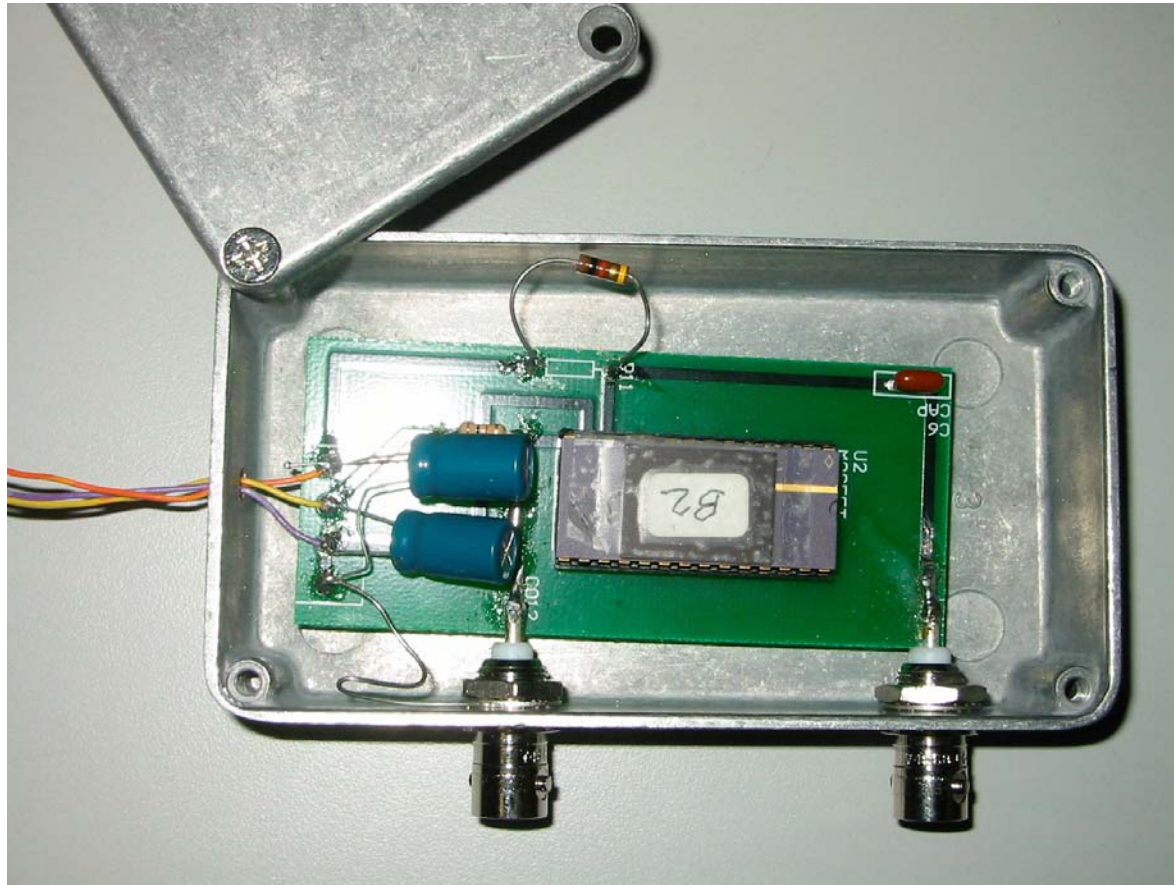
Drain Current



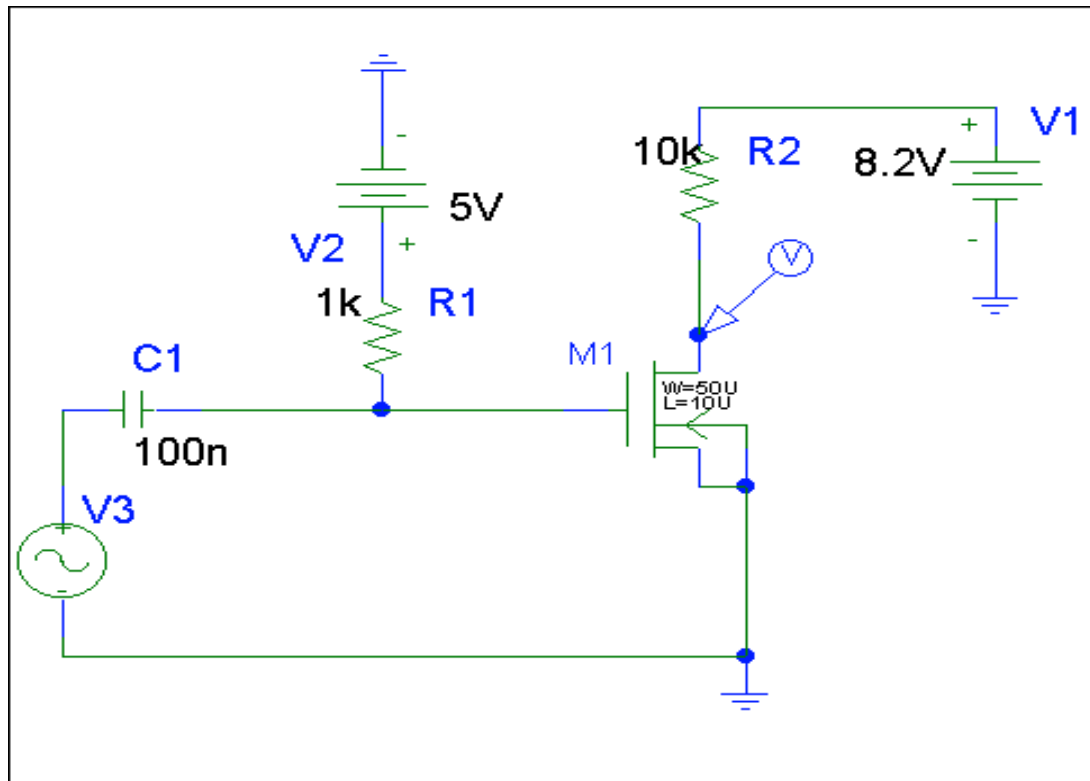
Drain Voltage

Input signal at gate is 100 MHz sinusoid. Output waveforms modulated by RF pulsed injection at the Body. Similar modulation is observed for RF injection at the Source. RF: 1 GHz, 3V

Device Under Test (DUT) on PC Board



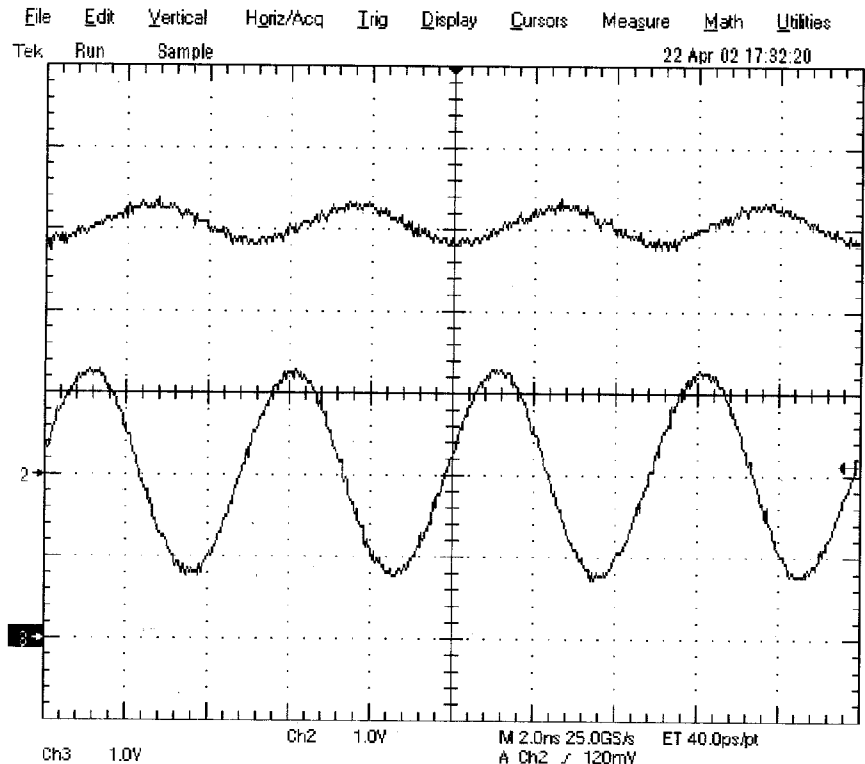
Circuit Diagram of the MOSFET RF Test Device



Circuit diagram of device under test (DUT). Device is in IC package and package is soldered onto PC board and in aluminum box. Matching components are shown.

RF injection at Gate

W/O RF:
 $V_{ds} = 5.552V$
 $I_d = 269\mu A$



With RF injected
(200MHz, 2.4 V)

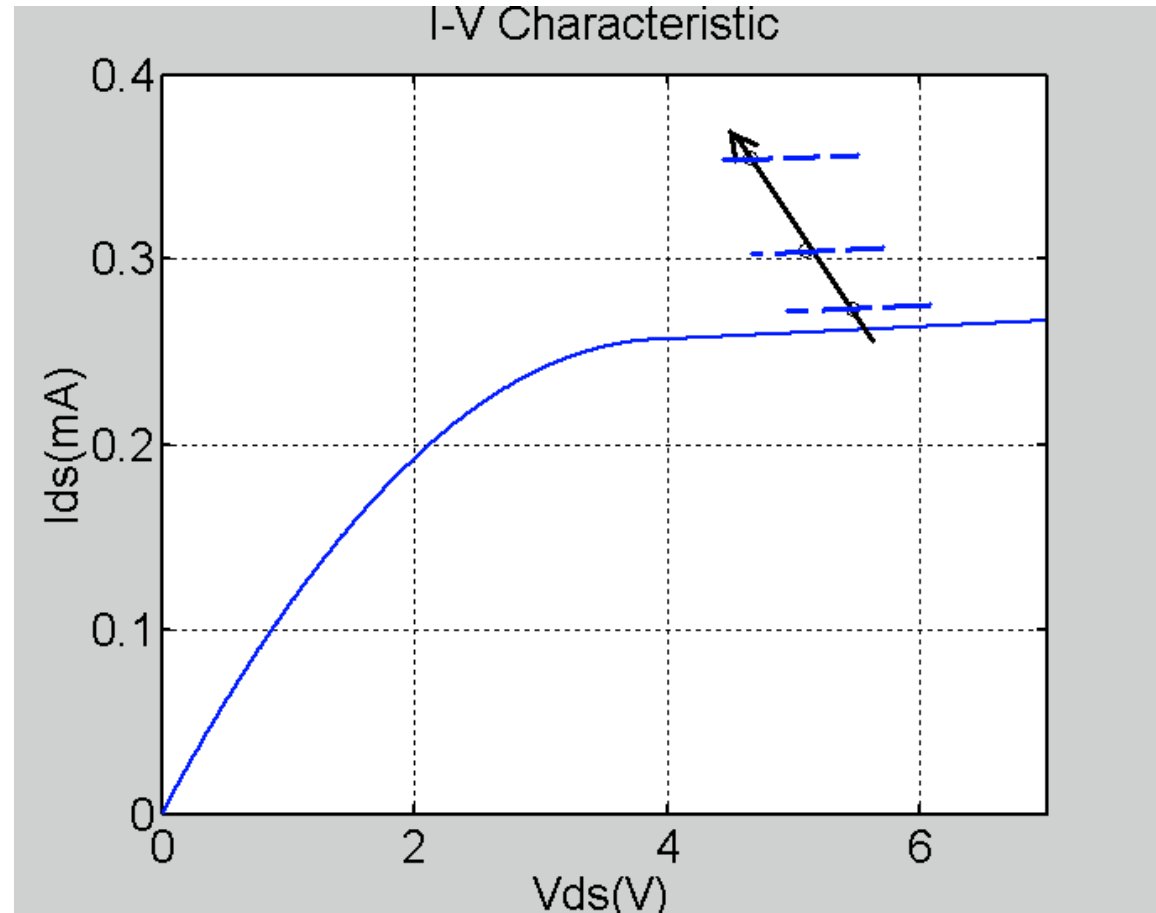
$V_{ds} = 5.051V$
 $I_d = 305\mu A$

$I_d = 36\mu A (13\%)$

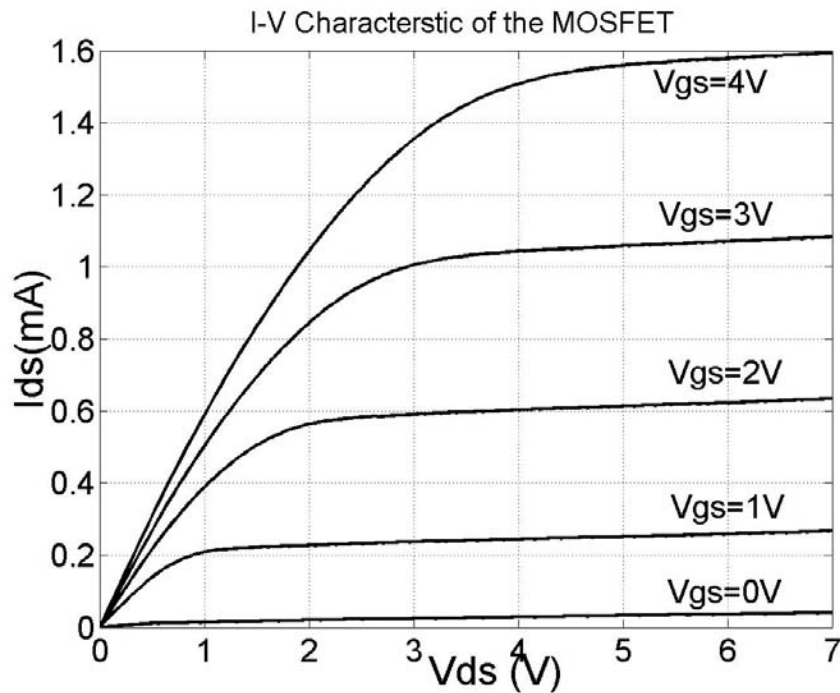
Upper line: experimental output voltage (V_{ds}) vs time with RF showing the dc average output voltage at the drain is reduced by 13%

Id increase due to RF injection at Gate

Equivalent I_d increase with amplitude of RF injection signal at gate



Id increase due to non-linearity?



$$I_d = \frac{\mu_n c_{ox} W}{2L} (V_{gs} - V_t)^2 (1 + \lambda V_{ds})$$

$$\frac{\mu_n c_{ox}}{2} = 1.3e-5 \quad V_t = -0.96$$

$$W/L = 5$$

$$\lambda = 1.3e-3$$

Device test for non-linearity



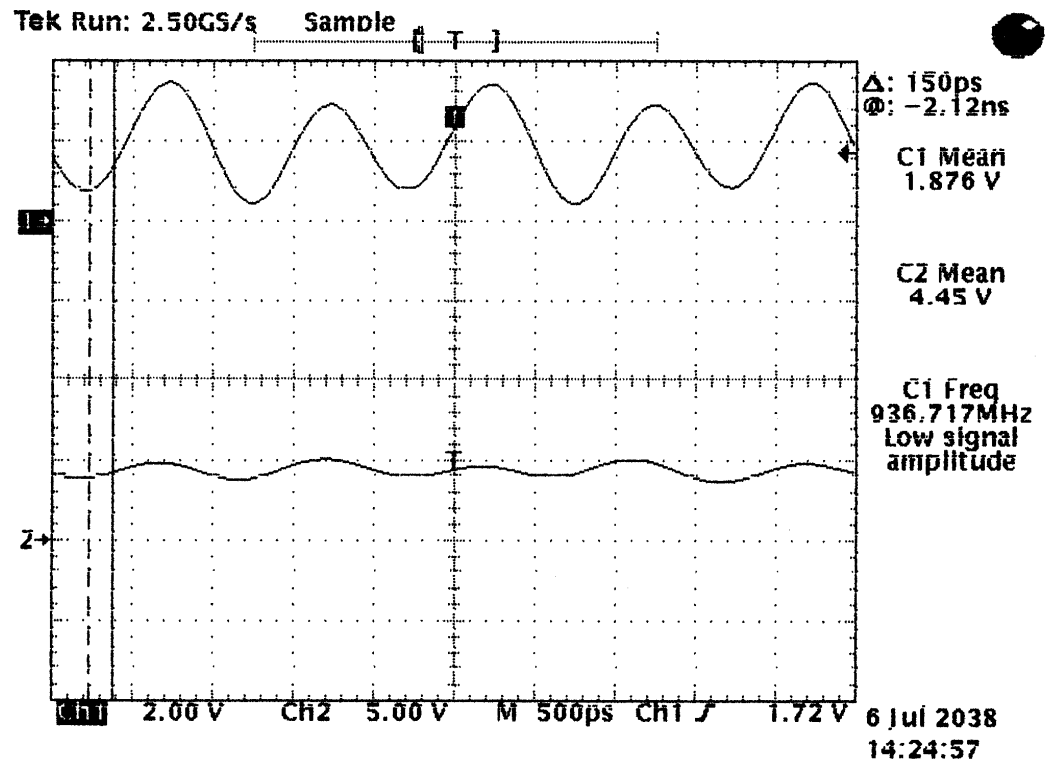
W/O RF: $V_d = 6.07V$

With RF at Gate:

1GHz, 3V

$V_d = 4.45V$

$I_d = 0.565mA$



Upper curve is V_{gs} , lower curve is V_{ds} (with RF). RF lowers the drain voltage and increased the drain current.

Simulation result for non-linearity

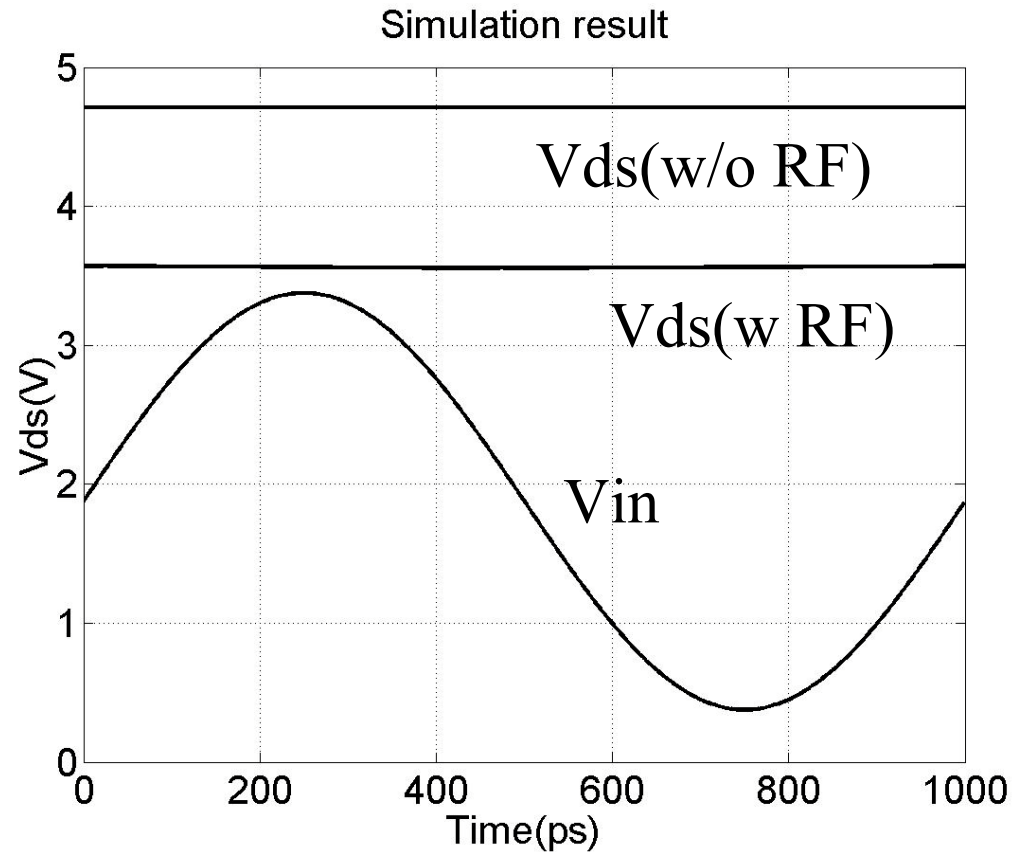
Measurement:

V_{ds} : 6.07V $\rightarrow$ 4.45V

Simulation:

V_{ds} : 4.71V $\rightarrow$ 3.57V

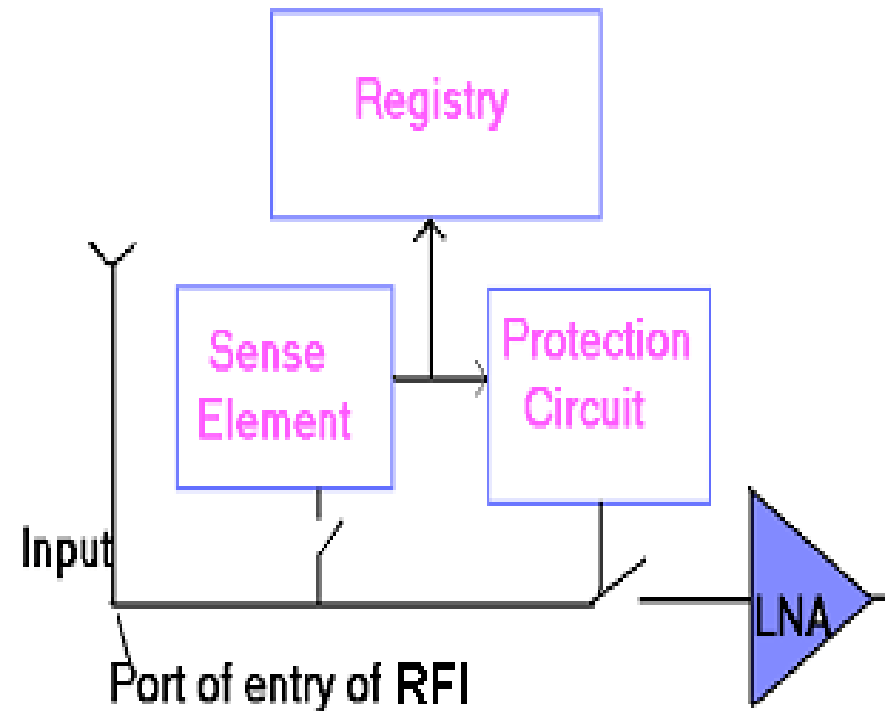
**Measurement and
simulation show
similar trend**



“Sense and Protect” Circuit Concept



- Sense element based on “floating gate” MOSFETs of different size and geometries.
- Protection based on comparators and fast switches.
- Efficient disconnect capability with minimal coupling to the rest of circuit in the off-state
- Designed for wide frequency and amplitude range of events
- It registers RF events
- **Patent Pending**



Schematic of Protection System

"Sense-and-protect" chip test

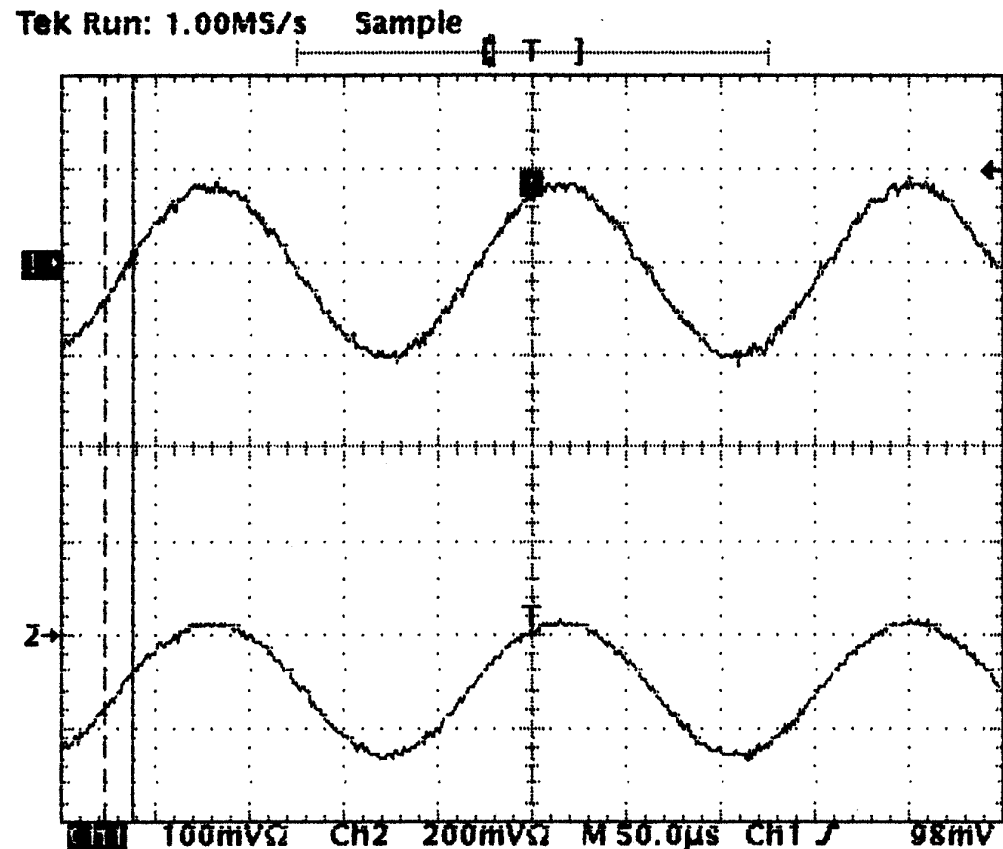
**Legitimate input
signal:**

Amplitude: 200mV

Output signal:

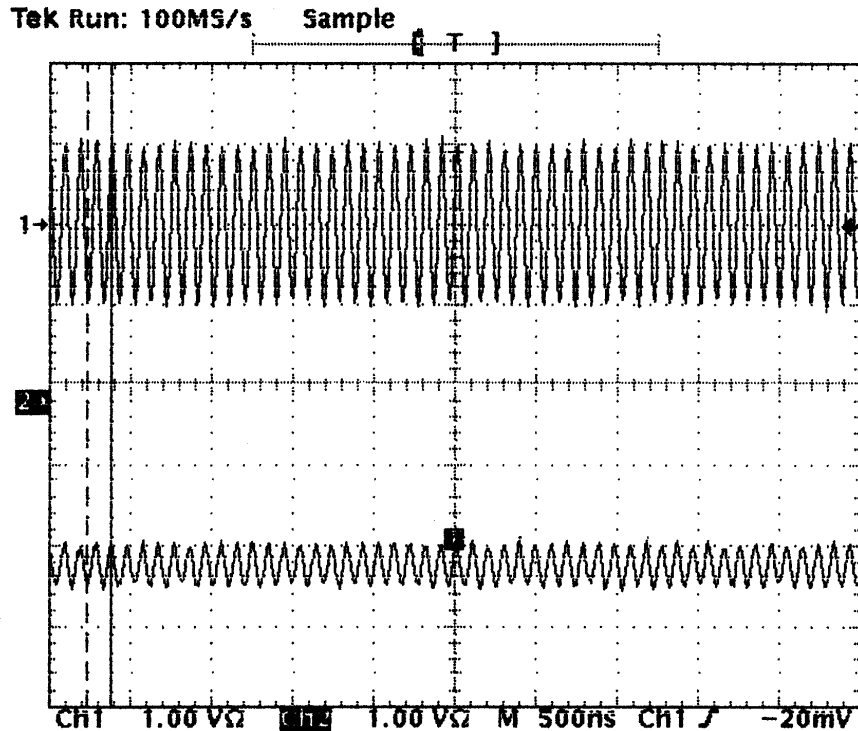
**amplitude: 280mV
(Gain:1.4)**

•Phase shift:0



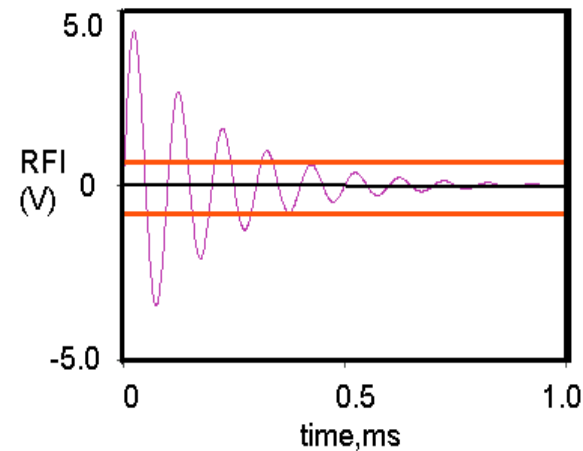
**Upper curve is input, lower curve is output
from S-P chip**

"Sense-and-Protect" RF Blocking



RF Input signal: $f \sim 10$ MHz, 2V
Output : 0.5V

**Expected
Response**



Upper curve is input, lower curve is output from S-P chip. Inset on right is the expected response for blocking RF.

Summary

- Simulated and experimental RF injection on MOSFETs at the gate, showed an increase in the drain current possibly due to the non-linearity in I-V characteristics.
- This drain current change appears to decrease with increasing RF frequency
- RF injection at the drain appears to reduce drain current probably due to non-ideal output conductance effects
- RF injection at body and source modulates and distorts legitimate input signals
- The non-linearities in I-V output characteristics (quadratic, output conductance, break-down) are some main factors
- On-chip “Sense-and-Protect” circuit was tested. All sections were tested and found to operate as designed, except for the switching elements that did not fully switched off thus a 20% signal pass-through.

Summary-Continuing Work



- Improvements in the design and fabrication of the switches and an additional circuit to avoid disruption of the operation while blocking the RF signal, are being implemented.
- The “sense-and-protect” circuit will also be scaled down to submicron gate lengths for faster response and higher RF frequencies and implemented with “wide” gates designed to effectively collect RF radiation as antennas and register each RF event to help with the understanding of radiation distribution within the packaging (Antonsen, Ott, Ramahi).
- It will then be incorporated in the design of the main communication chip (Goldsman, Jacob, Melngailis, Baker) to protect and register RF events at the I/O points of the chip.
- Direct RF radiation experiments are underway to establish vulnerabilities in the devices and map their dc and ac characteristics with RF amplitude and frequency.

Summary-Future Goals

- We have begun to experiment with protective coatings on polymers intended to completely shield the chips from radiation by developing a “spin-on” polymer and nano-composite metal system.
- Our overall approach is to develop the understanding of how the unit cells of IC circuits in analog and digital mode react to RF radiation, map the vulnerabilities, develop protection on the chip level, and (re)design devices to harden against RF.
- Develop active shielding within chip environment to disrupt radiation patterns.